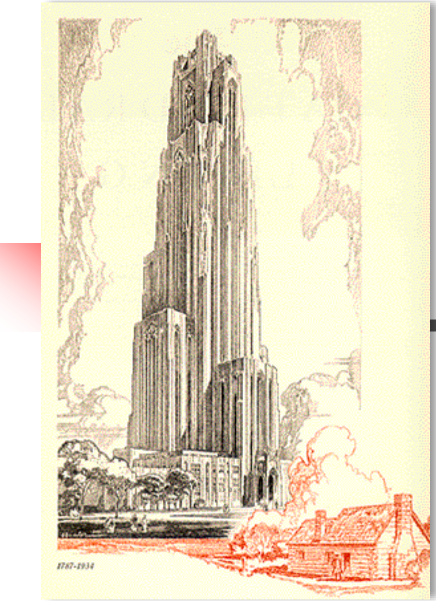
# IS 2955



James Joshi
Professor
Lecture 5
Oct 3-10, 2018

## Healthcare and Cloud - Security and Privacy

# What is Cloud Computing

- NIST definition:
  - Cloud computing is 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.
- Has
  - 5 Key characteristics
  - 3 service models
  - 4 deployment models

# Key Characteristics

- On-demand self-service
  - Get computing capabilities as needed automatically
- Broad network access
  - Services availability over the net using desktop, laptop, PDA, mobile phone
- Resource pooling
  - Location independence
  - Resource pooling at provider resources to serve multiple clients
- Rapid elasticity
  - Ability to quickly add or remove services
- Measured service
  - Control, optimize services based on metering/measurements/metric

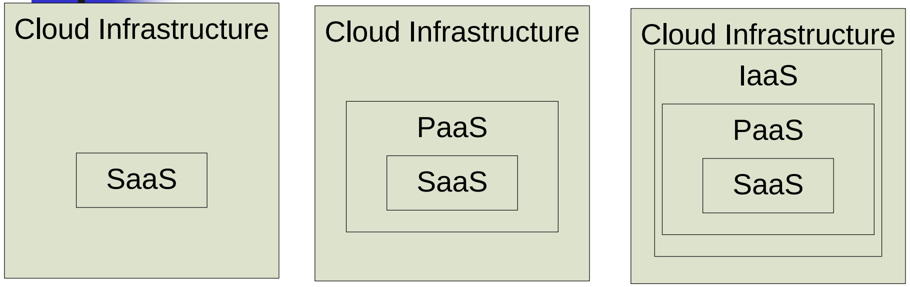
# Unique Features

- Outsourcing Data and Applications
- Extensibility and Shared Responsibility
- Multi-tenancy
- Service-Level Agreements
- Virtualization and Hypervisors
- Heterogeneity
- Compliance and Regulations

# Service Models

- Cloud Software as a Service (SaaS)
  - Providers provide software applications over networks
  - Client doesn’t manage or control the network, servers, OS, storage or applications
- Cloud Platform as a Service (PaaS)
  - Users deploy their own applications on a cloud
  - Users control their software/applications
  - Users don’t manage servers, storage, etc.
- Cloud Infrastructure as a Service (IaaS)
  - Provider provides processing, storage, network, and other key computing resources
  - Clients get access to the infrastructure to deploy their platform/software
  - Client do not manage or control the infrastructure but do manage or control the OS, storage, apps, selected network components

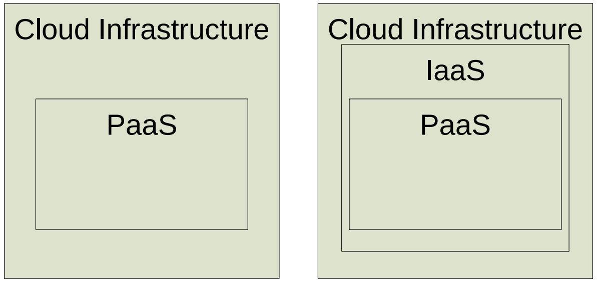
# Service Model Architectures



Software as a Service (SaaS) Architectures

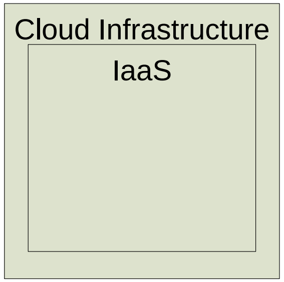
**SalesForce CRM**

**LotusLive**



Platform as a Service (PaaS) Architectures

**Google App Engine**

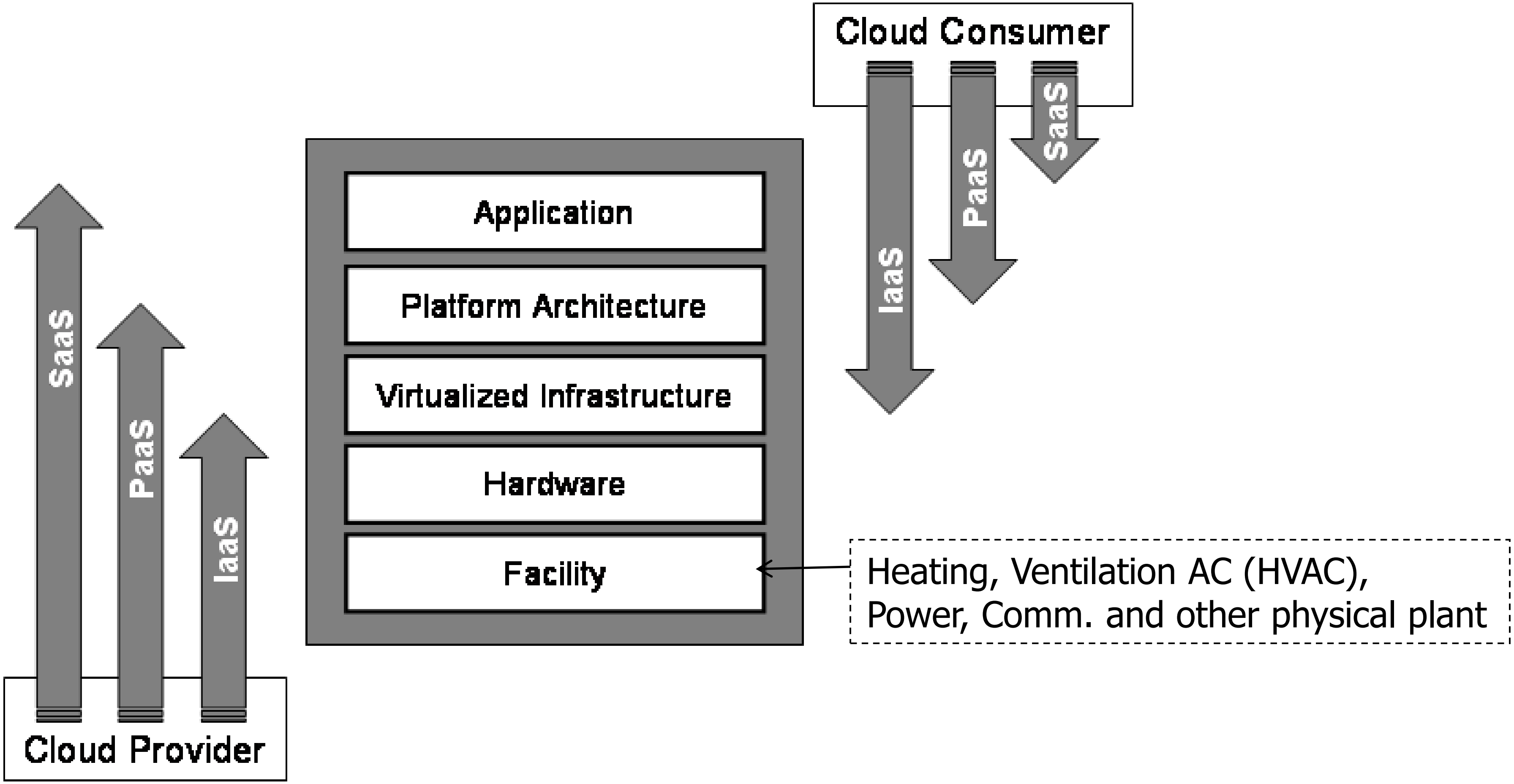


Infrastructure as a Service (IaaS) Architectures

amazon web services™

rackspace® HOSTING

# Scope and Control - differences



Heating, Ventilation AC (HVAC), Power, Comm. and other physical plant

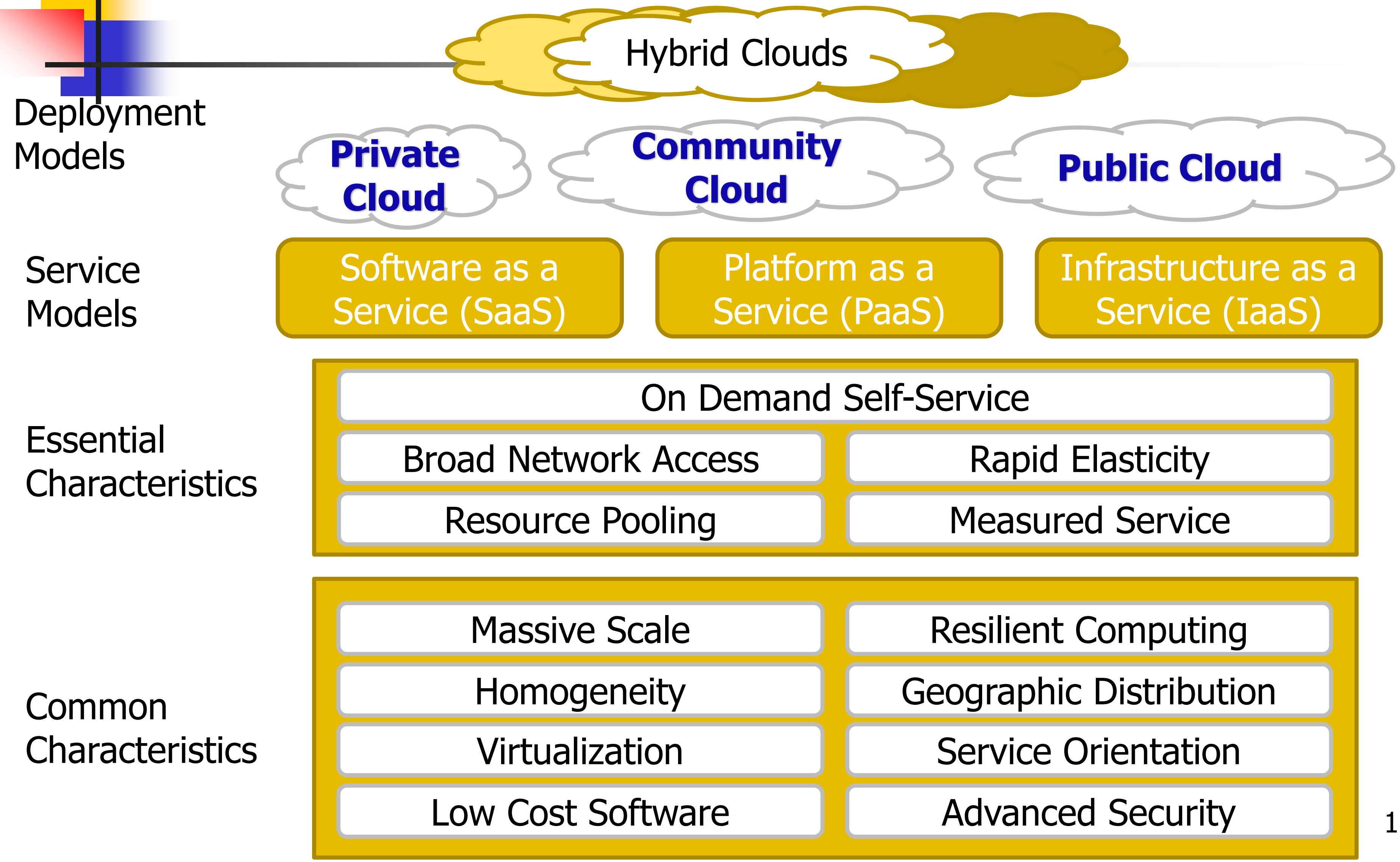
# Cloud Deployment Models

- Public cloud
  - Sold to the public, mega-scale infrastructure
  - available to the general public
- Private cloud
  - single org only; managed by the org or a 3rd party; on or off premise
- Community cloud
  - shared infrastructure for a specific community with shared concerns; managed by org or a 3rd party
- Hybrid cloud
  - composition of two or more clouds
  - bound by standard or proprietary technology

# Common Cloud Characteristics

- Cloud computing often leverages:
  - Massive scale
  - Homogeneity
  - Virtualization
  - Resilient computing
  - Low cost software
  - Geographic distribution
  - Service orientation
  - Advanced security technologies

# The NIST Cloud Definition Framework



Hybrid Clouds

Deployment Models: Private Cloud, Community Cloud, Public Cloud

Service Models: Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS)

Essential Characteristics:

- On Demand Self-Service
- Broad Network Access
- Rapid Elasticity
- Resource Pooling
- Measured Service

Common Characteristics:

- Massive Scale
- Resilient Computing
- Homogeneity
- Geographic Distribution
- Virtualization
- Service Orientation
- Low Cost Software
- Advanced Security

# Outsourcing and Availability Issue

- Outsourcing parts of Org computing is a key thrust
- Security & privacy implications if the public cloud is used
- Cost and efficiency motivation for move
- Org is responsible for S&P of outsourced services
- Org should oversee and manage how the provider secures the environment

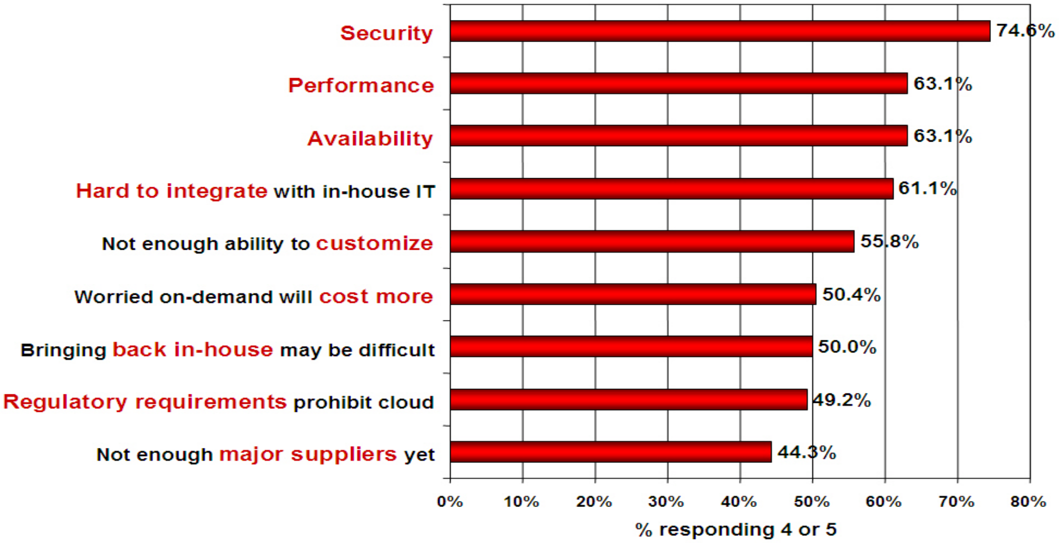
# Major Issue?

Top 12 threats – in order of severity!!

1. Data Breaches
2. Weak Identity, Credential and Access Management
3. Insecure APIs
4. System and Application Vulnerabilities
5. Account Hijacking
6. Malicious Insiders
7. Advanced Persistent Threats (APTs)
8. Data Loss
9. Insufficient Due Diligence
10. Abuse and Nefarious Use of Cloud Services
11. Denial of Service
12. Shared Technology Vulnerabilities

**Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model**

(1=not significant, 5=very significant)



Source: IDC Enterprise Panel, August 2008 n=244

# General Security Advantages

- Shifting public data to a external cloud
  - reduces the exposure of the internal sensitive data
- Cloud homogeneity
  - makes security auditing/testing simpler
- Clouds can enable automated security management
- Redundancy / Disaster Recovery

# Cloud Security Advantages

- NIST 800-144 (Security Upside)
  - Staff Specialization (in Cloud Providers)
  - Platform Strength – greater homogeneity
  - Resource Availability – scalability help!
  - Backup and recovery – may be superior
  - Mobile Endpoints – heterogeneous devices
  - Data concentration- specifically for an org with mobile workforce

# Cloud Security Advantages

- Other
  - Data Fragmentation and Dispersal
  - Greater Investment in Security Infrastructure – hence availability
  - Fault Tolerance and Reliability; Greater Resiliency
  - Hypervisor Protection Against Network Attacks
  - Possible Reduction of C&A Activities (Access to Pre-Accredited Clouds)
  - Simplification of Compliance Analysis
  - Data Held by Unbiased Party (cloud vendor assertion)
  - Low-Cost Disaster Recovery and Data Storage Solutions
  - On-Demand Security Controls
  - Real-Time Detection of System Tampering
  - Rapid Re-Constitution of Services
  - Advanced Honeynet Capabilities

# Cloud Security Downside

- NIST 800-144
  - System complexity –
    - e.g., public cloud is complex; attack surface increased
  - Shared Multi-tenancy
    - Logical separation instead of physical
  - Internet facing services
    - Exposure of admin/service interfaces
  - Loss of control – S&P are amplified!
    - On both physical/logical aspects; legal aspects

# Security Relevant Cloud Components

- Cloud Provisioning Services
- Cloud Data Storage Services
- Cloud Processing Infrastructure
- Cloud Support Services
- Cloud Network and Perimeter Security
- Elastic Elements: Storage, Processing, and Virtual Networks

# Provisioning Service

- Advantages
  - Rapid reconstitution of services
  - Enables availability
    - multiple data centers
    - multiple instances
  - Advanced honey net capabilities
- Challenges
  - Impact of compromising the provisioning service

# Data Storage Services

- Advantages
  - Data fragmentation and dispersal
  - Automated replication
  - Provision of data zones (e.g., by country)
  - Encryption at rest and in transit
  - Automated data retention
- Challenges
  - Isolation management / data multi-tenancy
  - Storage controller
    - Single point of failure / compromise?
  - Exposure of data to foreign governments

# Cloud Processing Infrastructure

- Advantages
  - Ability to secure masters and
  - Push out secure images
- Challenges
  - Application multi-tenancy
  - Reliance on hypervisors
  - Process isolation / Application sandboxes

# Cloud Support Services

- Advantages
  - On demand security controls
    (e.g., authentication, logging, firewalls…)
- Challenges
  - Additional risk when integrated with customer applications
  - Needs certification and accreditation as a separate application
  - Code updates

# Cloud Network and Perimeter Security

- Advantages
  - Distributed denial of service protection
  - VLAN capabilities
  - Perimeter security (IDS, firewall, authentication)
- Challenges
  - Virtual zoning with application mobility

# Other issues

- Issues with moving PII and sensitive data to the cloud
  - Privacy impact assessments
- Using SLAs to obtain cloud security
  - Suggested requirements for cloud SLAs
  - Issues with cloud forensics
- Contingency planning and disaster recovery for cloud implementations
- Handling compliance
  - FISMA; HIPAA; SOX; PCI ; SAS 70 Audits

# Obstacles & Opportunities

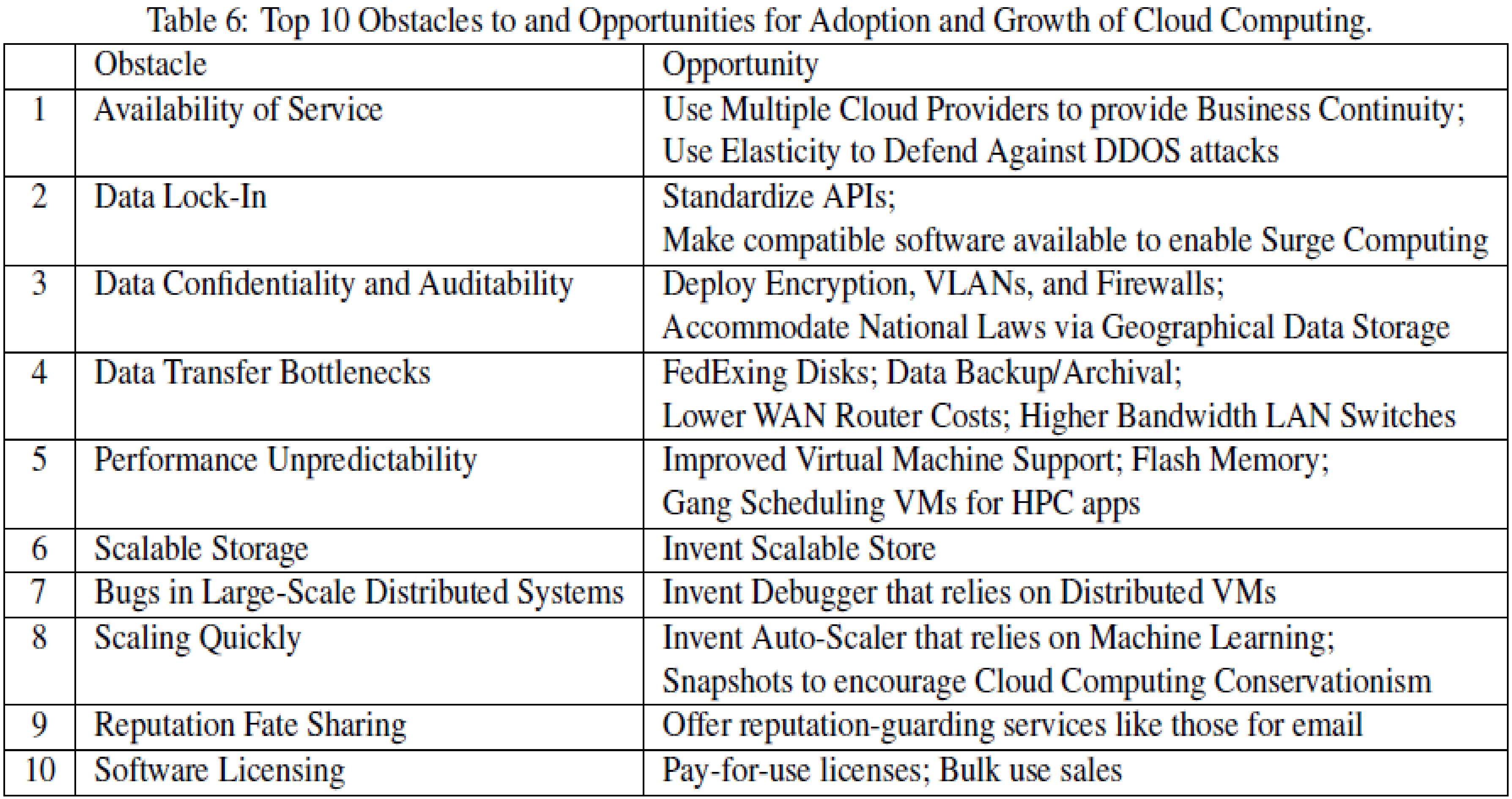


Table 6: Top 10 Obstacles to and Opportunities for Adoption and Growth of Cloud Computing.

| | Obstacle | Opportunity |
|---|---|---|
| 1 | Availability of Service | Use Multiple Cloud Providers to provide Business Continuity;<br>Use Elasticity to Defend Against DDOS attacks |
| 2 | Data Lock-In | Standardize APIs;<br>Make compatible software available to enable Surge Computing |
| 3 | Data Confidentiality and Auditability | Deploy Encryption, VLANs, and Firewalls;<br>Accommodate National Laws via Geographical Data Storage |
| 4 | Data Transfer Bottlenecks | FedExing Disks; Data Backup/Archival;<br>Lower WAN Router Costs; Higher Bandwidth LAN Switches |
| 5 | Performance Unpredictability | Improved Virtual Machine Support; Flash Memory;<br>Gang Scheduling VMs for HPC apps |
| 6 | Scalable Storage | Invent Scalable Store |
| 7 | Bugs in Large-Scale Distributed Systems | Invent Debugger that relies on Distributed VMs |
| 8 | Scaling Quickly | Invent Auto-Scaler that relies on Machine Learning;<br>Snapshots to encourage Cloud Computing Conservationism |
| 9 | Reputation Fate Sharing | Offer reputation-guarding services like those for email |
| 10 | Software Licensing | Pay-for-use licenses; Bulk use sales |

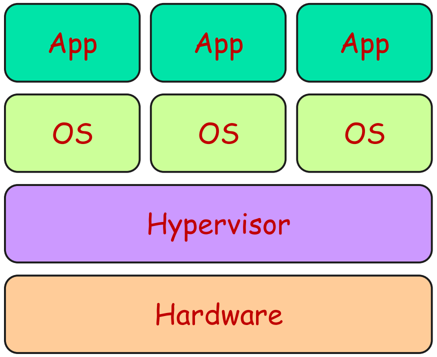
# Top 12 threats – in order of severity!! (2017)

1. Data Breaches
2. Weak Identity, Credential and Access Management
3. Insecure APIs
4. System and Application Vulnerabilities
5. Account Hijacking
6. Malicious Insiders
7. Advanced Persistent Threats (APTs)
8. Data Loss
9. Insufficient Due Diligence
10. Abuse and Nefarious Use of Cloud Services
11. Denial of Service
12. Shared Technology Vulnerabilities

SOURCE: https://downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf

# Virtualization

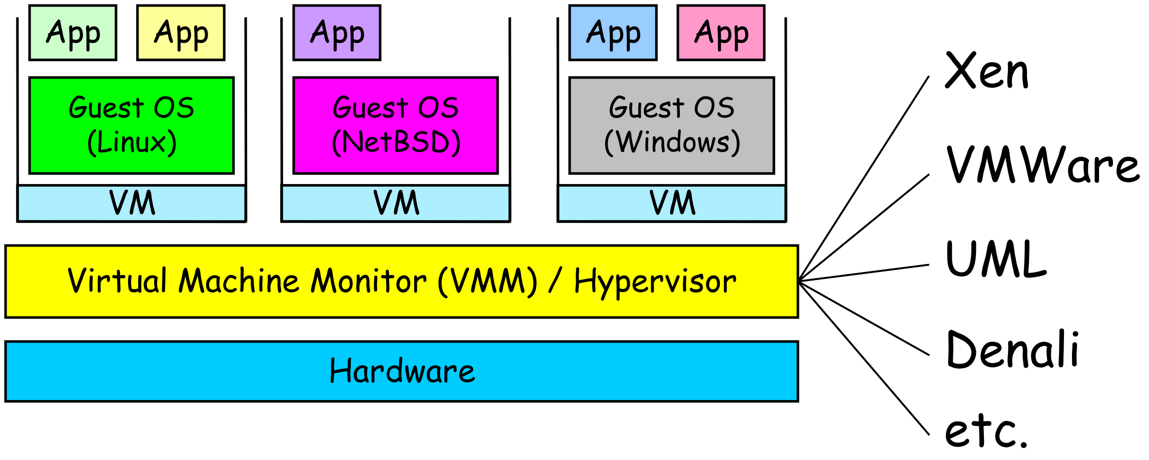
- Virtual workspaces:
  - An abstraction of an execution environment that can be made dynamically available to authorized clients by using well-defined protocols,
  - Resource quota (e.g. CPU, memory share),
  - Software configuration (e.g. O/S, provided services).
- Implement on Virtual Machines (VMs):
  - Abstraction of a physical host machine,
  - Hypervisor intercepts and emulates instructions from VMs, and allows management of VMs,
  - VMWare, Xen, etc.
- Provide infrastructure API:
  - Plug-ins to hardware/support structures



Virtualized Stack

# Virtual Machines

- VM technology allows multiple virtual machines to run on a single physical machine.



*Performance*: Para-virtualization (e.g. Xen) is very close to raw physical performance!

# Security Implications

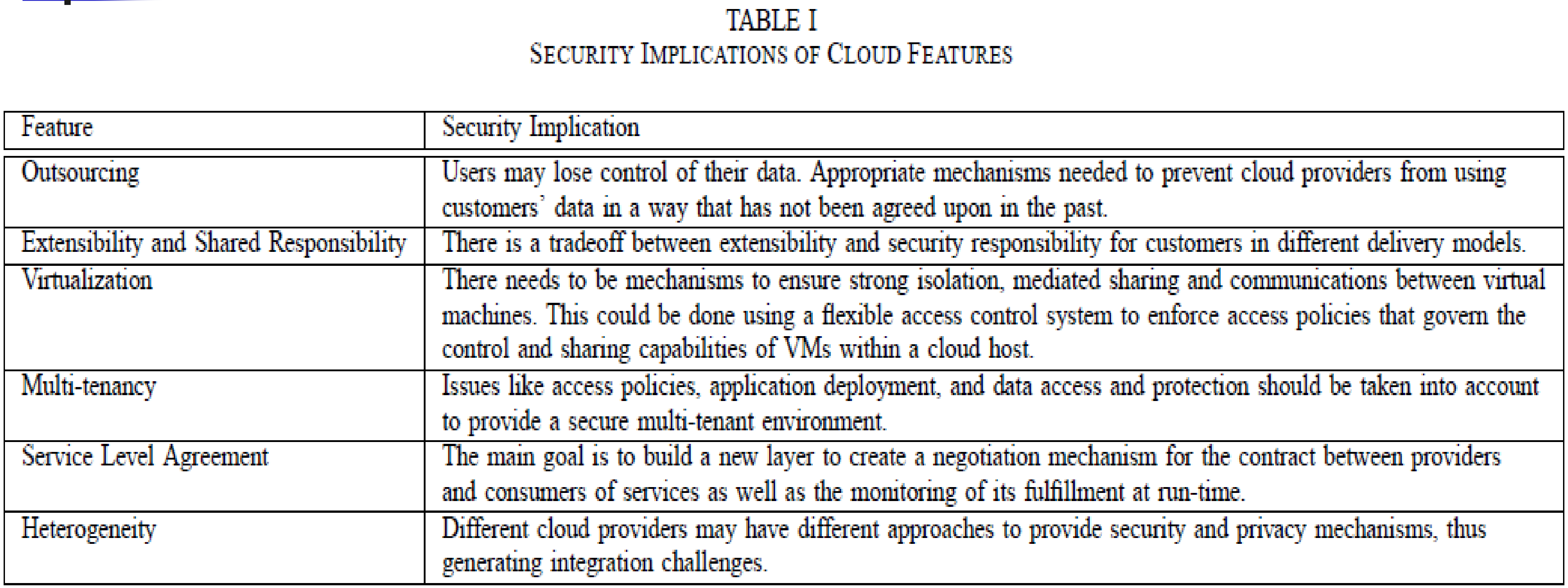


TABLE I
SECURITY IMPLICATIONS OF CLOUD FEATURES

| Feature | Security Implication |
|---|---|
| Outsourcing | Users may lose control of their data. Appropriate mechanisms needed to prevent cloud providers from using customers' data in a way that has not been agreed upon in the past. |
| Extensibility and Shared Responsibility | There is a tradeoff between extensibility and security responsibility for customers in different delivery models. |
| Virtualization | There needs to be mechanisms to ensure strong isolation, mediated sharing and communications between virtual machines. This could be done using a flexible access control system to enforce access policies that govern the control and sharing capabilities of VMs within a cloud host. |
| Multi-tenancy | Issues like access policies, application deployment, and data access and protection should be taken into account to provide a secure multi-tenant environment. |
| Service Level Agreement | The main goal is to build a new layer to create a negotiation mechanism for the contract between providers and consumers of services as well as the monitoring of its fulfillment at run-time. |
| Heterogeneity | Different cloud providers may have different approaches to provide security and privacy mechanisms, thus generating integration challenges. |

# Security and Privacy Challenges (Takabi et al.)

- Authentication and Identity Management
  - interoperability
  - password-based: inherited limitation
  - How multi-tenancy can affect the privacy of identity information isn’t yet well understood?
    - Healthcare organization likely to make sure areas are properly segregated
  - multi-jurisdiction issue
    - Laws/compliance requirement may differ
  - integrated with other security components.

# Security and Privacy Challenges (cont.)

- Access Control and Accounting
  - Heterogeneity and diversity of services, as well as the domains’ diverse access requirements
  - capture dynamic, context, or attribute- or credential-based access requirements
  - integrate privacy-protection requirements
  - interoperability
  - capture relevant aspects of SLAs

# Security and Privacy Challenges (cont.)

- Trust Management and Policy Integration
  - compose multiple services to enable bigger application services
  - efficiently capturing a generic set of parameters required for establishing trust and to manage evolving trust and interaction/sharing requirements
  - address challenges such as semantic heterogeneity, secure interoperability, and policy-evolution management.
    - Every stakeholder may have a different level of trust with the service provider.
    - Healthcare organizations and service providers have to confer and agree on the security properties that need to be applied in compliance with the HIPPA standard.

# Security and Privacy Challenges (cont.)

- Secure-Service Management
  - WSDL can’t fully meet the requirements of cloud computing services description
  - issues such as quality of service, price, and SLAs
  - automatic and systematic service provisioning and composition framework that considers security and privacy issues

# Security and Privacy Challenges (cont.)

- Privacy and Data Protection
  - storing data and applications on systems that reside outside of on-premise datacenters
  - shared infrastructure, risk of potential unauthorized access and exposure.
  - Privacy-protection mechanisms must be embedded in all security solutions.
  - Provenance
    - Balancing between data provenance and privacy

# Security and Privacy Challenges (cont.)

- Organizational Security Management
  - shared governance can become a significant issue if not properly addressed
  - Dependence on external entities
  - the possibility of an insider threat is significantly extended when outsourcing data and processes to clouds.

# Security and Privacy Approaches (Takabi et al.)

- Authentication and Identity Management
  - User-centric IDM
  - users control their digital identities and takes away the complexity of IDM from the enterprises
  - federated IDM solutions
  - privacy-preserving protocols to verify various identity attributes by using

# Security and Privacy Approaches (Takabi et al.)

- Access Control Needs
  - RBAC, Policy-integration needs
    - Cross domain accesses, Multi-tenant
  - credential-based RBAC, GTRBAC, location-based RBAC → Attribute-based

# Security and Privacy Approaches (Takabi et al.)

- Secure Interoperation
  - *Multi-domain*
  - centralized approaches
  - decentralized approaches
  - specification frameworks to ensure that the cross-domain accesses are properly specified, verified, and enforced
  - Policy engineering mechanisms

# Security and Privacy Approaches (Takabi et al.)

- Secure-Service Provisioning and Composition
  - Open Services Gateway Initiative (OSGi)
  - Declarative OWL-based language can be used to provide a service definition manifest, including
    - a list of distinct component types that make up the service,
    - functional requirements,
    - component grouping and topology instructions

# Security and Privacy Approaches (Takabi et al.)

- Trust Management Framework
  - trust-based policy integration
  - Delegation
  - must be incorporated in service composition framework

# Security and Privacy Approaches (Takabi et al.)

- Data-Centric Security and Privacy
  - shifts data protection from systems and applications
  - documents must be self-describing and defending regardless of their environments.

# Security and Privacy Approaches (Takabi et al.)

- Managing Semantic Heterogeneity
  - semantic heterogeneity among policies
  - Use of an ontology is the most promising approach
  - policy framework and a policy enforcement architecture
  - inference engines

# Key S&P Issues (NIST 800-144)

- Governance – amplifies this need!
  - Control and oversight challenging
  - Org programs should incorporate external entity
  - Role and responsibilities for risk mgmt
- Compliance
  - Law and regulations
  - Data location – in multiple physical locations? Disclosures? Cross border risks?
- Electronic Discovery
  - Does provider provide adequate e-discovery capabilities

HIPAA/HITECH
Addresses Cloud

# Key S&P Issues (NIST 800-144)

- Trust
  - Insider access
  - Data ownership – rights must be firmly established in SLA (e.g., controversy in SN related data ownership)
  - Composite Services
    - Composed through nesting and layering (e.g., SaaS, PaaS, etc.)
    - Compatibility, performance guarantees?
  - Visibility – of Provider's security measures
  - Ancillary data – accounts of consumers (payment info, client activity; access patterns; ..)!
  - Risk management

# Key S&P Issues (NIST 800-144)

- Architecture
  - Attack surface – VM/hypervisor introduce new attack surface
  - Virtual network protection
    - Software-based switches and network configurations
    - Potential loss of separation of duty in admin roles
  - Virtual Machine images
    - Must be up-to-date with patches
  - Client Side Protection – do not overlook this!
    - Involves mobile devices

# Key S&P Issues (NIST 800-144)

- Identity and Access Management
  - Org’s IAM framework may not extend to public cloud
    - Maintaining two may not be scalable/workable
  - Some form of identity federation is needed – SAML, OpenID standards
  - Authentication - SAML Standard
  - Access Control – XACML standard
- Software Isolation

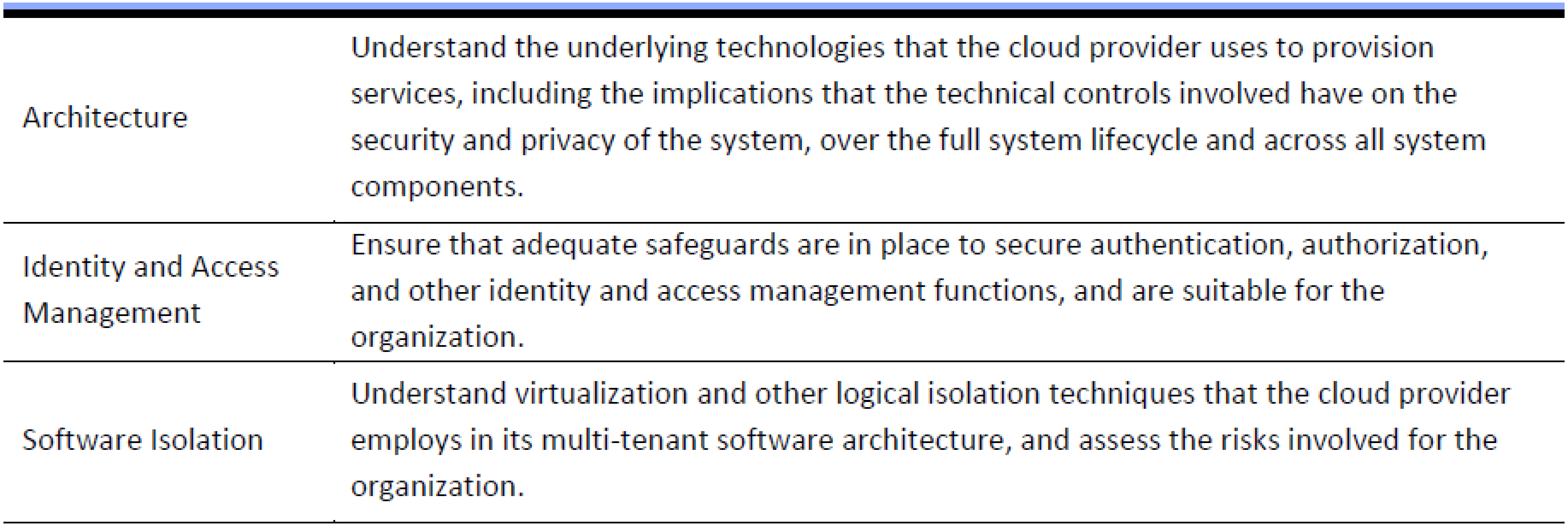
# Key S&P Issues (NIST 800-144)

- Software Isolation  - to support multitenancy!
  - Hypervisor complexity
  - Attack Vectors  -- new ones? Malicious code breaking isolation?
- Data Protection - Data in cloud exist in shared env
  - Value concentration
  - Data isolation
  - Data sanitization
- Availability – accessible and usable
  - Temporary,  Prolonged/Permanent Outages
  - Denial of Service attacks

# Key S&P Issues (NIST 800-144)

- Incidence Response
  - Data availability
    - Clients may not see event logs and viln info under provider
      - Complex when several providers are involved; multi-tenancy
  - Incident analysis and resolution
    - Lack of detailed info regarding architecture/mechanisms
    - Forensic copies may be difficult to create – multitenant?
    - How to contain an attack?

# Summary of Recommendations



| | |
|---|---|
| Architecture | Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components. |
| Identity and Access Management | Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization. |
| Software Isolation | Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization. |

# Outsourcing in Public Cloud - General Concerns

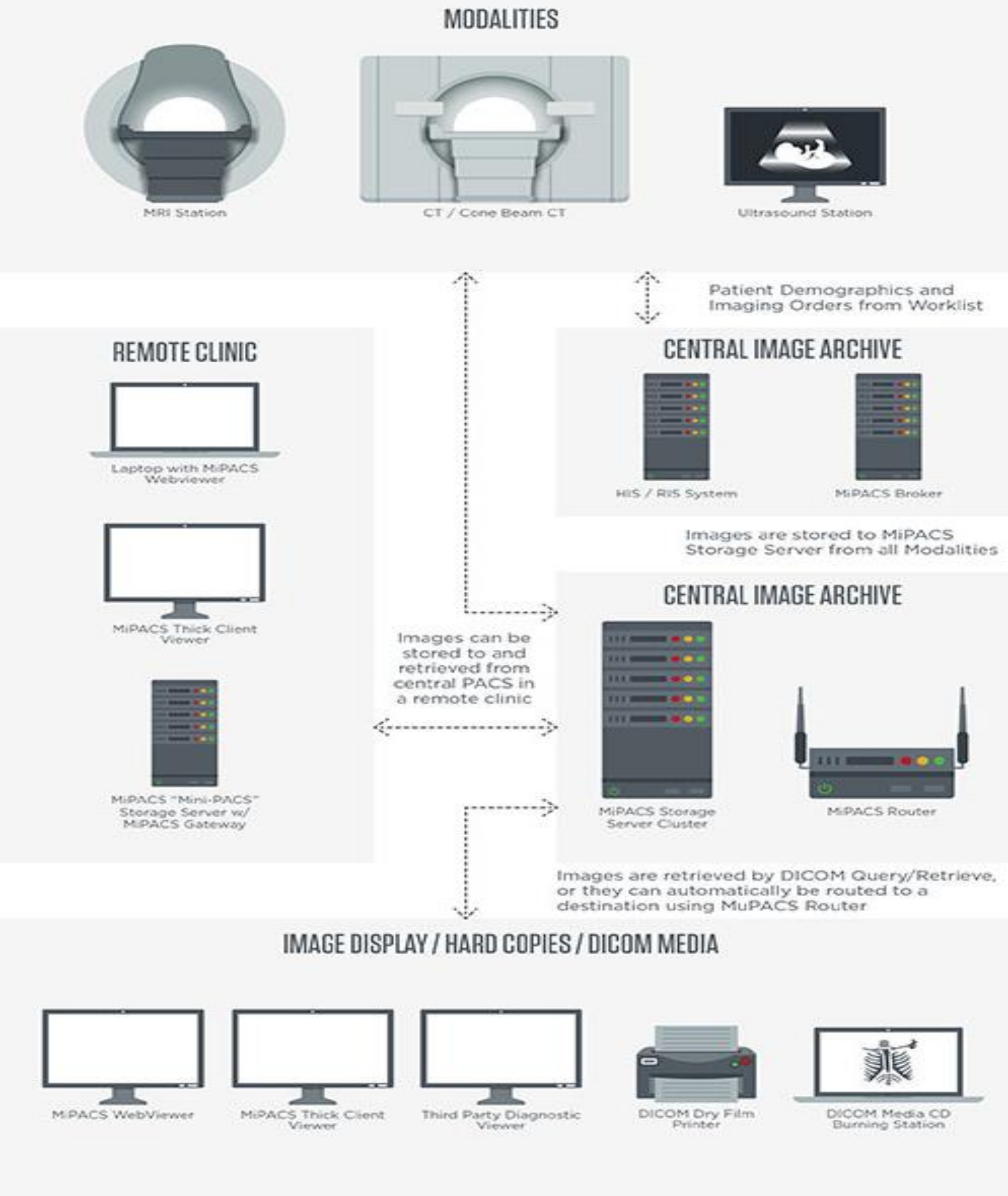
- Inadequate policies and practices
  - Undetected violations
  - Lack of sufficient data/configuration integrity
  - Loss of privacy – non-rigourous mechanisms?
- Weak confidentiality, Integrity, availability sureties
  - Need ways to establish assurances
- Other concerns
  - Principle-agent problem – need to make sure interest of the provider is consistent
- Attenuation of expertise
  - Organization may slowly lose expertise

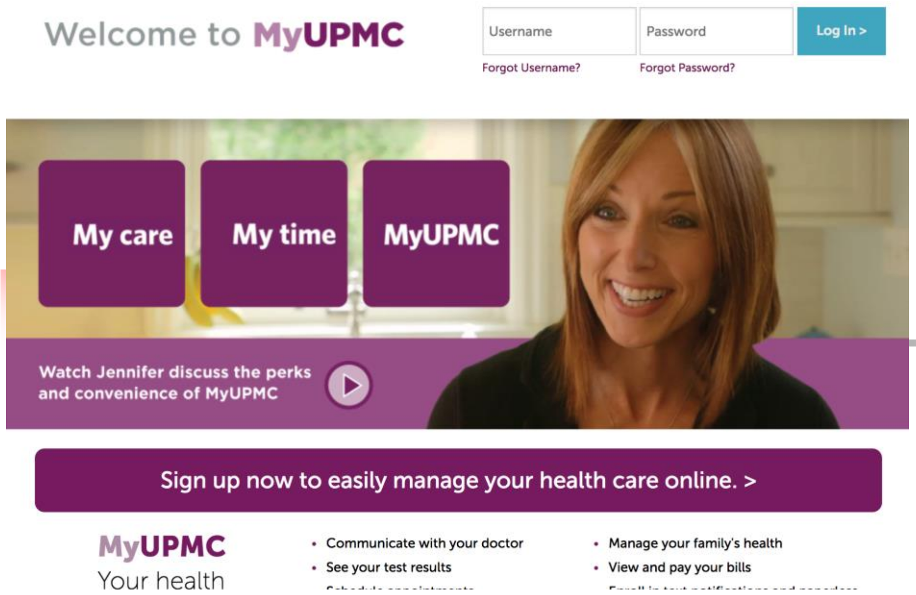
Telemedicine/Teleconsultation

*Supporting communications and sh among stakeholders in Healthcare*

Medical imaging focusing on the storage, sharing and computation of images

- e.g. Medicor imaging Picture Archive and Communication System (MiPACS) Storage Server
- Imaging Management Solutions for Radiology—Image Archiving Solutions


MODALITIES
MRI Station
CT / Cone Beam CT
Ultrasound Station
Patient Demographics and Imaging Orders from Worklist
REMOTE CLINIC
Laptop with MiPACS Webviewer
MiPACS Thick Client Viewer
MiPACS "Mini-PACS" Storage Server w/ MiPACS Gateway
CENTRAL IMAGE ARCHIVE
HIS / RIS System
MiPACS Broker
Images are stored to MiPACS Storage Server from all Modalities
CENTRAL IMAGE ARCHIVE
Images can be stored to and retrieved from central PACS in a remote clinic
MiPACS Storage Server Cluster
MiPACS Router
Images are retrieved by DICOM Query/Retrieve, or they can automatically be routed to a destination using MuPACS Router
IMAGE DISPLAY / HARD COPIES / DICOM MEDIA
MiPACS WebViewer
MiPACS Thick Client Viewer
Third Party Diagnostic Viewer
DICOM Dry Film Printer
DICOM Media CD Burning Station



Welcome to MyUPMC

Username | Password | Log In >

Forgot Username? Forgot Password?

My care | My time | MyUPMC

Watch Jennifer discuss the perks and convenience of MyUPMC

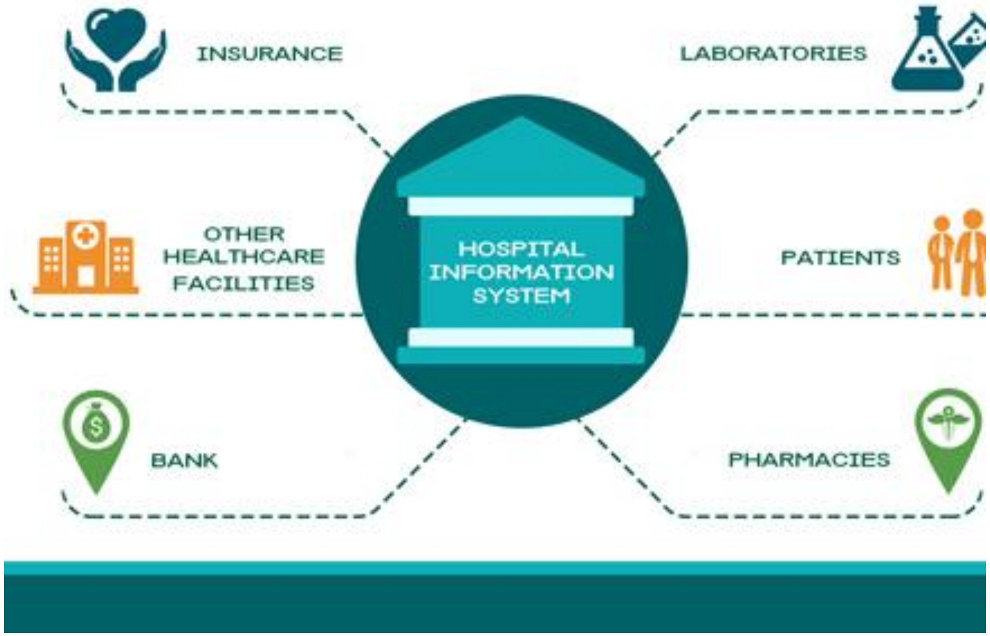
Sign up now to easily manage your health care online. >

MyUPMC
Your health

- Communicate with your doctor
- See your test results
- Manage your family's health
- View and pay your bills

Public Health & Patient’s Self Management -- is concerned with prevention, health promotion or improvement for individual citizens and patients but also for large population groups (epidemiology)

A hospital information system (HIS) is an element of health informatics that focuses mainly on the administrative needs of hospitals.



## Therapy

Applications for planning, managing or assessing therapeutic interventions

The Physical Therapist Centralized Application Service (PTCAS) is a service of the American Physical Therapy Association (APTA).

- PTCAS allows applicants to use a single application and one set of materials to apply to multiple DPT programs.

## Secondary Use of Data

Describing cloud computing utilization for enabling secondary use of clinical data

e.g. data analysis, text mining, or clinical research.

# Significant dependencies/ information flow

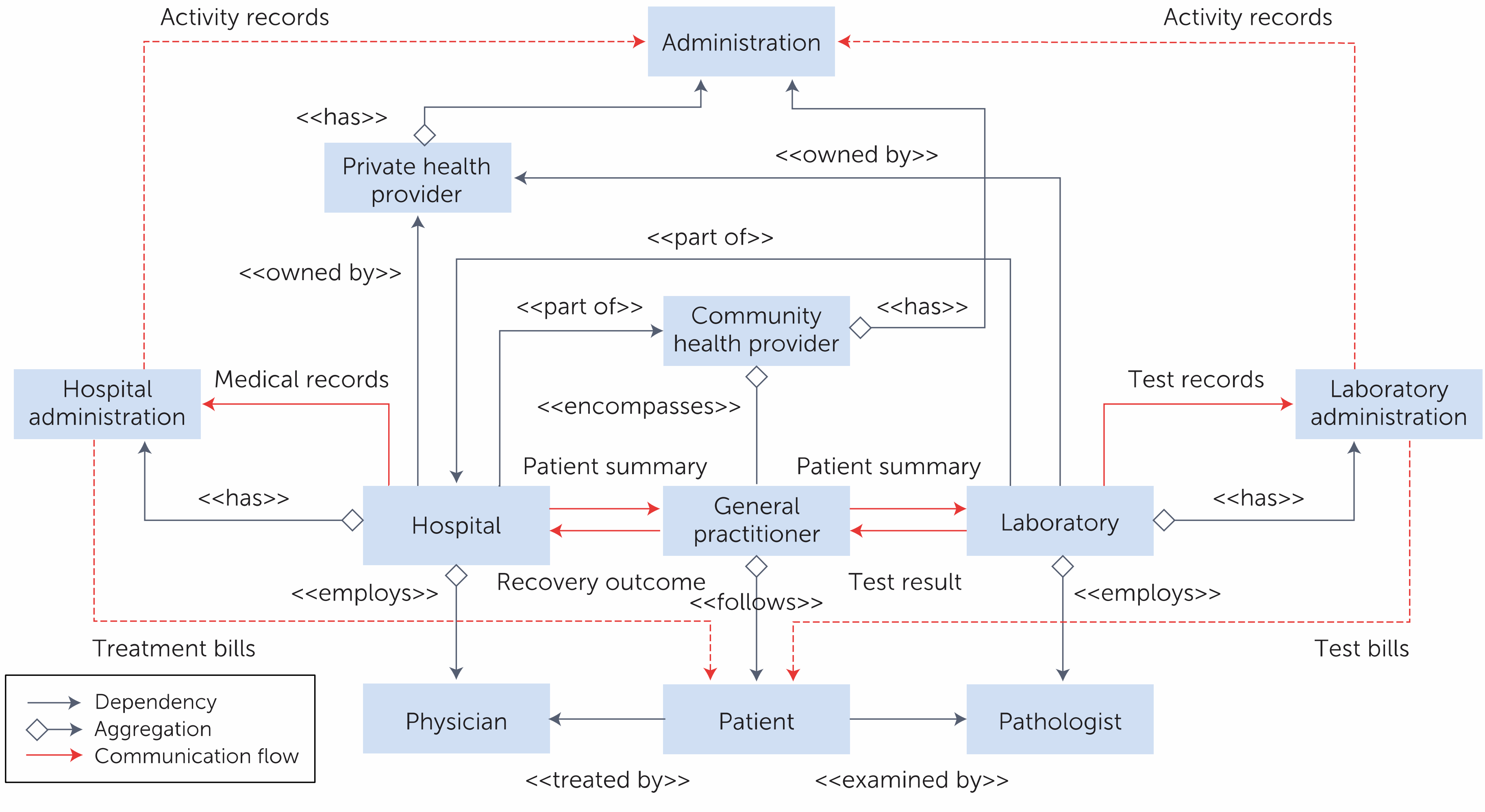
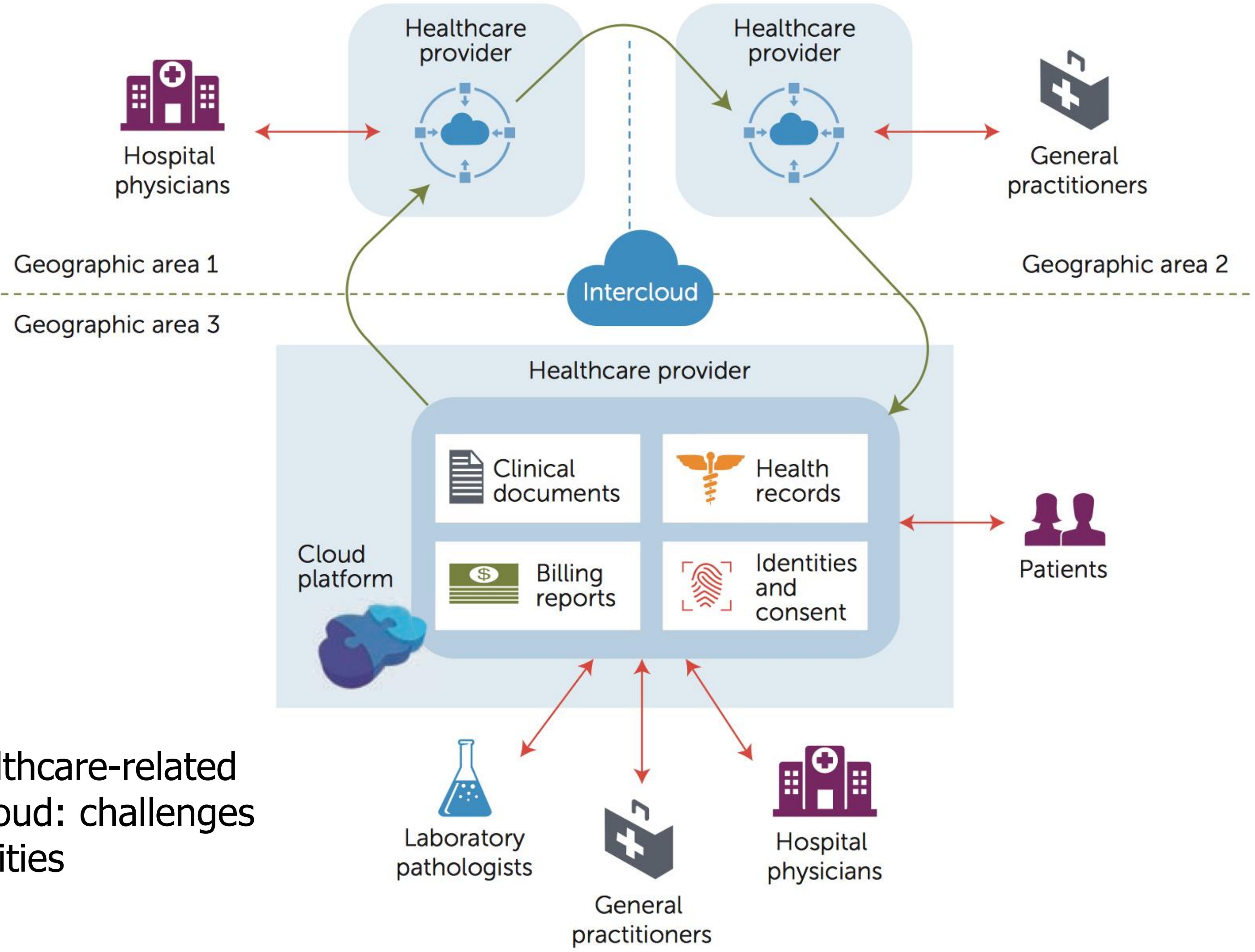


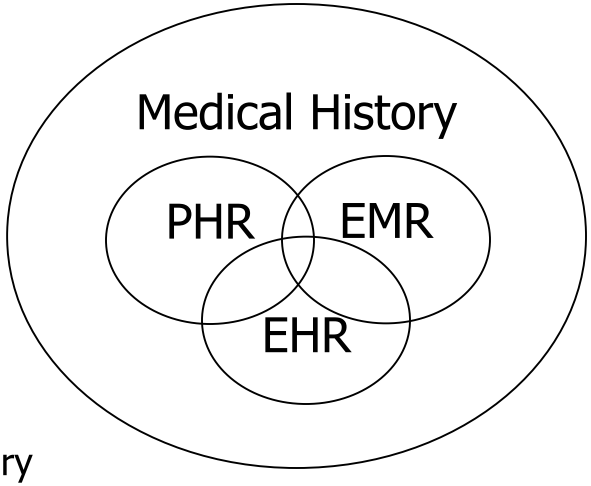
FIGURE 1. Overview of dependencies and communication flows in the healthcare domain.

# Cloud based health and medical data management



**Source**: Healthcare-related data in the cloud: challenges and opportunities

# PHR, EMR, EHR



- PHR (Personal Health Records)
  - initiated and maintained by an individual
  - Ideally an accurate summary of the health and medical history
- EMR (Electronic Medical Record) vs. EHR (Electronic Health Records)

**CDO**: Care delivery Organization

**CDR**: Clinical Data repository

**CDSS**: Clinical Decision Support System

**CMV**: Controlled Medical Vocabulary

| | EMR | EHR |
|---|---|---|
| Definition | The legal record of clinical services for a patient within a CDO. | A subset of EMR from one or more CDOs where the patient received clinical services. |
| Owner | Owned by the CDO | Owned by patient or stakeholder |
| Consumer & Usage Scope | EMR systems are supplied by enterprise vendors and installed by hospitals, health systems, clinics, etc. | EHR systems are run by community, state, or regional emergence, or national wide emergence organizations. |
| Right of patient | Patients can gain access to some EMR information once authorized by the EMR owner. | Patients are provided with interactive access as well as the ability to append information. |
| Interoperability with other CDOs | Each EMR contains the patient's encounter in a single CDO. It does not contain other CDO encounter data. | Sharing information among multiple CDOs, connected by National Health Information Network (NHIN). |

**As per: HIMSS (Health Information and Management System Society) Analytics**

# Taxonomy of Healthcare Clouds

- Applications in the Cloud (SaaS)
  - the security and privacy protection is provided as an integral part of the SaaS to the healthcare consumers.
- Platforms in the Cloud (PaaS)
  - two levels of protection for security and privacy are required.
  - **At the lower system level**: the cloud provider may provide basic security mechanisms such as end-to-end encryption, authentication, and authorization.
  - **At the higher application level**: the consumers need to define application dependent access control policies, authenticity requirements, and so forth.
- Infrastructure in the Cloud (IaaS)
  - has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).
  - Here, the healthcare application developers hold full responsibility for protecting patients' security and privacy.

# Taxonomy of Healthcare Clouds

- Private Cloud
  - Operated solely by CDO
  - Managed by the org or third party – on or off premise
  - Same type of security and privacy measure as those in the EMR system run by a CDO
- Community Cloud -- Microsoft Health Vault; Google Health
  - Several CDOs share the infrastructure – to serve a community with shared set of concerns, such as: mission, security requirements, policy, and compliance consideration
  - most likely managed by the third party or the CDOs and may exist on or off premise.
- Public Cloud
  - the healthcare application developers and consumers hold full responsibility for protecting patients' security and privacy.

# Some key S&P issues

- how to manage and control the access of the EMR data in the EHR system as accessing EMR data are typically controlled through authorization models.
- a patient may not want to divulge some of his sensitive health information in his EHRs to some family members or some healthcare providers who will offer healthcare for him due to varying concerns.
    - we need to address the requirement of privacy preserving access to EHRs.
- need to address the authenticity of EHR data with respect to both content authentication and source verifiability
- For practitioners –
    - important to provide secure mechanisms to obtain patients' information from multiple EMR/EHR repositories accurately, securely and fast
    - Authorization from CDOs as well as patient-consent enabled access control

# Healthcare Cloud – a patient-centric view

- Patient-centric view: the information stored in the community EHR system is imported by patients and only can be made available to a variety of applications under the control of patients

Microsoft HealthVault and Google Health: adopt a centralized architecture with patient-centric views

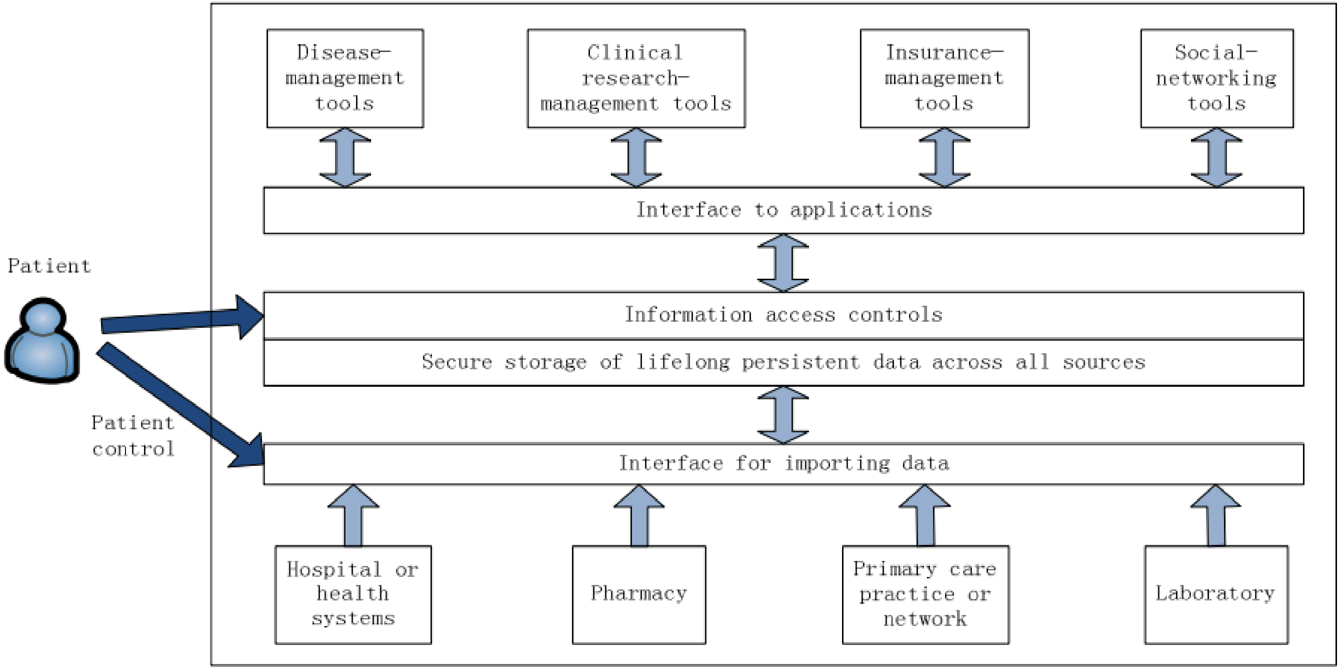

Disease-management tools
Clinical research-management tools
Insurance-management tools
Social-networking tools
Interface to applications
Patient
Information access controls
Secure storage of lifelong persistent data across all sources
Patient control
Interface for importing data
Hospital or health systems
Pharmacy
Primary care practice or network
Laboratory

Figure 2. Patient-Centric and Initial (Centralized) Healthcare Cloud

# Common security issues shared by healthcare cloud applications

- Ownership of Information
  - “owner” can refer to the person responsible for the information or the organization creating and storing the information.
  - “owner” may refer to “creator”, “author” and “manager” of the information.
- Authenticity and Authentication
- Non-repudiation
- Patient consent and authorization
  - How can patient express consent – one approach grant rights on the basis of role or attributes (ABEs)
- Integrity and confidentiality
- Availability and utility/usability
- Audit and archiving

# A healthcare scenario

A patient, named Alice, is recently diagnosed for a gastric cancer.

Surgical removal of the stomach (gastrectomy) is the only treatment. Chemotherapy and radiation therapy given after surgery can improve the chance of a cure.

Alice enters a cancer-treatment center at her chosen hospital.

Alice has a general practitioner whom she regularly visits. Upon entering the hospital, Alice also has an attending doctor from the hospital. Alice's health condition has caused some complications – so her attending doctor would like to seek for expert opinion and consultation for Alice's treatment from different CDOs, including Alice's specific general practitioner because he is fully informed about Alice's medical history.

In such a group consultation, every participant needs to obtain the medical records they request based on the HIPAA minimal disclosure principle.

Furthermore, the consultation result, such as the diagnosis and treatment suggestions, should be signed and certified by this group of specialists and practitioners.

The medical certificate with their signatures is sent to Alice.

If Alice would like to share this medical information with her loved ones and her family physician, she can put the new medical certificate into her PHR database.

**Patient's view**:

(i) be ensured that the diagnosis from the group of doctors can be trusted with a true medical certificate from the group of practitioner. This is the problem of secure EHR usage models.

(ii) Alice may prefer to disclose the minimal amount of her sensitive medical information and her family health history.

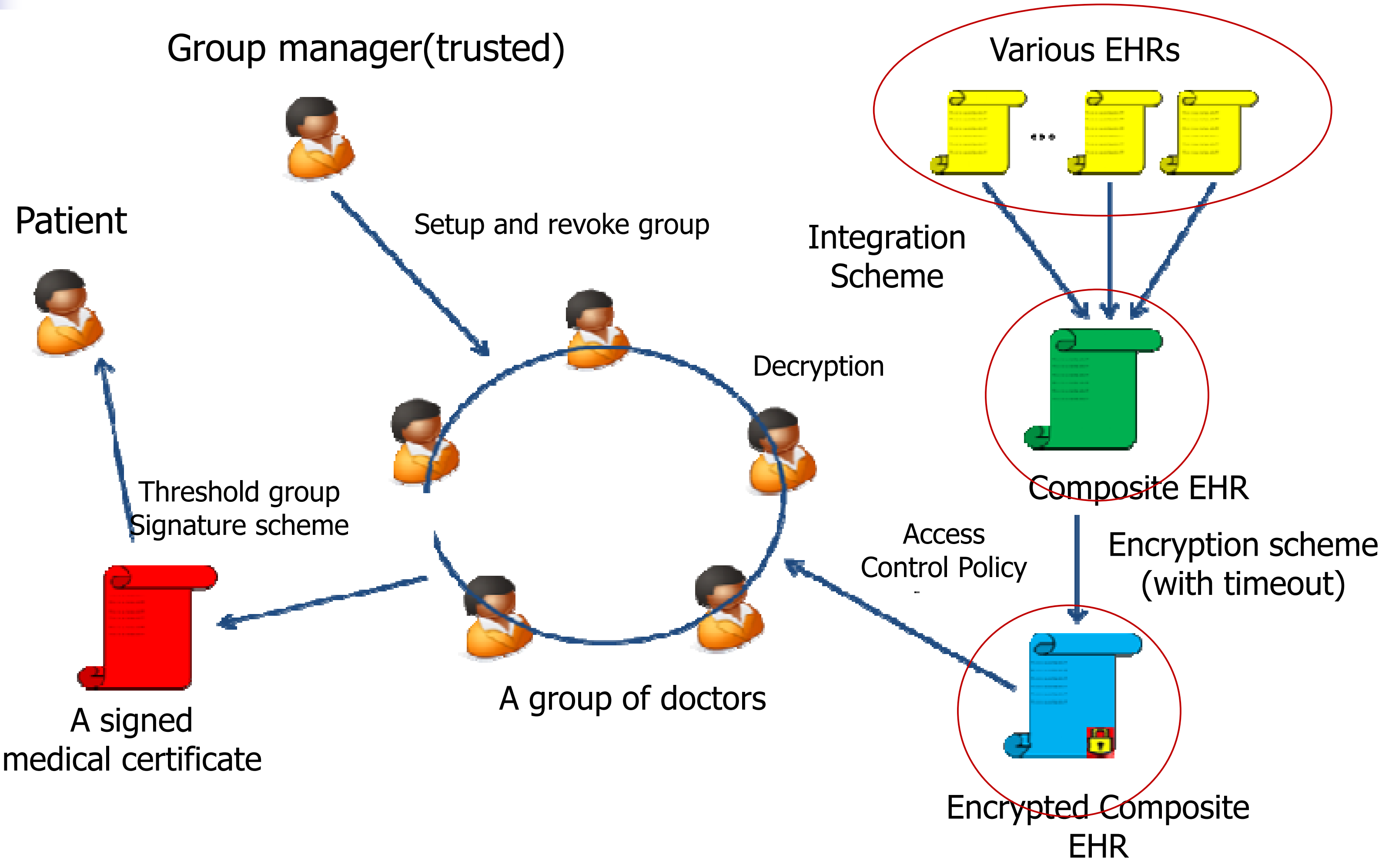
**Practitioners view**:

(i) How to securely obtain the EMRs of patient Alice, which is relevant to her gastric cancer treatment, with the compliance of HIPAA minimal disclosure. This concerns the problem of secure EHR collection and integration .. In cloud

(ii) How to certify the authenticity of EHRs obtained from different CDOs or information from Alice's PHR upon authorization by Alice. This relates to the problem of secure storage and management of HER … including in cloud

Mechanism needs to be thought from cloud perspective

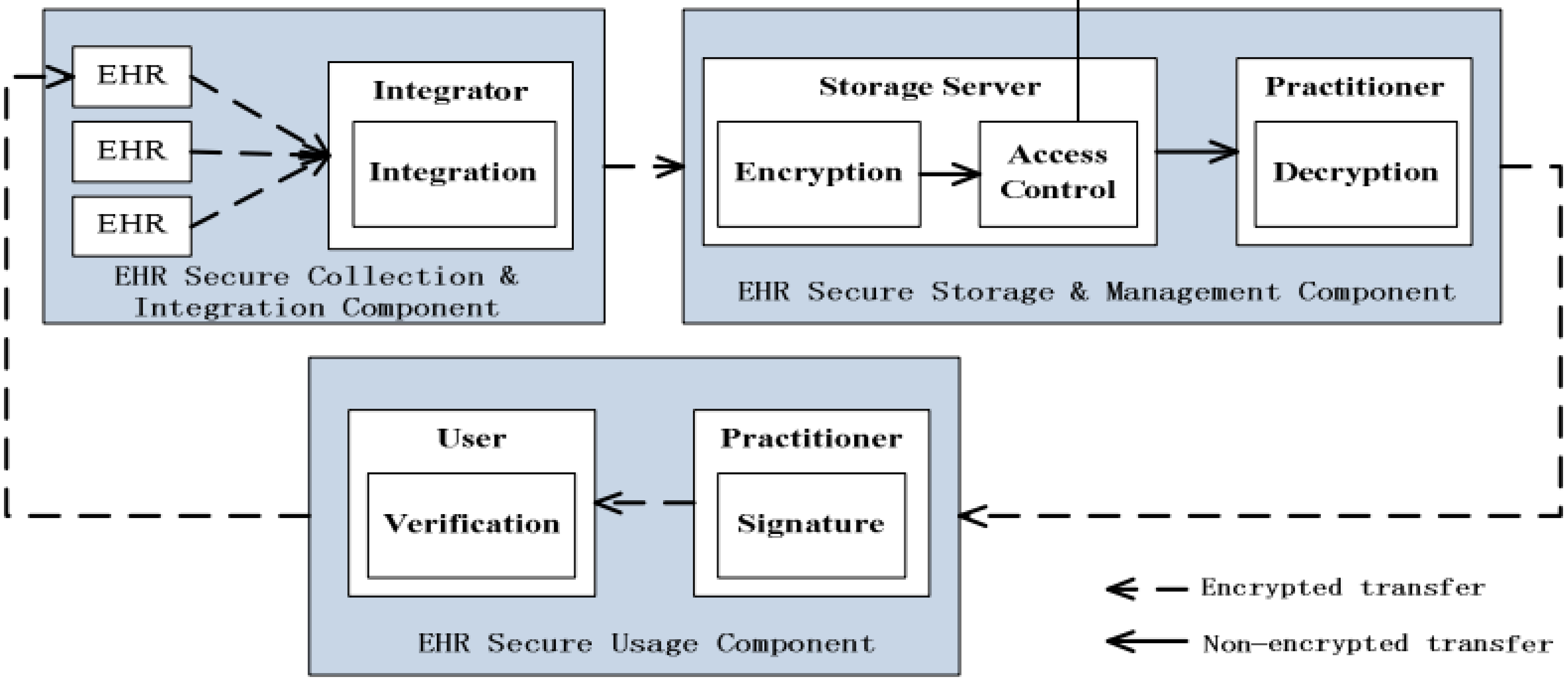
# EHR usage Scenario

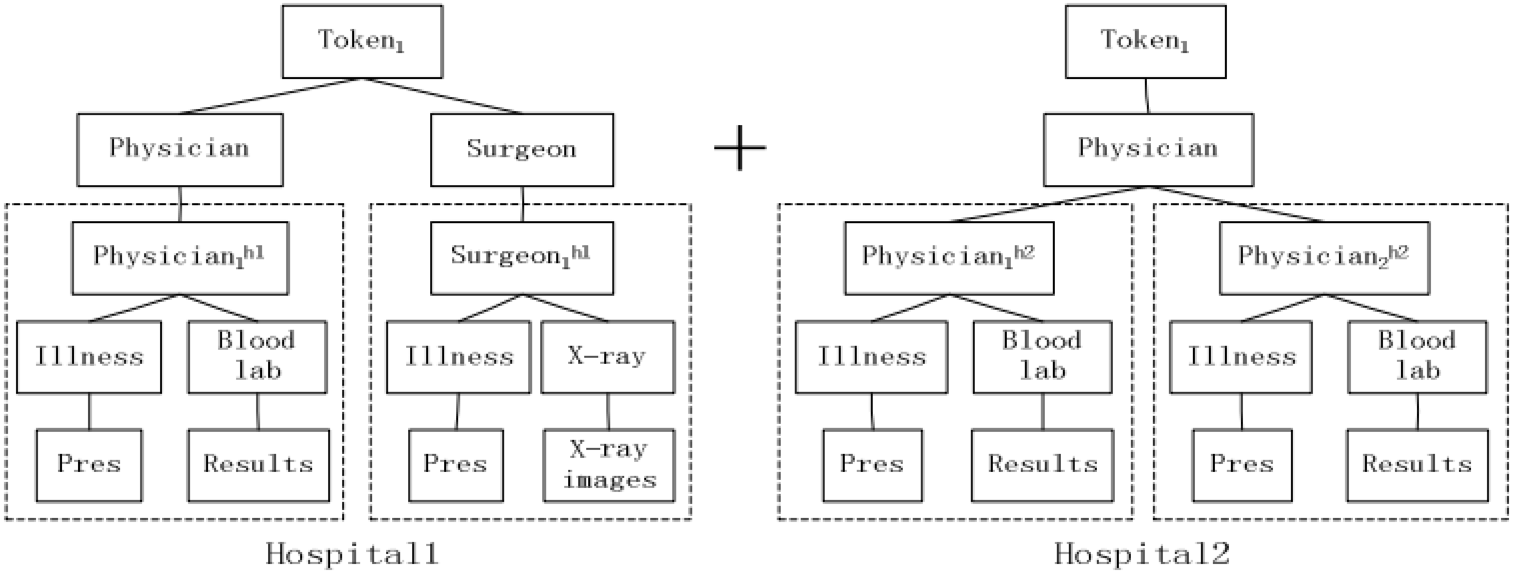


# System components: SC&I, SS&MC

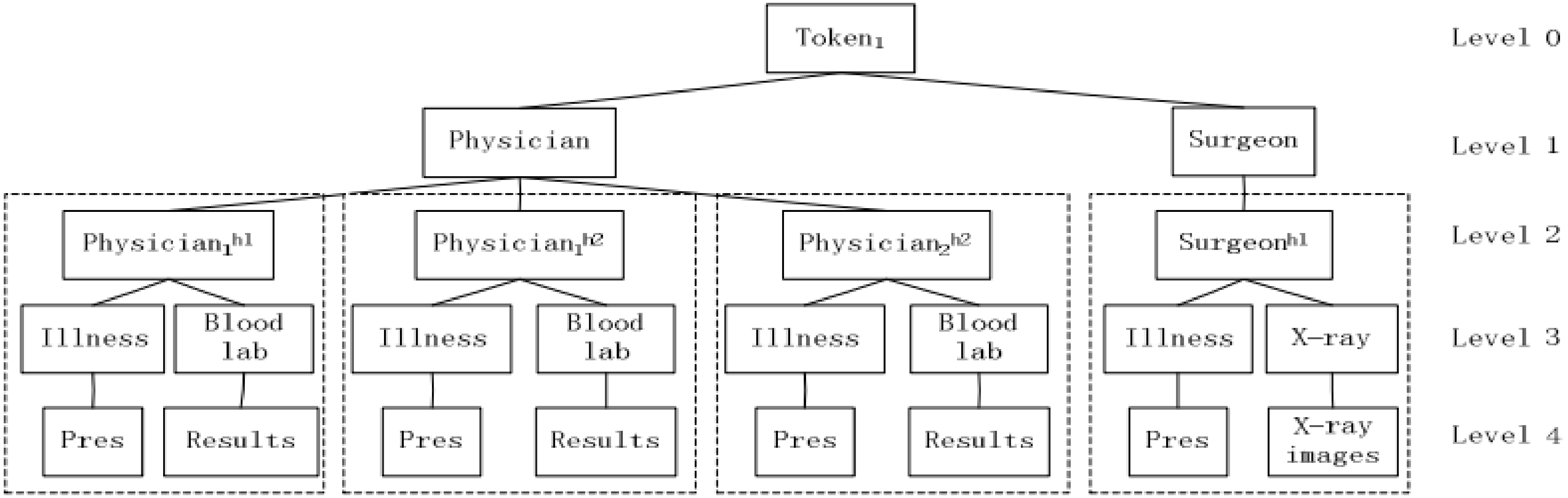
It is responsible for two important tasks: (i) It needs to verify various EHRs provided by different CDOs in terms of authenticity, confidentiality, integrity, and ensuring nonrepudiation as well as l
integrates the successfully verified E
security certificate signed by the int

manages a collection of role-based or attribute-based access control policies and HIPPA compliance policies, and enforces the access control policies to prevent the data from unauthorized access





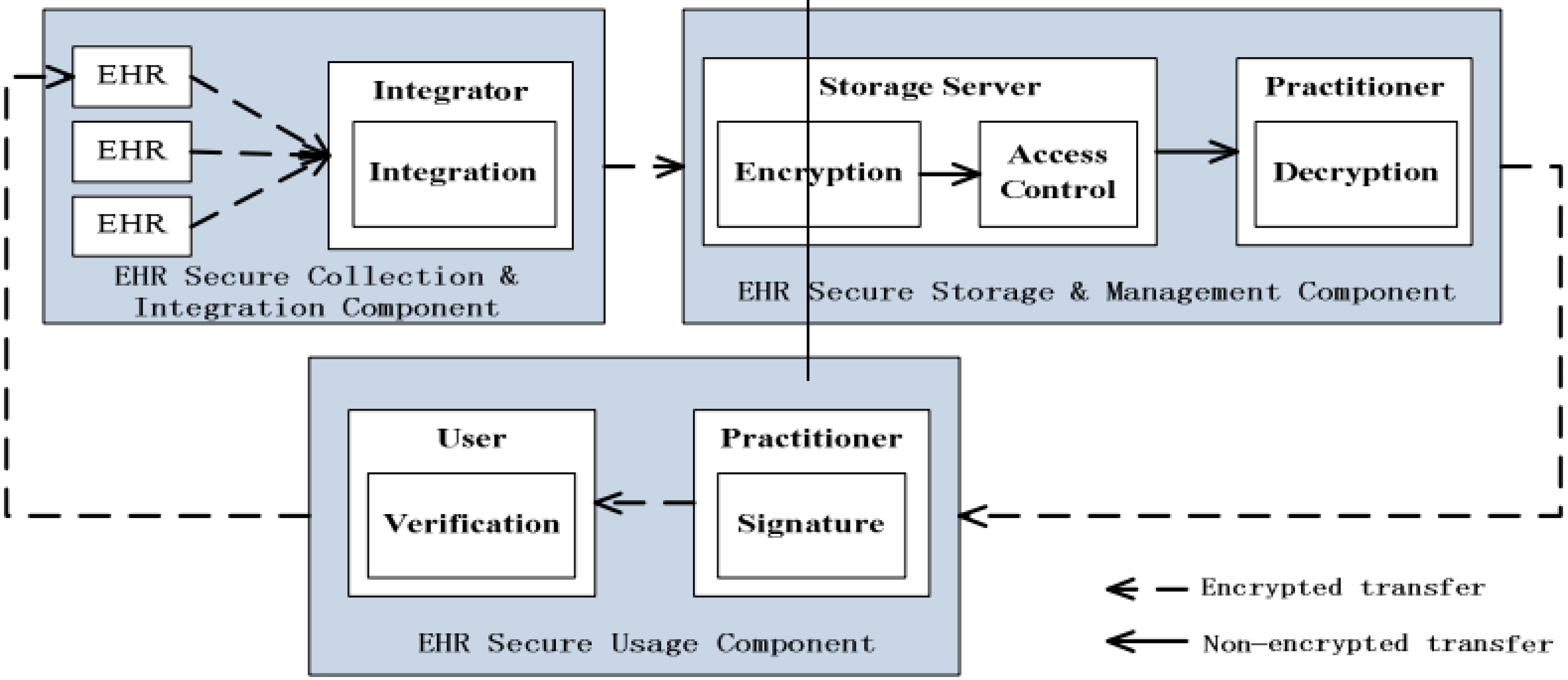
Attribute-based composite model [Gail’s team]
Role-based composite EHR model



The composite EHR tree

# System components:
# EHR secure usage model

Provides source verifiable content access for consumers of EHR data, including both patients and healthcare practitioners.
(i) Signature (ii) Verification



# A Review on the State-of-the-Art Privacy-Preserving : Approaches in the e-Health Clouds

Assad Abbas and Samee U. Khan, *Senior Member, IEEE*

# Privacy Requirements of e-Health Cloud

## Integrity

- *to ensure that the health data captured by a system or provided to any entity is true representation of the intended information and has not been modified in any way*

## Confidentiality

- *to ensure that the health data of patients is kept completely undisclosed to the unauthorized entities.*

## Authenticity

- *ensures that the entity requesting access is authentic.*
- *In the healthcare systems, the information provided by the healthcare providers and the identities of the entities using such information must be verified.*

# Privacy Requirements of e-Health Cloud

## Accountability

- *an obligation to be responsible in light of the agreed upon expectations.*
- *The patients or the entities nominated by the patients should monitor the use of their health information whenever that is accessed at hospitals, pharmacies, insurance companies etc.*

## Audit

- *to ensure that all the healthcare data is secure and all the data access activities in the e-Health cloud are being monitored.*

## Nonrepudiation

- *repudiation threats are concerned with the users who deny after performing an activity with the data.*
- *E.g, in the healthcare scenario neither the patients nor the doctors can deny after misappropriating the health data.*

# Privacy Requirements of e-Health Cloud

## Anonymity

- *refers to the state where a particular subject cannot be identified.*
- *E.g, identities of the patients can be made anonymous when they store their health data on the cloud so that the cloud servers could not learn about the identity.*

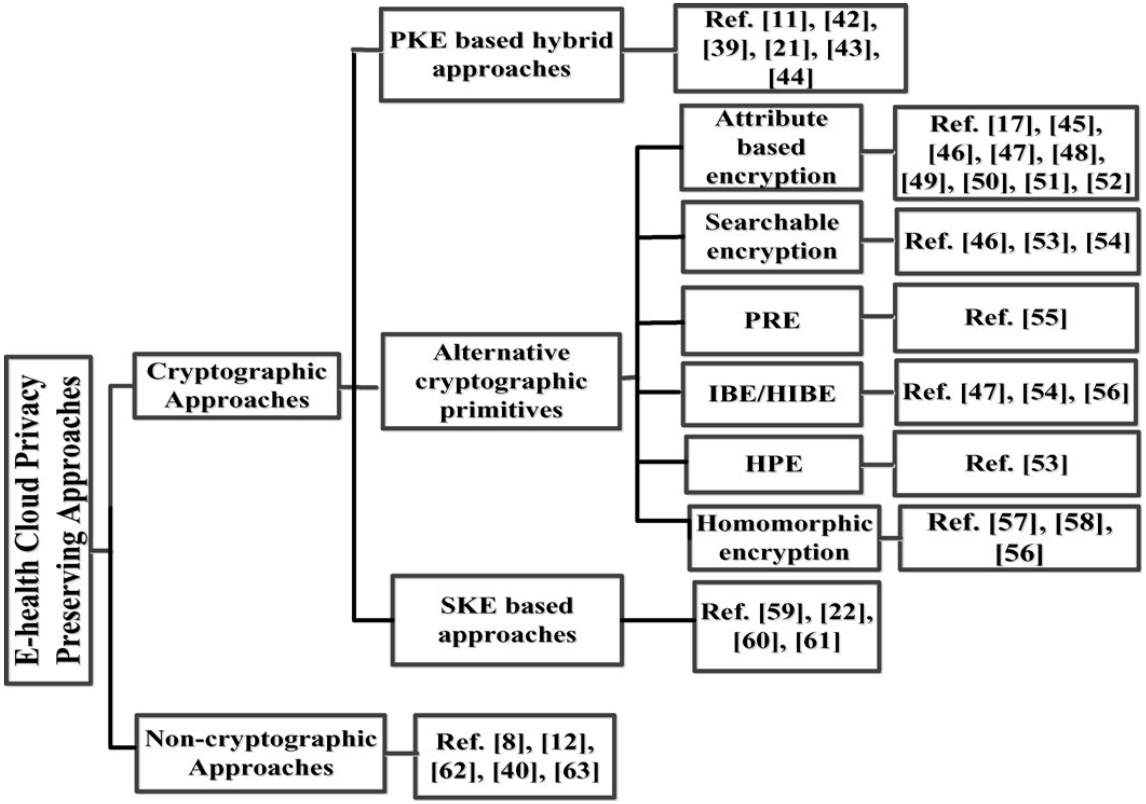
## Unlinkability

- *refers to the use of resources or items of interest multiple times by a user without other users or subjects being able to interlink the usage of these resources*

- Integrity, confidentiality, authenticity, accountability, audit, non-repudiation

# Approaches of e-Health Cloud

- There is no clear classification … so
  - Cryptographic approach
    - to mitigate the privacy risks utilize certain encryption schemes and cryptographic primitives
  - Noncryptographic approach
    - policy-based authorization infrastructure that allows the data objects to have access control policies.



E-health Cloud Privacy Preserving Approaches

Cryptographic Approaches

PKE based hybrid approaches

Ref. [11], [42], [39], [21], [43], [44]

Alternative cryptographic primitives

Attribute based encryption

Ref. [17], [45], [46], [47], [48], [49], [50], [51], [52]

Searchable encryption

Ref. [46], [53], [54]

PRE

Ref. [55]

IBE/HIBE

Ref. [47], [54], [56]

HPE

Ref. [53]

Homomorphic encryption

Ref. [57], [58], [56]

SKE based approaches

Ref. [59], [22], [60], [61]

Non-cryptographic Approaches

Ref. [8], [12], [62], [40], [63]

Fig. 1. Taxonomy of the privacy preserving approaches in the e-Health cloud.

# Cryptographic Approaches

- Commonly used in the e-Health cloud-based systems to protect data use encryption schemes
  - Basic ways
    - Public Key Encryption
    - Symmetric Key Encryption
  - Cryptographic primitives
    - Searchable Encryption
    - (Hierarchical) Identity-Based Encryption (HIBE)
    - Proxy Re-encryption (PRE)
    - Predicate/Hierarchical Predicate Encryption (HPE)
    - (Fully) homomorphic encryption

# Approaches Based on the SKE

- The SKE uses the same keys for encryption and decryption.
- The SKE-based algorithm currently in use and acting as standard is the Advanced Encryption Standard (AES).
  - was recommended as a standard by the National Institute of Standards and Technology (NIST)
- Commonly used stream ciphers
  - such as RC4and A5/1.

# Example ([Li et al. [59])

- A mechanism for *unlinkability* between the patients and electronic medical records in the cloud environment
  - The patients’ EMRs are encrypted through the SKE and are stored in an anonymous way.
  - The doctors use digital signatures to process the patient health records after the treatment for storage at the cloud.
  - Requirements to access EMR
    - Electronic Medical Record number (PID)
    - identity seed stored inside the Patients’ Health Card (SID)
    - a random value (R)
    - a serial number for treatment (SN)
      - Required to access health data
    - a smart card is required that contains the SID
    - Furthermore, the PID is stored in two parts separately that restricts the illegitimate access over the patient data.

# PKE-Based Hybrid Approaches

- The PKE technique requires two separate keys
  - One of the keys is private whereas the other is public
  - Limitations
    - the slower operations and the larger key sizes
    - using the PKE alone seems computationally less efficient
- The PKE is used in combination with the SKE
  - symmetric keys are used to encrypt the contents
  - public/private keys are used to secure the symmetric keys.

# Example ([Javari et al.])

- A patient-centric control over the EHRs
  - Digital Rights Management (DRM)-based approach for secure management of the health records in the cloud.
    - the data is always stored in an encrypted form and the license is issued by the owner
    - the policies expressed in the license are enforced by the agent
    - Content Key Encryption (CKE) is used in DRM systems
      - Data is encrypted using a content key & only the user with valid license are allowed to decrypt and use the content
      - The health record service provider acts as the distributor by providing the protected content only to the authorized users.
      - The provider cannot access the contents in clear text form.
      - Patients and physicians are assigned the public and the private keys for encryption and decryption.

# Approaches Based on Alternative Cryptographic Primitives

- Attribute-based encryption (ABE) approaches
    - the messages can be encrypted and decrypted on the basis of user attributes.
    - enables the users to selectively share the encrypted data and also provides a fine-grained access
    - Ciphertext policy attribute-based encryption (CP-ABE)
        - a message in the CP-ABE is encrypted under an access policy that defines the access structure, whereas the users' private keys are associated with a set of attributes.
    - Key policy attribute-based encryption (KP-ABE)
        - the access policies in the KP-ABE are associated with the private key whereas a set of descriptive attributes is used to label the ciphertext
    - Multiauthority attribute-based encryption (MA-ABE)
    - Broadcast ciphertext-policy attribute-based encryption (bABE)
        - Direct revocation of the user keys without the need of refreshing system parameters or data re-encryption - increased overheard

# Approaches Based on Alternative Cryptographic Primitives

- Approaches based on miscellaneous cryptographic primitives
  - Searchable encryption
    - permits to perform search operations over the encrypted data without revealing the information about the contents and the user query to the untrusted servers
  - Predicate encryption and hierarchical predicate encryption
    - the secret keys correspond to the predicates and these secret keys are used to decrypt the ciphertext associated with the attributes corresponding to the predicate
    - HPE facilitates the delegation of the search capabilities.
  - Identity-based encryption
    - uses any string for instance, a name or an email address as the public key and the corresponding decryption keys are issued by a trusted party.
  - (Fully)Homomorphic Encryption (FHE)
    - permits computations on ciphertexts and also results are obtained in an encrypted form.

# Noncryptographic Approaches

- mainly use certain policy-based authorization infrastructure that allows the data objects to have access control policies
  - May use few cryptographic primitives (e.g., hash, digital signatures)
- Data Capture and Auto Identification Reference (DACAR) platform
  - deal with the issues of security, integrity, confidentiality, and integration of various health services
  - the private cloud for data storage and the hybrid cloud for hosting the services.
  - **SOA for integration**

A service refers to a course-grained, discoverable software entity that exists as a single instance and interacts with applications and other services through a loosely coupled, message-based communication model .

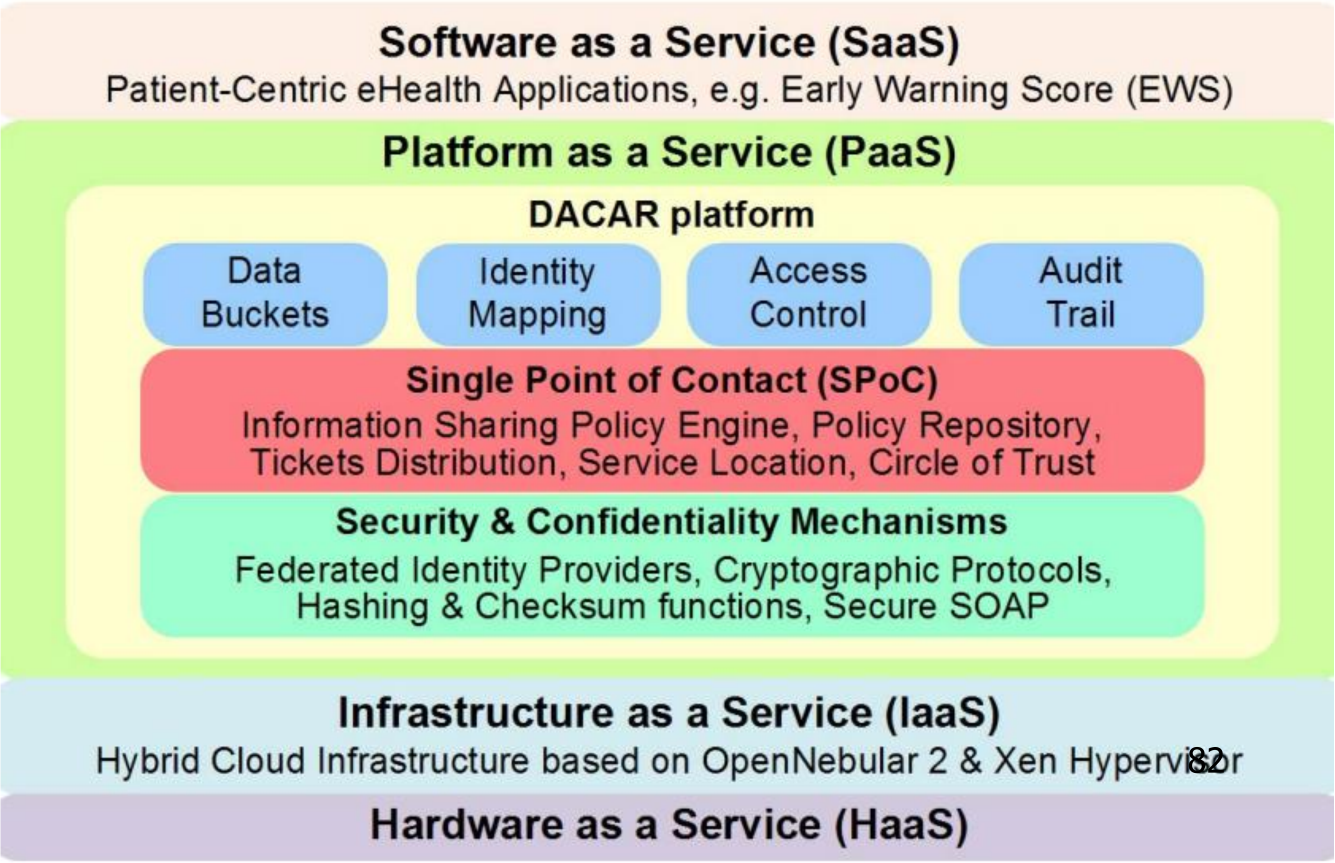
SOA captures many of the best practices of previous soft- ware architectures, including abstraction, autonomy, testability, loose coupling, reusability and statelessness.

# Noncryptographic Approaches

DACAR Platform includes:

- Authorization
- Audit Trail
- Data persistence

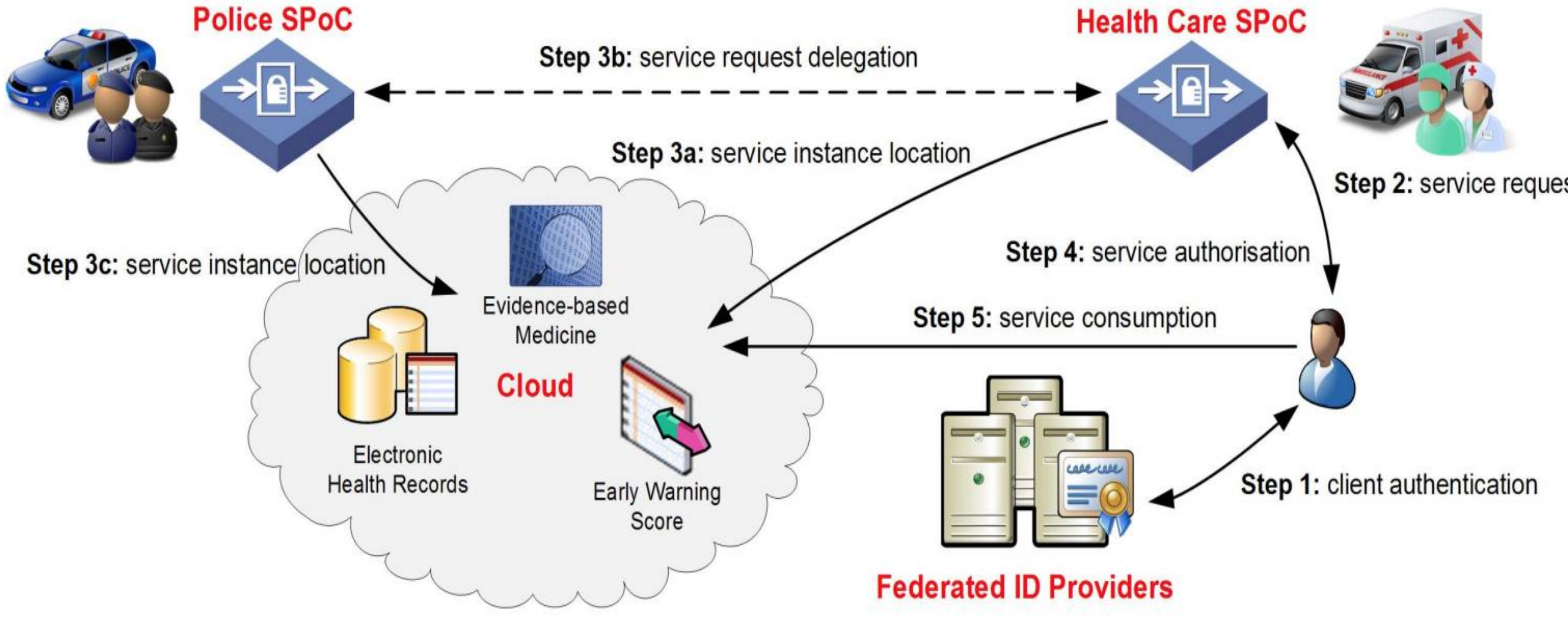
- Authentication
- Data Integrity
- Data Confidentiality



Software as a Service (SaaS)
Patient-Centric eHealth Applications, e.g. Early Warning Score (EWS)
Platform as a Service (PaaS)
DACAR platform
Data Buckets
Identity Mapping
Access Control
Audit Trail
Single Point of Contact (SPoC)
Information Sharing Policy Engine, Policy Repository, Tickets Distribution, Service Location, Circle of Trust
Security & Confidentiality Mechanisms
Federated Identity Providers, Cryptographic Protocols, Hashing & Checksum functions, Secure SOAP
Infrastructure as a Service (IaaS)
Hybrid Cloud Infrastructure based on OpenNebular 2 & Xen Hypervisor
Hardware as a Service (HaaS)

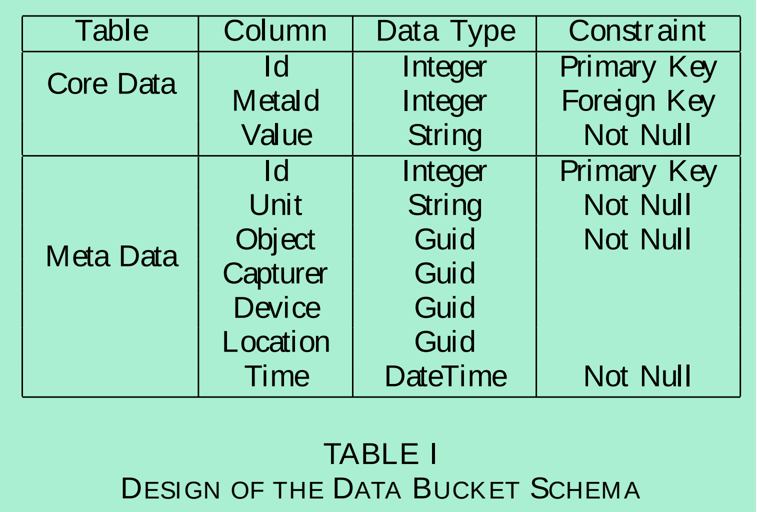
# DACAR workflow

- Data Capture and Auto Identification Reference (DACAR) platform
  - To integrate different health services, the DACAR uses Service Oriented Architecture (SoA).


Police SPoC
Health Care SPoC
Step 3b: service request delegation
Step 3a: service instance location
Step 2: service reques
Step 3c: service instance location
Step 4: service authorisation
Step 5: service consumption
Evidence-based Medicine
Cloud
Electronic Health Records
Early Warning Score
Step 1: client authentication
Federated ID Providers

# Other design aspects

- Data Capture
  - RFID/Mobile devices
- Data Storage
  - Attributes in an automatic format; data bucket
- Data sharing
  - Info sharing policy



| Table | Column | Data Type | Constraint |
|---|---|---|---|
| Core Data | Id | Integer | Primary Key |
| | MetaId | Integer | Foreign Key |
| | Value | String | Not Null |
| Meta Data | Id | Integer | Primary Key |
| | Unit | String | Not Null |
| | Object | Guid | Not Null |
| | Capturer | Guid | |
| | Device | Guid | |
| | Location | Guid | |
| | Time | DateTime | Not Null |

TABLE I
DESIGN OF THE DATA BUCKET SCHEMA

# Reading List

- Security Models and Requirements for Healthcare Application Clouds; Rui Zhang and Ling Liu. College of Computing, Georgia Institute of Technology, Atlanta, GA, USA,
- H. Takabi, J. Joshi, G-J Ahn, “Security and Privacy Challenges in Cloud Computing Environments” IEEE Security and Privacy, 2010
- NIST 800-144, “Guidelines on Security and Privacy in Public Cloud Computing”
- Vivek Kundra, “Federal Cloud Computing Strategy,” 2011
- Ernst&Young Report:”Cloud Computing Issues and Impacts”
- COSO report, “Enterprise Risk Management for Cloud Computing,” 2012
- Peter Mell’s NIST presentation: Effectively and Securely Using the Cloud Computing Paradigm