CSE 465
Information Assurance

Information Assurance in Service-based and Cloud Systems

Professor Stephen S. Yau

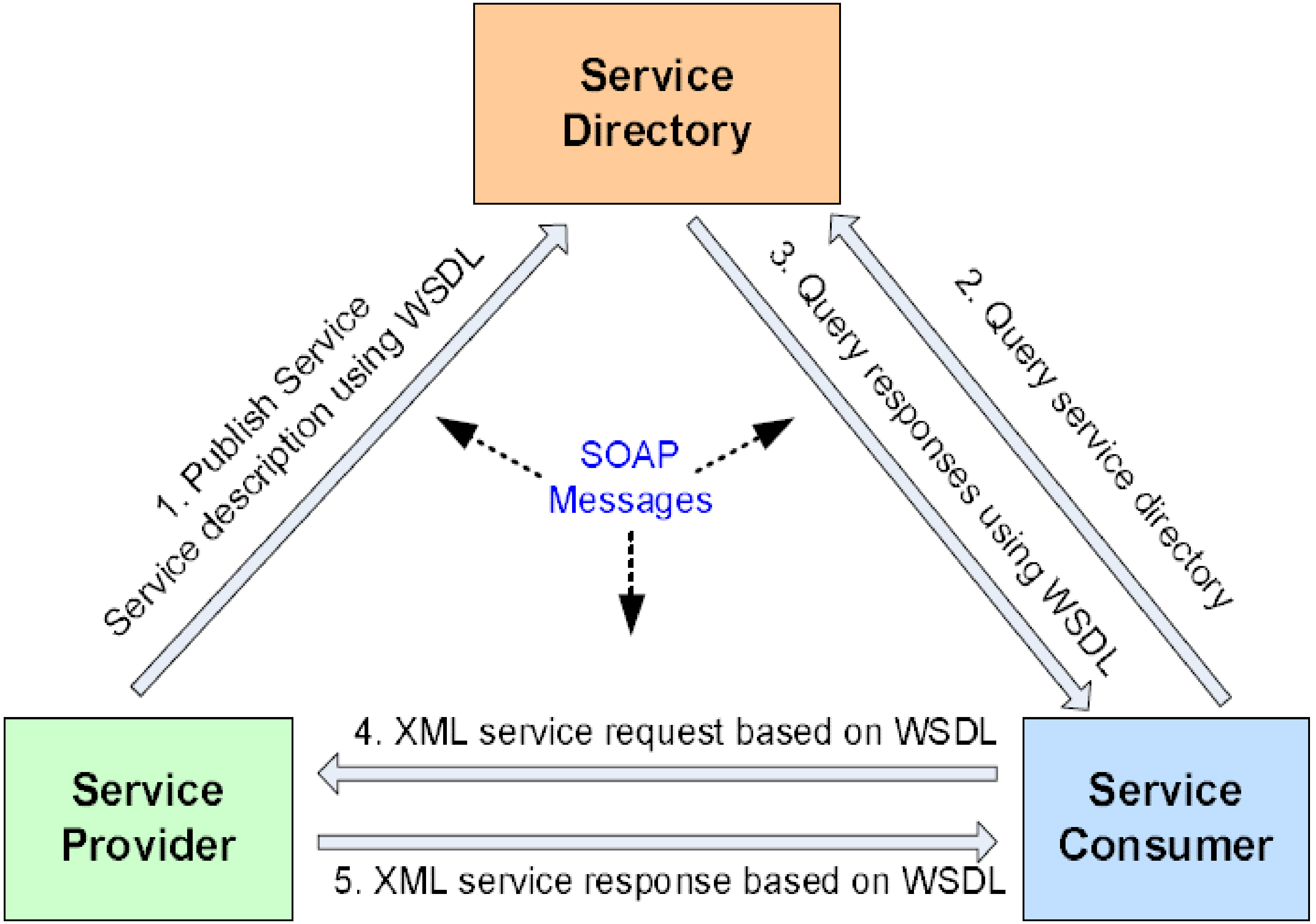
Concept of Service-based Computing

- A ***service*** is a software/hardware entity with well-defined ***standard interfaces*** to provide certain functions over the networks.
  - Services are ***self-contained, stateless, and platform-independent.*** A service accepts one or more requests and returns one or more responses through standard interfaces.
  - Services may be managed and governed by ***different organizations*** with different policies.
  - Services from various organizations and locations ***can be composed*** together to provide an integrated application.
  - Interoperability between web services is achieved by use of common standard protocols.
  - Web service is currently one of most prevalent forms of service

Concept of Service-based Computing (cont.)

- A ***service-based system*** is a software system developed by ***composition and coordination*** of individual services available over network.
  - Individual services can reside on a single host server or be spread across the network on multiple servers.
  - Interactions between these individual services are governed by contracts, called ***Service Level Agreements (SLA)***.
  - SLA specifies ***QoS requirements*** including security requirements that the service providers have to meet.

Service Oriented Architecture


Service Directory
1. Publish Service
Service description using WSDL
2. Query service directory
3. Query responses using WSDL
SOAP Messages
4. XML service request based on WSDL
5. XML service response based on WSDL
Service Provider
Service Consumer

Characteristics of Service-based Systems

- ***Loose coupling*** – No dependencies among individual services.
- ***Service contract*** – Services interact with each other by establishing ***SLA*** , which describes each service and defines the terms of communications.
- ***Abstraction*** – Beyond what is described in SLA, services hide logic from the outside world.
- ***Autonomy*** – Services have control over the logic they encapsulate.

Characteristics of Service-based Systems (cont.)

- ***Reusability*** – Services are designed to support potential reuse.
- ***Composability*** – Services may compose other services. Collections of services can be coordinated and assembled to form composite services.
- ***Statelessness*** – Services do not maintain state information specific to an activity (service request) in order to remain loosely-coupled.
- ***Discoverability*** – Services allow their descriptions to be discovered and understood by service users via available discovery mechanisms.

Concept of Cloud Computing

- Derived from ***service-based computing and resource virtualization technologies***.
- Massively scalable computing capabilities are provided ‘**as a service**’ to multiple customers simultaneously
- IT resources across the Internet are ***dynamically configured and virtualized***
- IT as an ***on-demand*** service

Characteristics of Cloud Systems

- ***On-demand service***
- ***Automation***: Service requests automatically processed
- ***Broad network access***: Computing capabilities are available over networks and accessed through standard protocols at any time and anywhere
- ***Usage accounting***:
- ***Heterogeneity***: Computing capabilities can be used by heterogeneous client platforms/devices

Characteristics of Cloud Systems (cont.)

- ***Resource pooling***: Providers' computing resources are pooled and dynamically allocated to various tasks to increase resource utilization. For the consumer, capabilities and resources often appear unlimited and can be purchased any time with any quantity.
- ***Agility***: Computing capabilities rapidly and elastically provided according to demands.
- ***Usability***: Services are highly virtualized and abstracted so that complexity concealed from users

Mobile Cloud Systems

- Emerging as cloud computing infrastructure with ***mobile devices*** primarily for ***assessing information and receiving results***
  - Applications involving ***use of mobile devices***, including handset centric and network related features, such as GPS, cell-based location information
- Providing ***ubiquity***, and improving ***availability***

Major Benefits of Service-based and Cloud Systems

- Reduce system and application ***development cost***
- Shorter ***development and deployment time*** (rapid development of large scale distributed systems)
- Reduce infrastructure *maintenance cost*
- Easy access to latest innovations
- Facilitate joining ***community*** of interest (social networking)

Major Benefits of Service and Cloud Computing (cont.)

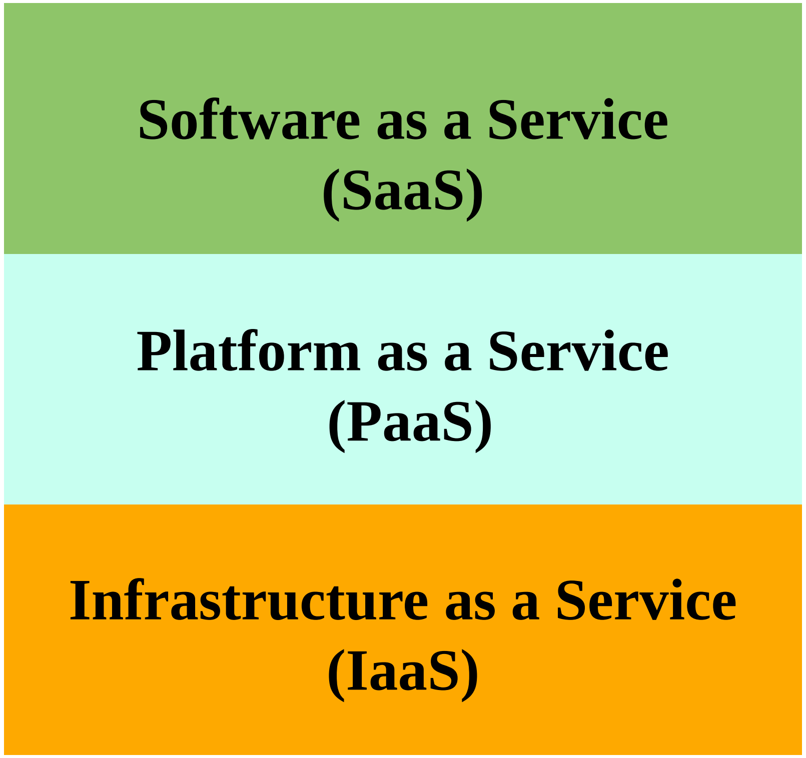
- Larger ***scalability*** (quantity, size and variety)
- More ***powerful computation capability***
- ***Transfer*** more management and operational ***risks to service providers***
- Higher ***mobility*** – access clouds any time, anywhere and by any devices
- ***Expand collaborative activities and applications***

Expanding Application Domains

- ***E-commerce***
- Supply chain
- Banking
- Marketing
- Health care
- ***Telecommunications***
- Transportation
- Aerospace
- Entertainment
- Education
- Research and development
- Collaborative work
- Government services
- Homeland security
- ***Military***
- ***Social networks***
- …..

Cloud Service Layers

- **SaaS** – Software as a Service
  - Networked-hosted applications
- **PaaS**– Platform as a Service
  - Network-hosted platform
- **IaaS** – Infrastructure as a Service
  - Computing, storage and network resources to host platforms

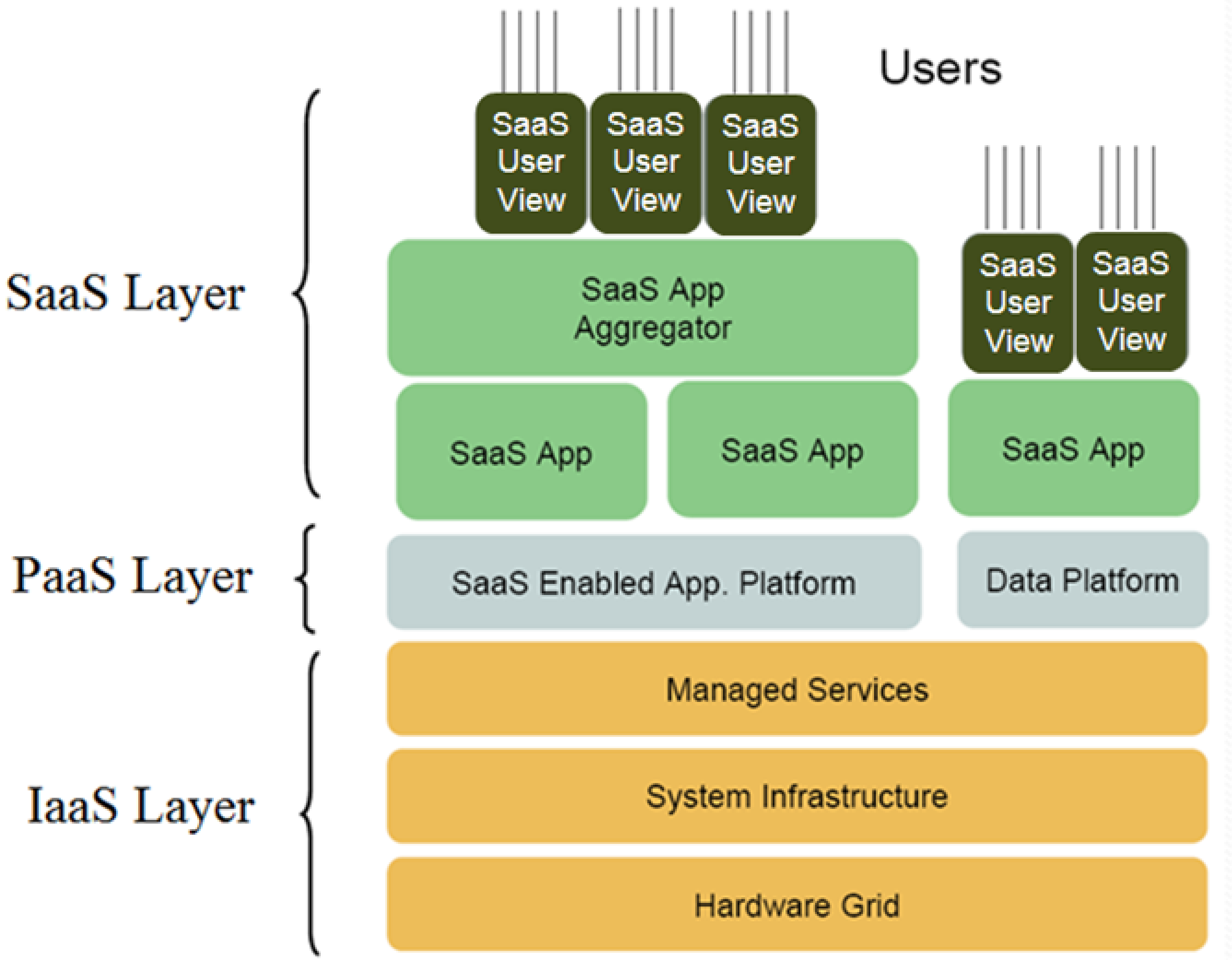


Software as a Service (SaaS)

Platform as a Service (PaaS)

Infrastructure as a Service (IaaS)

Cloud Computing Layers (cont.)



SaaS Layer

- A model of software application, whereby a service provider licenses an application to customers for use as ***a service on demand***
- Network-based access to, and management of, ***commercially available software***
- Activities managed from central locations rather than at each customer's site, enabling customers to ***access applications remotely via the web***
- Centralized feature ***updating***, which obviates the need for end-users to download patches and upgrades.

SaaS Layer (cont.)

- SaaS ***user's views*** (functional, non-functional descriptions and user interfaces) are available for users for purchasing.
- Multiple software services can be aggregated to a workflow dynamically in runtime (***dynamic service composition***).
- The number of service-requests for each workflow, QoS requirements, priorities of workflows, and available system resource as well as various relevant environmental attributes can be ***dynamically changing***

PaaS Layer

- With PaaS, software service developers can build web applications without installing any tools on their computers and deploy those applications without any specialized system administration skills.

IaaS Layer

- A cloud service layer in which an organization outsources the equipment used to support its operations, including process, storage, communication, hardware, servers and networking components.
- System resources are dynamically virtualized and scalable.
- The infrastructure service provider owns the equipment and is responsible for its infrastructure management - housing, operating, maintaining, and updating

Cloud Deployment Models

- ***Private cloud***
  - Infrastructure owned and managed by one organization
  - Infrastructure located within one organization
  - Only accessible and consumed by users within one organization (trusted users)
  - Pros
    - Full control over the cloud
    - Simpler security and trust management
    - Can be customized for the organization's security policies
  - Cons
    - Limited capability and capacity
    - Higher cost for operations and maintenance

Cloud Deployment Models *(cont.)*

- ***Community cloud***
  - Infrastructure owned and managed by the community
  - Infrastructure located within the boundary of the community
  - Must have agreements/contracts among the organizations of the community
  - Only accessible and consumed by the users within the organizations of the community (trusted users)
  - Pros
    - Full control over the cloud by the community
    - Simpler security and trust management
    - Larger capacity and more capability than the private cloud
    - Less cost for operations and maintenance than the private cloud
  - Cons
    - Conflicts among organizations' security policies may cause problems
    - Capability and capacity are still quite limited

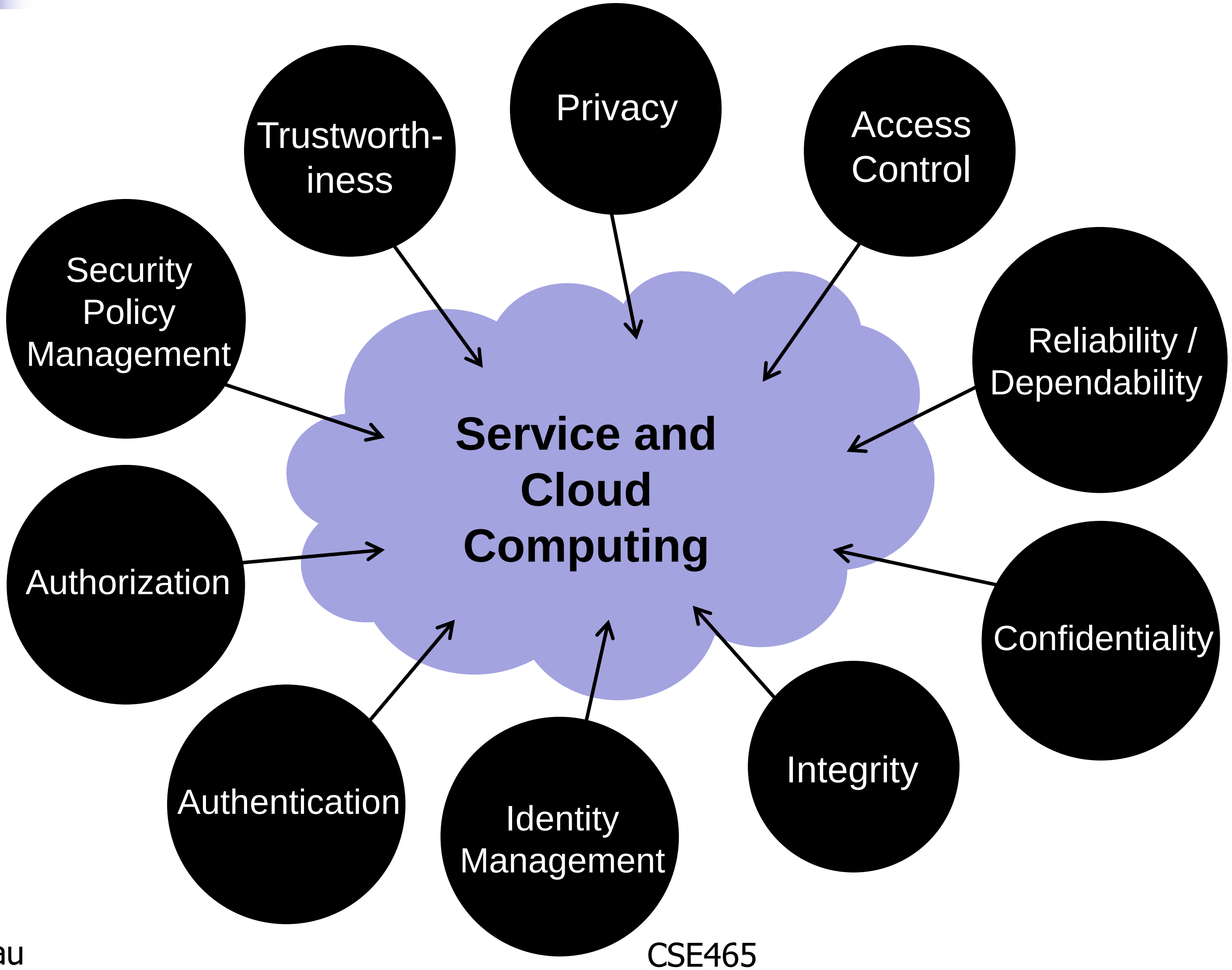
Cloud Deployment Models *(cont.)*

- ***Public cloud***
  - Infrastructure owned and managed by third-party provider
  - Infrastructure located at third-party provider’s site
  - Open to the public and accessible by untrusted users
  - Pros
    - Users need not be concerned with the operations and maintenance
    - Very large capability and capacity
  - Cons
    - No control over the cloud system
    - More difficult for security and trust management
    - Difficult to customize the cloud service for the organization’s security policies
    - Data confidentiality and privacy are not protected.

Cloud Deployment Models *(cont.)*

- ***Hybrid cloud***
  - Infrastructure owned and managed by both multiple user organizations and third-party providers
  - Infrastructure located at the sites of both multiple user organizations and third-party provider
  - Users are both trusted and untrusted
  - Pros
    - Can take advantages from each of the deployment models
  - Cons
    - Complex architecture

Security Challenges of Services and Cloud Computing



Security Specification Standards for SOA

- Organization for the Advancement of Structured Information Standards (**OASIS**) (https://www.oasis-open.org/
- World Wide Web Consortium (**W3C**) (http://www.w3.org/)

Established a list of security specification standards for implementing security mechanisms in Service Oriented Architecture (**SOA**).

Confidentiality and Privacy Protection in Cloud Systems

- **Challenges**
  - Who has access to my sensitive data?
  - How can we assure the service providers do not collect/abuse my sensitive data?
  - How can we assure that service providers provide proper protections on my sensitive data against outside attackers?
- **Research topics**
  - User-centric identity management and access control
  - Trustworthy computing: Trust management in cloud
  - Data encryption and obfuscation
  - Privacy-preserving data mining
  - Anonymous computing

Integrity Protection in Cloud Systems

- **Challenges**
  - Who else is running on these same machines?
  - How can we assure there isn’t data mixing?
  - How is my data be backed up? How often? Where is it stored?
  - What is the recovery model? Who has that access?
- **Research topics**
  - Dynamic auditing
  - Efficient data backup and recovery planning
  - Virtual machine isolation
  - Integrity verification of outsourced storages in clouds

Security Policy Establishment and Enforcement in Cloud Systems

- **Challenges**
  - How to specify security policies?
  - How to ensure the completeness and consistency of the policies?
  - Is there efficient policy enforcement mechanisms?
- **Research topics**
  - Dynamic establishment and enforcement of service level agreement (SLA) between service providers and consumers
  - Security policy specification
  - Security policy conflict detection and resolution

QoS Assurance in Cloud Systems

- **Challenges**
  - How to ensure QoS, such as performance, timeliness, throughput?
  - How will service providers manage system resources to satisfy dynamically changing consumers' requirements?
  - How to address tradeoffs among various QoS?
- **Research topics**
  - QoS requirement specification
  - Dynamic resource allocation
  - Efficient trade-off techniques for multiple QoS aspects
  - System design for QoS monitoring and adaptation

Preventing Abuse of Cloud Systems by Cyber Attackers

- **Challenges**
  - Attackers may purchase huge amount of computing and network capacity anytime for various malicious activities, such as cracking passwords or encryption keys, sending out spam mails, distributing viruses and worms, creating botnets, launching DDOS attacks, and hosting phishing websites
- **Research topics**
  - Monitoring, detecting and preventing users' malicious activities in cloud computing systems
  - Comprehensive introspection of users' network traffics
  - User identity validation
  - Security auditing and computer

References

- Article on security of cloud computing: http://technet.microsoft.com/en-us/magazine/hh641415.aspx
- Article on cloud computing security by Gartner: http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853
- "The NIST Definition of Cloud Computing". National Institute of Standards and Technology. Retrieved 24 July 2011.
- Voorsluys, William; Broberg, James; Buyya, Rajkumar (February 2011). "*Cloud Computing: Principles and Paradigms*" ISBN 978-0-470-88799-8.
- "Securing the Cloud", by Vic Winkler, ISBN 978-1-59749-592-9
- S. S. Yau, Y. Yao, A. Buduru, "An Adaptable Distributed Trust Management Framework for Large-scale Secure Service-based Systems", *Computing Journal*, *Springer*, October 2013