Cloud Computing & Security

Kyle Lai
CISSP, CSSLP, CISA, CIPP/G
KLC Consulting, Inc.
Cell: 617-921-5410
Email: klai@klcconsulting.net

Cloud Computing History

- Distributed Computing , Web Computing , Parallel Computing, Cluster Computing, Grid Computing
- 1999 - Distributed Computing Example:
  - Build a super-computer with small computers
  - SETI@Home (Search for Extra-Terrestrial Intelligence) – UC Berkley project
  - Volunteers donate their their home computer's extra processing power
- Name was too techie, too complicated.
- Need a name that's easy, catchy, good for headline – CLOUD (Amazon CEO, Jeff Bezos, made it famous in 2007)
- 2010 – Wikipedia, Google, Facebook – similar distributed computing model, just without volunteers.

KLC COUNSULTING

What is Cloud Computing

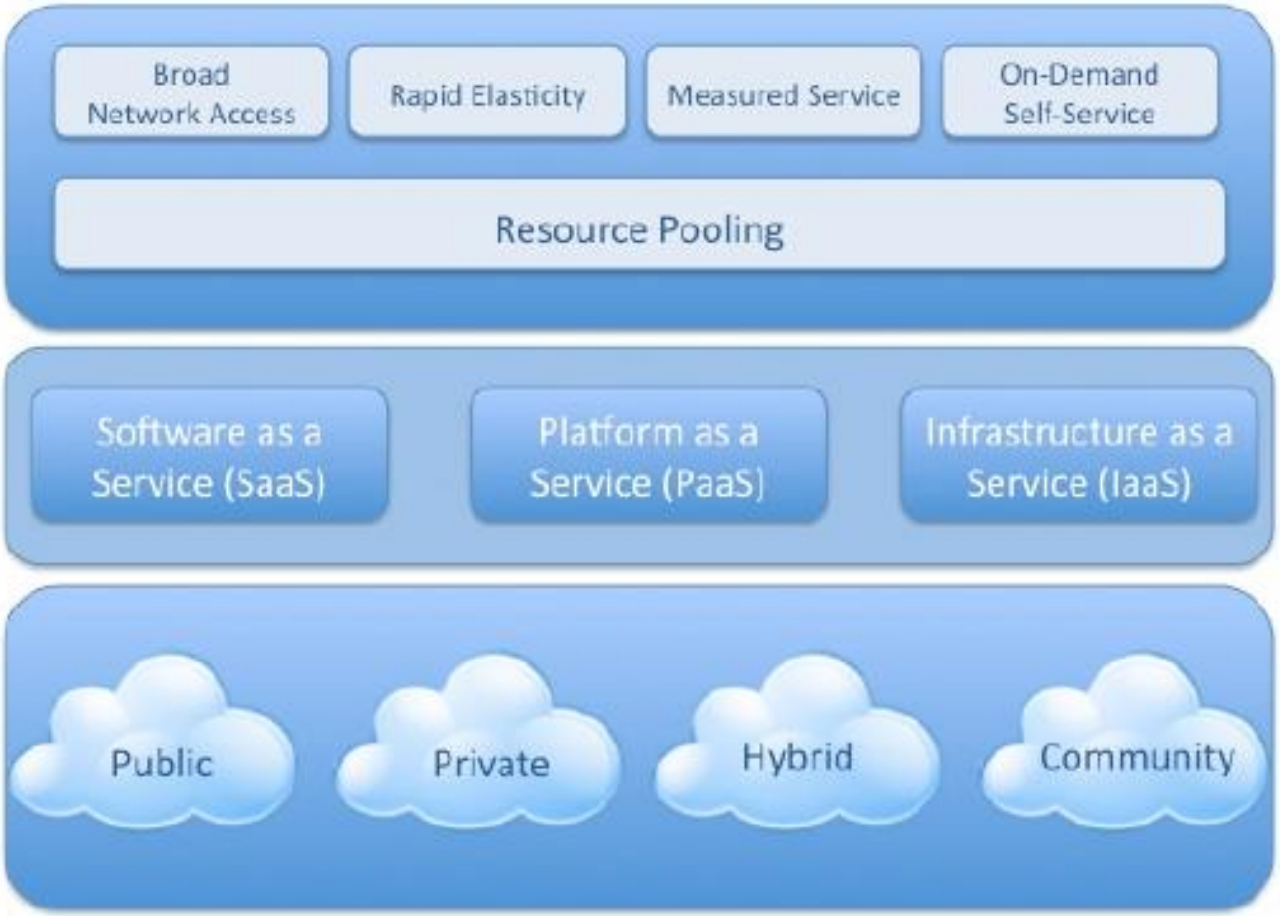
- Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential **characteristics,** three **service models**, and four **deployment models**. (NIST definition)

- Cloud enhances collaboration, agility, scalability, availability, and provides the potential for cost reduction through optimized and efficient computing.

KLC COUNSULTING

What is Cloud Computing (cont.)

Visual Model Of NIST Working Definition Of Cloud Computing
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html



KLC COUNSULTING

Cloud Service Models

- Software as a Service (SaaS)
  - Use provider's applications over a network
    - Salesforce.com, gmail, Facebook, Twitter, Google Apps
- Platform as a Service (PaaS)
  - Deploy customer-created applications to a cloud
    - AppEngine from Google: based on Python and Django
    - Force.com from SalesForce: based on the SalesForce SaaS infrastructure and Apex language
- Infrastructure as a Service (IaaS)
  - Rent processing, storage, network capacity, and other fundamental computing resources
    - Amazon EC2, S3 storage service

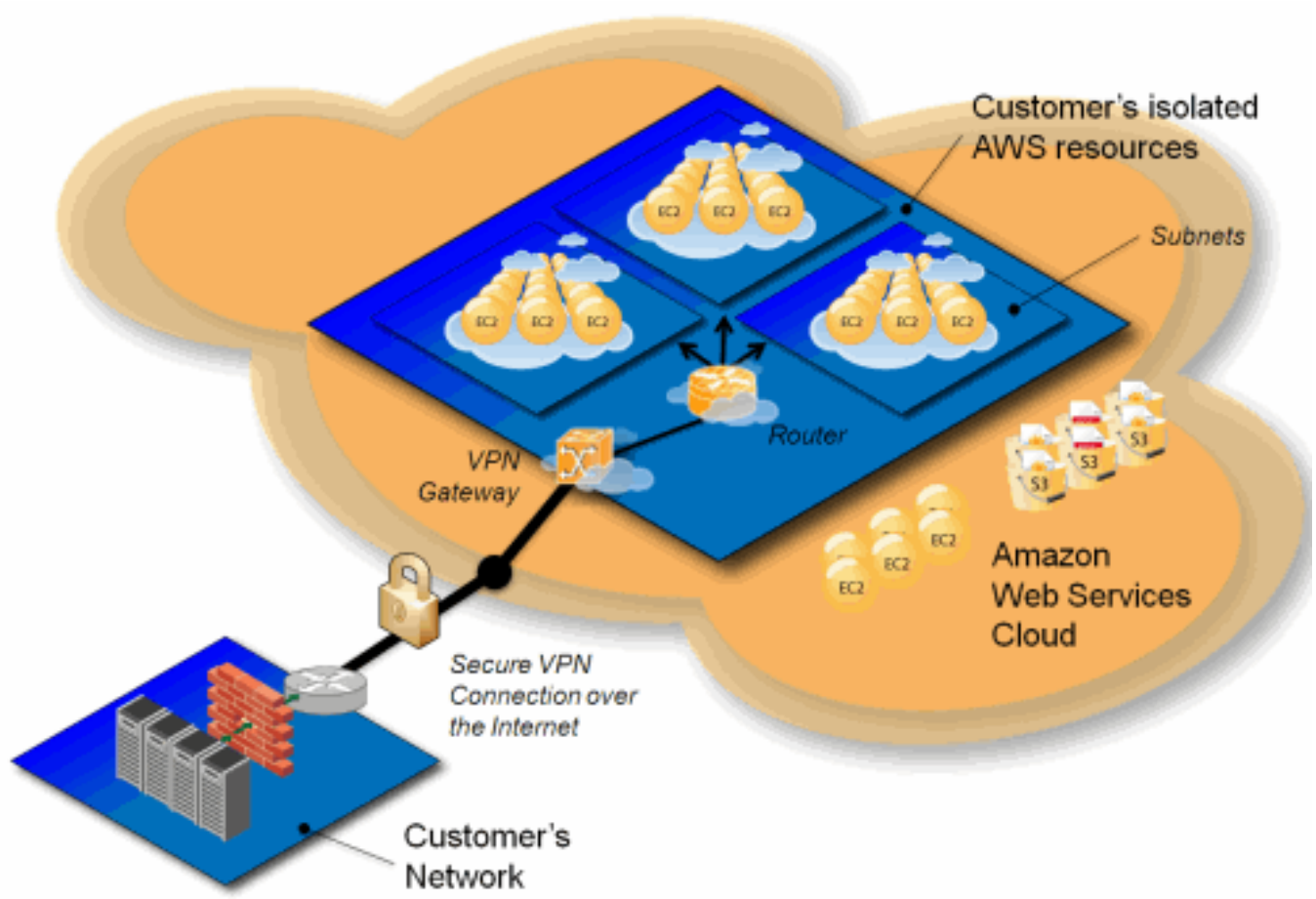
KLC COUNSULTING

Cloud Deployment Models

- Private cloud
  - enterprise owned or leased
- Community cloud
  - shared infrastructure for specific community
    - i.e. DISA RACE (Dept. of Defense Community Cloud)
- Public cloud
  - sold to the public, mega-scale infrastructure
    - i.e. Google, Amazon, Microsoft cloud services
- Hybrid cloud
  - composition of two or more clouds
- Virtual Private Cloud (** not in NIST definition)
  - use public cloud in private manner and interconnect to private datacenter resources via VPN

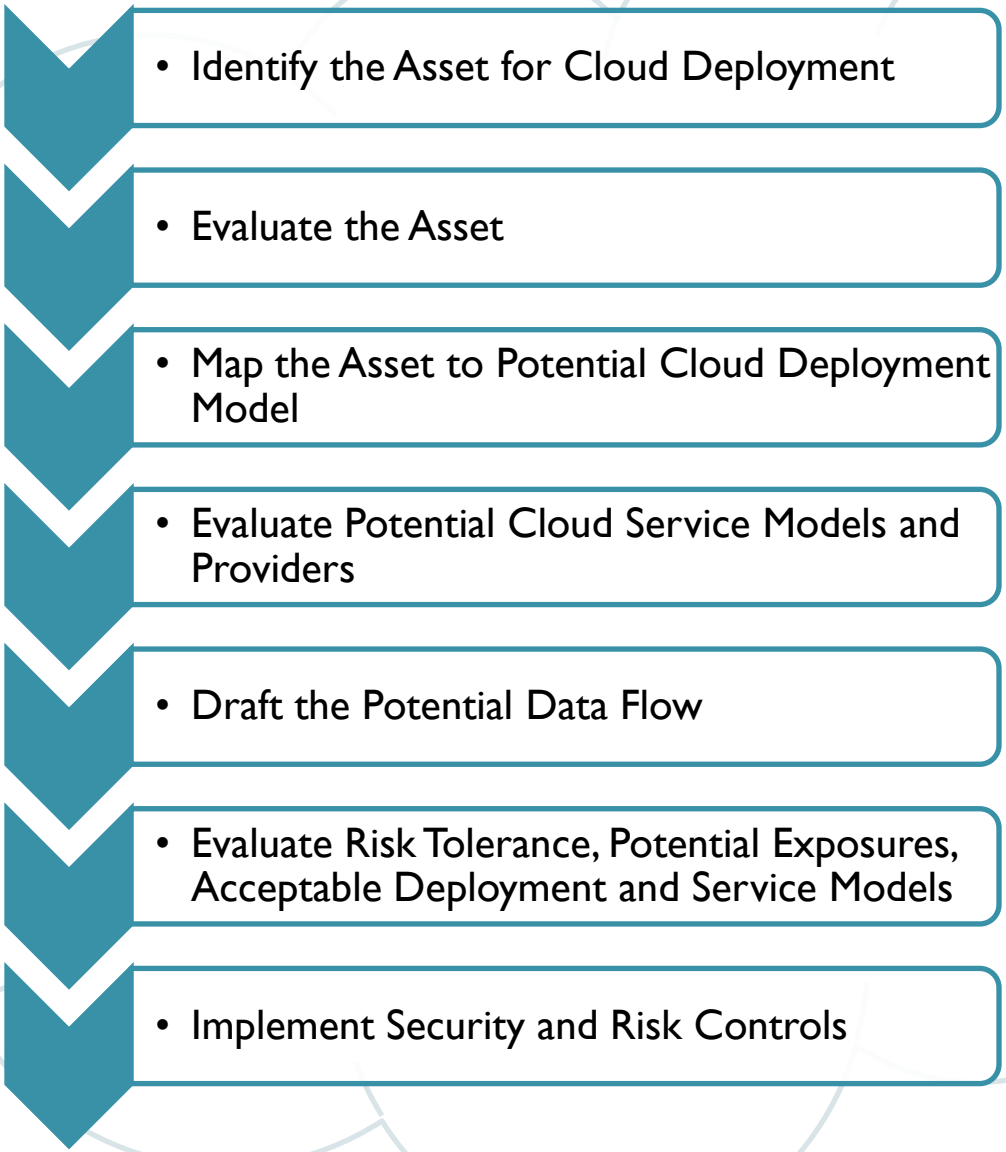
KLC COUNSULTING

Virtual Private Cloud



A diagram of Amazon Virtual Private Cloud and how it connects cloud-based resources to existing private networks.

What It Takes to Move to the Cloud



KLC COUNSULTING

Cloud Security – Areas of Focus*

- Governance & Enterprise Risk Management
- Legal & e-Discovery
- Compliance & Audit
- Information Lifecycle Management
- Portability & Interoperability
- Business Continuity & Disaster Recovery
- Incident Response, Notification, & Remediation
- Application Security
- Encryption & Key Management
- Identity & Access Management
- Virtualization – Cloud Service Provider's VM environment

*based on Cloud Security Alliance (CSA) Security Guidance Domains

KLC COUNSULTING

Cloud Security – Sample Questions

- Some questions to answer between Cloud Service Providers (CSP) and you:
  - Data ownership – When you put data to CSP's environment, who owns data in cloud? Make sure you are comfortable with the arrangement!
  - Service Level Agreement – what's reasonable downtime / uptime?
  - US and International Privacy Laws – where does the data reside?
  - Security of Virtual Operating Systems – how does CSP manage them?
  - Encryption for admin access, application access, and data at rest – Is there a single key for all customers or one key per customer?
  - Availability of logs for accountability
  - Version control for the SaaS applications
  - Business Continuity and Disaster Recovery Planning for cloud
  - Compliance (HIPAA, PCI, SOX, SAS70, FISMA, FFIEC, Privacy)
  - Review CSP's SAS 70 Report – verify effective security measures are in place

KLC COUNSULTING

Cloud Computing Security (Cont.)

- Some questions to answer between Cloud Service Providers (CSP) and you (Continue):
  - Understand the responsibilities between CSP and you – Understand what you need to do. Read User Controls Consideration section in SAS 70 report
  - Plan for expected and unexpected termination of CSP contract
  - Retrieve data from CSP – understand how you get all your data back?
  - Delete data in the cloud (Data remanance) – data is really destroyed or CSP just made it inaccessible to you?
  - Monitoring CSP service performance
  - Vulnerability Assessment on the CSP – ensure sound security
  - Switching CSP – how easy is it? (in event of degrading service, cease of bus)
  - Incident response, notification and remediation – what is the CSP's procedure?
  - Legal e-Discovery
- Refer to CSA Cloud Security Guide for more details: http://www.cloudsecurityalliance.org/csaguide.pdf

KLC COUNSULTING

Cloud Security References

- Cloud Security Alliance (CSA) - http://www.cloudsecurityalliance.org/
- CSA's Cloud Security Guide - http://www.cloudsecurityalliance.org/csaguide.pdf
- ENISA – Cloud Computing Risk Assessment - http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment
- Cloud Computing Use Cases Group – common use cases - http://www.cloudusecases.org/
- NIST Cloud Computing Group – http://csrc.nist.gov/groups/SNS/cloud-computing/index.html
- GAO Report: Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing - http://www.gao.gov/products/GAO-10-513
- GAO Testimony: Information Security: Government-wide Guidance Needed to Assist Agencies in Implementing Cloud Computing - http://www.gao.gov/new.items/d10855t.pdf
- Gartner: Know Your Rights in IT Maintenance and Cloud Computing - http://www.gartner.com/DisplayDocument?doc_cd=201001&ref=g_sitelink&ref=g_noreg
- Gartner Free Report: Rights and Responsibilities for Consumers of Cloud Computing Services - http://www.gartnerinsight.com/Landing.aspx?WT.mc_id=PCP_GITCLD
- PCWorld: Lawmakers Question the Security of Cloud Computing
- Pew Report: The Future of Cloud Computing

KLC COUNSULTING

KLC Consulting Overview

- KLC was founded in 2002
- SBA **8(a)** Certified Small Business
- Navy **Seaport-e** Contract Vehicle
- Past Performance: DoD, DISA, VA, NIH
- Participates in Cloud Security Alliance (CSA) projects
- Focus on providing Information Assurance / Security and IT Audit services to government and Fortune 1000 companies.
- Dedicated consultants at Central, East and West Coast
- KLC staff hold certifications including CISSP, CSSLP, CISM, CISA, CIPP/G, CCNA, CCNP, CCSP, MCSE, ISO 27001 Lead Auditor.
- Most of KLC Consultants are Infragard Members (passed FBI Security Background Check) with at least 8 years of experience
- KLC also publishes SMAC, a popular network privacy and security software with more than 1.5 Million users worldwide

KLC COUNSULTING

Questions?
Next step?

Kyle Lai
President
617-314-9721
klai@klcconsulting.net

Tarek El Heneidy
Director of Operations
781-424-2257
telheneidy@klcconsulting.net