Security, Privacy, and Data Protection for Trusted Cloud Computing

Prof. Kai Hwang, University of Southern California
Keynote Address, International Conference on Cloud Computing (CloudCom2010)
Indianapolis, Indiana  Dec.3,  2010

- Cloud Platforms over Datacenters
- Cloud Infrastructure and Services
- Reputation-based Trust Management
- Data Coloring and Software Watermarking
- Cloud Support of The Internet of Things
Handy Tools We Use over the Evolutional Periods In History

Is it safe to play with your computer, when you are naked and vulnerable?
Top 10 Technologies for 2010

**Top 10 Strategic Technology Areas for 2009**

1. Virtualization
2. Business Intelligence
3. Cloud Computing
4. Green IT
5. Unified Communications
6. Social Software and Social Networking
7. Web-Oriented Architecture
8. Enterprise Mashups
9. Specialized Systems
10. Servers — Beyond Blades

**Top 10 Strategic Technology Areas for 2010**

1. Cloud Computing
2. Advanced Analytics
3. Client Computing
4. IT for Green
5. Reshaping the Data Center
6. Social Computing
7. Security — Activity Monitoring
8. Flash Memory
9. Virtualization for Availability
10. Mobile Applications

(Modified for 2010) (New for 2010) (Dropped for 2010)
Web 2.0, Clouds, and Internet of Things

HPC: High-Performance Computing
HTC: High-Throughput Computing
P2P: Peer to Peer
MPP: Massively Parallel Processors

Cloud Computing as A Service

The Internet

Public clouds (over Internet)

Hybrid clouds (over Internet/Intranets)

Private clouds (over Intranets)

Provisioning of both physical and virtualized cloud resources

Application layer (SaaS)

Platform layer (PaaS)

Infrastructure layer (IaaS, HaaS, DaaS, etc.)
Amazon Virtual Private Cloud VPC
(http://aws.amazon.com/vpc/)
vSphere 4: An OS for Cloud Platform

- Self-service data center
- Test/development
- Disaster recovery
- Security and policy enforcement
- Optimized resource management (e.g. power)
- Automated app management
Marc Benioff, Founder of Salesforce.com

1986 graduated from USC
1999 started salesforce.com
2003-05 appointed chairman of US Presidential IT Advisory Committee
2009 announced Force.com platform for cloud business computing

A SaaS and PaaS Cloud Provider

Dec. 3, 2010

Kai Hwang, USC
Security and Trust Crisis in Cloud Computing

- Protecting datacenters must first secure cloud resources and uphold user privacy and data integrity.

- Trust overlay networks could be applied to build reputation systems for establishing the trust among interactive datacenters.

- A watermarking technique is suggested to protect shared data objects and massively distributed software modules.

- These techniques safeguard user authentication and tighten the data access-control in public clouds.

- The new approach could be more cost-effective than using the traditional encryption and firewalls to secure the clouds.
Trusted Zones for VM Insulation

- Federate identities with public clouds
- Control and isolate VM in the virtual infrastructure
- Segregate and control user access
- Insulate information from other tenants
- Insulate infrastructure from Malware, Trojans and cybercriminals
- Insulate information from cloud providers’ employees
- Strong authentication
- Data loss prevention
- Encryption & key mgmt
- Tokenization
- Cybercrime intelligence
- Anti-malware
- Strong authentication
- Data loss prevention
- Encryption & key mgmt
- Tokenization
- Cybercrime intelligence
- Anti-malware

Identity federation
Virtual network security
Access Mgmt
Security Info. & Event Mgmt
Cloud Service Models and Their Security Demands

Cloud computing will not be accepted by common users unless the trust and dependability issues are resolved satisfactorily [1].

Dec. 3, 2010

Kai Hwang, USC
Data Security and Copyright Protection in A Trusted Cloud Platform

Cloud Platform: Provisioning of virtualized compute, storage, network, and devices plus software and datasets from cooperative datacenters to satisfy the demands of many user applications.

Trust Delegation, Reputation Systems, and Data Coloring for Protecting Cloud Resources provisioned from Datacenters

Resource Provisioning, Virtualization, Management, and User Interfaces

Services Catalogs

Security and Performance Monitoring

Source: Reference [3, 4]
## Security Protection Mechanisms for Public Clouds

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Brief Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust delegation and Negotiation</td>
<td>Cross certificates must be used to delegate trust across different PKI domains. Trust negotiation among different CSPs demands resolution of policy conflicts.</td>
</tr>
<tr>
<td>Worm containment and DDoS Defense</td>
<td>Internet worm containment and distributed defense against DDoS attacks are necessary to secure all datacenters and cloud platforms.</td>
</tr>
<tr>
<td>Reputation System Over Resource Sites</td>
<td>Reputation system could be built with P2P technology. One can build a hierarchy of reputation systems from datacenters to distributed file systems.</td>
</tr>
<tr>
<td>Fine-grain access control</td>
<td>This refers to fine-grain access control at the file or object level. This adds up the security protection beyond firewalls and intrusion detection systems.</td>
</tr>
<tr>
<td>Collusive Piracy prevention</td>
<td>Piracy prevention achieved with peer collusion detection and content poisoning techniques.</td>
</tr>
</tbody>
</table>
Trust Management for Protecting Cloud Resources and Safeguard Datacenter Operations [3]

- Alert vulnerable hosts
- Terminate DDoS Attacks
- Penalize Pirates
- Misuse Detection
- Anomaly Detection
- Worm containment
- DDoS defense and Piracy prevention
- Hybrid intrusion detection

Distributed defense against worms, DDoS attacks, and copyright violations

- Defense against Piracy or Network Attacks
- Trust overlay networks over cloud resources sites and datacenters
- Reputation aggregation and integration

Distributed reputation aggregation and probing of piracy colluders

<table>
<thead>
<tr>
<th>User/Server Authentication</th>
<th>Access Authorization</th>
<th>Trust Delegation</th>
<th>Data Integrity Control</th>
</tr>
</thead>
</table>

Trust Integration/Negotiation over distributed cloud resource sites

Source: [4]
PowerTrust: Built over A Trust Overlay Network

Data Coloring via Watermarking

Each drop implies user’s logo information

Forward Coloring

Backward Coloring

Cloud drops
Color Matching To Authenticate Data Owners and Cloud Service Providers
24 Satellites of GPS Deployed in Outerspace
Service-Oriented Cloud of Clouds (Intercloud or Mashup)

Geoffrey Fox: Cloud of clouds -- from Raw Data to Wisdom.

SS = Sensor service, fs = filter services
Supply Chain Management supported by the Internet of Things.

(http://www.igd.com)
Facebook Applications
(550 Millions users registered today)
# Mobility Support and Security Measures for Mobile Cloud Computing

<table>
<thead>
<tr>
<th>Cloud Service Models</th>
<th>Mobility Support and Data Protection Methods</th>
<th>Hardware and Software Measures for Cloud Security</th>
</tr>
</thead>
</table>
| Infrastructure Cloud (The IaaS Model) | - Special air interfaces  
- Mobile API design  
- File/Log access control  
- Data coloring | - Hardware/software root of trust,  
- Provisioning of virtual machines,  
- Software watermarking  
- Host-based firewalls and IDS |
| Platform Cloud (The PaaS Model) | - Wireless PKI,  
- User authentication,  
- Copyright protection  
- Disaster recovery | - Network-based firewalls and IDS  
- Trust overlay network  
- Reputation system  
- OS patch management |

Dec. 3, 2010  
Kai Hwang, USC
**Cloudlets**—A trusted, VM-based, and Resource-Rich Portal for Upgrading Mobile Devices with Cognitive Abilities for Mobile access of the cloud to explore Location-Aware Cloud Applications such as:

- Opportunity Discovery,
- Fast Information Processing,
- and Intelligent Decision Making on The Road, etc.

Conclusions:

- Computing clouds are changing the whole IT, service industry, and global economy. Clearly, cloud computing demands ubiquity, efficiency, security, and trustworthiness.

- Cloud computing has become a common practice in business, government, education, and entertainment leveraging 50 millions of servers globally installed at thousands of datacenters today.

- Private clouds will become widespread in addition to using a few public clouds, that are under heavy competition among Google, MS, Amazon, Intel, EMC, IBM, SGI, VMWare, Salesforce.com, etc.

- Effective trust management, guaranteed security, user privacy, data integrity, mobility support, and copyright protection are crucial to the universal acceptance of cloud as a ubiquitous service.
Cloud Security Responsibilities by Providers and Users

Table 1:

Source: Reference [4]
Cloud Computing – Service Provider Priorities

- Ensure confidentiality, integrity, and availability in a multi-tenant environment.
- Effectively meet the advertised SLA, while optimizing cloud resource utilization.
- Offer tenants capabilities for self-service, and achieve scaling through automation and simplification.
Using Twitter Crowd to Check Weather Conditions in Remote Cities
IOT Telemedicine Applications: Measured Patient Data Transferred to Doctor Using a Wireless Sensor Network.
Opportunities of IOT in 3 Dimensions

- Any TIME connection
  - On the move
  - Outdoors and indoors
    - Night
    - Daytime
- Any PLACE connection
  - On the move
  - Outdoors
  - Indoors (away from the PC)
  - At the PC
- Any THING connection
  - Between PCs
  - Human to Human (H2H), not using a PC
  - Human to Thing (H2T), using generic equipment
  - Thing to Thing (T2T)
A "smart grid" is a digital energy system that uses new technology to incorporate clean energy and provide more efficient, reliable electricity.

Solar panels, wind farms, and other sources of energy feed into the grid.

Home energy sources feed into the same grid as major suppliers, and customers are reimbursed for energy contribution.

Users view their energy usage in real time from any computer and make decisions about what is on or off while they are away.

Users decide when outlets are in use; e.g., refrigerators could be turned to a lower setting at night or during the day.

The utility company is able to pinpoint problems in the grid so service is more reliable.

The smart meter tracks when customers use electricity, which is more expensive during peak usage hours.
Public, Private and Hybrid Clouds

A typical Public Cloud
- Cloud Service Queues
- Platform Frontend (Web Service API)

Datacenter
- Server Cluster (VMs)
- Cloud Storage

The Internet
- Microsoft Azure
- Amazon AWS
- IBM Blue Cloud
- Google AppEngine
- Salesforce.com Force.com

A Hybrid Cloud
- Public Cloud
- Private Cloud (IBM RC2)

An Intranet

Cloud Users

To users or other public clouds over the Internet
# Cloud Providers, Services and Security Measures

<table>
<thead>
<tr>
<th>Model/Features</th>
<th>IBM</th>
<th>Amazon</th>
<th>Google</th>
<th>Microsoft</th>
<th>Salesforce.com</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PaaS</strong></td>
<td>BlueCloud, WCA, RC2,</td>
<td>EC2, S3, SQS, SimpleDB</td>
<td>AppEngine (GAE)</td>
<td>Windows Azure</td>
<td>Force.com</td>
</tr>
<tr>
<td><strong>IaaS</strong></td>
<td>Ensembles</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SaaS</strong></td>
<td>Lotus Live</td>
<td></td>
<td>Gmail, Docs</td>
<td>.NET service, Dynamic CRM,</td>
<td>Online CRM, Gifttag</td>
</tr>
<tr>
<td><strong>Reported services</strong></td>
<td>SOA, B2, TSAM, RAD, Web 2.0</td>
<td>AWS, Hadoop</td>
<td>GFS, BigTable, MapReduce</td>
<td>Live, SQL Azure, Hotmail</td>
<td>Apex, visual force, Record-security</td>
</tr>
<tr>
<td><strong>Security Features</strong></td>
<td>WebSphere2 and PowerVM tuned for protection</td>
<td>PKI and VPN for security, EBS to recover from failure</td>
<td>Some HW security in datacenters</td>
<td>Replicated Data, rule-based access control</td>
<td>Adm./Record security, Use Metadata API</td>
</tr>
</tbody>
</table>

**Abbreviations:**
- WCA: Websphere CloudBurst Appliance
- RC2: Research Compute Cloud
- RAD: Rational Application Developer
- SOA: Service Oriented Architecture
- TSAM: Tivoli Service Automation Manager
- EC2: Elastic Compute Cloud
- S3: Simple Storage Service
- SQS: Simple Queue Service
- GAE: Google AppEngine
- AWS: Amazon Web Services
- SQL: Structured Query Language
- EBS: Elastic Block Store
- CRM: Customer Relationship Management

Note: Blank entries in the table refer to unknown services or cloud applications that are still under development.

Kai Hwang and Deyi Li, “Trusted Cloud Computing with Secure Resources and Data Coloring”, *IEEE Internet Computing*, Sept. 2010
The Internet of Things

Internet of Things (IOT)

Smart Earth: An IBM Dream
# Enabling and Synergistic Technologies for Building The Internet of Things

<table>
<thead>
<tr>
<th>Enabling Technologies</th>
<th>Synergistic Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine-to-machine interfaces</td>
<td>Geo-tagging/geo-caching</td>
</tr>
<tr>
<td>Cloud Computing Services</td>
<td>Biometrics</td>
</tr>
<tr>
<td>Microcontrollers</td>
<td>Machine vision</td>
</tr>
<tr>
<td>Wireless communication</td>
<td>Robotics</td>
</tr>
<tr>
<td>Radio frequency iden. (RFID)</td>
<td>Augmented reality</td>
</tr>
<tr>
<td>Energy harvesting technologies</td>
<td>Telepresence and autonomy</td>
</tr>
<tr>
<td>Sensors and sensor networks</td>
<td>Life recorders and personal assistant</td>
</tr>
<tr>
<td>Actuators</td>
<td>Tangible user interfaces</td>
</tr>
<tr>
<td>Location technology (GPS)</td>
<td>Clean technologies</td>
</tr>
<tr>
<td>Software engineering</td>
<td>Mirror worlds</td>
</tr>
</tbody>
</table>