Are You the Locksmith of Your Cloud?

Key Management Challenges in a Cloud Ecosystem

– A Discussion Starter Based on the Cloud Security WG's Research -

Dr. Michaela Iorga, *NIST (presenting)*
Anil Karmel, *C2 Lab, Inc. (presenting)*
Juanita Koilpilai, *Waverley Labs*

March 04, 2014

Disclaimer

- *No official endorsement of any particular product or brand is implied or intended.*
- *Any logos, brand names or characters depicted remain the property of their owners.*
- *The views expressed in this presentation are those of the presenters and not necessarily the views of the U.S. Government.*

Cloud Demystified

- What is Cloud Computing - Definition (NIST 800-145)
  - *"Cloud computing is a model for enabling ubiquitous, 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."*

Composed of :

- *5 essential characteristics (On-demand self service, Broad network access, Resource pooling, Rapid elasticity, Measured services.*
- *3 service models: Infrastructure-aaS (IaaS), Platform-aaS (PaaS), Software-aaS (SaaS);*
- *4 deployment models: Private, Public, Community, Hybrid*

Cloud Forecasts

Vivek Kundra, Federal CIO, *Cloud First Policy, 2012*

(paraphrasing Sir Arthur Eddington)

*"Cloud computing will not just be more innovative than we imagine; it will be more innovative than we **can** imagine".*

GigaOM

- *Total worldwide addressable market for cloud computing will reach $158.8 B by 2014*
- *An increase of 126.5% from 2011*

Gartner

- *By 2016 cloud will grow to become the bulk of new IT spend*

2013 Advanced Threat Report

Courtesy of FireEye

Relative to 2006, cyber crimes increased by 782%:

- *A malware activity every 3 minutes*
- *65% of attacks target financial services, healthcare, manufacturing and entertainment*
- *89% of callback activities were linked with Advanced Persistent Threat (APT) tools made in China or by Chinese hacker groups*

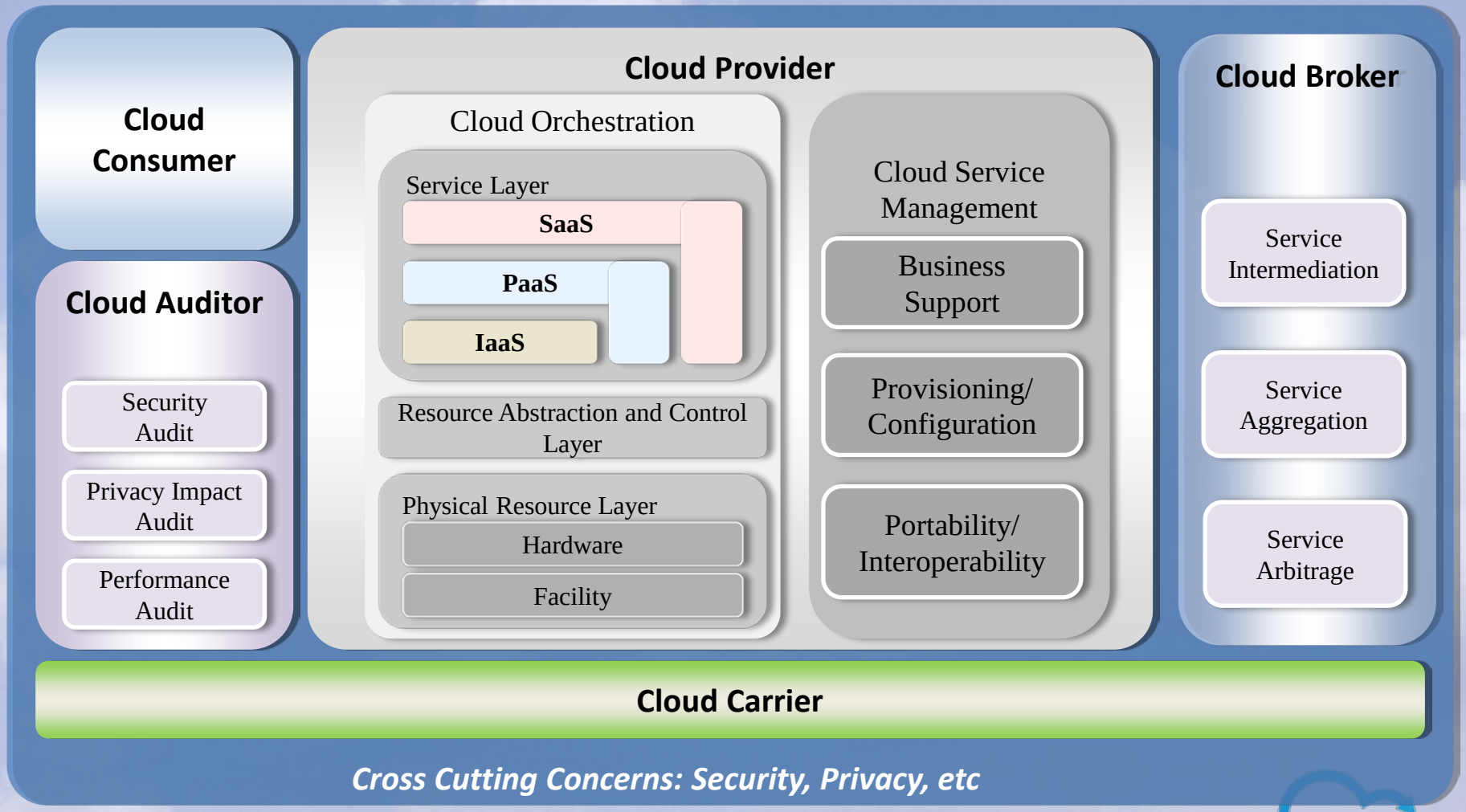
NIST Cloud Computing Special Publications

- CC Standards Roadmap ..... SP 500-291
- CC Reference Architecture..... SP 500-292
- USG CC Technology Roadmap..... SP 500-293
- CC Security Reference Architecture..... SP 500-299

- Guidelines on Security and Privacy ..... SP 800-144
- Definition of Cloud Computing ..... SP 800-145
- CC Synopsis & Recommendations..... SP 800-146
- Trusted Geo-location in the Cloud.....NISTIR 7904
- Key Management Challenges..... NISTIR 7956 *(just starting!)*

NIST CC Reference Architecture (SP 500-292)

with Cross Cutting Concerns shown



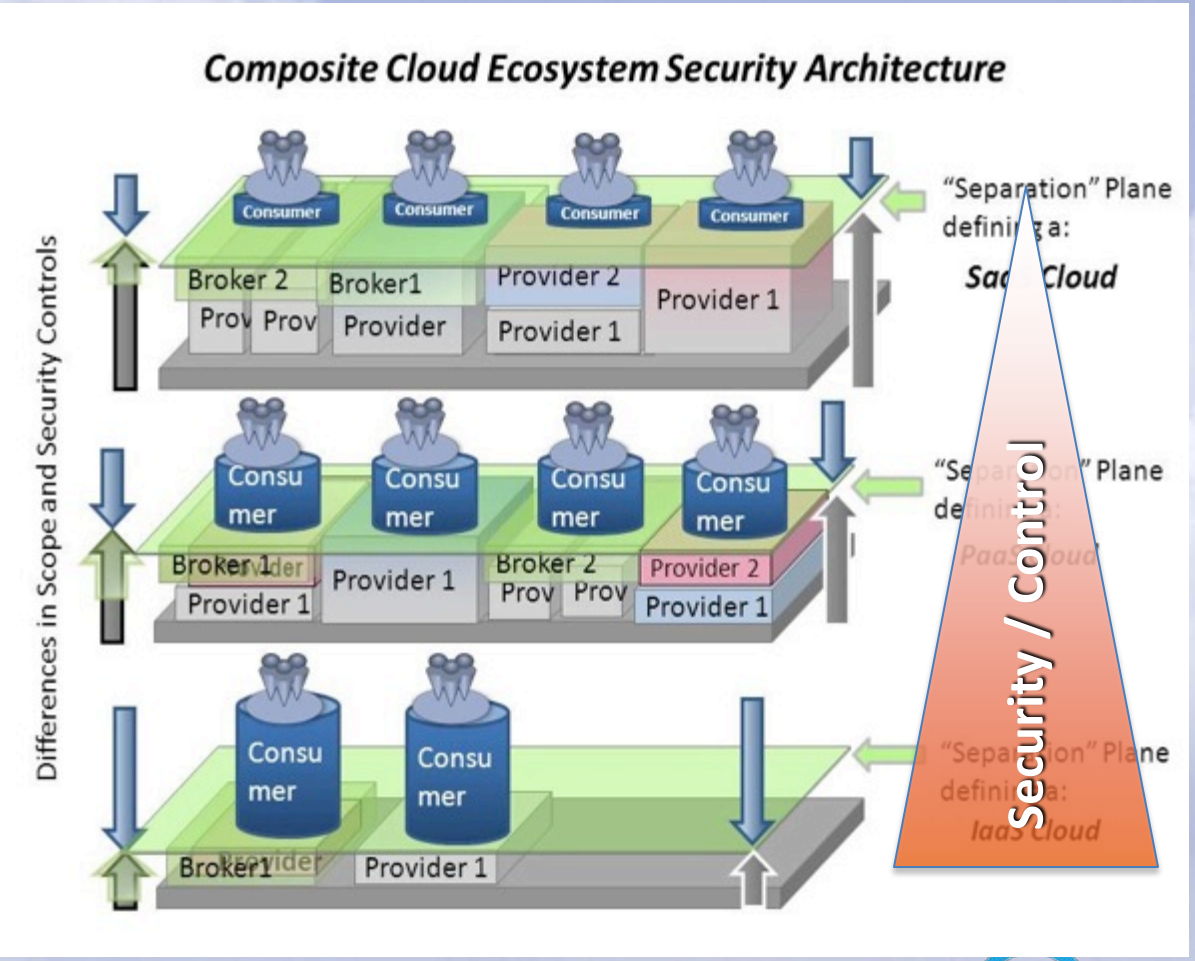
Cloud Demystified

- What is a Cloud Ecosystem

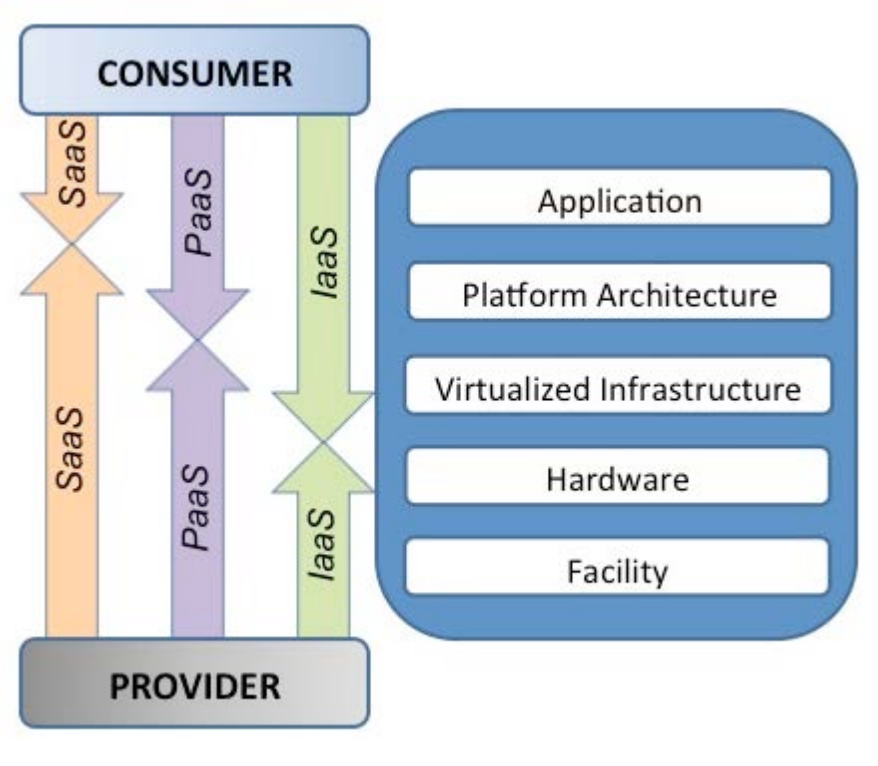
Software as a Service

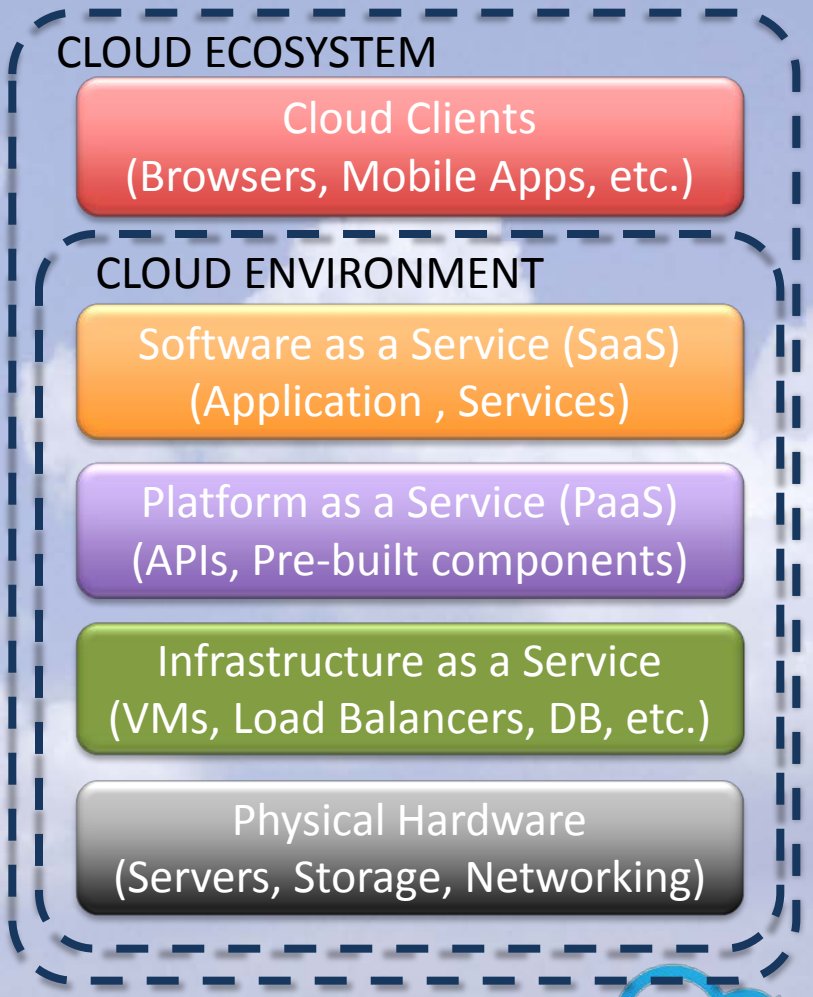
Platform as a Service

Infrastructure as a Service

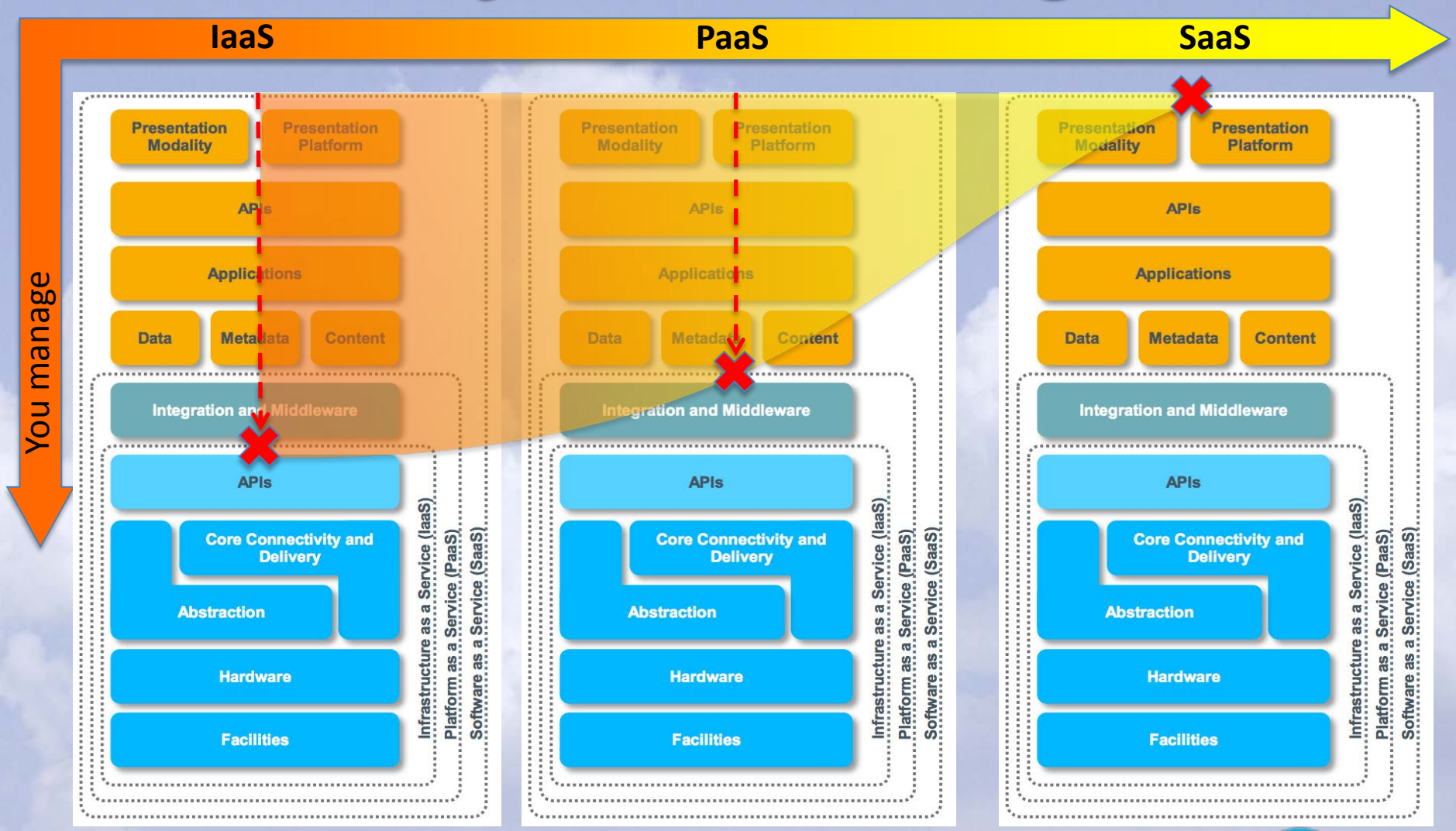


Distributed Architecture = Split Control / Responsibilities



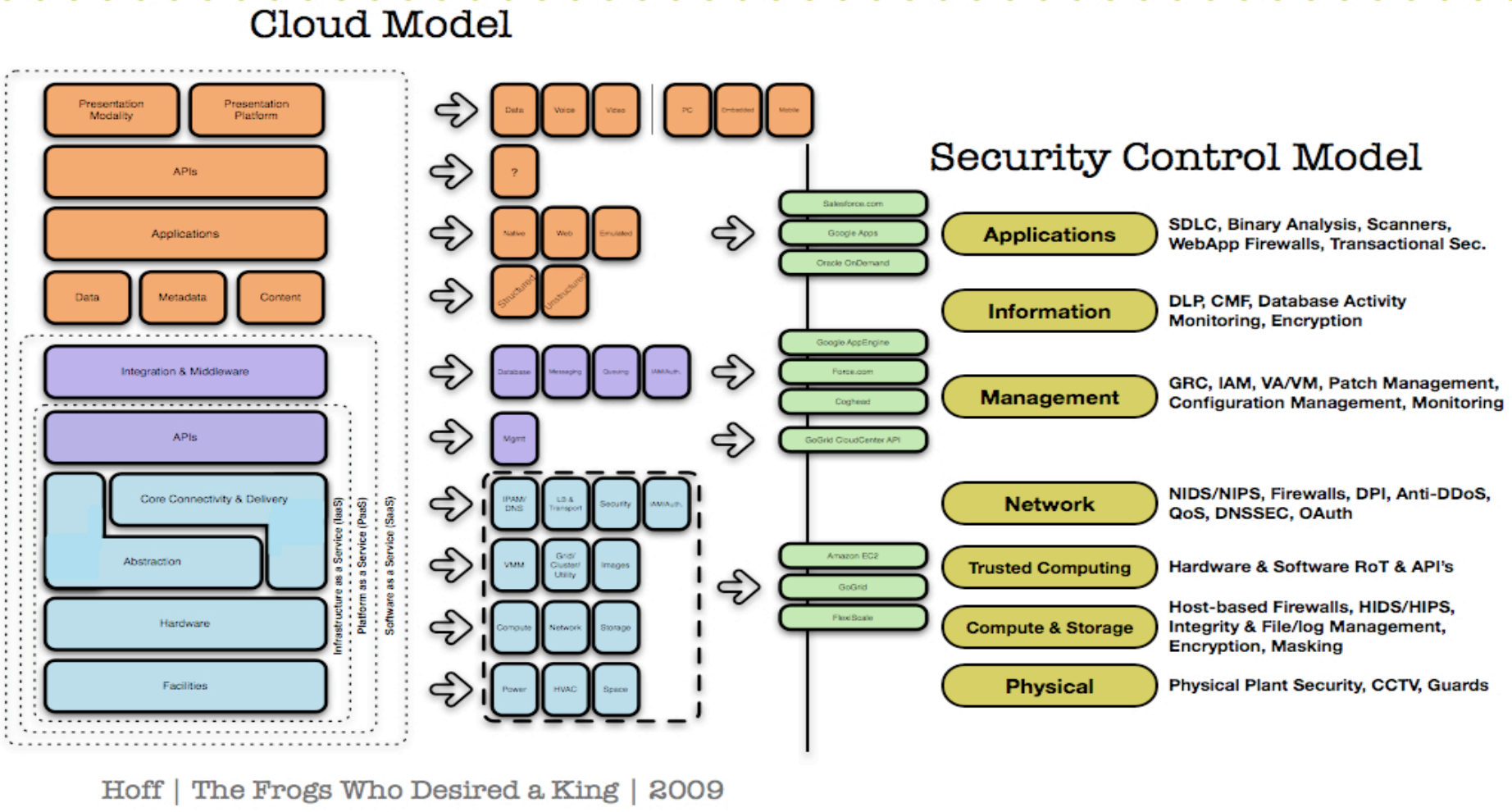


What you can manage…



Stack image source: Cloud Security Alliance specification, 2009

Mapping the Model to the Metal



Hoff | The Frogs Who Desired a King | 2009

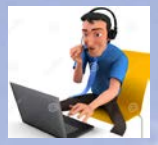
Use Case: Storage of Data in the Cloud (UC6)

- Store application data securely ⇔ Encrypt it (easy to say! what does it take to do it?).

- Encrypting a Database in the Cloud – can be done:
  - Transparent/External Data Encryption
  - DB-level or User-level Encryption

Where All the Magic Happens…

(different Cloud service models)



Client Data

T

T1

T2

T3, T4

T5

T6

T7

Data, Voice,

UI

Web

Application

Strct Data

UnStrct Data

DBM

KS

VM

Mngmt

Transport, Security

VMM

Storage

Physical Space

Hardware Sec Module

Presentation Modality

Presentation Platform

APIs

Applications

Data

Metadata

Content

Integration and Middleware

APIs

Core Connectivity and Delivery

Abstraction

Hardware

Facilities

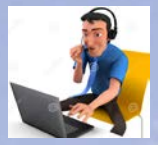
Infrastructure as a Service (IaaS)

Platform as a Service (PaaS)

Softw as a Se ce (Sa

Where All the Magic Happens…

(different system architectures)



Client Data

T

T1

T2

T3, T4

T5, T6

T7

Presentation Modality

Presentation Platform

APIs

Applications

Data

Metadata

Content

Integration and Middleware

APIs

Core Connectivity and Delivery

Abstraction

Hardware

Facilities

Infrastructure as a Service (IaaS)

Data, Voice,

UI

Web

Application

Strct Data

UnStrct Data

DBM

KS

VM

Software Sec Module

Mngmt

Transport, Security

VMM

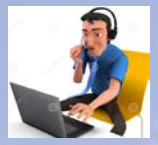
Storage

Software Sec Module

Physical Space

Where All the Magic Happens…

(different system architectures)



Client Data

T

T1

T2

T3, T4

T5

Presentation Modality

Presentation Platform

APIs

Applications

Data

Metadata

Content

Integration and Middleware

APIs

Core Connectivity and Delivery

Abstraction

Hardware

Facilities

Infrastructure as a Service (IaaS)

Data, Voice,

UI

Web

Application

Strct Data

UnStrct Data

DBM

VM

Mngmt

Transport, Security

VMM

Storage

Physical Space

KS

S/F/H Sec Module

Software/ Firmware/ Hardware

NIST National Institute of Standards and Technology U.S. Department of Commerce

NIST Cloud Computing Program

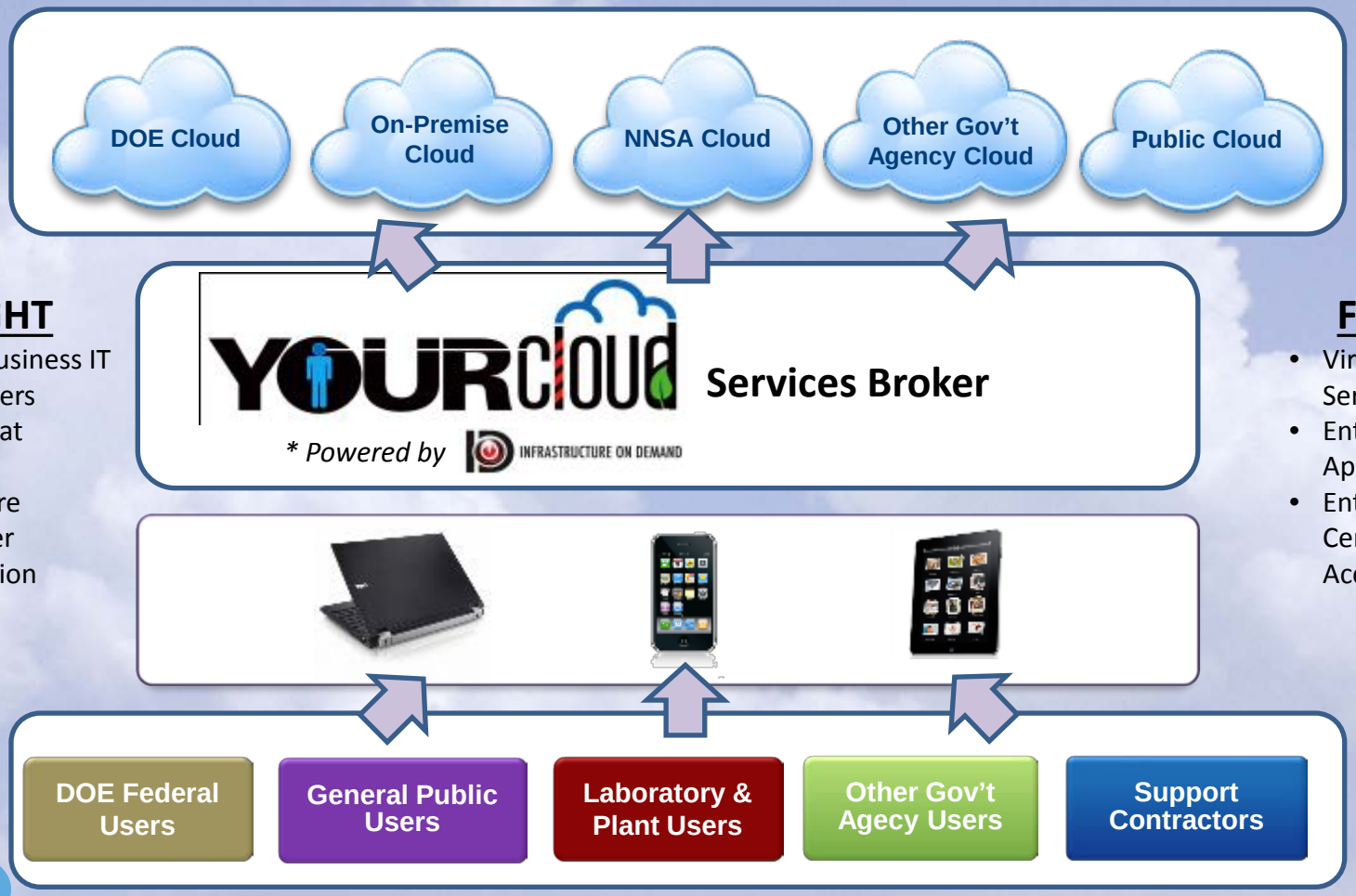
A Real-Life Implementation and the Challenges Encountered:

DOE's YOURcloud - A Cloud Services Broker

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST Cloud Computing Program

DOE YOURcloud: A Cloud of Clouds approach brokering any organization, through any device, to any service respectful of site autonomy



INSIGHT

- Green & Business IT Smart Meters
- PortfolioStat
- Enterprise Architecture
- Data Center Consolidation

FEATURES

- Virtual Desktops & Servers
- Enterprise Application Store
- Enterprise Certification & Accreditation

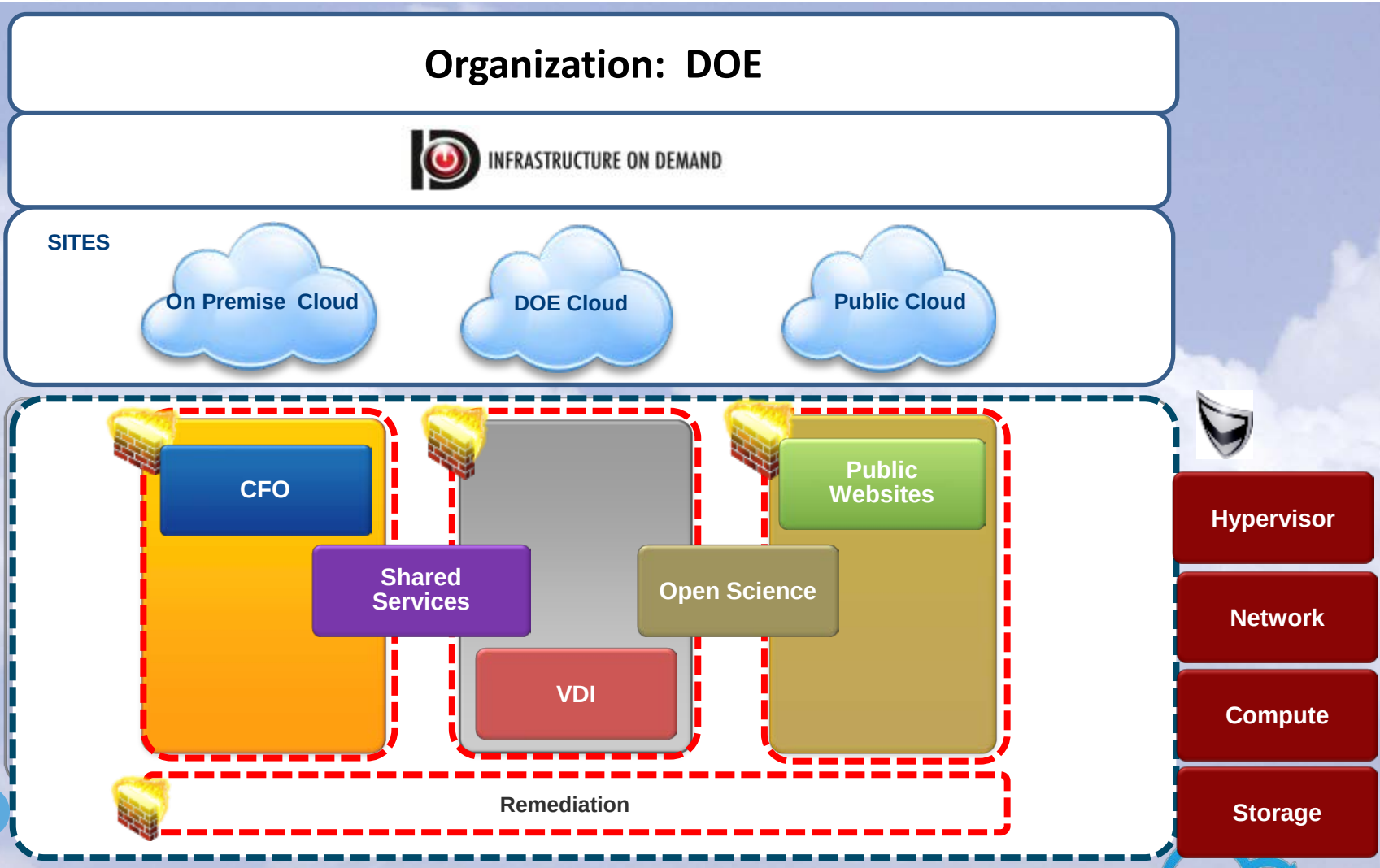
Anil Karmel | Building YOURcloud | 2013

NIST National Institute of Standards and Technology U.S. Department of Commerce

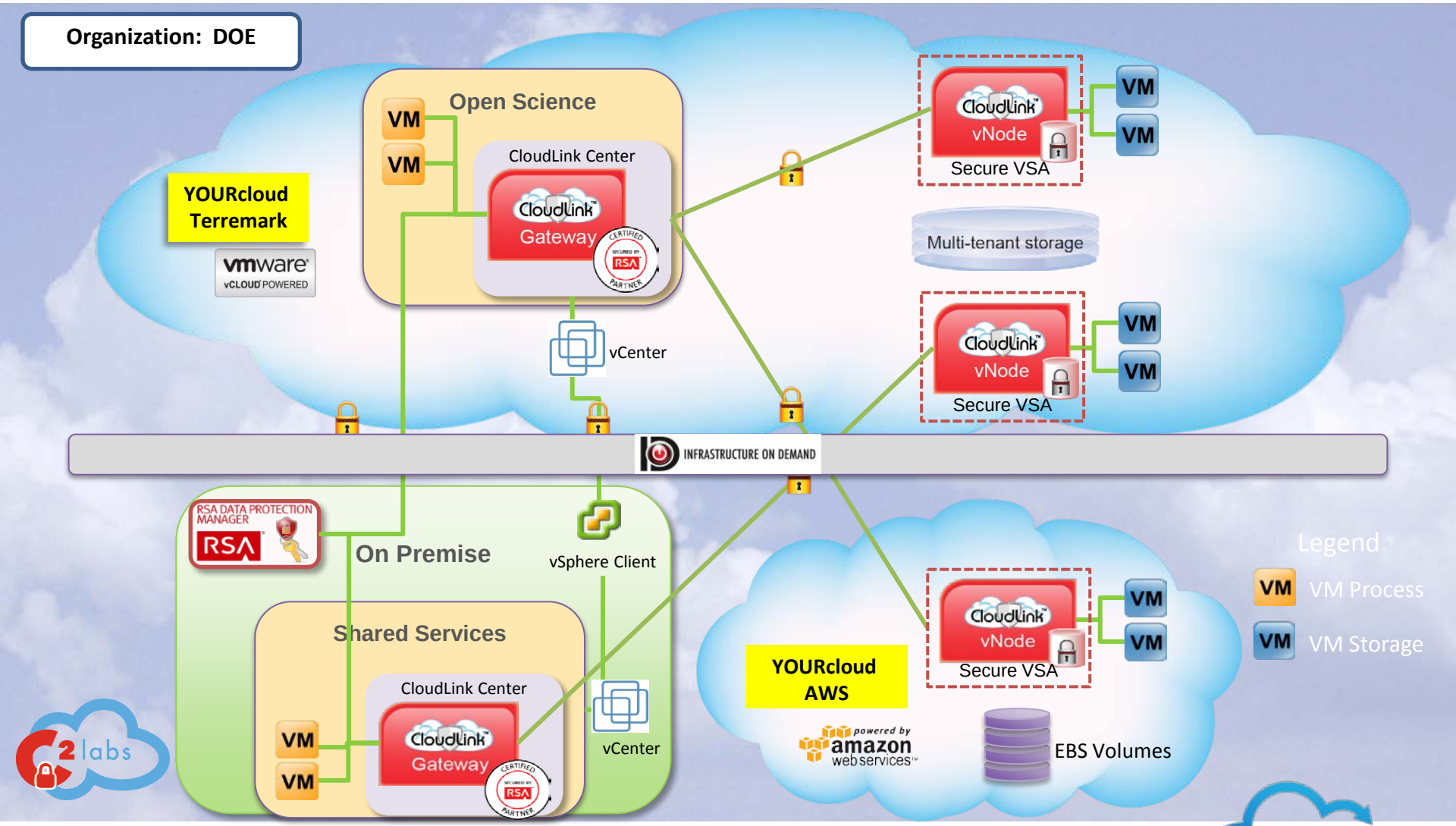
NIST Cloud Computing Program

Services Broker Enclaves

Anil Karmel | Building YOURcloud | 2013



UC6 – Storage of Data in the Cloud



Questions?

Thank you !

Contributors:

- *Aradhna Chetal*
- *Juanita Koilpilai (lead)*
- *Prabha Kumar*
- *Chan Lim*
- *Dylan Lobo*
- *Ginger Ross*
- *Go Yamamoto*

Discussion of the FCKMS with a Cloud Ecosystem in Mind

Reviewers:

Wayne Armour
Vince Grimaldi
Yin Lee
Mark Potter
Ken Stavinoha

Bill Butler (presenting)
Nancy Landreville
Dylan Lobo
Virginia Ross

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST Cloud Computing Program

Cloud Challenges to Implementing FCKMS (1/4)

The team was tasked with reviewing NIST Publication 800-152 *"A Profile for U. S. Federal Cryptographic Key Management Systems (FCKMS)"* to identify challenges to implementing a FCKMS in the cloud environment from the *"FCKMS procurers, installers, configuration personnel, administrators, managers, operators, and users"* perspective.

Cloud Challenges to Implementing FCKMS (2/4)

- Step 1 Review 10 chapters (4-14)
- Step 2 Identify challenges, comment and compile to capture sheet
- Step 3 Characterize each cloud challenge by 3 service models: Infrastructure-aaS, Platform-aaS, Software-aaS and 4 deployment models: Private, Public, Community, Hybrid
  - 12 possible combinations to analyze as future use cases)

Cloud Challenges to Implementing FCKMS (3/4)

- The team found **45** challenges within the 10 chapters; discussed and tagged them **4-1 to 12-7** (Chapter, Challenge).
- **4 Security Policies:**
  4-1 Identification and Categorization of information to be protected (e.g. Tagging)
  5 Roles and Responsibilities:
  5-1 Definition of all Operational Roles within the CKMS
  6 Cryptographic Keys and Metadata
  6-1 CKMS metadata standards impact portability

My USG network is operated by Cloud Provider(s), Who is responsible for protecting my keys and metadata?

Challenges

My Cloud Providers are NOT interoperable, how do I build a enterprise wide FCKMS?

Public	Private	Community	Hybrid	IAAS	PAAS	SAAS
4-1 X	X	X	X	X	X	
5-1 X	X	X	X	X	X	X
6-1 X	X	X	X	X	X	X

Cloud Challenges to Implementing FCKMS (4/4)

4-1 Identification and Categorization of information to be protected (e.g. Tagging)

- Challenge: The Security policy MUST specify the level of protection for cryptographic keys, algorithms, and mechanisms that provide confidentiality and integrity protection for both the keys and their metadata in each unique service/deployment model (i.e. (Public, IaaS), (Hybrid, SaaS).
- **The next steps are to develop useful "*use cases*" to investigate the challenge in detail to inform SP 800-152 User Community**

Should we stick with private cloud and IaaS or go public and SaaS? The answer is always. It depends on the requirement

Decisions ??

Public	Private	Community	Hybrid	IAAS	S	SAAS
4-1 X	X	X	X	X		
5-1 X	X	X	X	X		X
6-1 X	X	X	X	X	X	X

Questions?

Thank you !

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST Cloud Computing Program