Trusted Mobile and Cloud Computing with Assured Big-Data Security and Privacy

Prof. Kai Hwang
University of Southern California

A. Pervasive mobile and wireless applications demand cloud computing services
B. Big-data integrity, security and privacy hinder the acceptance of clouds by users and business world
C. Cloud roles in support of Internet of Things (IoT)
D. Case studies: Clouds for mobile gaming, secure big data repository, and wide-area sensor grid
E. Impact of proposed new Internet Architectures on future clouds and IoT evolution.

A. Mobile Devices and Wireless Networks for Pervasive Computing, Communications, and Entertainment

- Mobile Devices are often referred as handsets or hand-held computers. They appear as smartphones, PDAs, tablet and notebook computers.
- In 2012, smartphones sales exceeded 150 millions of units and 31% US Internet users were ported to have a tablet.
- Tablet computers appears as tablet PCs, PDAs, booklet and mini tablet such as iPad, Galaxy Tab, Nokia N800, and ASUS e-Pad, etc.
- The sale of tablet computers grows faster than traditional portable notebook computers. They all emphasize light weight, thin computing, GPS, WiFi and 3G/4G access of the Internet.

Acknowledgements:
New ideas and research results presented are based on collaborative work with several colleagues in the USA, China, and Norway in recent years. Relevant publications are listed on the last slide.

- Yogesh Simmhan, Viktor Prasanna, Runfang Zhou, Zhou Zhao, and Jose Villeta, University of Southern California [1, 2, 3]
- Geoffrey Fox and Judy Qiu, Indiana University [4]
- Deyi Li, Yongwei Wu and Junwei Cao, Tsinghua University, China [5, 6]
- Chunming Rong, Stavanger University, Norway [6]
State of Cloud Ecosystem:

- At the system level, the cloud ecosystem includes the cloud platform and infrastructure, resource management policies, etc.
- At the service level, the service-level agreement (SLAs), global standards, reputation system, billing and accounting systems, cloud business models, etc.
- At the user (client) level, application programming interfaces (APIs), cloud programming environment, Quality of Service (QoS) control, etc.

Case Study 1: Cloud for Video Gaming by Massive Number of Players

- The 4G LTE replaces 2G/3G gradually
- WiMAX based on the IEEE 802.16m standard for advanced mobile applications.
- WiMAX could merge with LTE with similar radio technology and core IOP-based data networks
Cloud Gaming Advantages and Design Goals

1. Game cloud delivers both SaaS for game players and PaaS for game developers
2. Advantages:
   1. Customers no longer need to purchase and update expensive game console
   2. Customer can use smartphone to experience high-quality graphics
   3. Pay-as-you-go model applied
   4. Game developer focus on uniform platform
   5. Software piracy is prevented
3. Design goals:
   1. Minimize response time or latency
   2. Maximize frame rate.
   3. Improve Quality of Experiences (QoE)
   4. Taking advantage of client computing resources.

Prototype Game Cloud built at the USC GamePipe Lab

Game Cloud Design at USC GamePipe Lab.

Prototype Game Cloud built at the USC GamePipe Lab

(Courtesy of donated CPU, GPU and Hypervisors from Intel, Nvidia, and Microsoft)

Latency Analysis and Frame Rate in Video Gaming Cloud

Frame rate increase 35% from local thin client to using cloud platform.

120 ms latency is acceptable in gaming cloud with only small delay due to cloud overhead


All rights reserved, Kai Hwang, USC, Presentation at IEEE CloudCom2012, Taipei, Taiwan, Dec.5, 2012
B. Security, Privacy and Trust Management in Cloud Computing

- To secure cloud resources and uphold user privacy and data integrity, we need to safeguard user authentication and tighten the data access-control in public clouds.
- Trust overlay networks could be applied to build reputation systems for establishing the trust among interactive datacenters or cloud providers.
- Performance boosting techniques are in demand for grid and cloud computing to achieve high performance with maximum profits in scientific and business computing areas.

Available Cloud Security and data Protection Techniques [4]

<table>
<thead>
<tr>
<th>Schemes</th>
<th>Brief Description and Deployment Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use redundancy at multiple sites</td>
<td>Multiple power supplies, alternate network connections, multiple databases at separated sites, data consistency, etc.</td>
</tr>
<tr>
<td>Trust delegation/ Negotiation</td>
<td>Cross certificates delegate trust across PKI domains for various datacenters. Trust negotiation to resolves conflicts.</td>
</tr>
<tr>
<td>Worm and DDoS Defense</td>
<td>Network worm containment and defense against DDoS attacks to secure all datacenters and cloud platforms.</td>
</tr>
<tr>
<td>Reputation system</td>
<td>Reputation system built with a P2P trust overlay network and coordinated file systems over multiple datacenters.</td>
</tr>
<tr>
<td>Fine-grain file access control</td>
<td>Fine-grain access control at the file level. This adds up a level beyond firewalls and intrusion detection systems.</td>
</tr>
<tr>
<td>Copyright Protection</td>
<td>Piracy prevention to stop peer collusion, removal of poisoned contents, non-destructive read, alteration detection, etc.</td>
</tr>
<tr>
<td>Data Privacy Preservation</td>
<td>Use double authentication, biometric identification, plus enforcement by data coloring and accountability support.</td>
</tr>
</tbody>
</table>

(B1). Shared Big Data Protection and Trust Management in Clouds

(B2): PowerTrust built over A Trust Overlay Network


**Trusted Zones for VM Insulation**

- Federate identities with public clouds
- Control and isolate VM in the virtual infrastructure
- Insulate information from cloud providers’ employees
- Insulate information from other tenants
- Insulate infrastructure from Malware, Trojans and cybercriminals
- Segregate and control user access
- Enable end-to-end view of security events and compliance across infrastructures

**How to Secure VMs in the Cloud?**

- **Access Control** is discretionary. Fine-grained multilevel controls are needed (integrity lock architecture)
- **Secure Boot** – The boot process needs to be secured. Proper attestation methods desired. More robust logging is needed.
- **Component Isolation** – Dom0 in XEN supports networking, disk I/O, VM boot loading, hardware emulation and workload balancing, all need to be decomposed into components
- **Logging –Introspection** – A VM running security software is allowed to look inside the memory of another VM. Software such as IPS and antiviruses, using introspection should be safe from tampering.
- **Avoid man-in-the-middle attack** on VMs during VM migration.

**Data Coloring for Preserving Data Privacy in Cloud Processing**

(Source: K. Hwang and D. Li, "Trusted Cloud Computing with Secured Resources and Data Coloring", IEEE Internet Computing, Sept. 2010.) [5].

**Use of Color Matching to Secure the Access of Shared Data Objects in a Cloud Environment**

(Source: K. Hwang and D. Li, “Trusted Cloud Computing with Secured Resources and Data Coloring”, IEEE Internet Computing, Sept. 2010.) [5].

- New datacenter architecture that can preserve data privacy, enforce security policy, and scale well with future dataset growth.
- Trust management of time-varying datasets with intrusion and anomaly detection to assure data integrity.
- Securing access to data using innovative techniques to avoid excessive replication of data to external entities.
- Protect privacy and maintenance of security in aggregated personal and proprietary data.
- Establishing community standards, provenance tracking, and communication strategies for public outreach and engagement.

Case Study 2: Secure BigData Repository Testbed for SmartGrid Informatics Research [1]:

- This is a cyber-physical system built at USC for campus-wide smart power grid management, data governance and security control in green cloud computing.
- The table lists the access restrictions on each data class for different user groups at USC campus, involving 60,000 consumers (students and staff, workers).

Cryptonite Data Repository Design for Elastic Scaling and Security Enforcement in Cloud Storage

(Easy Key Management using Broadcast Encryption and StrongBox)

(sign(SB), K_{pri_erv})

<table>
<thead>
<tr>
<th>Data Repository</th>
<th>encrypt(L_1, K_{sym_enc1})</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Handle</td>
<td>Init. Vector</td>
</tr>
<tr>
<td>UUID-1</td>
<td>IV-1</td>
</tr>
<tr>
<td>UUID-2</td>
<td>IV-2</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

StrongBox for storing shared encryption or decryption and signature keys for a given access control list shared by a set of files.
C: Cloud Roles in Internet of Things

Application Layer
- Merchandise Tracking
- Environment Protection
- Intelligent Search
- Telemedicine
- Intelligent Traffic
- Smart Home

Network Layer
- Mobile Telecom Network
- Information Network
- Cloud Computing Platform
- The Internet

Sensing Layer
- RFID
- Sensor Network
- GPS
- Sensor Nodes
- Road Mapper

Wireless Technologies for Cost-Effective Deployment of Sensor Networks and IoT

<table>
<thead>
<tr>
<th>Name and Standard</th>
<th>ZigBee 802.15.4</th>
<th>4G LTE mobile network</th>
<th>WiFi 802.11 n</th>
<th>Bluetooth 802.15.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application focus</td>
<td>Monitoring and control</td>
<td>Wide-area voice/data/multimedia telecommunication</td>
<td>Web, e-mail, video streaming</td>
<td>Cable replacement</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>20–250 Kbps</td>
<td>100+ Mbps</td>
<td>100-300 Mbps</td>
<td>720 Kbps</td>
</tr>
<tr>
<td>Operating Range</td>
<td>100+ meters</td>
<td>Cell &lt; 2 KM, unlimited with handover and global roaming</td>
<td>1–100 meters</td>
<td>1 - 2 meters</td>
</tr>
<tr>
<td>Success Metrics</td>
<td>Reliability, power, cost</td>
<td>Reach clients, Quality of Service</td>
<td>Speed, flexibility</td>
<td>Cost, convenience</td>
</tr>
</tbody>
</table>

Wireless Internet Access Trend: from Dispersion to Convergence

1. Smart and pervasive cloud applications for individuals, homes, communities, companies, and governments, etc.
2. Coordinated calendar, itinerary, job management, eventing, CRM services, word processing, on-line presentations, web-based desktops, sharing on-line documents, datasets, photos, video, and databases, content distribution, etc.
3. Deployment of P2P and social networking applications in the cloud environments, more cost-effectively. This will benefit earthbound applications that demand elasticity and parallelism to avoid large data movement and reduce the storage costs.
Case Study 3: Sensor Grids supported by Clouds*

- Sensors (“Things”) appear pervasively
- In the thin client era, smart phones, Kindles, tablets, Kinects, web-cams are sensors
- Robots, distributed instruments such as environmental measures are sensors
- Web pages, Googledocs, Office 365, WebEx are sensors
- Ubiquitous Cities/Homes are full of IP-addressed sensors

Use clouds to consolidate, control and collaborate with small and massively distributed sensors.

* In collaboration with Geoffrey Fox and associates at Indian University

Mobility Support and Security Measures for Trusted Mobile Cloud Computing

- Special air interfaces
- Mobile API design
- File/Log access control
- Data coloring
- Wireless PKI
- User authentication,
- Copyright protection
- Disaster recovery

Hardware and Software Measures for Cloud Security

- Hardware/software root of trust,
- Provisioning virtual machines,
- Software watermarking
- Host-based firewalls and IDS
- Network-based firewalls/IDS
- Trust overlay network
- Reputation system
- OS patch management

(E. Frontier Research Directions for Developing the Future Internet)

- Programmable Networking Architecture
- Fusion of The Internet, Mobile and TV Networks
- Named Data Networking beyond the TCP/IP
- Federated Intercloud Computing Applications
- New Ideas for Security and Privacy Protection
- Service Migration and Disaster Recovery
Future Internet Architectures

- **OpenFlow for Programmable Virtual Networking**
  (Stanford, Princeton, etc., 2008)

- **Content-Centric Networking (CCN)**
  : Named Data Networking, (HP Lab, etc. 2009)

- **Service-Oriented Future Internet Architecture**
  (SOFIA) : Chinese Academy of Sciences, Institute of Computing Technology (2011)

---

Conclusions:

- Cloud industrialization demands a major overhaul of our computer science and computer engineering educational programs.

- Mobile and pervasive computing applications must leverage the clouds to store and process big data, which are changing rapidly in time and space.

- Clouds, IoT and social networks are changing our world, reshaping human relations, elevating the global economy, and even causing political system reform quietly.

---

Relevant Publications:


3. Z. Zhao, K. Hwang and J. Villete, "GamePipe: Game Cloud Design with Virtualized CPU/GPU Cluster", *ACM ScienceCloud 2012*.

