Distributed Systems

Cloud Advanced Topics

Issues

- Security Privacy and Trust are major obstacles for massive adoption of cloud
- Massive use of virtualisation exposes the system to new threats

Issues – Private Clouds

- System administration gets pushed to end-users rather than centralised IT and therefore IT security measure may not be as secure.
- Secondly users end up with elevated privileges within the institutional LAN putting the network at risk (to incompetence or malicious activities).

Issues – Public Clouds

- When buying into public cloud services there are certain risks and special care needs to be taken for point-to-point communications over public channels
- SLA terms and agreements concerning user data and even the companies client data
- Backup procedures and datacentre security protocols
- System updates and security protocols at the cloud provider level.

Security and Trust Barriers 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.

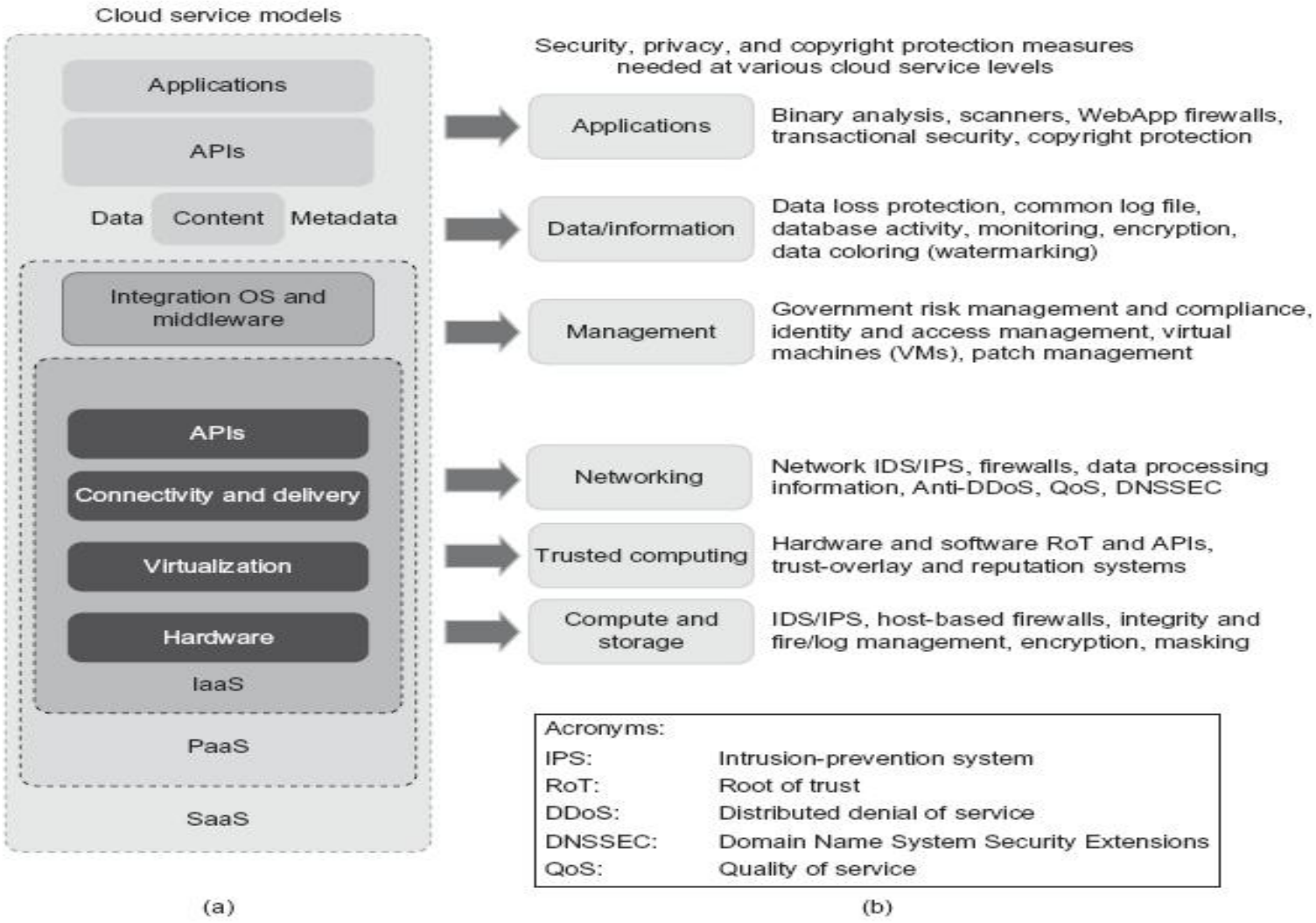


FIGURE 4.31

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])

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.

Security

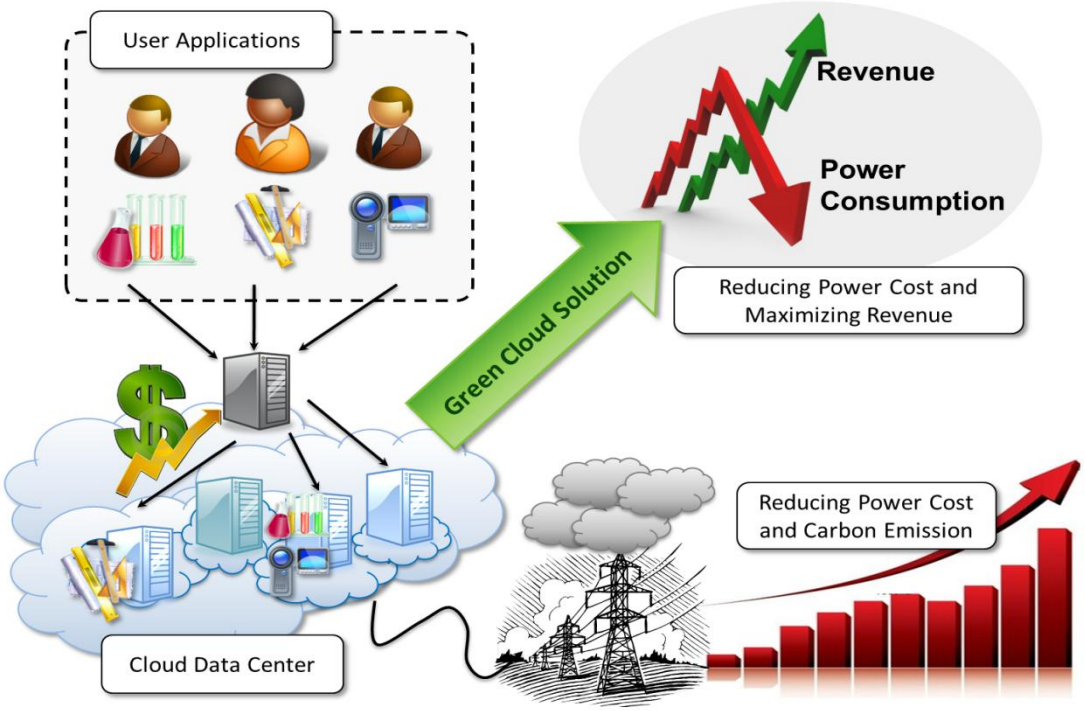
- Traditional IT systems
  - Security responsibility of the service provider
- Cloud Computing Environments
  - Security management divided between provider and customer
- Existing security frameworks and standards starting point
  - ISO/IEC 27001/27002
  - Information Technology Infrastructure Library (ITIL)

Security: Customer responsibilities

Activities	IaaS	PaaS	SaaS
Availability management	Manage VM availability with fault-tolerant architecture	Manage this activity for applications deployed in the PaaS platform (the provider is responsible for runtime engine and services)	Provider responsibility
Patch and configuration management	Manage VM image hardening Harden your VMs, applications, and database using your established security hardening process Manage activities for your VMs, database, and applications using your established security management process	Manage this activity for applications deployed in the PaaS platform Test your applications for OWASP Top 10 vulnerabilities[20]	Provider responsibility
Vulnerability management Access control management	Manage OS, applications, and database vulnerabilities leveraging your established vulnerability management process Manage network and user access control to VMs, secure privileged access to management consoles, install host Intrusion Detection System (IDS), and manage host firewall policies	Manage this activity for applications deployed in the PaaS platform (the provider is responsible for their runtime engine and service) Manage developer access to provisioning Restrict access using authentication methods (user- and network-based controls) Federate identity and enable SSO if SAML[21] is supported	Provider responsibility Manage user provisioning Restrict user access using authentication methods (user- and network-based controls) Federate identity and enable SSO if SAML is supported

Energy

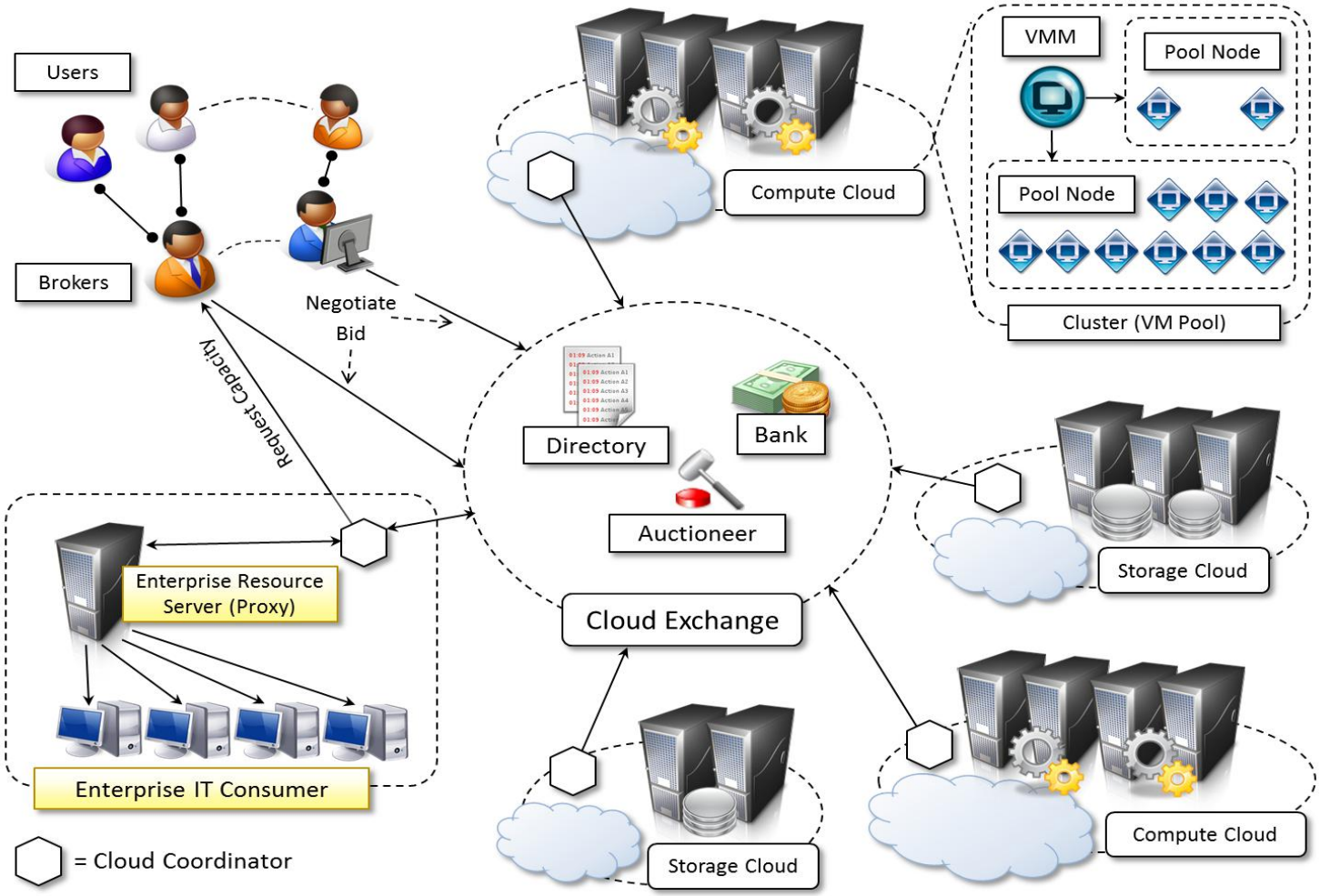
- Datacentres host a variety of heterogeneous applications with different execution time requirements
- Resource allocation static based on peak oad characteristics
- High performance vs Energy vs SLAs
  - A typical data centre consumes as much energy as 25000 households
  - energy costs double every five years
  - Datacentre carbon emmissions > Argentina+Netherlands
  - Amazon: energy costs 42% of budget (power + cooling)
- The Green Grid



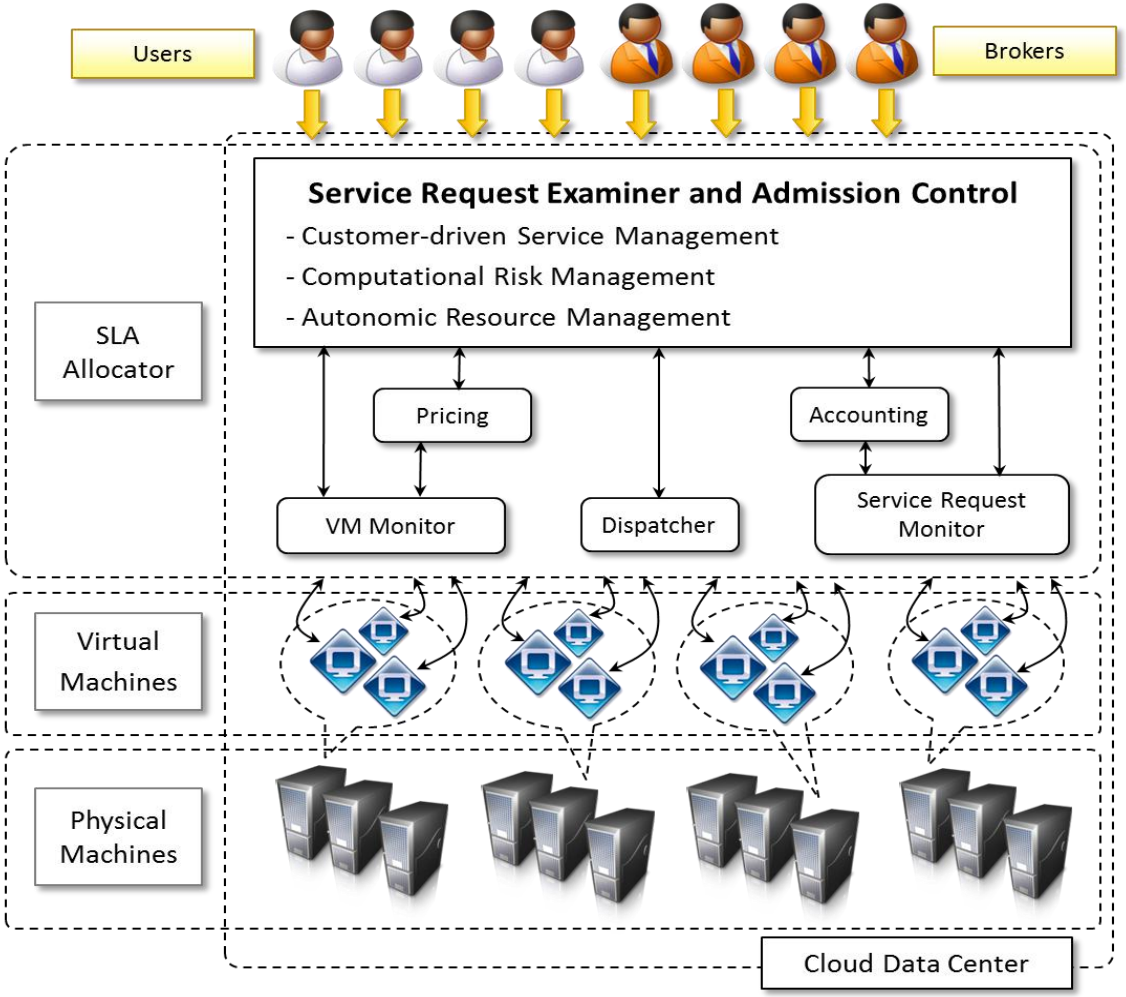
Market-based Management

- Cloud computing today mainly for
  - Complete replacement of in-house IT infrastructure with outsourced equivalent
  - Elastic scaling of existing systems to address peak workloads
- Currently Inflexible pricing
- Proprietary interfaces vendor lock-in
- Need for Market for trading IT utilities (assets and services)
- IaaS more mature
- MOCC

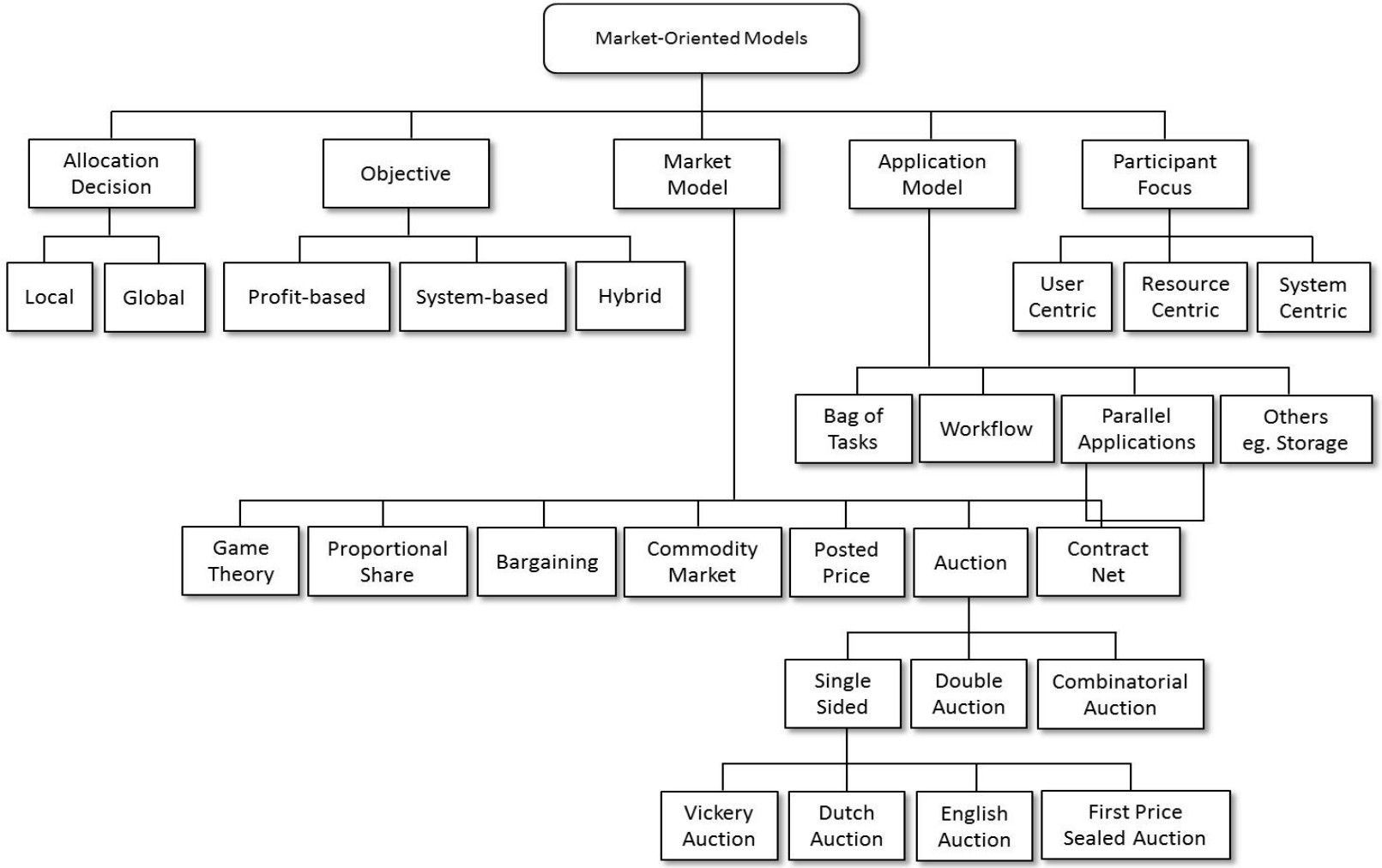
MOCC Scenario and Reference Model



Market Oriented Architecture for DataCenters



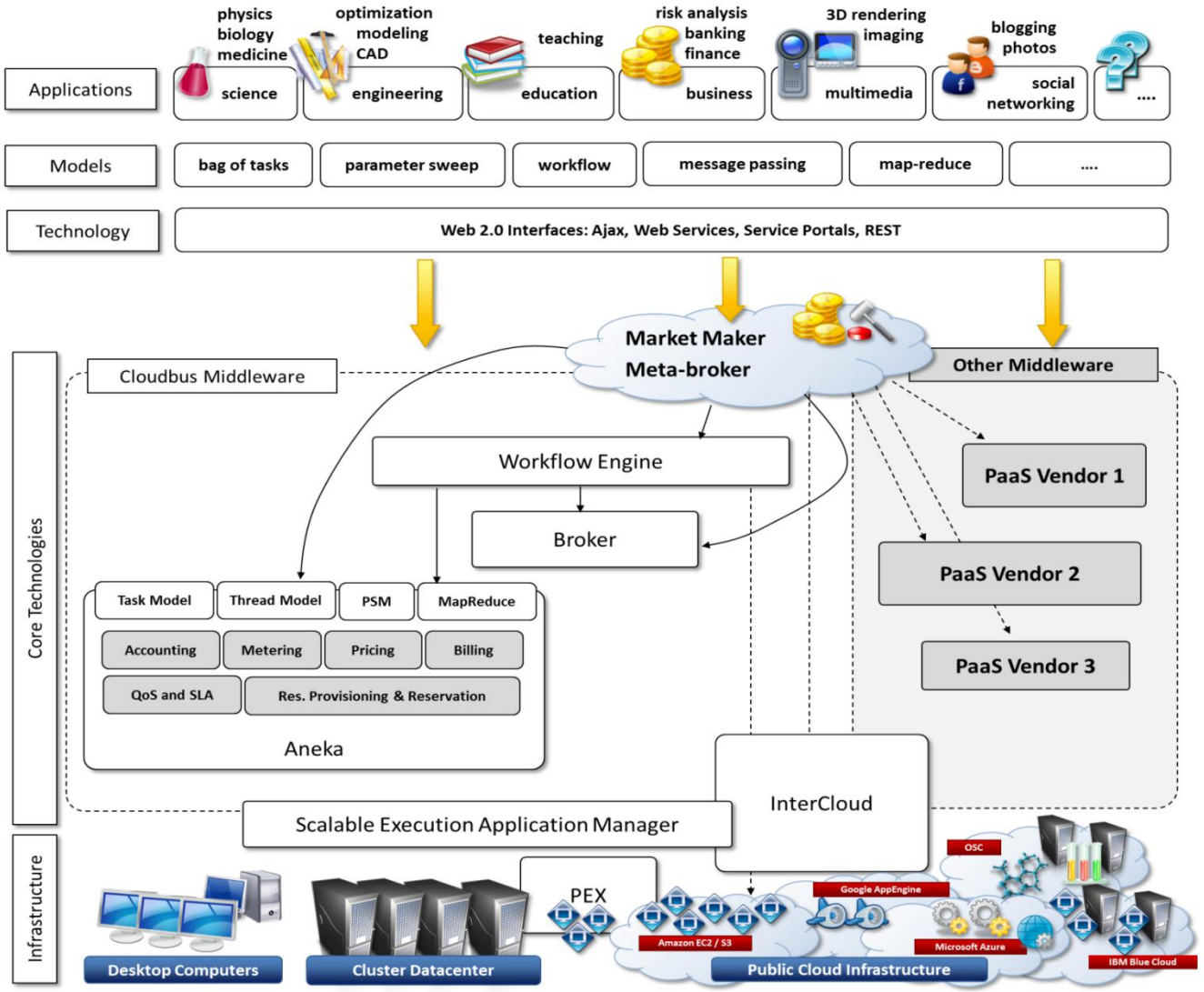
Trading Computing Utilities (Grid computing)



Trading Computing Utilities

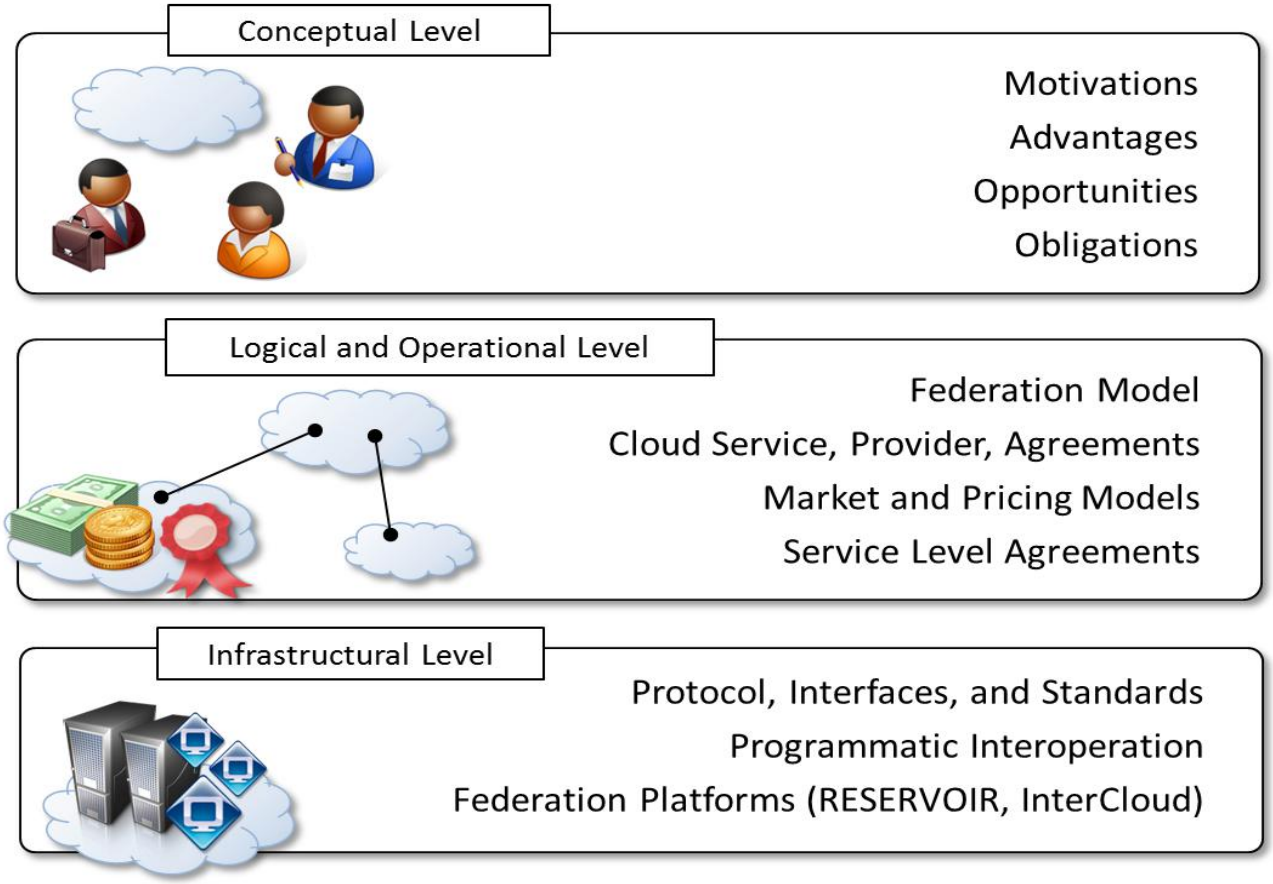
- Scheduling Systems:
  - SHARP
  - Tycoon
  - Bellagio
  - Shirako
  - Nimrod-G
  - Gridbus Broker
- Industrial Implementations
  - Amazon Web Services: flexible pricing models
    - spot instances: bid on ususued EC2 capacity
  - Splotcloud: virtual market place for IaaS
    - on top of Google AppEngine
- Research ongoing to realise MOCC
  - CloudBus

CloudBus


Applications
physics
biology
medicine
science
optimization
modeling
CAD
engineering
teaching
education
risk analysis
banking
finance
business
3D rendering
imaging
multimedia
blogging
photos
social
networking
....
Models
bag of tasks
parameter sweep
workflow
message passing
map-reduce
....
Technology
Web 2.0 Interfaces: Ajax, Web Services, Service Portals, REST
Market Maker
Meta-broker
Other Middleware
Cloudbus Middleware
Workflow Engine
Broker
PaaS Vendor 1
PaaS Vendor 2
PaaS Vendor 3
Core Technologies
Task Model
Thread Model
PSM
MapReduce
Accounting
Metering
Pricing
Billing
QoS and SLA
Res. Provisioning & Reservation
Aneka
InterCloud
Scalable Execution Application Manager
Infrastructure
PEX
Desktop Computers
Cluster Datacenter
Amazon EC2 / S3
Google AppEngine
Microsoft Azure
OSC
IBM Blue Cloud
Public Cloud Infrastructure

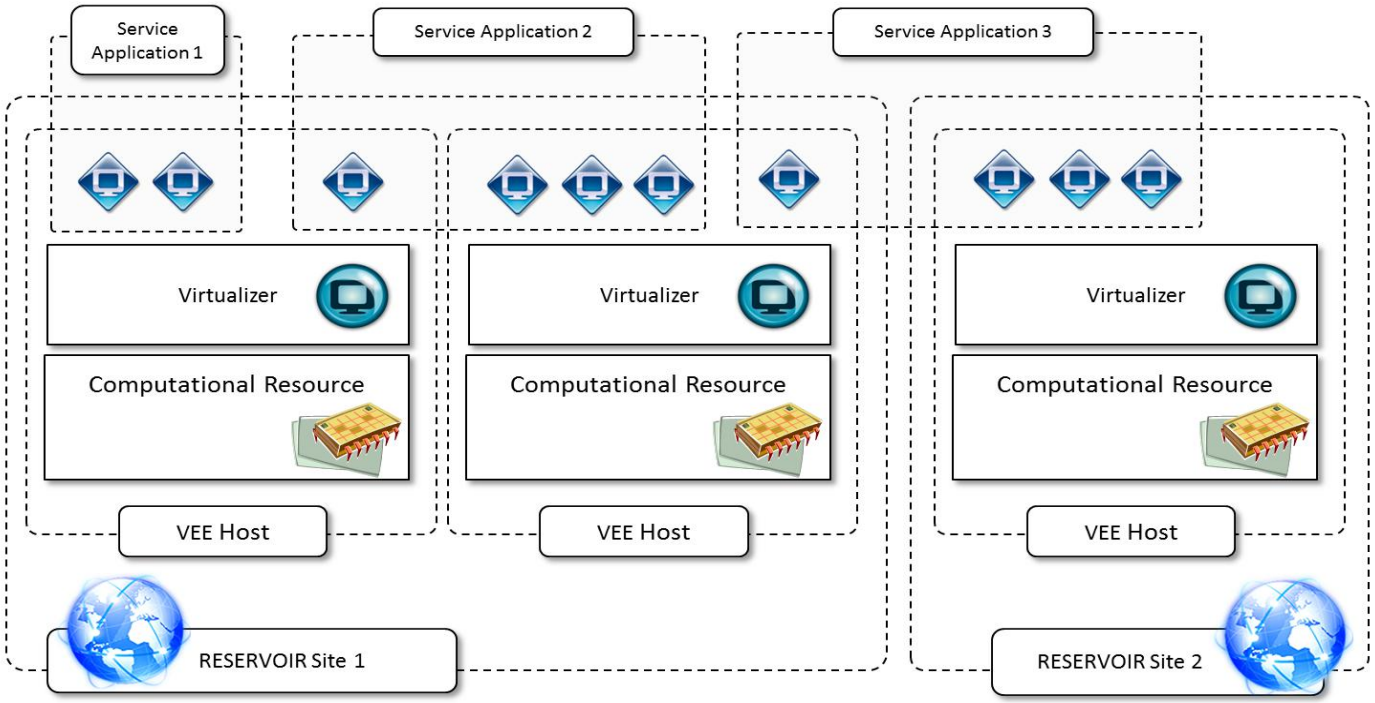
Federated Clouds

- Enablers for MOCC
- Provide for interoperation between different cloud providers

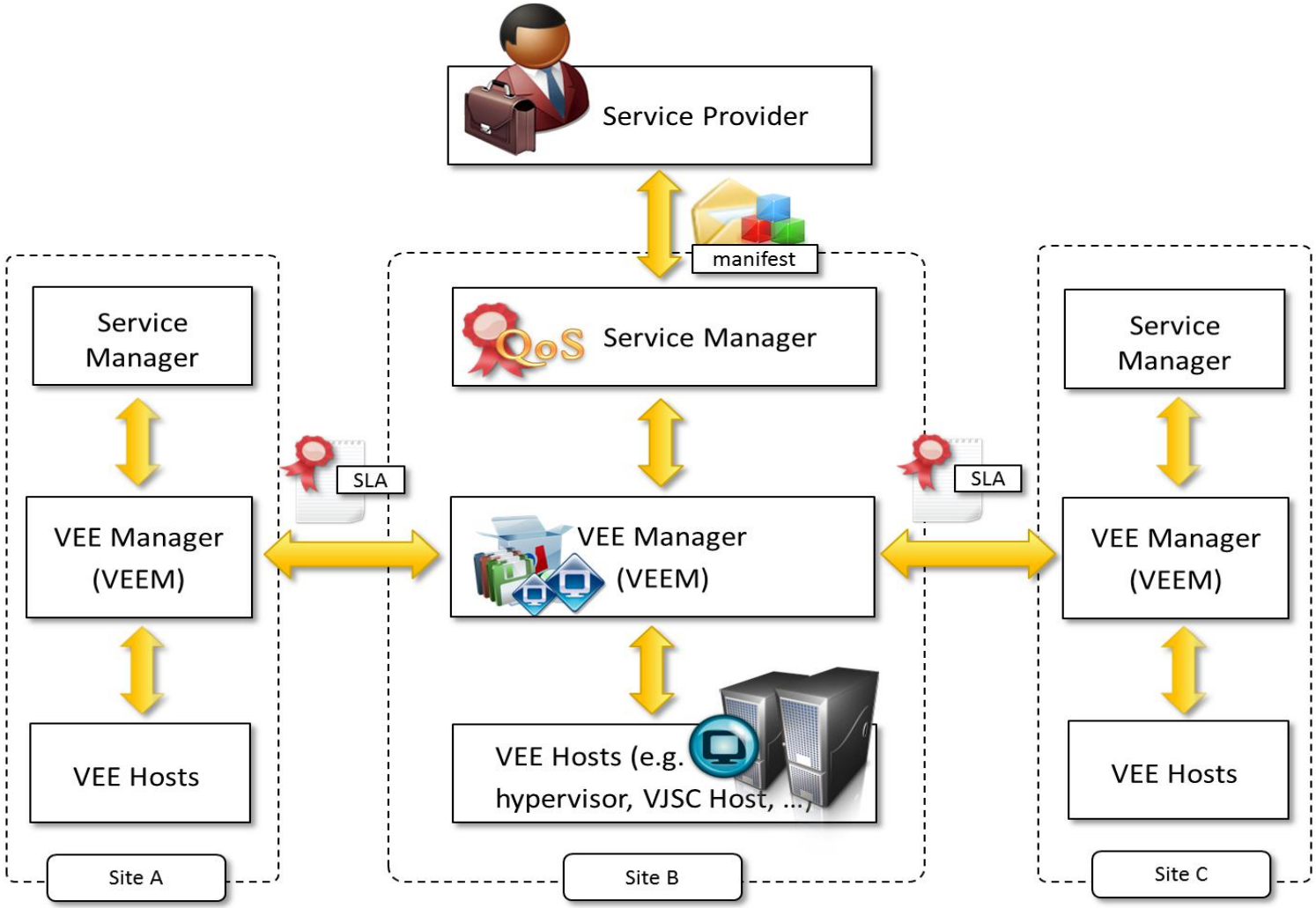


Reservoir Cloud Deployment

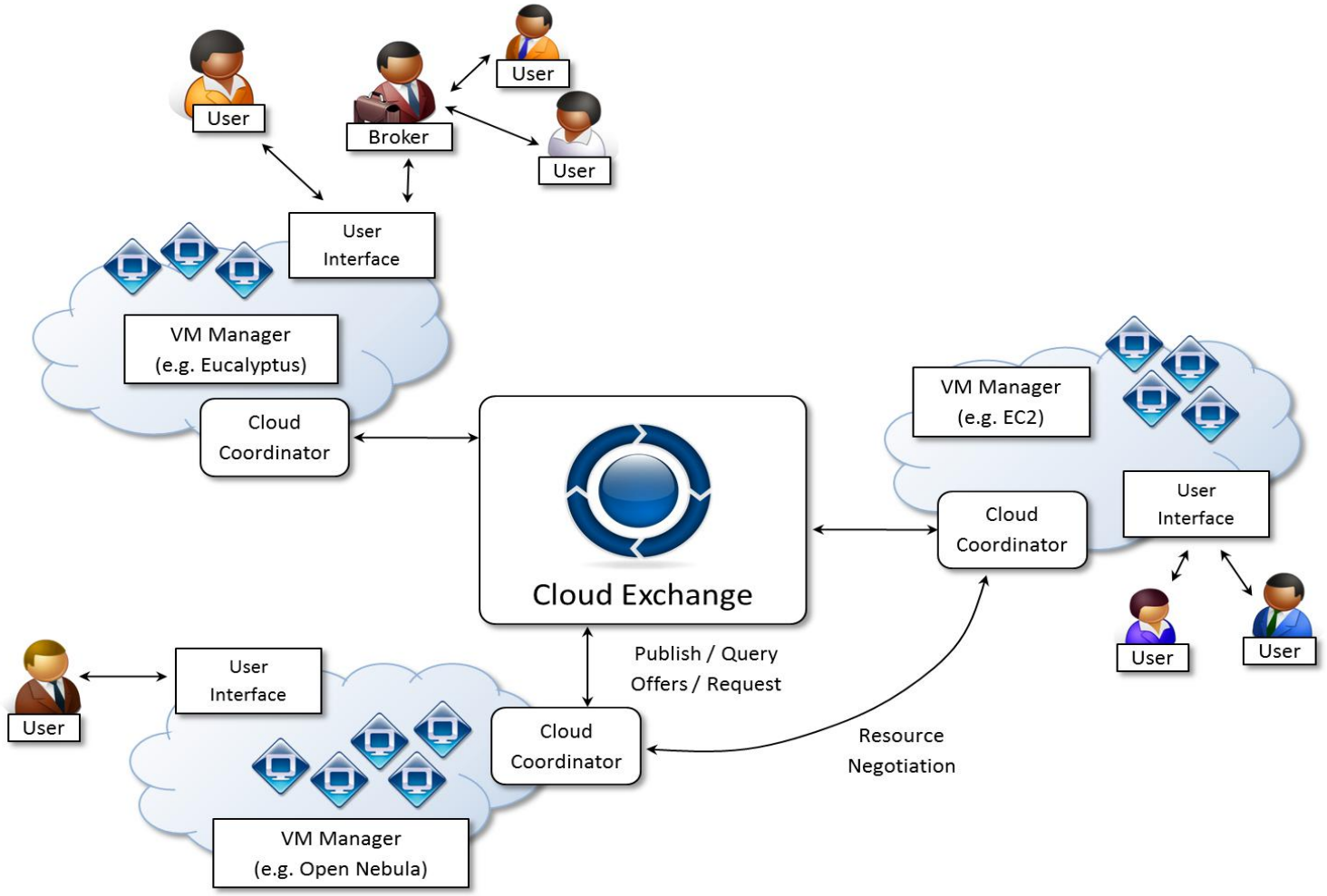
- European project
- Dynamic federation



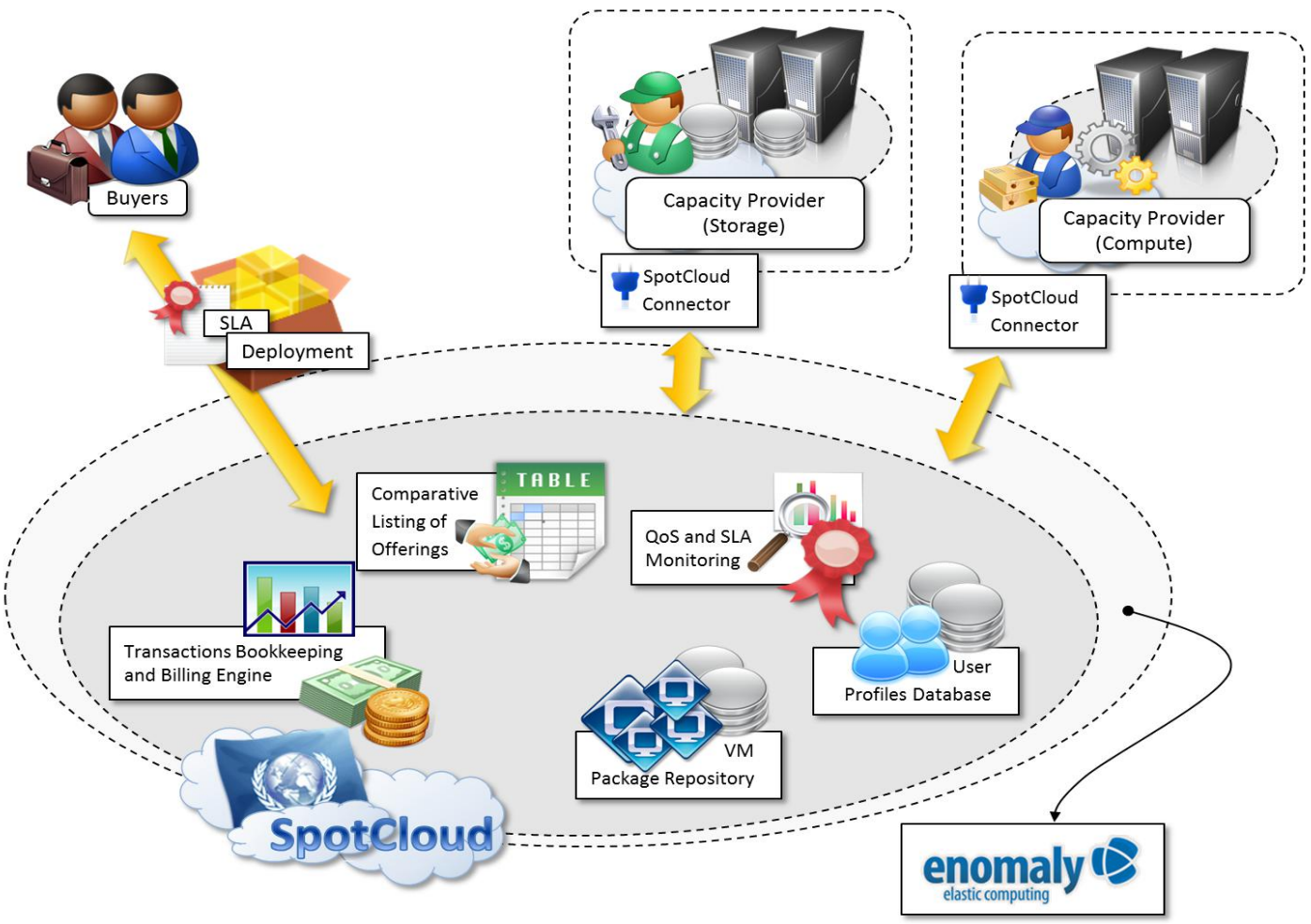
Reservoir Cloud Architecture



InterCloud


User
Broker
User
User
User Interface
VM Manager
(e.g. Eucalyptus)
Cloud Coordinator
Cloud Exchange
VM Manager
(e.g. EC2)
Cloud Coordinator
User Interface
User
User
User
User Interface
Cloud Coordinator
VM Manager
(e.g. Open Nebula)
Publish / Query
Offers / Request
Resource
Negotiation

SpotCloud


Buyers
SLA
Deployment
Capacity Provider (Storage)
SpotCloud Connector
Capacity Provider (Compute)
SpotCloud Connector
Comparative Listing of Offerings
TABLE
QoS and SLA Monitoring
Transactions Bookkeeping and Billing Engine
User Profiles Database
VM Package Repository
SpotCloud
enomaly
elastic computing