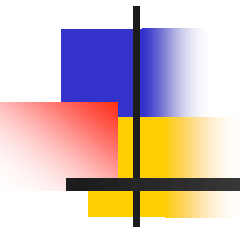
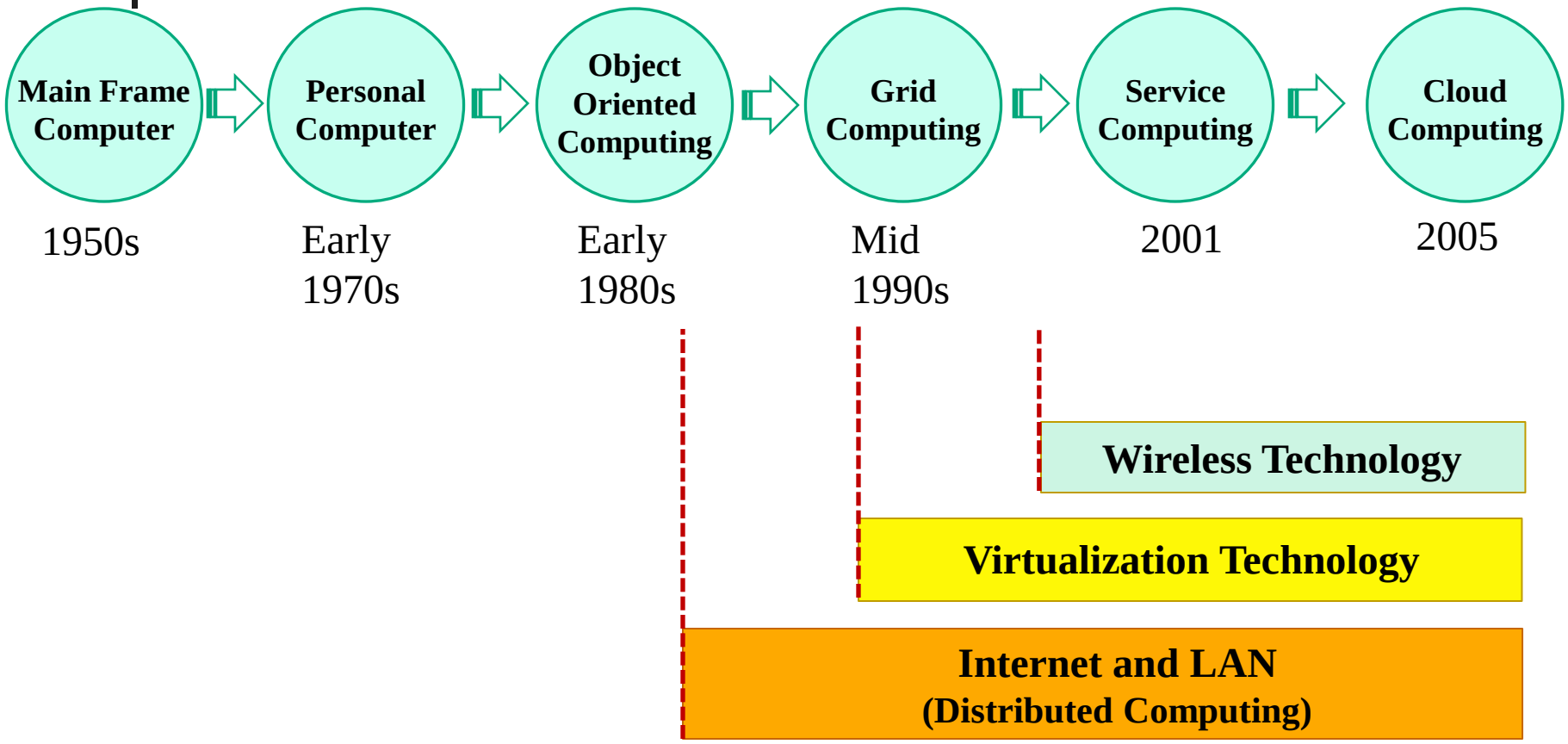


Information Assurance in Cloud Computing Systems

Professor Stephen S. Yau

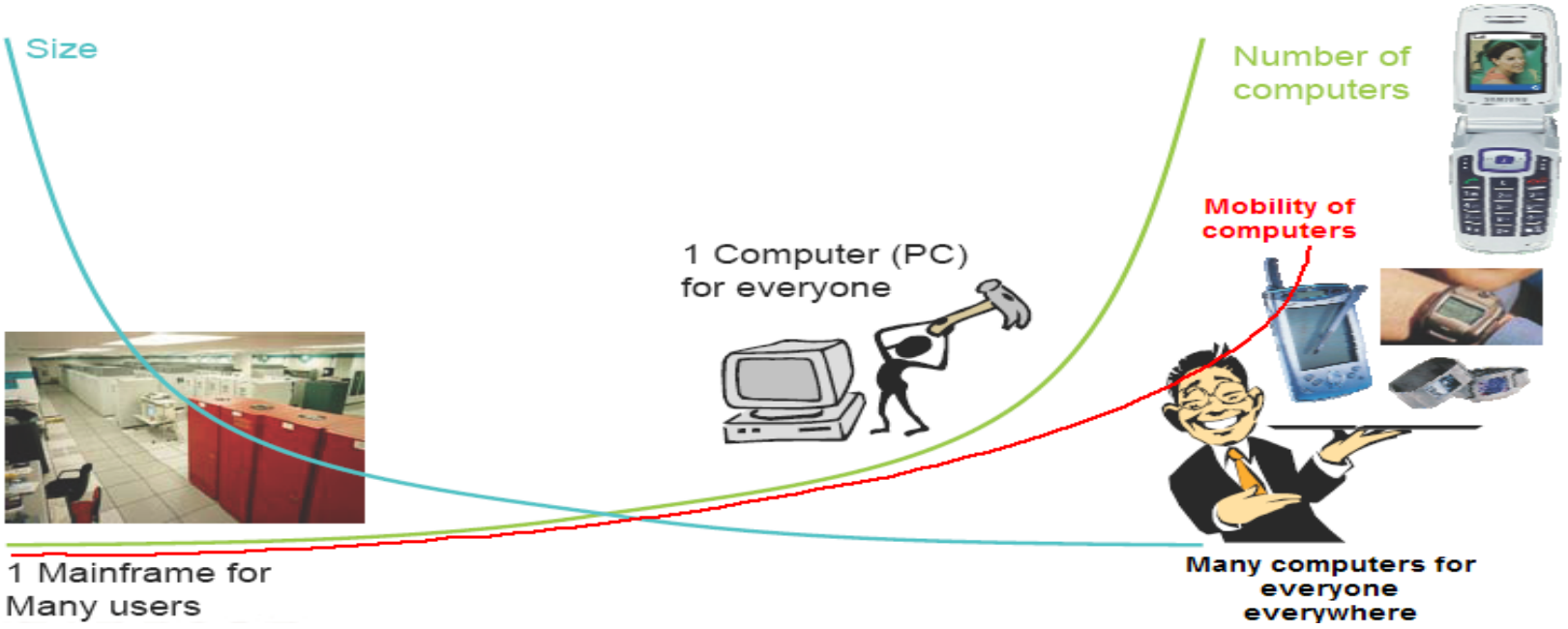
Evolution of Computing Paradigms



Major New Computing Paradigms

- Ubiquitous Computing

- Ubiquitous computing
  - Computing anywhere, anytime
  - Ad hoc wireless connectivity
  - Mobility, efficiency, context/situation awareness



Major New Computing Paradigms (cont.)
- Service-oriented Computing

- Service-oriented computing
  - Abstraction of functional units as software services with discoverable and interoperable interfaces, which can be described using common standards, such as WSDL
  - Major characteristics: loosely-coupling, late-binding, autonomy, composability
  - Realize workflows (business processes) by service composition

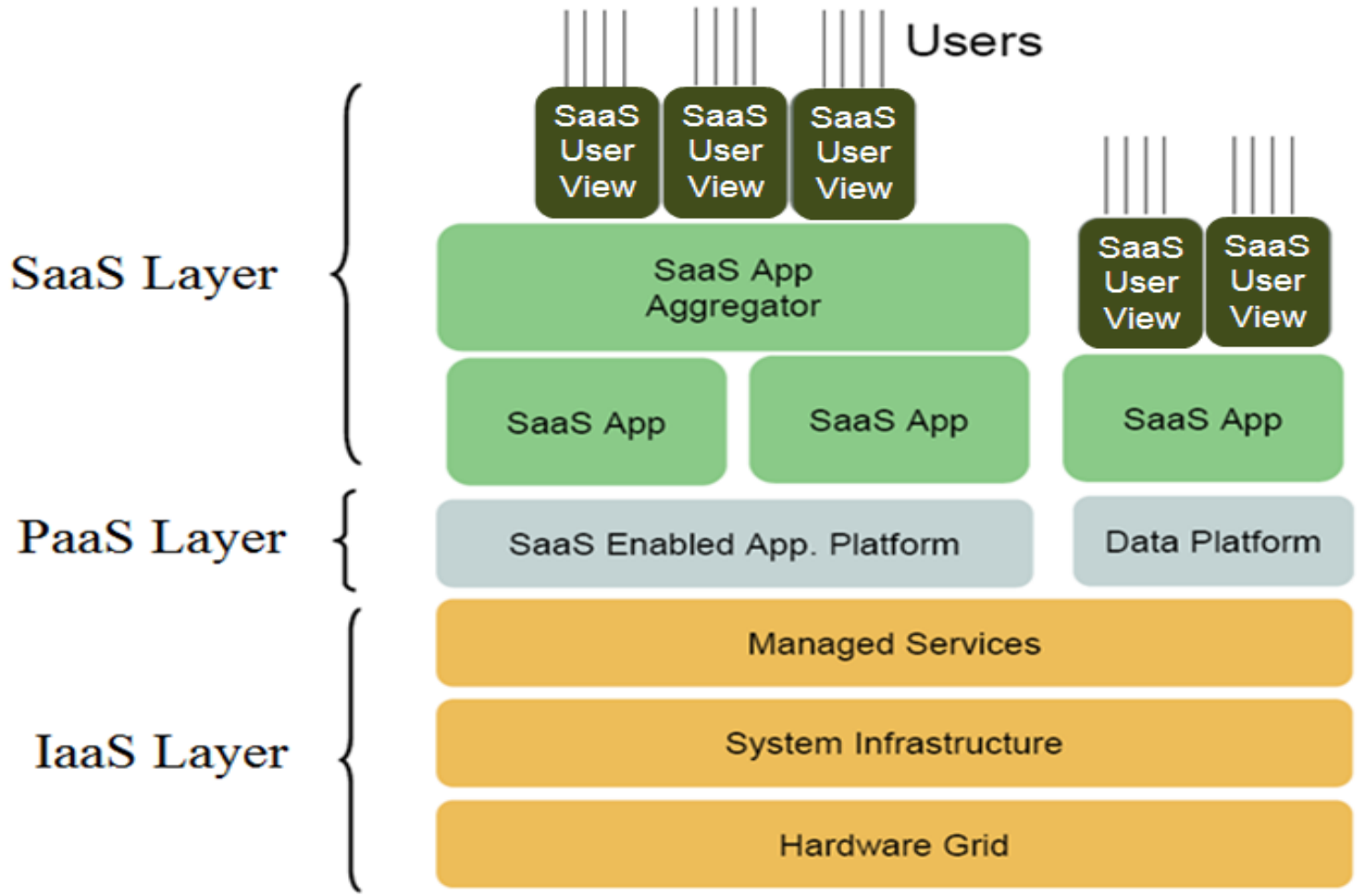
Cloud Computing

- Derived from ***service computing*** and ***resource virtualization*** technologies (including ***Internet***)
- ***Massively scalable computing capabilities*** provided '***as a service***' to multiple customers simultaneously
- IT resources across the Internet are ***dynamically configured and virtualized***
- IT as an ***on-demand*** service
- ***Private, public and hybrid*** cloud systems

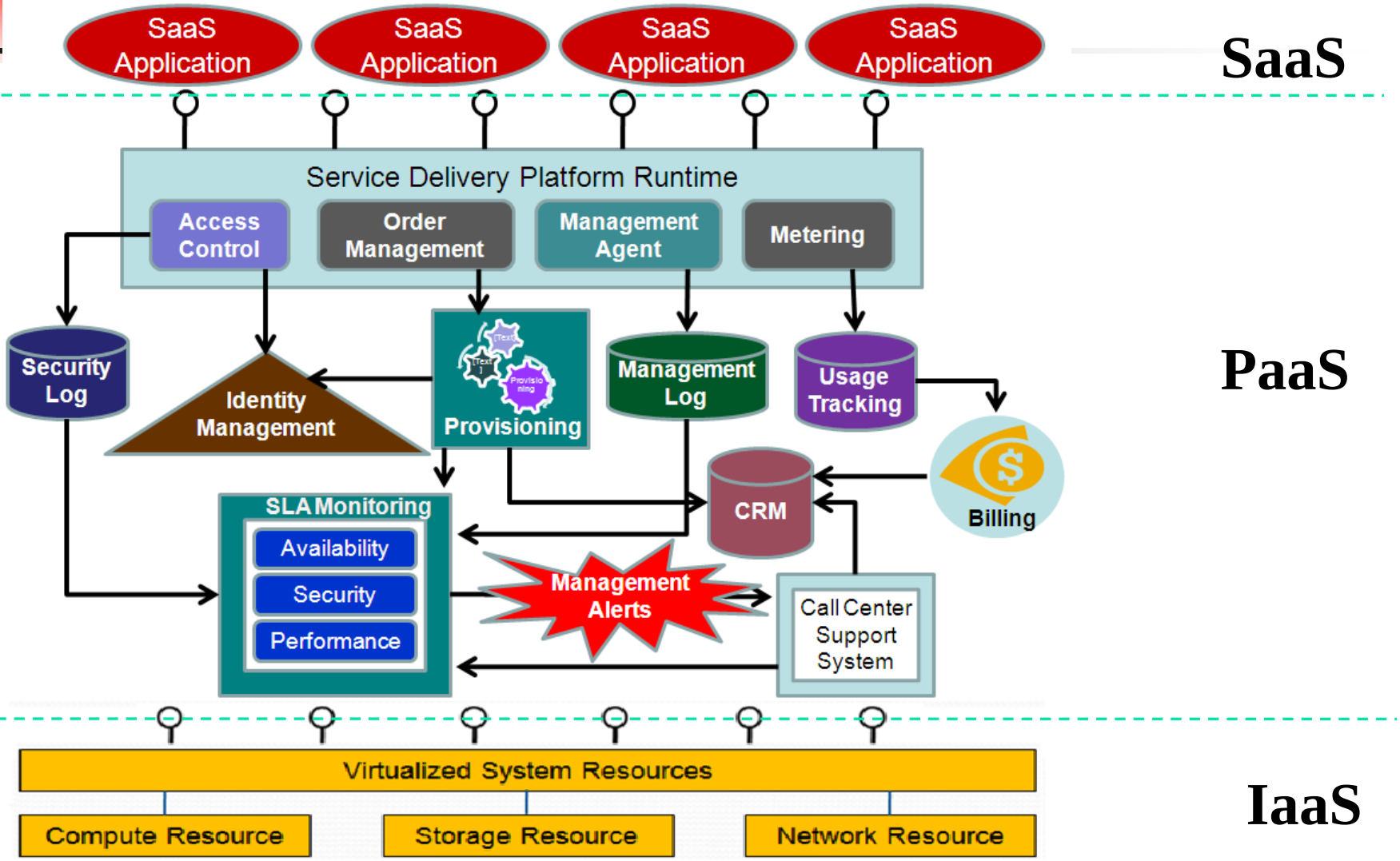
Major Characteristics of Cloud Computing

- Resource pooling
- Heterogeneity
- Broad network access
- Agility
- Usability
- On-demand service
- Usage accounting
- Automation

Cloud Computing Paradigms (cont.)



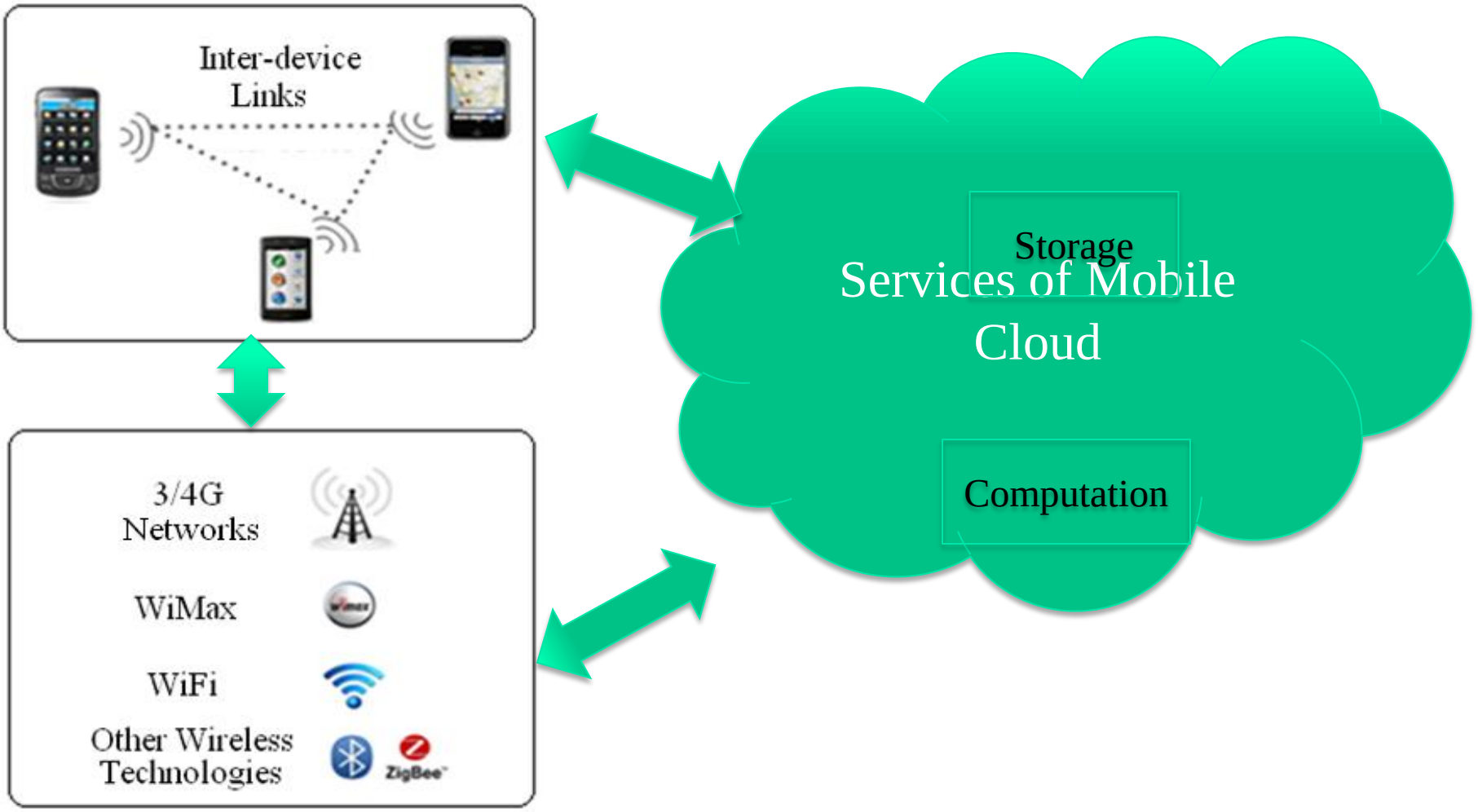
Cloud Computing System Architecture



Mobile Cloud Computing

- Emerging and considered as a cloud computing infrastructure, where ***data*** and ***processing*** occur outside mobile devices
  - enabling new types of applications involving use of mobile devices, including handset centric features and network related features, such as GPS and/or cell-based location information.

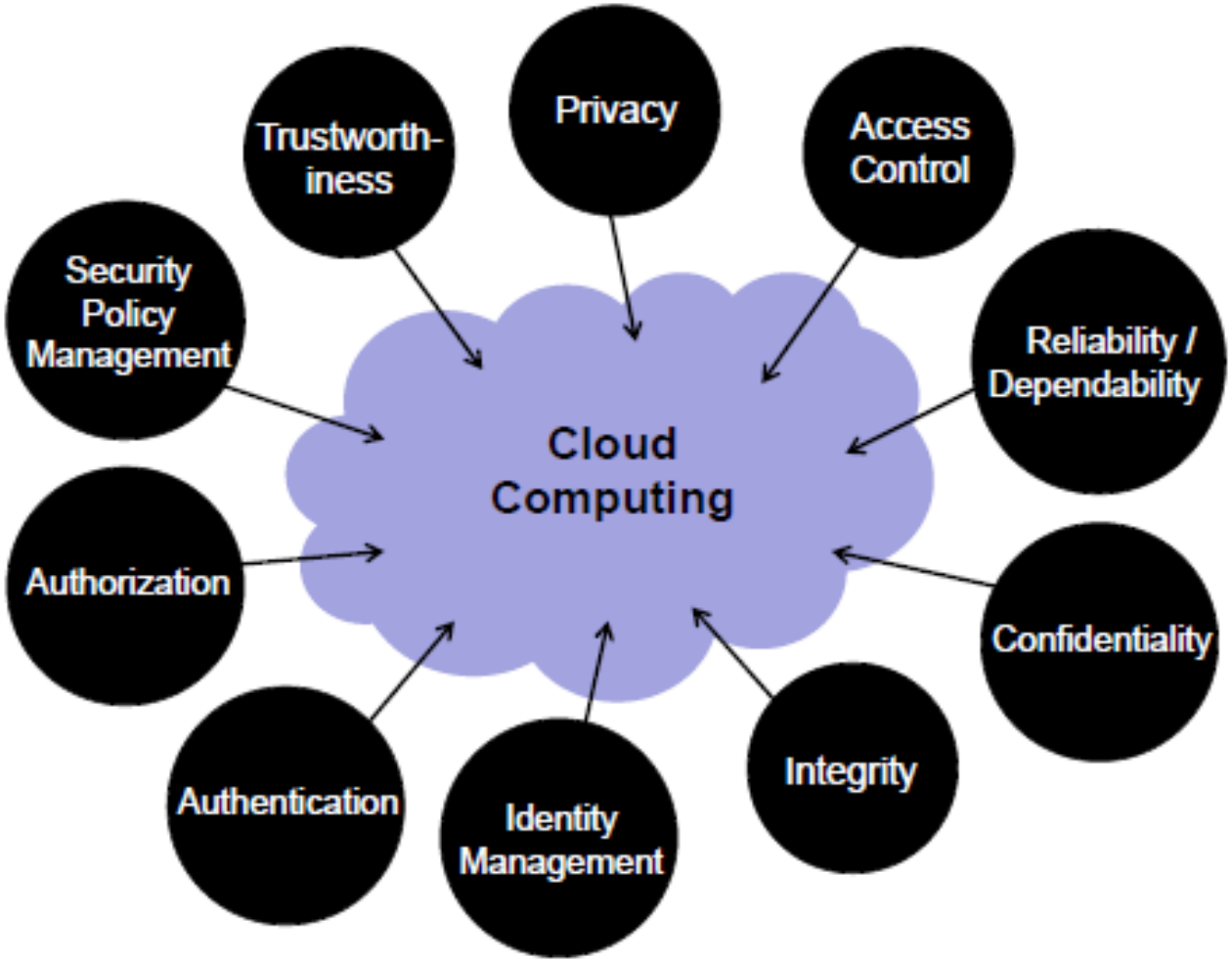
Mobile Cloud Computing Model



Concerns of Cloud and Mobile Cloud Users

- Most cloud users are concerned with ***leakage of their sensitive data*** in the cloud because their data is processed and stored on machines owned and operated by various service providers, not controlled by users.
- Due to the severe limitation of resources available in mobile devices and characteristics of mobile cloud computing, the ***security*** issues for mobile cloud computing are ***more severe***.

Challenges: IA in Cloud Computing



Challenges: IA in Cloud Computing (cont.)

- How to protect ***confidentiality and privacy*** of users' sensitive data ***from service providers***?
  - ***Who*** have access to my data?
  - How can we be sure that the ***service providers*** do not abuse our sensitive data?
  - How can we be sure that ***service providers*** provide proper protections on our sensitive data against attackers?

Challenges: IA in Cloud Computing (cont.)

- How to protect ***integrity of users' data*** within cloud?
  - ***Who*** are running applications on these same machines?
  - How can we be sure that there is ***no data mixing***?
  - What are ***data backed up policies and mechanisms***? How often? Where is the back up stored?
  - Is the ***recovery process*** effective?
- How to ensure that ***service providers*** will ***comply with security policies***?
  - How to specify ***security policies***?
  - Are there ***effective policy enforcement mechanisms***?
  - How to protect ***intellectual property rights*** of service users?

Challenges: IA in Cloud Computing

- How to ensure the ***availability and reliability*** of each ***third-party service***?
  - Are service providers' data centers safe from natural disasters?
  - Are the services always ***available on demand***?
  - Are the services always ***functioning properly***?
  - Will the services work properly ***under stress conditions***?
  - Are the services ***resilient to failures***?
  - Are the services vulnerable to various ***cyber attacks, viruses and worms***?

Challenges: IA in Cloud Computing (cont.)

- How to support ***QoS adaptation*** in dynamic situation of the cloud?
  - How to ***adapt SLAs*** between service providers and consumers ***dynamically***, including ***trade-offs*** among multiple QoS factors and multiple consumers?
  - How to ensure the service providers can satisfy ***multiple QoS factors***, such as security, performance, timeliness, throughput, and reliability, for ***multiple consumers simultaneously and dynamically***?

Challenges: IA in Mobile Cloud Computing

- How to improve ***authentication and authorization*** of mobile devices in mobile cloud?
  - What kinds of ***information can be collected*** by mobile devices?
  - How the information can ***prevent attackers from successfully attacking*** the mobile cloud after its mobile devices are lost or stolen?
  - What ***effective mechanisms*** are needed for authentication and authorization of mobile devices in mobile cloud?

Challenges: IA in Mobile Cloud Computing (cont.)

- How to improve ***network security,*** including mobile networks?
  - Which ***interfaces*** have the potential to expose sensitive information and possibly receive malicious data?
  - How service providers and users can interact in a ***trusted and secure network***?
  - What are ***the security requirements*** for monitoring and checking of the trusted and secure networks of mobile cloud?
  - What are the requirements for establishing ***secure routing and connections*** in mobile cloud?

Challenges: IA in Cloud Computing (cont.)

- How to avoid ***threat of malwares*** in cloud computing, especially in mobile cloud?
  - How to avoid the malware ***injected in mobile cloud, especially via lost or stolen mobile devices***?
  - How to avoid leveraging ***social networks*** to deliver malwares?
  - How to avoid ***data leakage***?
  - How to avoid ***backdoor*** triggered via SMS?
  - How to avoid ***account privilege escalated*** to root?

Current State of Art: IA in Cloud Computing

- Protection of ***confidentiality and privacy*** of users' sensitive data from service providers
  - User-centric identity management and access control
  - Trustworthy computing: Trust management in cloud
  - Data encryption and obfuscation
  - Privacy-preserving data mining
  - Anonymous computing

Current State of Art: IA in Cloud Computing (cont.)

- Protection of ***integrity of*** cloud
  - Dynamic auditing
  - Efficient backup and recovery planning
  - Virtual machine isolation
  - Integrity verification in the cloud
- Assurance that service providers will ***comply with security policies***
  - Dynamic establishment and enforcement of SLA between service providers and consumers
  - Security policy specification
  - Security policy conflict detection and resolution

Current State of Art: IA in Cloud Computing (cont.)

- Assurance of ***availability and reliability*** of third party services
  - Critical infrastructure protection: Intrusion detection, cyber attack prevention, analyzing and defeating malware, worms and viruses
  - Cyber situational awareness
  - Automated efficient risk management: risk identification, assessment and mitigation
  - Data backups and contingency plans
  - Fault/error tolerant computing
  - High availability through virtual machine live migration

Current State of Art: IA in Cloud Computing (cont.)

- Support for ***QoS adaptation*** in cloud computing
  - QoS requirement specification for dynamic situation
  - Dynamic resource allocation to support situation changes and dynamic users' requirements
  - Efficient trade-off techniques for multiple QoS factors and multiple consumers

Current State of Art: IA in Mobile Cloud Computing

- Improve ***authentication and authorization for*** mobile cloud
  - Location-based authentication and authorization
  - Policy-based authorization
  - Biometrics: notably keystroke dynamics and typing patterns

Current State of Art: IA in Mobile Cloud Computing (cont.)

- Improve ***mobile network security***.
  - Virtualization
    - Virtual network construction, backup and recovery in mobile network environments
    - Monitoring of hypervisors
  - Light weight encryption and obfuscation
- Reduce ***threat of malware*** in mobile cloud
  - Monitoring and auditing the use of mobile devices
  - Location-based access control
  - Host-based mobile malware detection

Future Research on IA in Cloud Computing

- Many research issues on IA in cloud computing still need to be addressed
- Security of mobile cloud is more severe
  - Mobile devices are easy to lose or stolen
  - More easily compromised
    - More interfaces with various networks
    - More limited resources available
    - Limited anti-virus software
    - …..