

# Cloud & Security

**Dr Debabrata Nayak**

**[Debu.nayak@huawei.com](mailto:Debu.nayak@huawei.com)**

# AGENDA

- **General description of cloud**
- **Cloud Framework**
- **Top issues in cloud**
- **Cloud Security trend**
- **Cloud Security Infrastructure**
- **Cloud Security Advantages / Challenges**
- **Compliance and certification of cloud security**
- **Cloud Security standard participation**
- **Summary**

# Cloud Computing



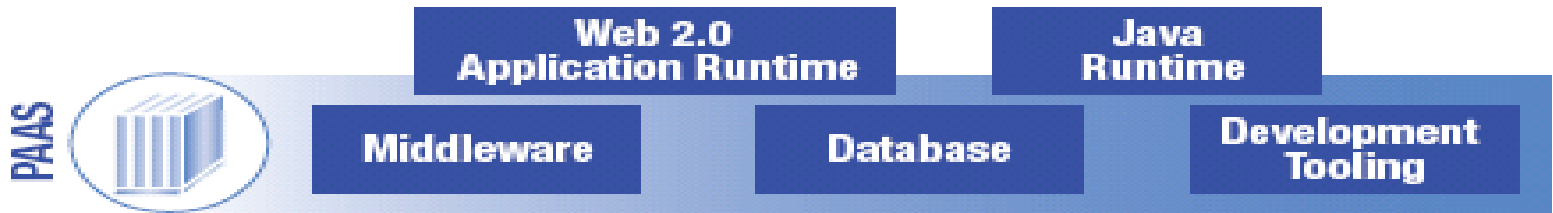
# What is Cloud Computing?

- Cloud Computing
  - 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
  - describes the use of a collection of services, applications, information, and infrastructure comprised of pools of computer, network, information, and storage resources
- NIST defines cloud computing by describing five essential characteristics and attribute
  - On-demand self-service (service-based)
  - Broad network access (uses internet technologies)
  - Resource pooling (shares a pool of resources)
  - Rapid elasticity (scalable and elastic)
  - Measured service (pay-as-you-go)
- NIST defines three cloud service models
  - PaaS (Platform as a Service)
  - IaaS (Infrastructure as a Service)
  - SaaS (Software as a Service)
- NIST defines four cloud deployment models
  - Private
  - Public
  - Community
  - Hybrid

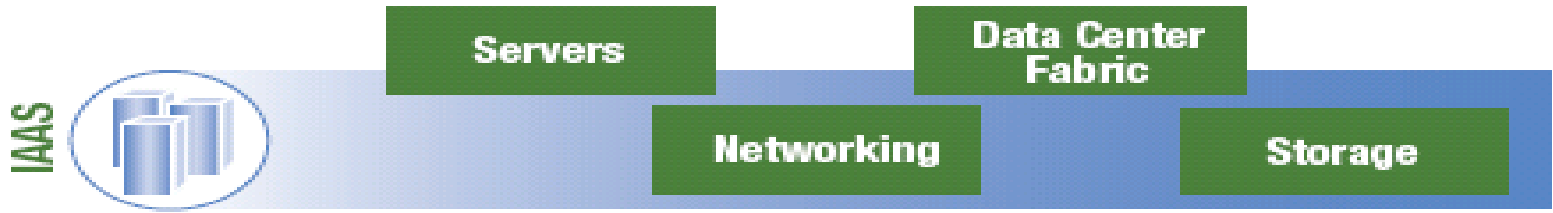
# Cloud Computing Models



Software as a Service

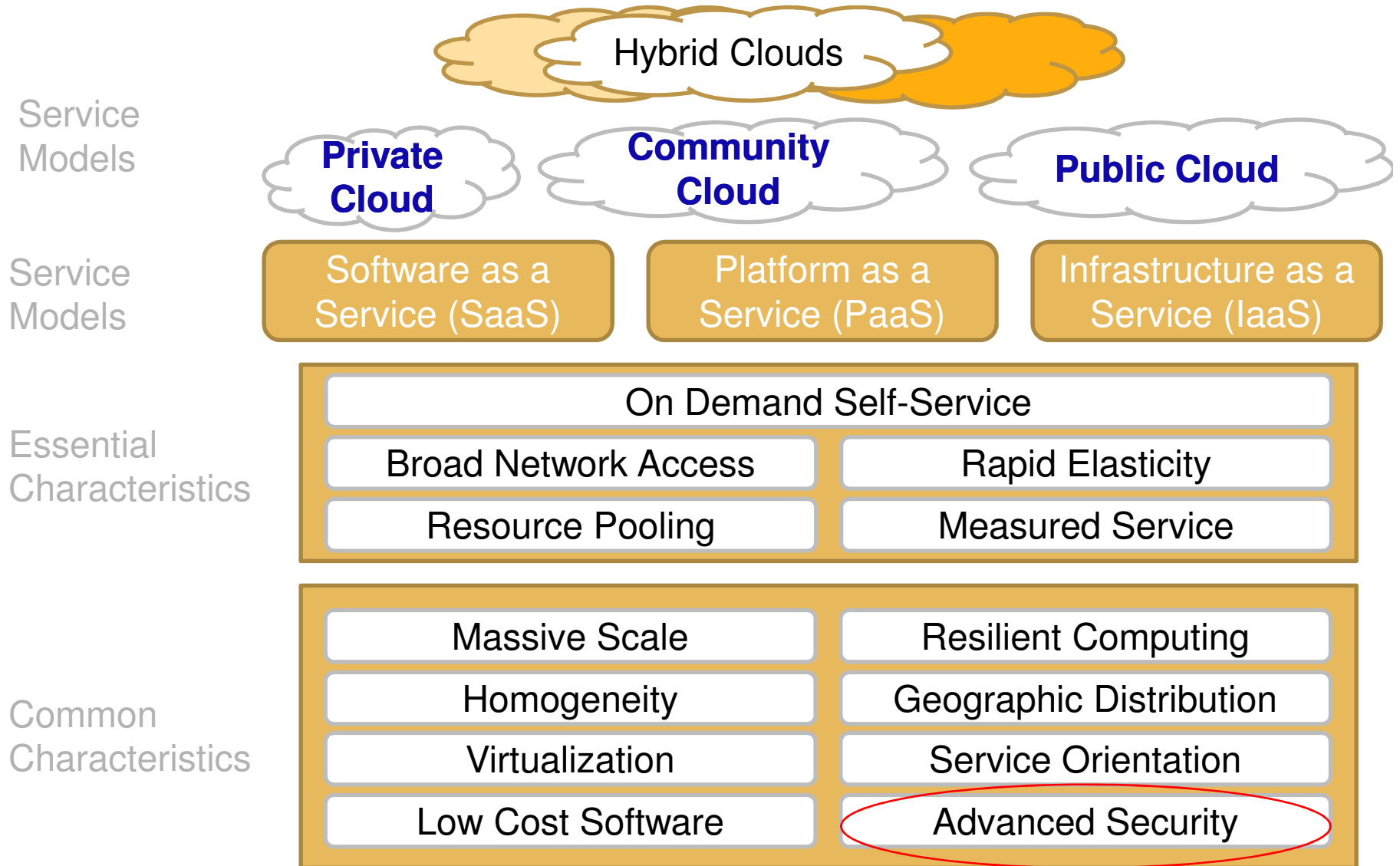


Platform as a Service

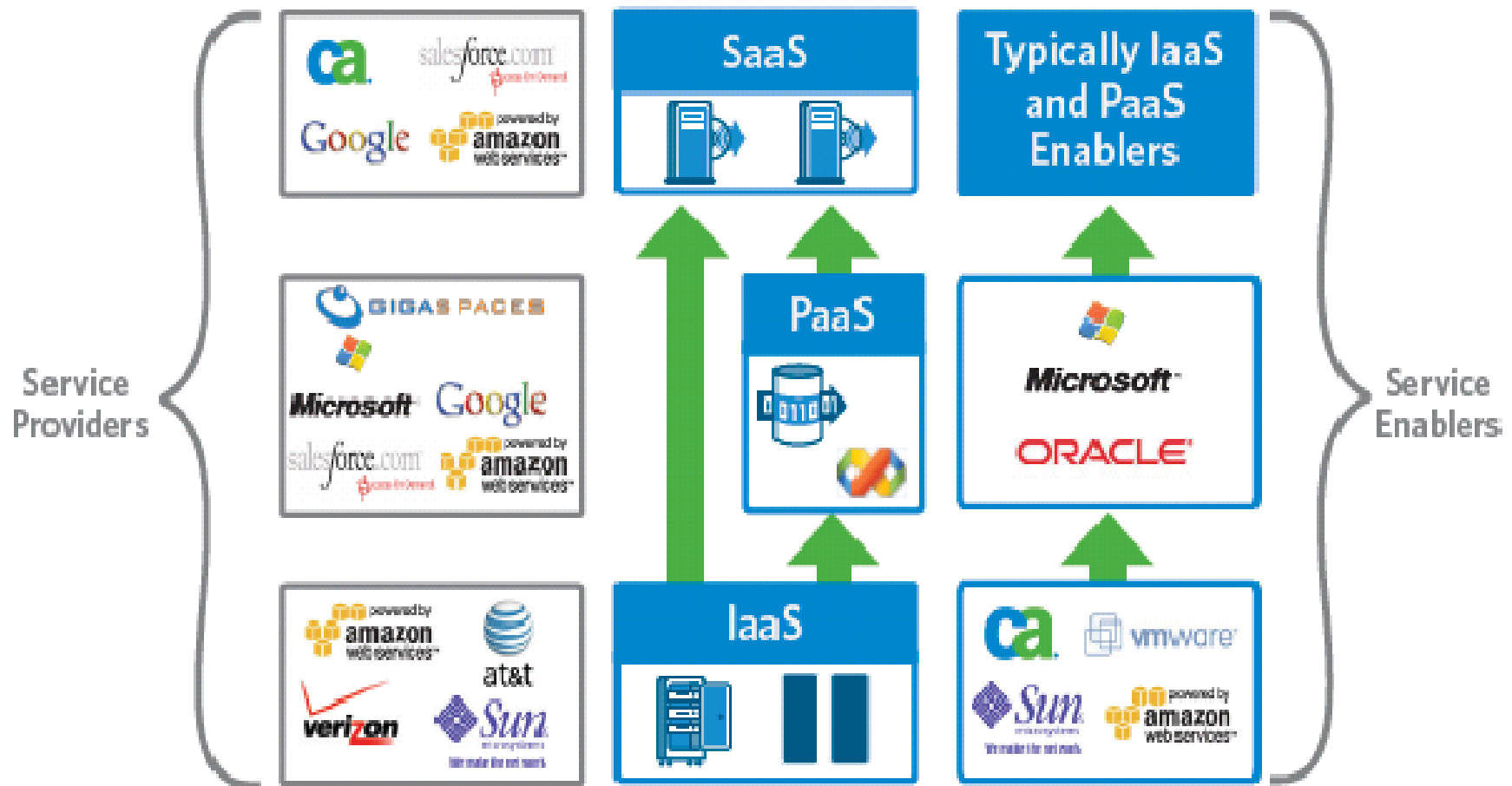


Infrastructure as a Service




# Cloud Framework



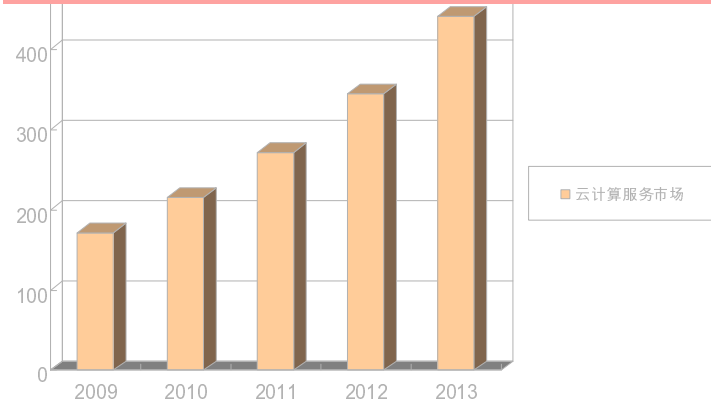
# Cloud Service Models Working Together



# The cloud security is getting lot of attention

<p><b>The cloud service raises For business</b></p>	<p><b>The cloud moves safely</b></p>
	<ul style="list-style-type: none"> <li>•cisco purchases with 183,000,000 US dollars <b>based on Web security</b> software company ScanSafe.</li> <li>•Cisco, NetApp VMware promote the end-to-end security multi-renters to design the construction,Strengthens sharing <b>private and the enterprise cloud environment security</b>.</li> </ul>
	<p>in December, 2009 IBM purchase database security company Guardium. This purchase causes IBM Corporation has obtained the Guardium Corporation's database safety work. According to IBM said that This purchase is an its information management strategic planning part, the IBM enterprise database The real-time monitor and the data protection will promote to a new level.</p>
	<p>Microsoft will be planning in 2010 will promote one later face the multi-renter cloud environment The new safety mechanism, and provides based on Azure uses same technical the private cloud software Namely "Sydney" security plan. Sydney user's cloud resources and network empty Plans to decompose separates, provides the enterprise the internal data center equipment and in the clouds between the equipment Safe connection.</p>

in 2013, the global cloud computing service market size is 44,200,000,000 US dollars



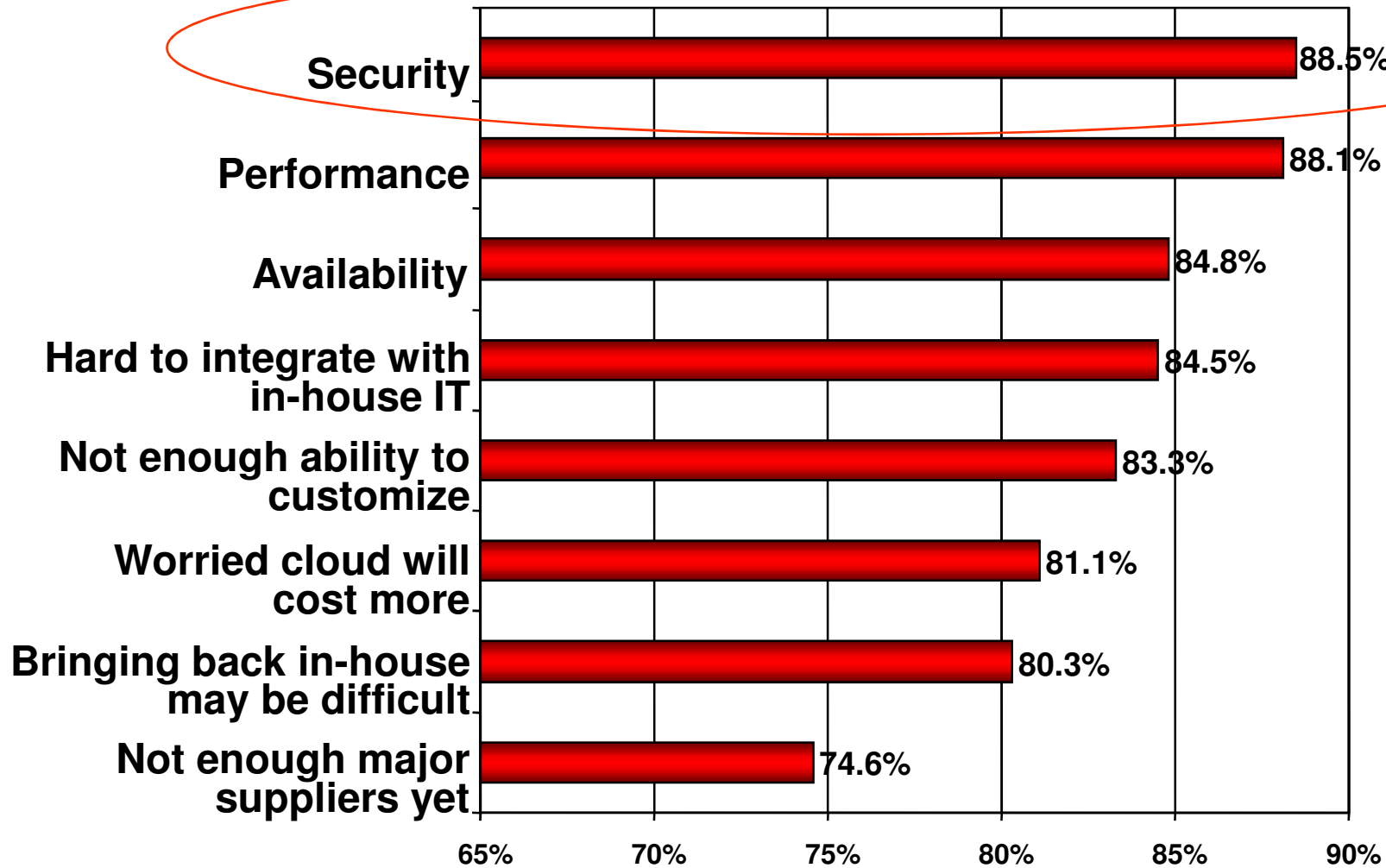
Source: IDC, 2009

Cisco forecast that in 2012 the data central order volume amounts to 10,000,000,000 US dollars






# Top Issues in Cloud Computing



% responding 3, 4 or 5 on scale of 1 to 5 (5 being most significant)

# Cloud security by security vendors paying attention

Traditional security factoryBusiness	The cloud moves safely
 <p>TREND MICRO 趋势科技</p>	<p>in 2009 the second quarter, the tendency science and technology purchase provides the security management software's privacyPerson enterprise Third Brigade. This purchase lets the tendency be able to bring more needlesTo virtualization and cloud computation security tool. According to the tendency indicated that this purchase realityPresent they have ensured the business data center security the strategy to anticipate.</p>
 <p>McAfee Proven Security™</p>	<p>in 2009 Mike Philippine Purchase Security Software Company MX Logic. Regarding the Mike PhilippinesSaid that this is a very important transaction, has integrated for own product mix whenNext wields great power with great arrogance “the software and the service”. In and Symantec's competition,This purchase let the Mike Philippines occupy the vantage point.</p>
 <p>symantec.</p>	<p>The Symantec Corporation 2008 year's end have purchased the online correspondence and the network security service raiseFor discusses MessageLabs, the conformity MessageLabs service founds one newlySaaS product department.</p> <p>in April, 2009 Symantec Corporation purchases the OEM partner, the SaaS specialized manufacturerAppStream. AppStream will bring a brand-new market to SymantecOpportunity - - tabletop virtualization.</p>

# News Headlines

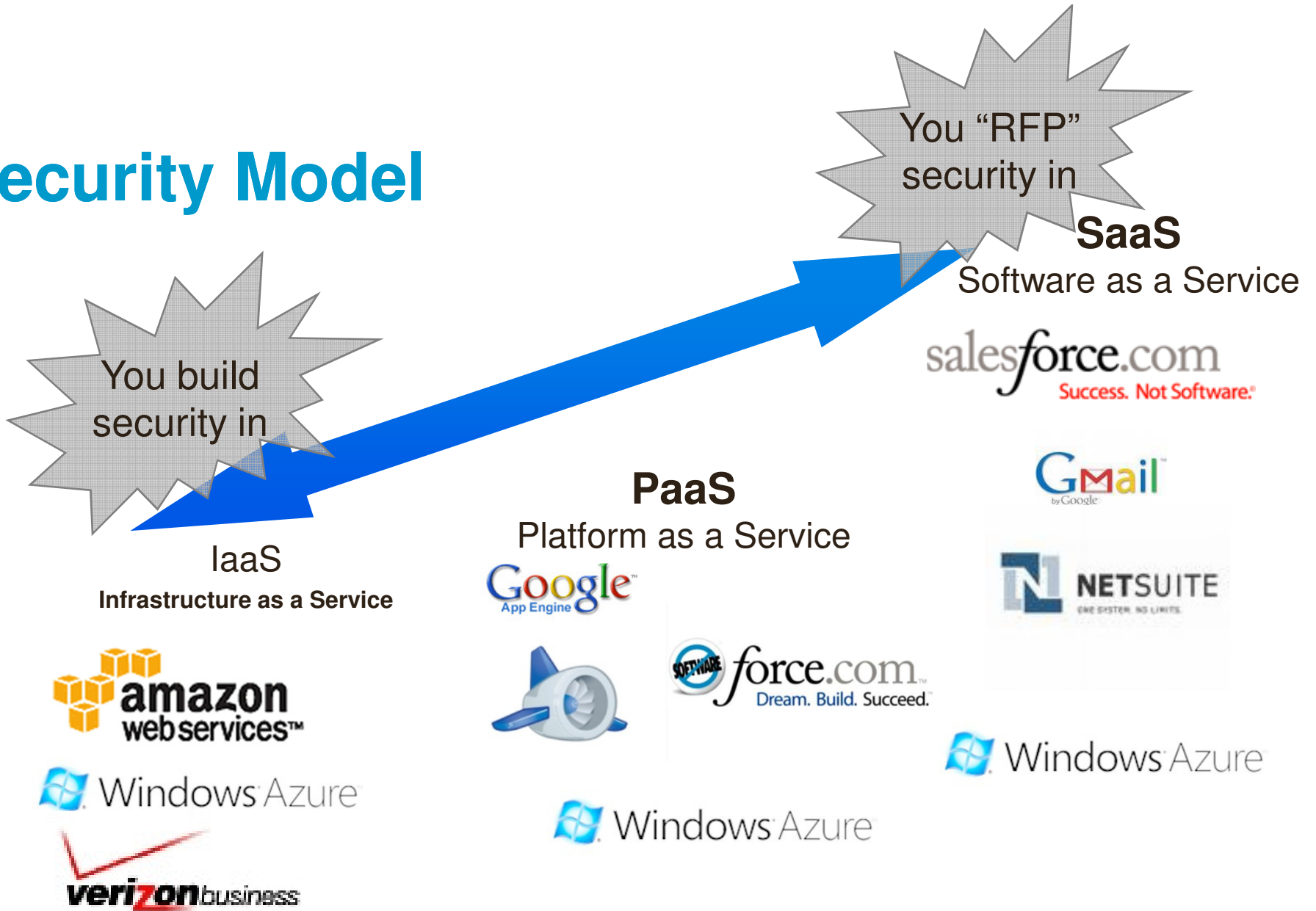
**Amazon Encrypts CloudFront,  
but Security Comes at a  
Price!**

**Google Security Breach a  
Warning Sign for Cloud  
Security?**

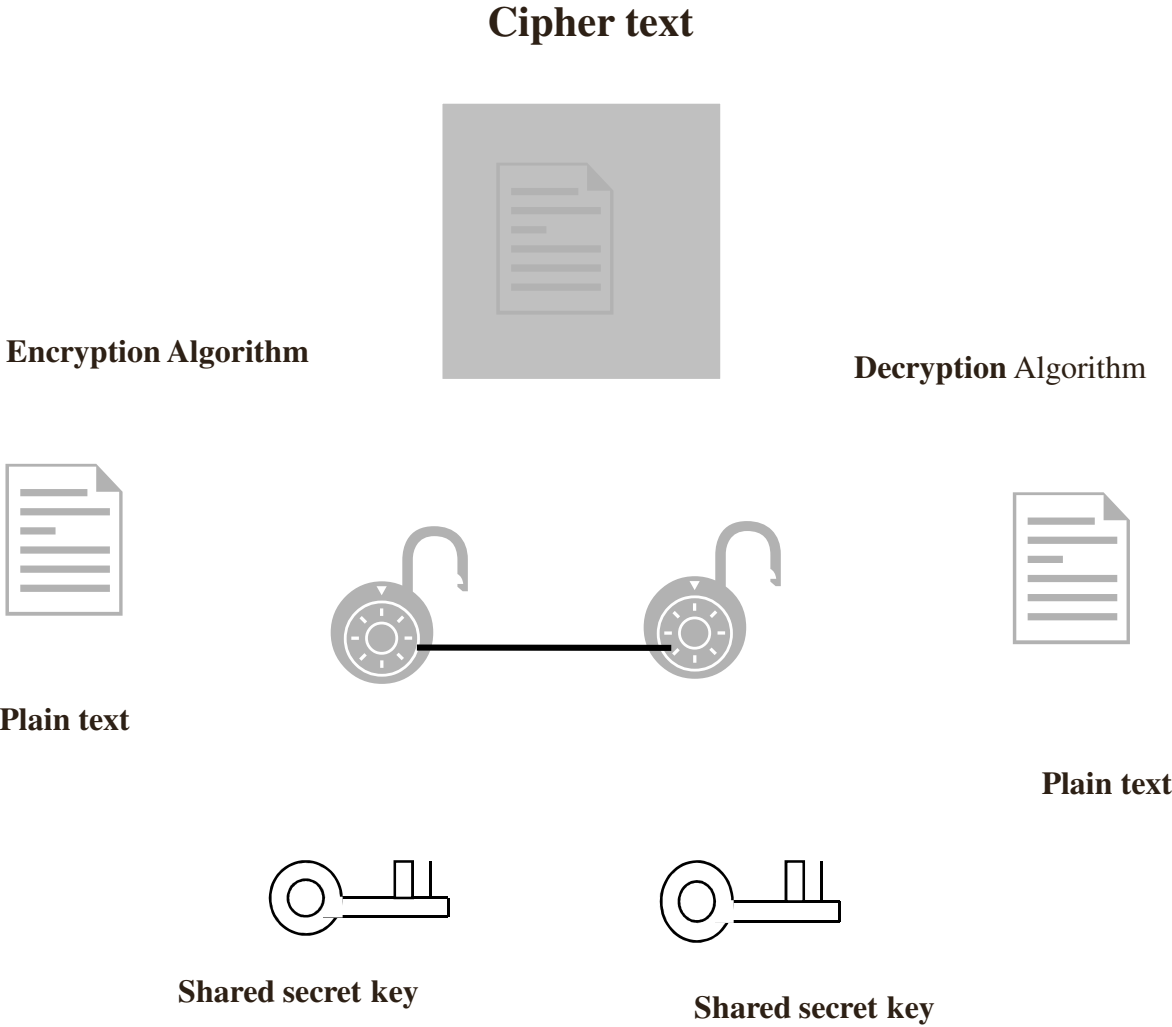
**IBM Managed Security Helps  
Shore Up Cloud Offerings**

**Multi-tenant SaaS Secured By  
Oracle Identity Management**

# Security Model



# A Basic cryptography model



# SYMMETRIC KEY CRYPTOSYSTEM

**D    E    B    A**

1101 1110 1011 1010 (Message)

1000 1000 1000 1000 (Encryption Key)

---

0101 0110 0011 0010 (5632 Ciphertext)

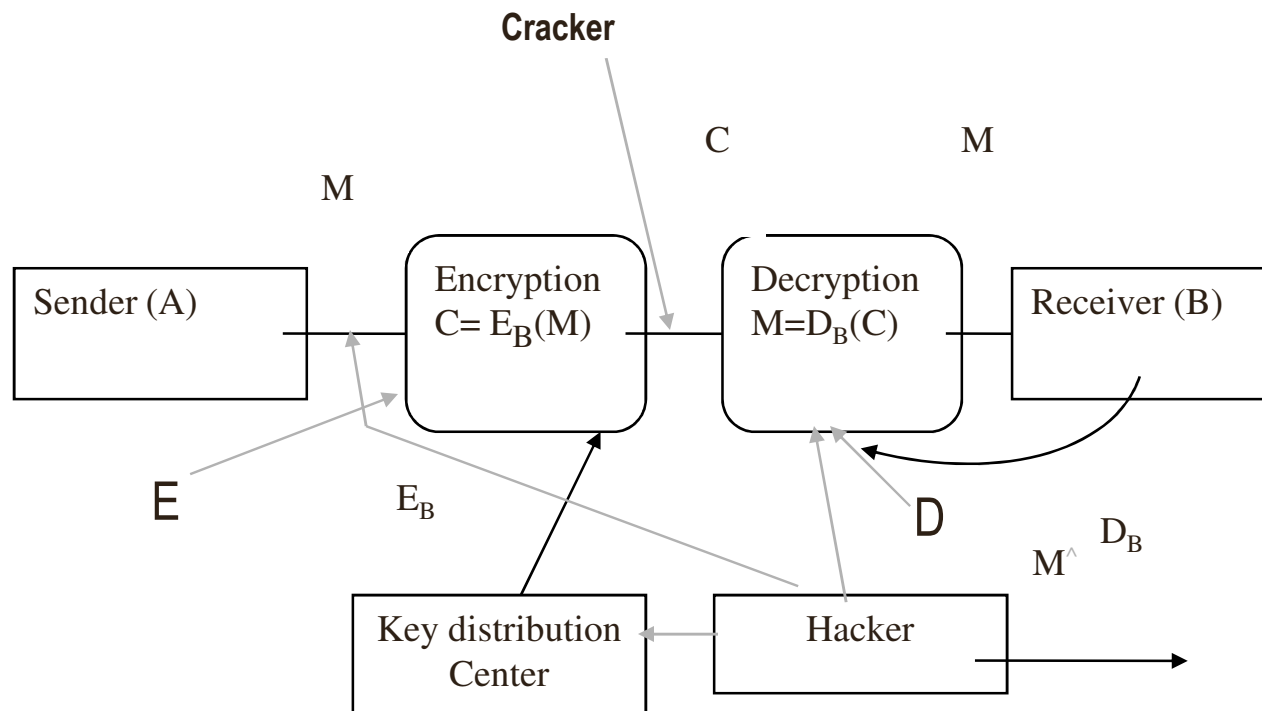
1000 1000 1000 1000 (Decryption Key)

---

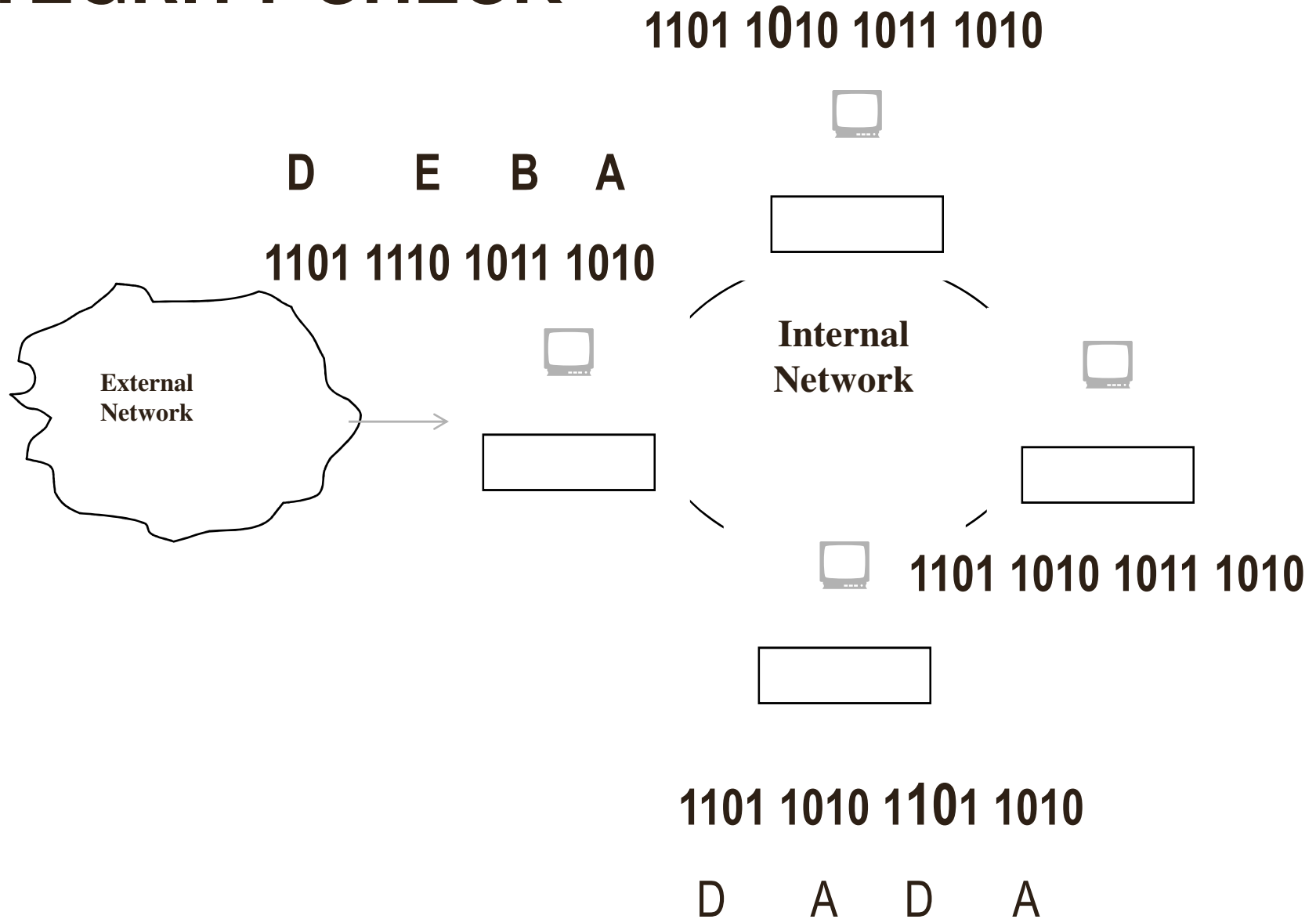
1101 1110 1011 1010

**D    E    B    A** (Original Message)

# Design of secure cryptographic system

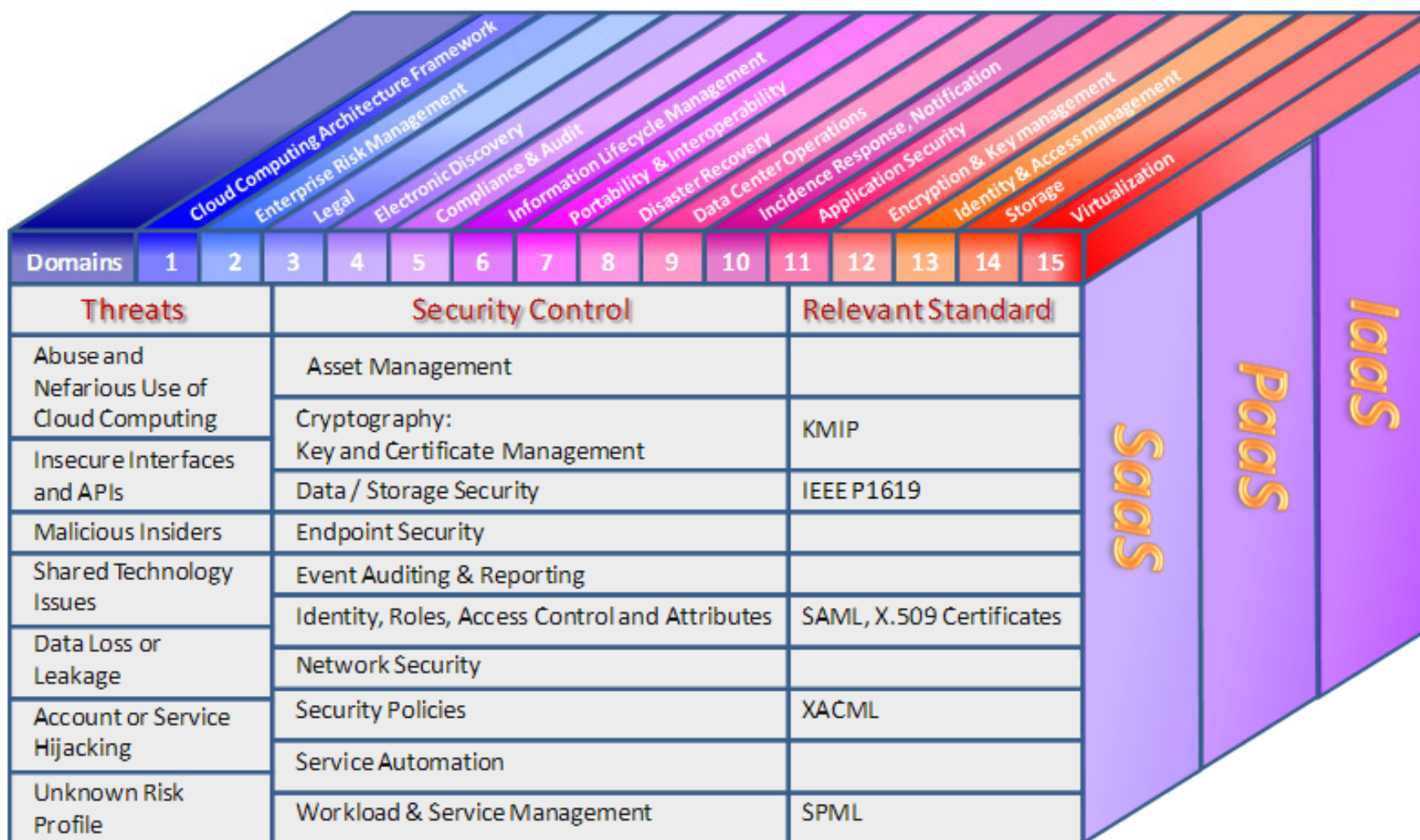


# INTEGRITY CHECK





# Cloud Computing Security Architecture



# Cloud Security Advantages

- ❑ **Exposure of internal sensitive data reduced by shifting public data to a external cloud**
- ❑ **Cloud homogeneity simplifies security auditing/testing**
- ❑ **Clouds enable automated security management both internally and externally**
- ❑ **Redundancy / Disaster Recovery**
- ❑ **Reduces in-house IT security administration**

# Cloud Security Challenges

## □ Trust

- Putting too much trust to vendor's security model

## □ Auditing and investigation

- Customer may be out of loop in audit events and findings
- Obtaining support for investigations at mercy of the provider
- Logging Challenges

## □ Administration

- Indirect security administrator accountability
- Security configurations
- Identity management

## □ Implementation

- Black box implementations can't be examined
- Public cloud vs internal cloud security

## □ Data

- Regulatory differences and difficulties across national boundaries
- Data retention issues
- Data protection in storage and transit
- Ownership

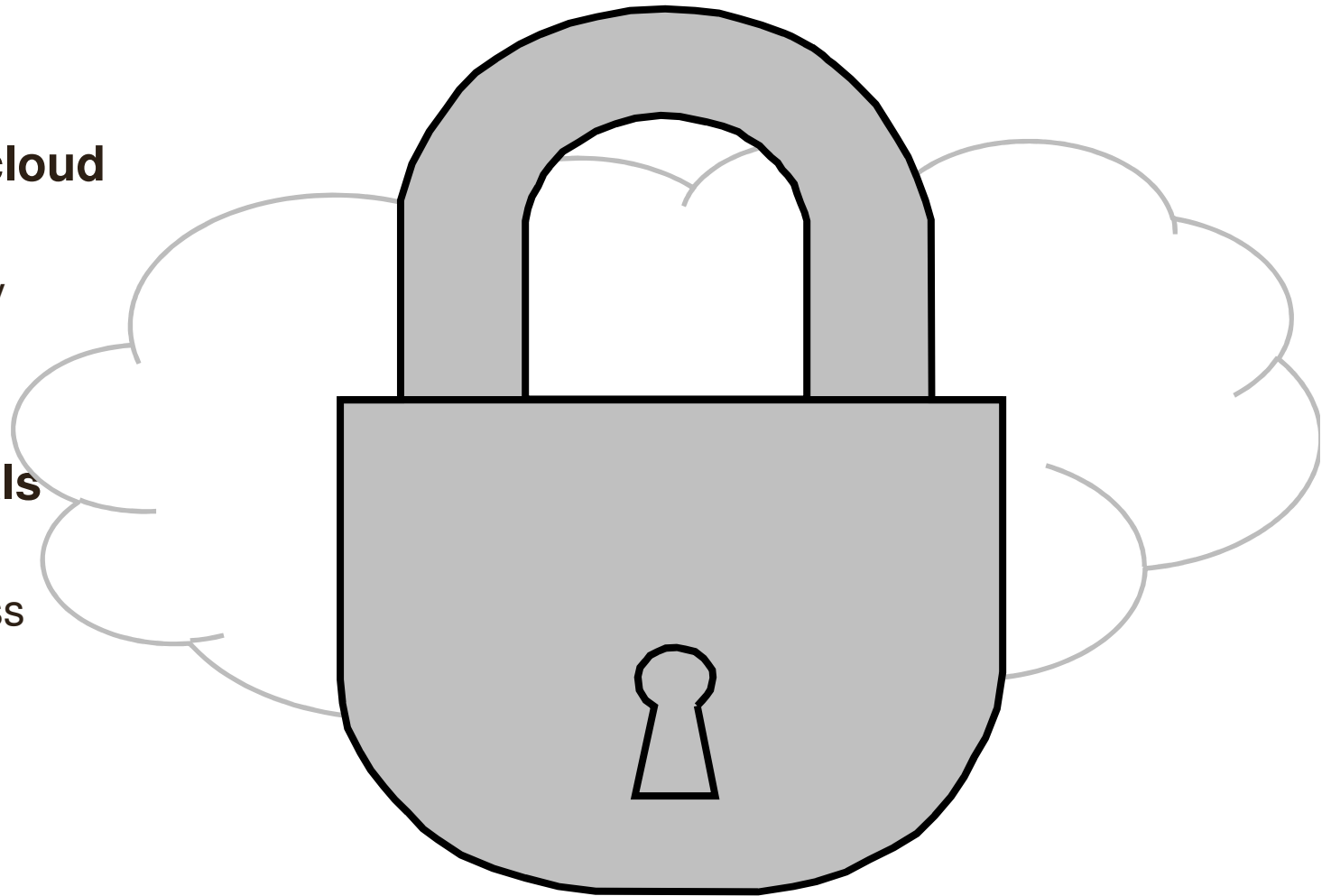
# Locking down the cloud

## ❑ **Securing the cloud**

- trust
- multi-tenancy
- encryption
- compliance

## ❑ **Achieving goals**

- privacy
- secure access
- transparency



# Security Requirements and Features

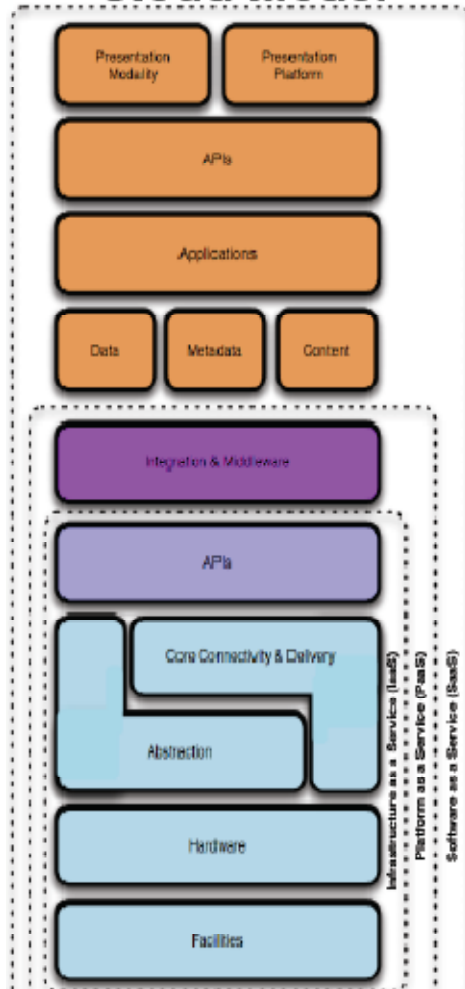
- **All of your IT security requirements apply**
- **Trust**
  - Platform trust and trusted computing
  - identity management, user provisioning and access control
  - Federation, control of privileges, SSO
  - Authentication, authorization and auditing
  - Privileged user management
  - Web access management
- **Encryption**
  - Key management and provisioning
  - Data leak protection
  - Data storage and transit Security profile per network
- **Multi-tenancy**
  - Multi-tenant logging management
  - Network, VM, Application, process, and data isolation
  - Security, OS, and Resource Management
  - Security DMZ per virtual application
  - Security profile per compute profile
- **Compliance**
  - Auditing
  - Log management
  - Regional/national/international compliances and certification
  - Legal intercept
  - Data Privacy

# Compliance and Certification

- **Security related Cloud-specific group**
- **ITU Cloud Focus Group**
- **ETSI cloud security group**
- **SAS70**
  - **Auditing compliance**
- **TIA942**
  - **US Data Center**
- **ISO 27001**
  - **Common Criteria certification and compliance**
- **ISO 15489**
  - **Records and Information Management**
- **LEED**
  - **Leadership in Energy and Environmental Design: green data center**
- **NIST FIPS 140-2**
  - **Security Requirements for Cryptographic Modules**
- **ISA's Security Assurance Certification**
  - **Embedded Device Security Assessment**

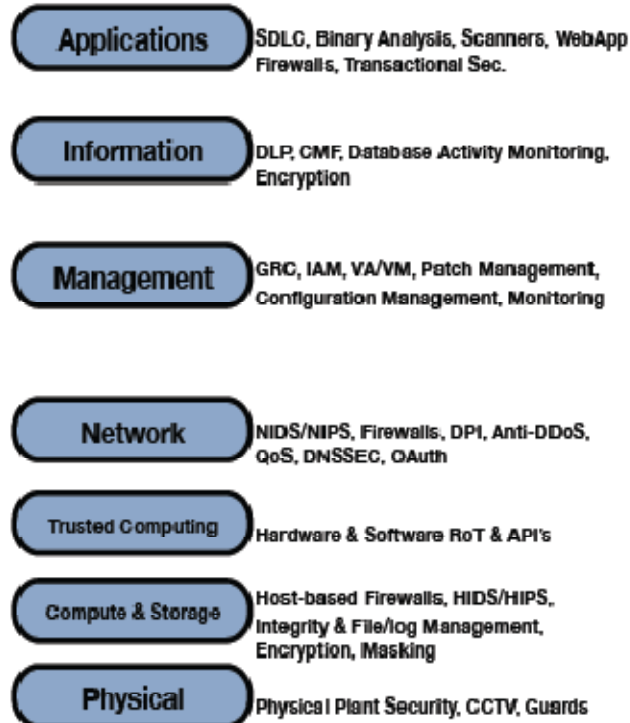
# Mapping the Model to the Metal

## Cloud Model

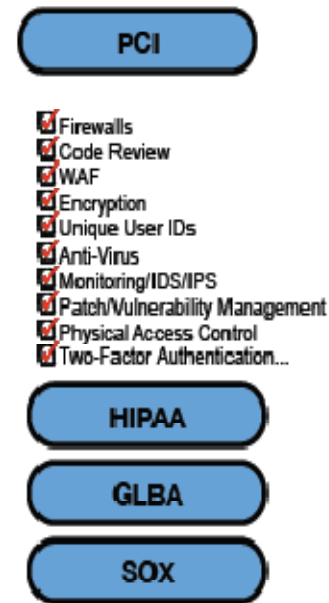


Find the Gaps!

## Security Control Model



## Compliance Model



# ITU activities in Cloud Security

- **Making a balance between all the standards**
- **Cloud definition and ecosystem**
- **Identity in Cloud**
- **PKI Infrastructure for cloud**
- **Key Management Scheme for Cloud**
- **Cloud Security Architecture**
- **Cloud service, resource management and middleware**
- **Cloud computing platform secure architecture**

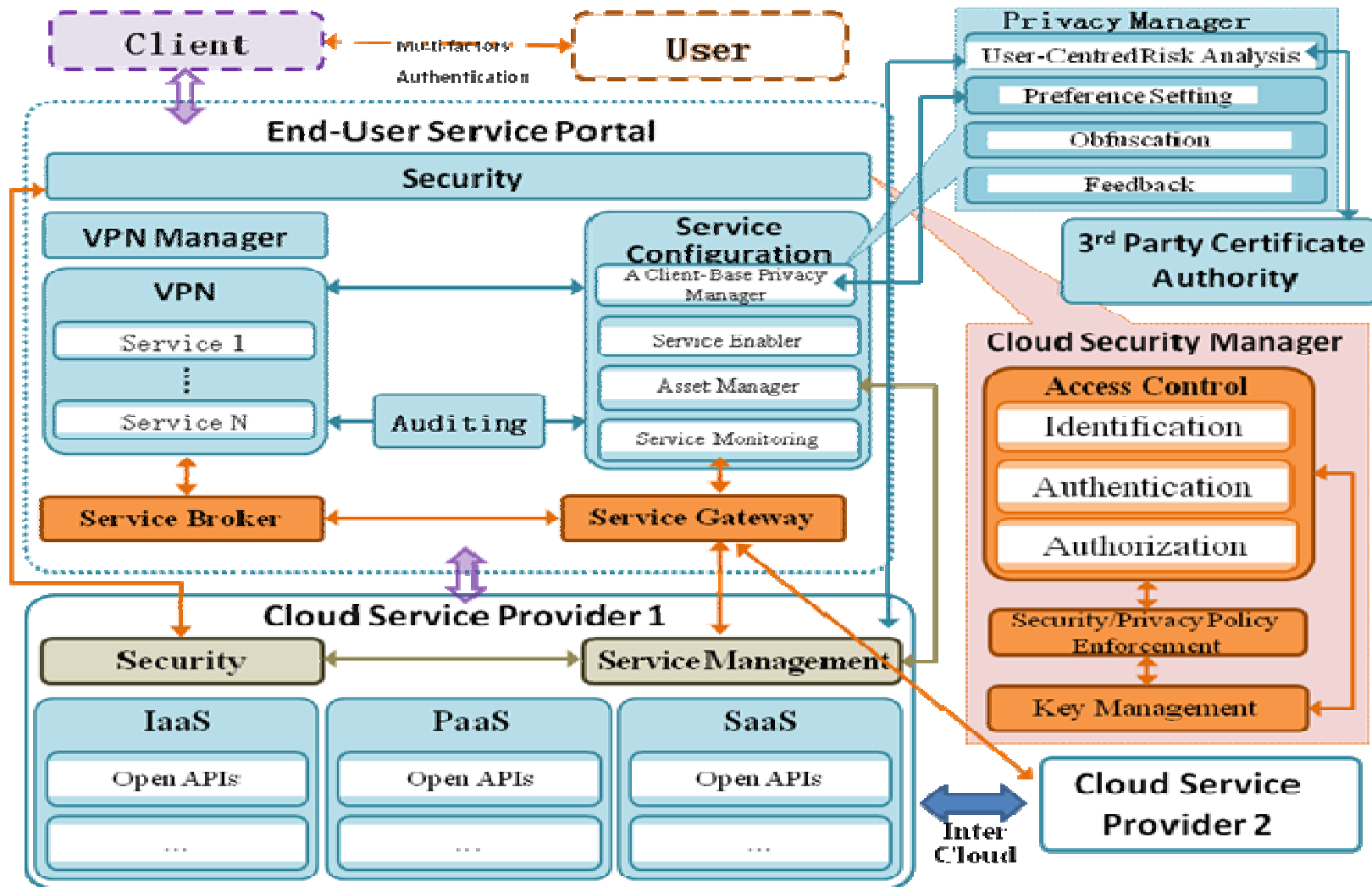


# Key management

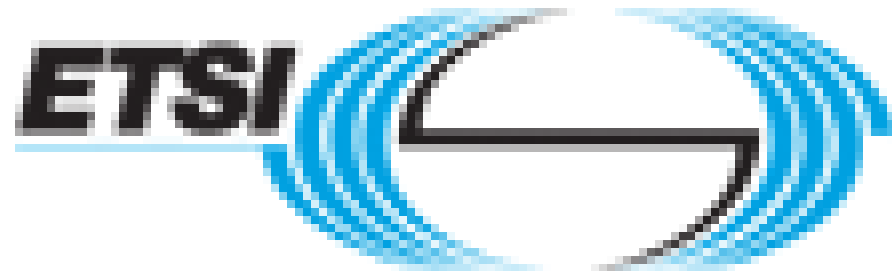
- \* Key management is (currently) the responsibility of the cloud customer
- \* Key provisioning and storage is usually off-cloud
- \* One key-pair per machine – doesn't scale to multiple account holders/RBAC
- \* Credential recovery sometimes available through management interface (protected by UN/PWD by)
- \* Copies of VM images may contain keys if not well-managed



# Cloud Security Framework



# Standards/Fora and Cloud Computing



# Summary

- **Security is the number one concern in cloud computing**
- **New challenges in cloud computing bring forward new threats and risks**
  - More complex than traditional IT security
- **The Cloud needs to be secure, guarantee privacy, access and transparency**
- **Regulations and laws are catching up but need to expand beyond data privacy**
- **Compliance and certification are very important in measuring the effort put into building the cloud and to provide assurances**
- **Standards and forum play important role in promoting openness and interoperability**

**THANK YOU**