CPET 581 Cloud Computing: Technologies and Enterprise IT Strategies

Lecture 6

Cloud Platform Architecture over Virtualized Data Centers

Part -4

Cloud Security and Trust Management

Text Book: Distributed and Cloud Computing, by K. Hwang, G C. Fox, and J.J. Dongarra, published Elsevier/Morgan Kaufmann, 2012.

Spring 2015

A Specialty Course for Purdue University's M.S. in Technology Graduate Program: IT/Advanced Computer App Track

Paul I-Hai Lin, Professor

Dept. of Computer, Electrical and Information Technology

Purdue University Fort Wayne Campus

Ch. 4 - Topics of Discussion

- Cloud Computing and Service Models
- Data-Center Design and Interconnection Networks
- Architectural Design of Computer and Storage Clouds
- Public Cloud Platforms: Google App Engine, Amazon Web Services and Microsoft Window Azure
- **Inter-Cloud Resource Management**
  - **Resource Provisioning and Platform Deployment**
- **Cloud Security and Trust Management**

Figure 4.23 A stack of six layers of cloud services and their providers

- Six layers of cloud services: Hardware, Network, Collocation, Infrastructure, Platform, and Software Apps

Cloud application (SaaS)	Concur, RightNOW, Teleo, Kenexa, Webex, Blackbaud, salesforce.com, Netsuite, Kenexa, etc.
Cloud software environment (PaaS)	Force.com, App Engine, Facebook, MS Azure, NetSuite, IBM BlueCloud, SGI Cyclone, eBay
Cloud software infrastructure: Computational resources (IaaS); Storage (DaaS); Communications (Caas)	Amazon AWS, OpSource Cloud, IBM Ensembles, Rackspace cloud, Windows Azure, HP, Banknorth
Collocation cloud services (LaaS)	Savvis, Internap, NTTCommunications, Digital Realty Trust, 365 Main
Network cloud services (NaaS)	Owest, AT&T, AboveNet
Hardware/Virtualization cloud services (HaaS)	VMware, Intel, IBM, XenEnterprise

Three Cases of Cloud Resource Provisioning without Elasticity

- Case (a): Overprovisioning with the peak load
  - Fixed capacity
  - Heavy resource waste shown in shaded area
- Case (b): Under provisioning #1 along the capacity line (results in losses by both user and provider)
  - Fixed capacity
  - Paid demand by the users is not served
  - Wasted resources still exist
- Case (c): Under provisioning # 2
  - Fixed capacity
  - Under provisioning, and then over provisioning, Under, …
  - Worse resource waste

Three Cases of Cloud Resource Provisioning without Elasticity

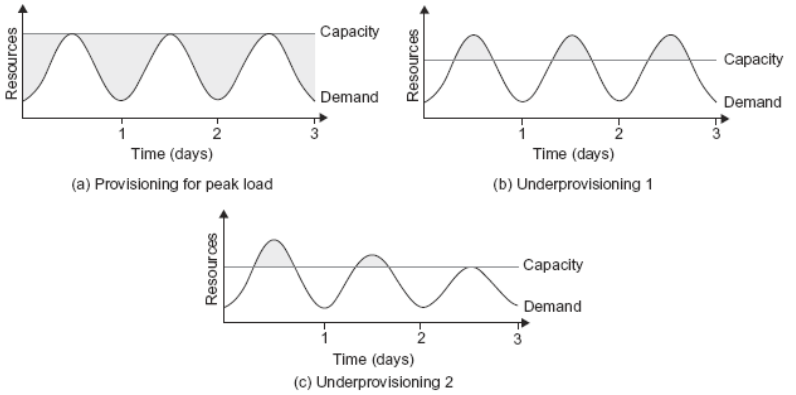


FIGURE 4.24

Three cases of cloud resource Provisioning without elasticity: (a) heavy waste due to overprovisioning, (b) underprovisioning and (c) under- and then overprovisioning.

(Courtesy of Armbrust, et al., UC Berkeley, 2009 [4])

Three Resource-Provisioning Methods

- Demand-driven method
  - Amazon implements auto-scale feature in EC2 platform
  - Easy to implement
  - Does not work out right if the workload changes abruptly
- Event-driven method
  - For seasonal or predicted events
  - Anticipates peaks traffic before it happens
  - Minimum loss of QoS
  - Christmas time in the West, Lunar New Year in the East
- Popularity-driven method
  - Internet searches for popularity of certain applications and creates the instances
  - Has a minimum loss of QoS

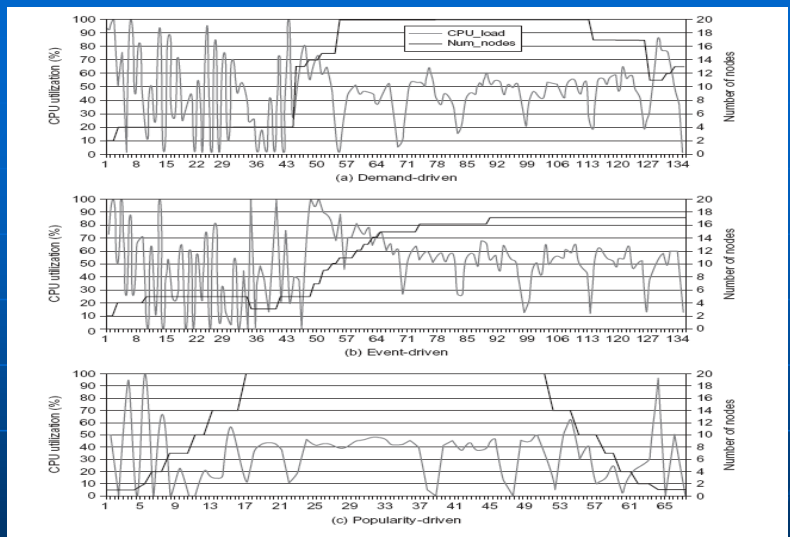


FIGURE 4.25

EC2 performance results on the AWS EC2 platform, collected from experiments at the University of Southern California using three resource provisioning methods.

(Courtesy of Ken Wu, USC)

- X axis: time scale in milli seconds

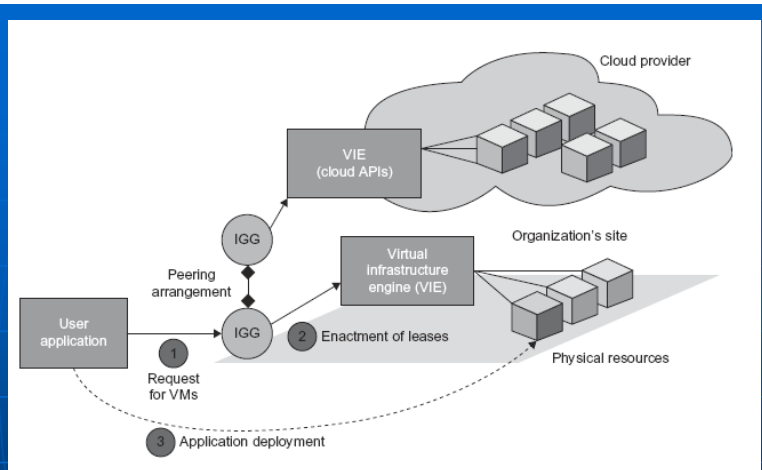


FIGURE 4.26

Cloud resource deployment using an IGG to allocate the VMs from a Local cluster to interact with the IGG of a public cloud provider.

(Courtesy of Constanzo, et al. [23])

- Under peak demand: IGG (Intergrid Gateway) ⇔ Other IGG to allocate needed resources
- Deploy applications in three steps: (1) requesting the VMs, (2) enacting the leases, (3) deploying the VMs

Provisioning of Storage Resources

- Storage Services in Three Cloud Computing Systems
  - Google File System (GFS)
  - Hadoop Distributed File System (HDFS)
  - Amamzon S3 and EBS (Elastic Block Storage)
- Typical Cloud Databases
  - BigTable from Google
  - SimpleDB from Amazon
  - SQL service from Microsoft Azure

Interactions among VM Managers for Cloud Creation and Management

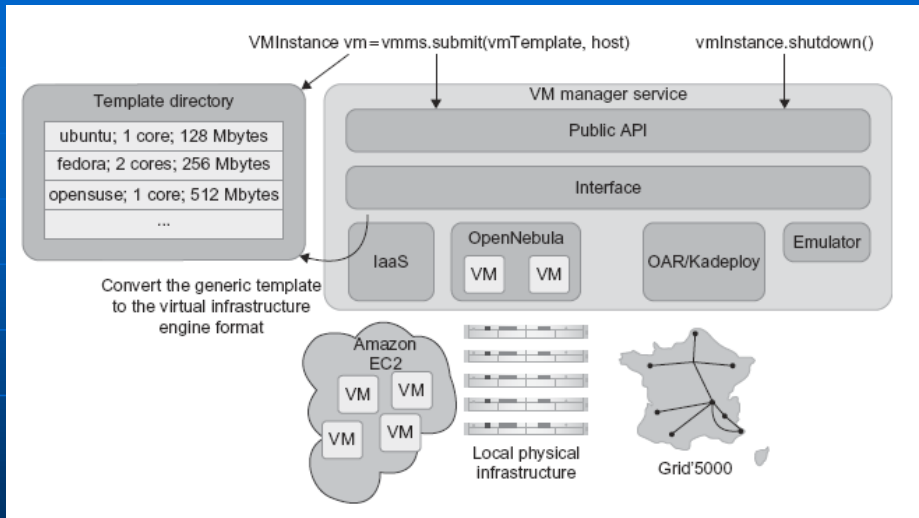


FIGURE 4.27

Interactions among VM managers for cloud creation and management; the manager provides a public API for users to submit and control the VMs.

(Courtesy of Constanzo, Assuncao, and Buyya [17])

Example 4.6 Experiments on an InterGrid Test Bed Over Grid'5000

Figure 4.28 (French experimental grid platform: 4,792 processor cores on nine grid sites across France); https://www.grid5000.fr/mediawiki/index.php/Grid5000:Home

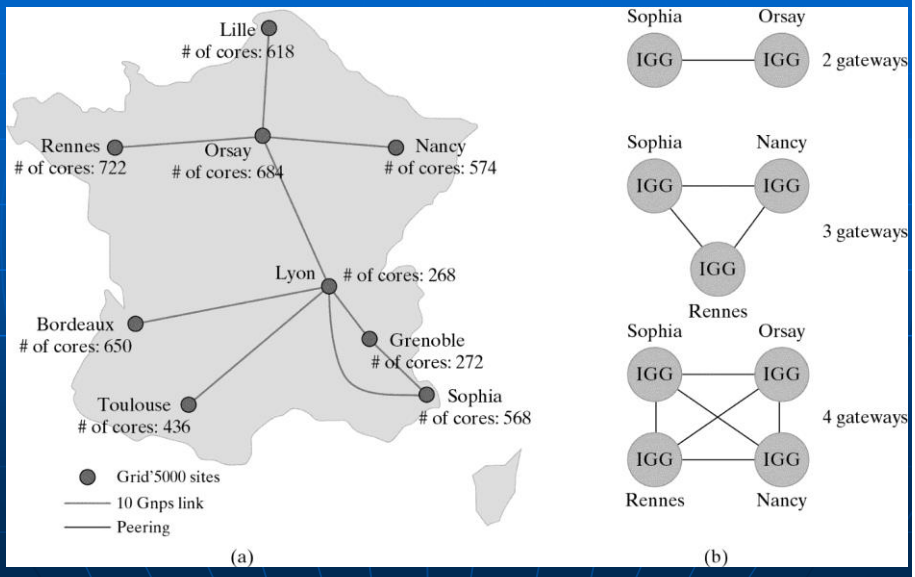
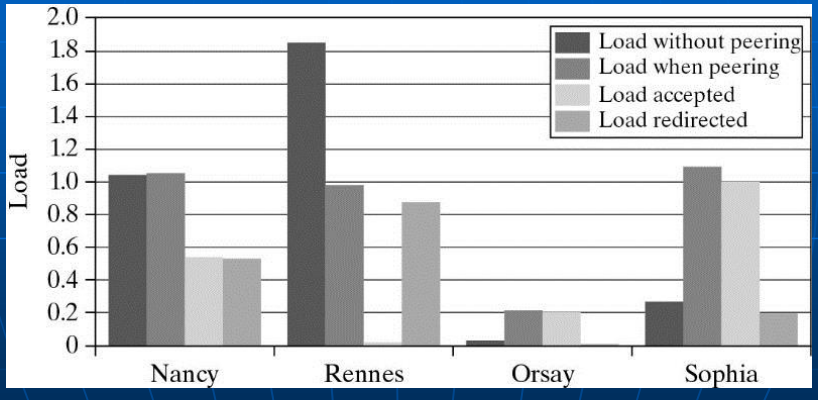


Figure 4.28 Cloud loading results at four gateways at resource sites in the Grid5000 system

- Load Characteristics under 4 Gateway Scenario
- Rennes, the site with a heavy load benefits from peering with other gatewas



4.5.4 Global Exchange of Cloud Resources Melbourne group's Inter-Cloud Architecture

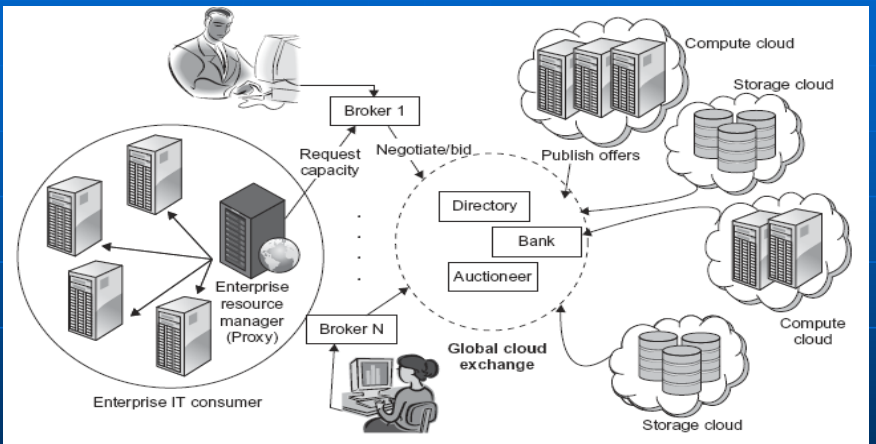


FIGURE 4.30

Inter-cloud exchange of cloud resources through brokering.

(*Courtesy of R. Buyya, et al., University of Melbourne [12]*)

Cloud Security and Trust Management

- Cloud Services Users should be free from
  - Abuses, Violence, Cheating, Hacking, Viruses, Rumors, Pornography, Spam, Privacy and copyright violations
- Trust (social problem) – solved by technical approaches
- Three basic cloud security enforcements
  - 1) **Facility security** in data centers
  - 2) **Network security**
    - Fault-tolerant external firewalls
    - Intrusion detection systems
    - Third-party vulnerability assessment
  - 3) **Platform security**
    - SSL (Secure Socket Layer) and data decryption
    - Strict password policies
    - System trust certification

Cloud Security Responsibilities

- Confidentiality, Integrity, Availability

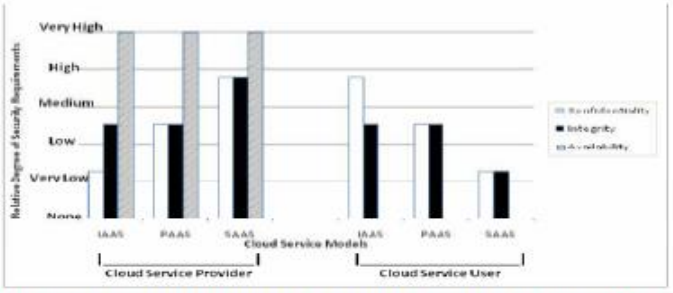


Figure 1.28 Internet security responsibilities by cloud service providers and by users.

Figure 4.31 Basic Cloud Security

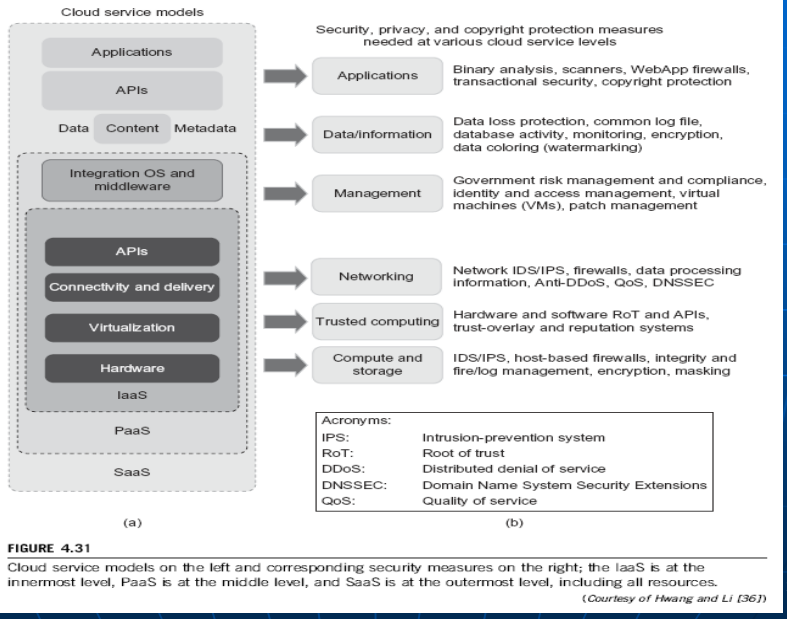


FIGURE 4.31

Cloud service models on the left and corresponding security measures on the right; the IaaS is at the innermost level, PaaS is at the middle level, and SaaS is at the outermost level, including all resources.

(Courtesy of Hwang and Li [36])

Eight Protection Schemes to Secure Public Clouds and Data Centers

Table 4.9 Physical and Cyber Security Protection at Cloud/Data Centers

Protection Schemes	Brief Description and Deployment Suggestions
Secure data centers and computer buildings	Choose hazard-free location, enforce building safety. Avoid windows, keep buffer zone around the site, bomb detection, camera surveillance, earthquake-proof, etc.
Use redundant utilities at multiple sites	Multiple power and supplies, alternate network connections, multiple databases at separate sites, data consistency, data watermarking, user authentication, etc.
Trust delegation and negotiation	Cross certificates to delegate trust across PKI domains for various data centers, trust negotiation among certificate authorities (CAs) to resolve policy conflicts
Worm containment and DDoS defense	Internet worm containment and distributed defense against DDoS attacks to secure all data centers and cloud platforms
Reputation system for data centers	Reputation system could be built with P2P technology; one can build a hierarchy of reputation systems from data centers to distributed file systems
Fine-grained file access control	Fine-grained access control at the file or object level; this adds to security protection beyond firewalls and IDSes
Copyright protection and piracy prevention	Piracy prevention achieved with peer collusion prevention, filtering of poisoned content, nondestructive read, alteration detection, etc.
Privacy protection	Uses double authentication, biometric identification, intrusion detection and disaster recovery, privacy enforcement by data watermarking, data classification, etc.

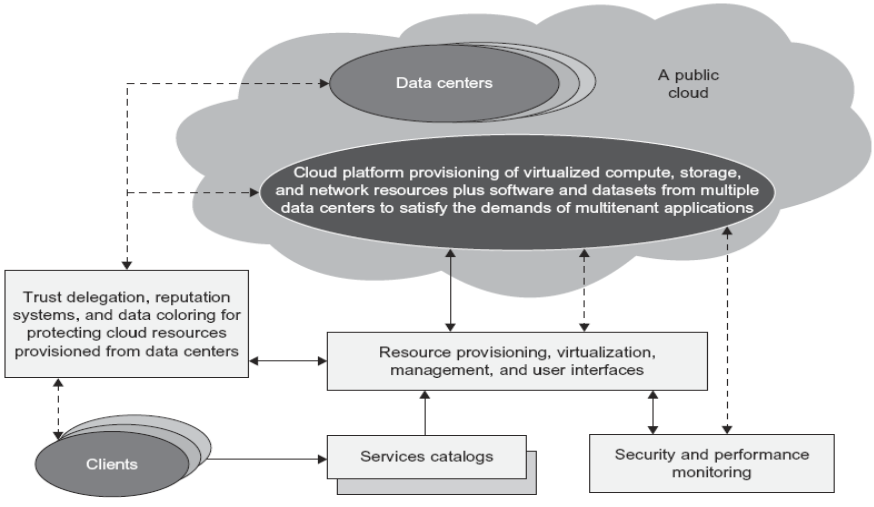
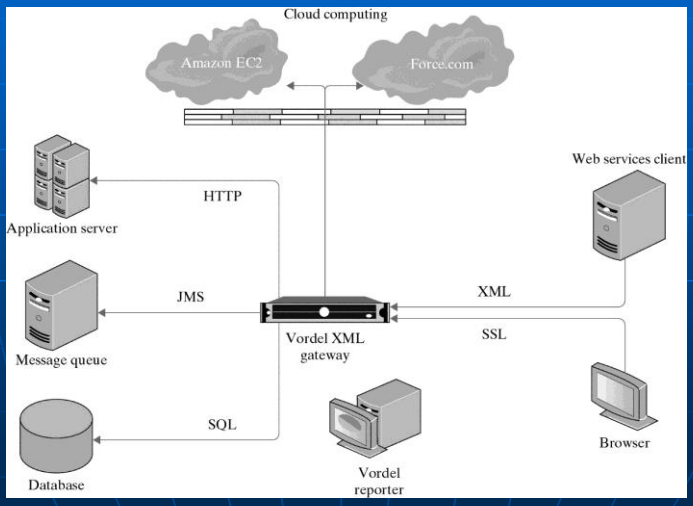


FIGURE 4.14

A security-aware cloud platform built with a virtual cluster of VMs, storage, and networking resources over the data-center servers operated by providers.

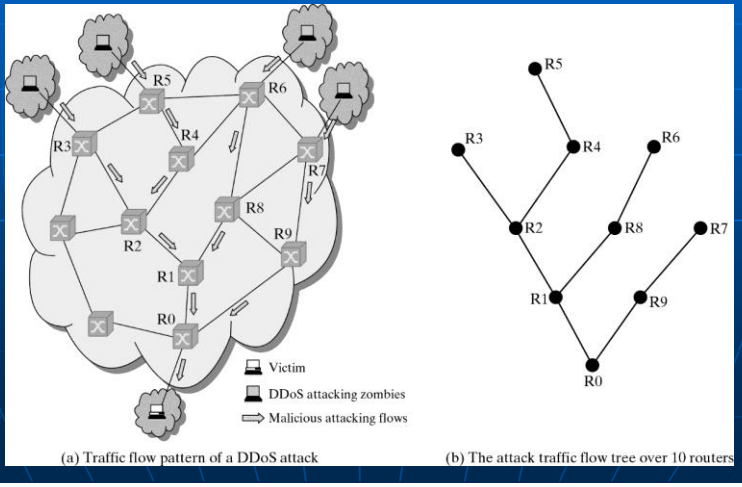
Example 4.7 Cloud Security Safeguarded by Gateway and Firewalls

- Figure 4.32 The typical security structure by a secured gateway plus external firewalls to safeguard the access of public or private clouds



4.6.2 Distributed Intrusion/Anomaly

- Other Cloud security concerns: Data lock-in problem, network attacks or abuse
- Figure 4.33 Distributed Defense against DDoS (Distributed Denial of Service)
  - Flooding attack pattern
  - Hidden attacker launched the attack from many zombies toward a victim server at the bottom Router R0.



Example 4.8 Man-in-the-Middle Attacks

- VM migration from VMM A => Security Vulnerable Network => VMM B
- The attacker can view the VM contents, steal sensitive data , or modify content

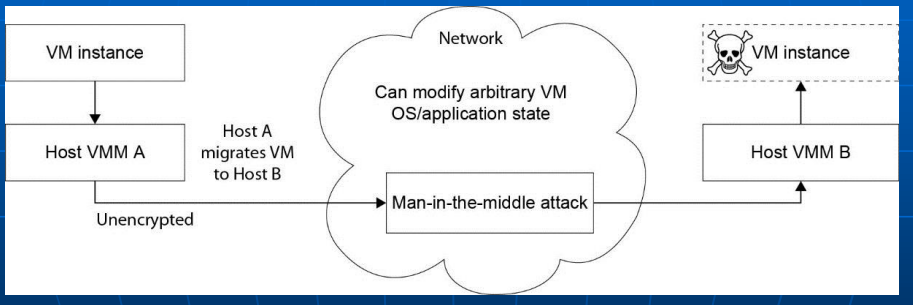
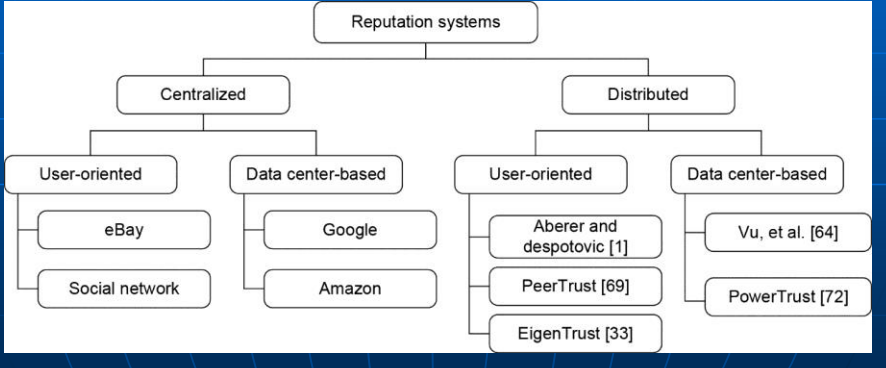


Figure 4.36 Reputation Systems for Social Networks and Cloud Systems

- Design options
  - Centralized reputation system
  - Decentralized reputation system



Trust Overlay Networks

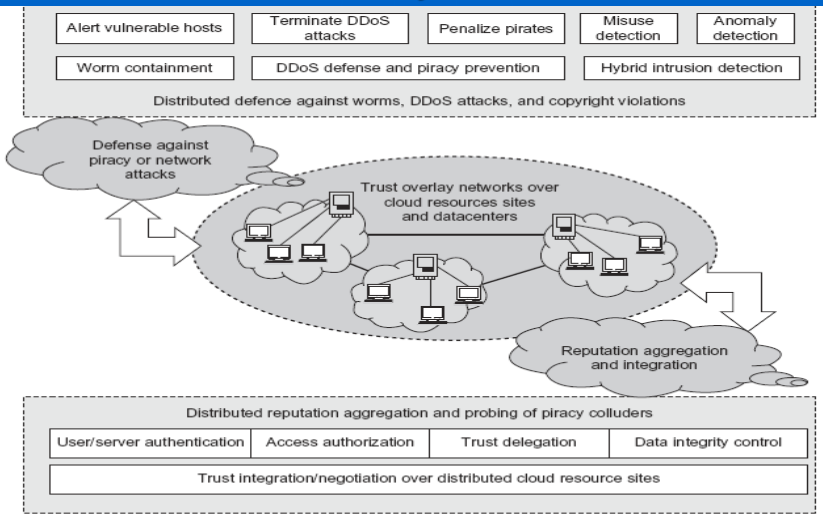


FIGURE 4.36

DHT-based trust overlay networks built over cloud resources provisioned from multiple data centers for trust management and distributed security enforcement.

(Courtesy of Hwang and Li [36])

Data Coloring and Cloud Watermarking

- Data coloring: Labeling each data object by a unique color

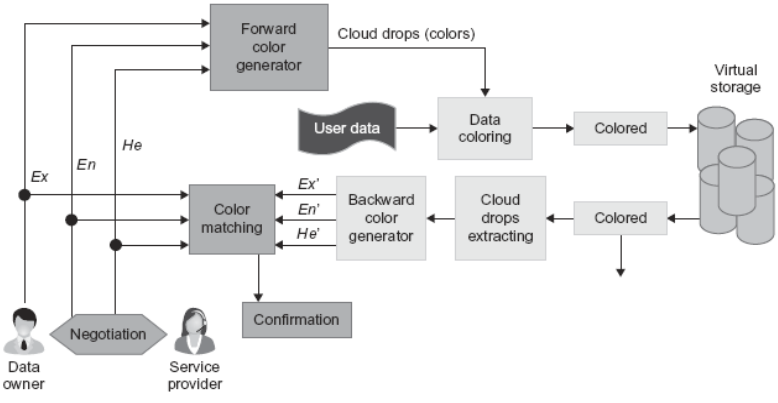


FIGURE 4.35a

Data coloring with cloud watermarking for trust management at various security clearance levels in data centers.

(Courtesy of Hwang and Li [30])

Basic Papers to Read

1. M. Armbrust, et al, "Above the Clouds: A Berkeley View of Cloud Computing", *Technical Report*, UCB/EECS-2009-28, Feb.2009.
2. K. Hwang and D. Li, " Trusted Cloud Computing with Secure Resources and Data Coloring", *IEEE Internet Computing,* Sept. 2010.
3. M. Rosenblum and T. Garfinkel, "Virtual Machine Monitors: Current Technology and Future Trends", *IEEE Computer,* May 2005, pp.39-47.
4. B. Sotomayor, R. Montero, and I. Foster, "Virtual Infrastructure Management in Private and Hybrid Clouds", *IEEE Internet Computing*, Sept. 2009

Conclusion and Summary