Fundamental of Cloud Security

Salim Hariri, UA Site Director
NSF Center for Cloud and Autonomic Computing
The University of Arizona
nsfcac.arizona.edu
hariri@ece.arizona.edu

Presentation Outline

- Introduction
- Cloud Computing Standers
- Cloud Security Issues
- Cloud Attack Mechanisms
- Cloud Protection and Solutions

INTRODUCTION

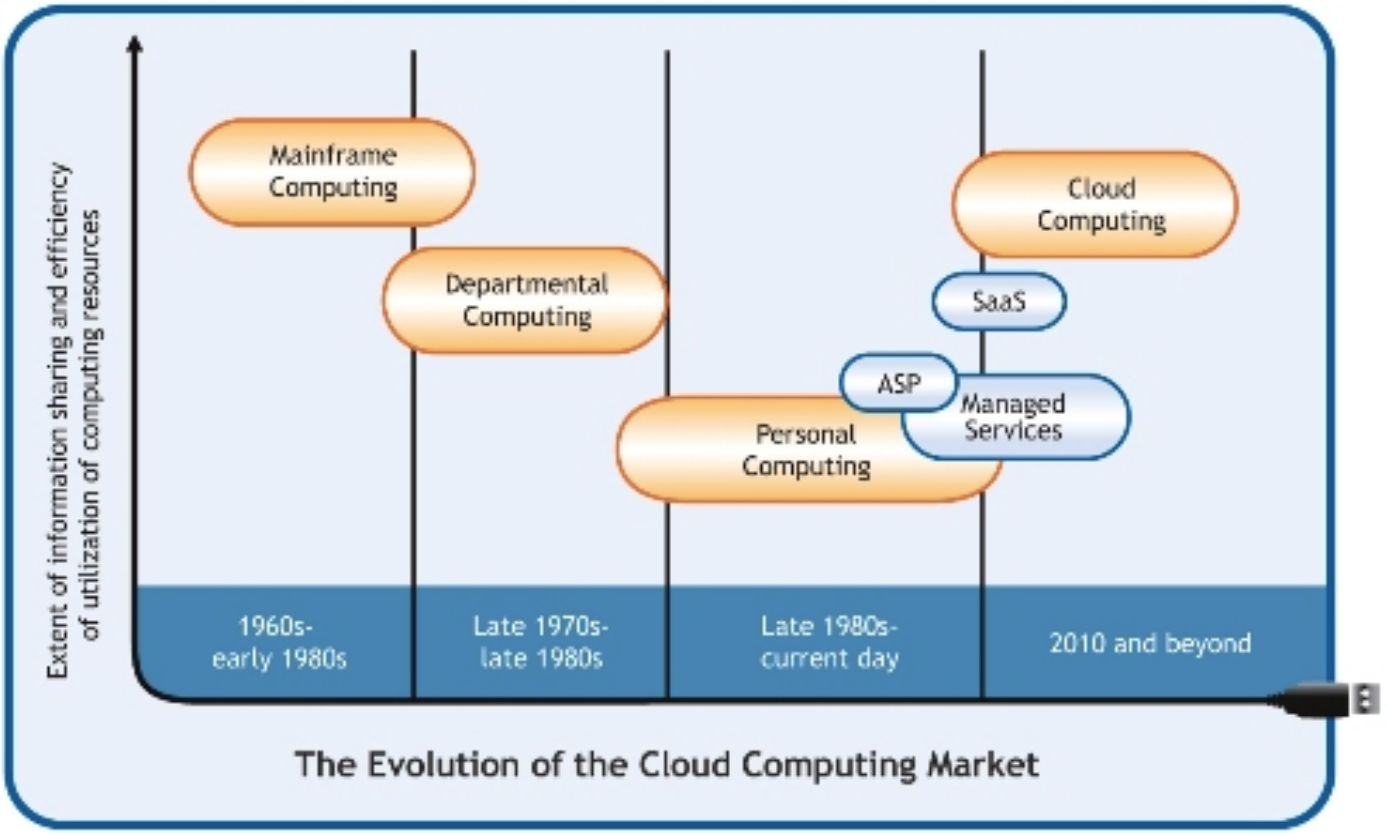
Cloud Computing – Motivation

- Car rental services
  - For short period
  - Before you get your own car
  - No need to maintain and upgrade
  - Is popular
- Cloud rental services
  - For short period
  - Before you get your own devices
  - No need to maintain and upgrade

Cloud Computing Potential Benefits

- Increased Reliability – Duplicated data, logs, better maintenance
- Reduction in IT operating costs (Pay-as-you-Go)
- Scalability and Agility
- Ubiquitous Accessibility – Internet, and perform same task from any where and using any network device
- Levels the playing field
- Fast request-driven provisioning (On Demand)
- Improves collaboration

How the Cloud is growing?



* Source:http://www.forbescustom.com/TechnologyPgs/CloudComputingP1.html [accessed: May 26, 2013]

Cloud Computing Growth

- Cloud usage is like having a customized cellular plan with all the features and functionality that you want, paying only for what you use, and with the ability to cancel at anytime without penalties or additional fees.
- Worldwide cloud service revenue grew at 16.6% in 2010, reaching $68.3 billion, according to Gartner report.
  - It is expected that enterprises will spend in the next five years around $112 billion on cloud technologies and services

- # CLOUD COMPUTING STANDARD

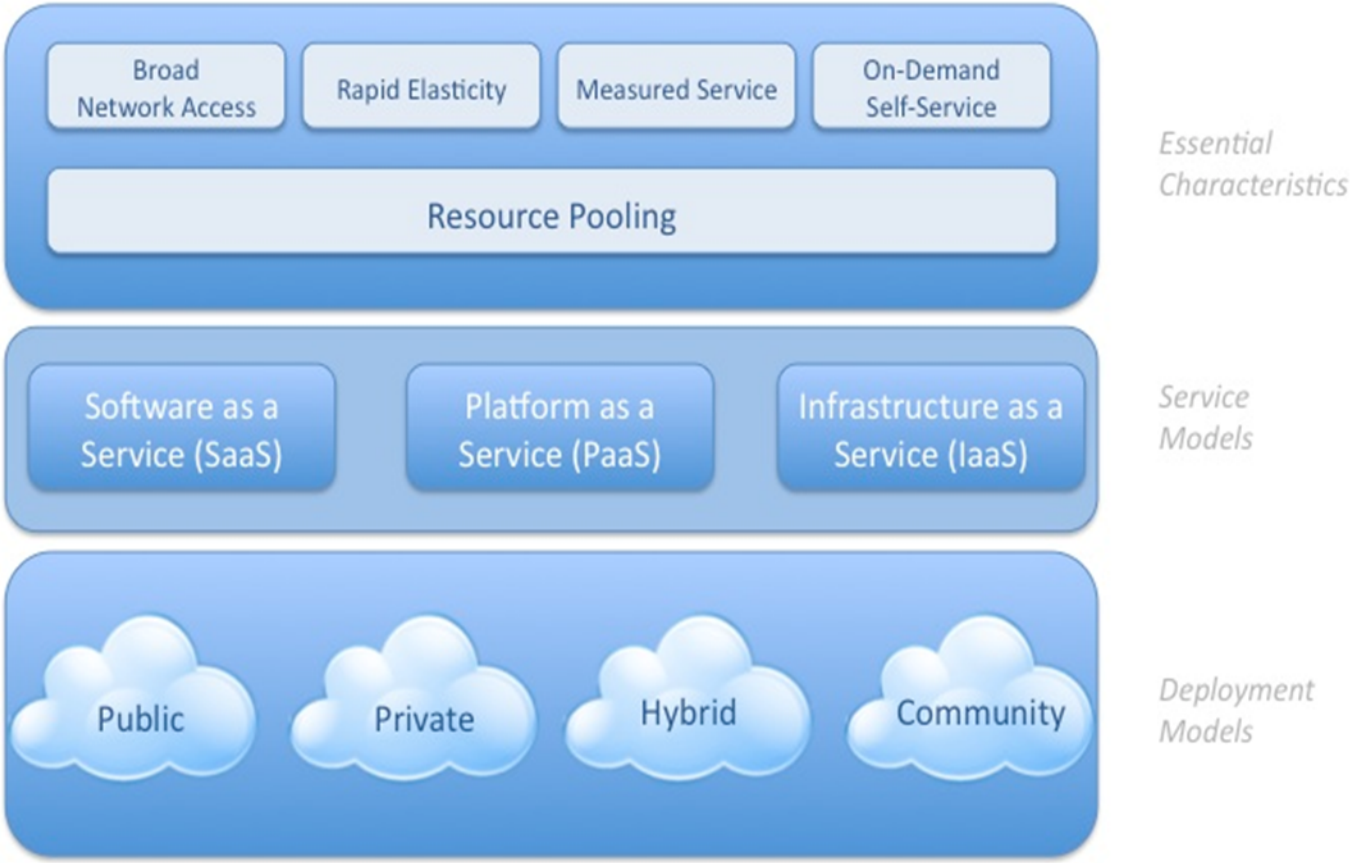
NIST definition of cloud computing

- Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

What Comprises Cloud Computing?

- NIST defines:
  - Five essential cloud characteristics
  - Three cloud service models
  - Four cloud deployment models.

NIST Model of Cloud



Five Essential Cloud Characteristics

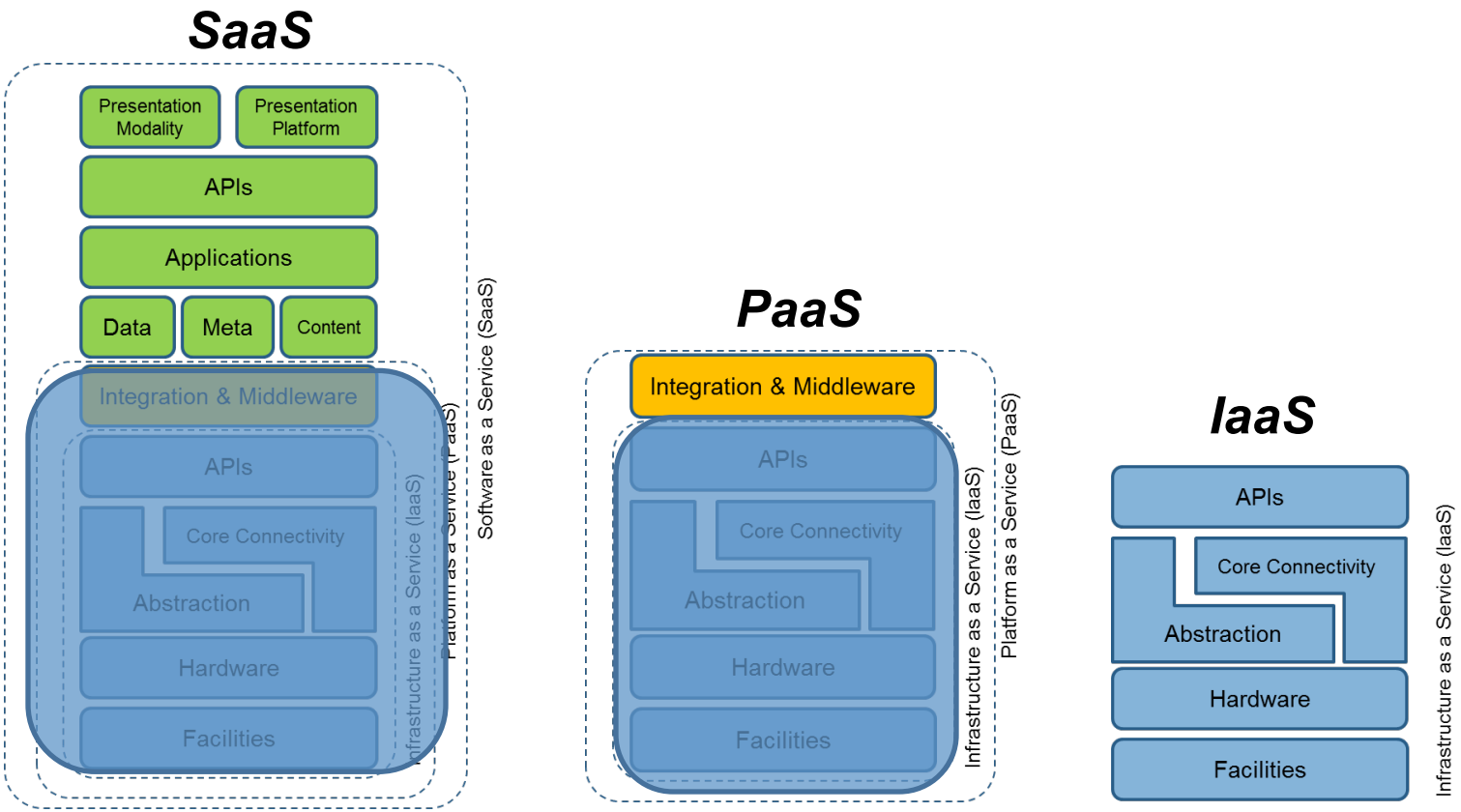
- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

Three Cloud Service Models

- Cloud Software as a Service (SaaS)*
  - To use the provider's applications
- Cloud Platform as a Service (PaaS) *
  - To deploy customer-created and acquired applications
- Cloud Infrastructure as a Service (IaaS)
  - To provision processing, storage, networks, and other fundamental computing resources

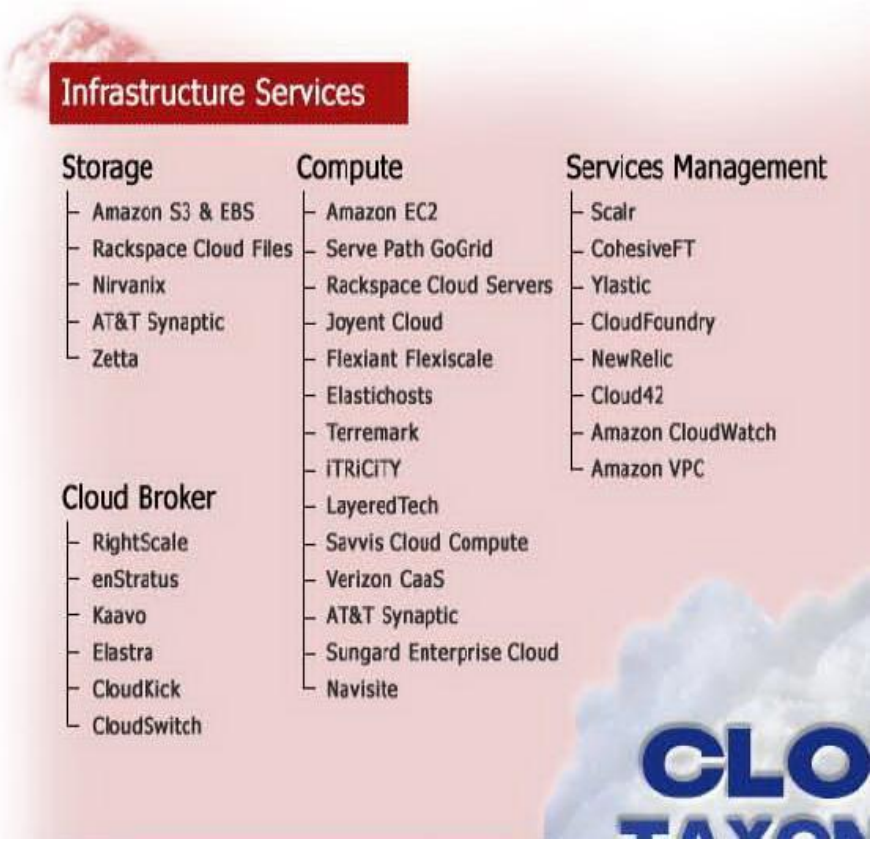
* *To be considered as cloud services, they must be running on top of an cloud infrastructure.*

Cloud Service Delivery Models

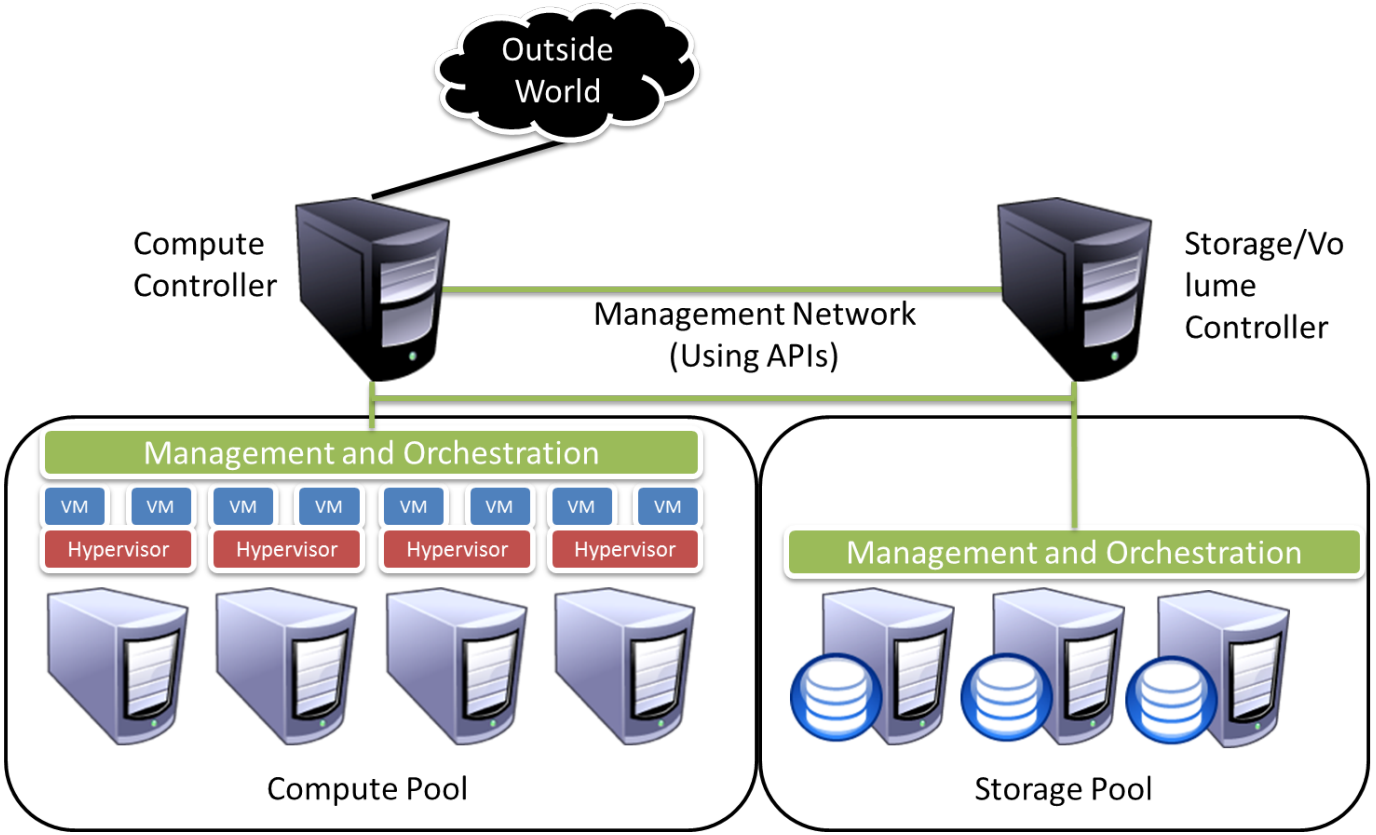


Cloud Service Models –IaaS

- It delivers computer infrastructure as a service, along with raw storage and networking
- Rather than purchasing servers, software, data-center space, or network equipment, clients buy them as a fully outsourced service



What is IaaS?



Source: *Securosis, L.L.C. / Cloud Security Alliance*

IaaS

Benefits

- Tremendous control to use whatever content system makes sense.
- Flexibility to secure data to whatever degree necessary.

Issues

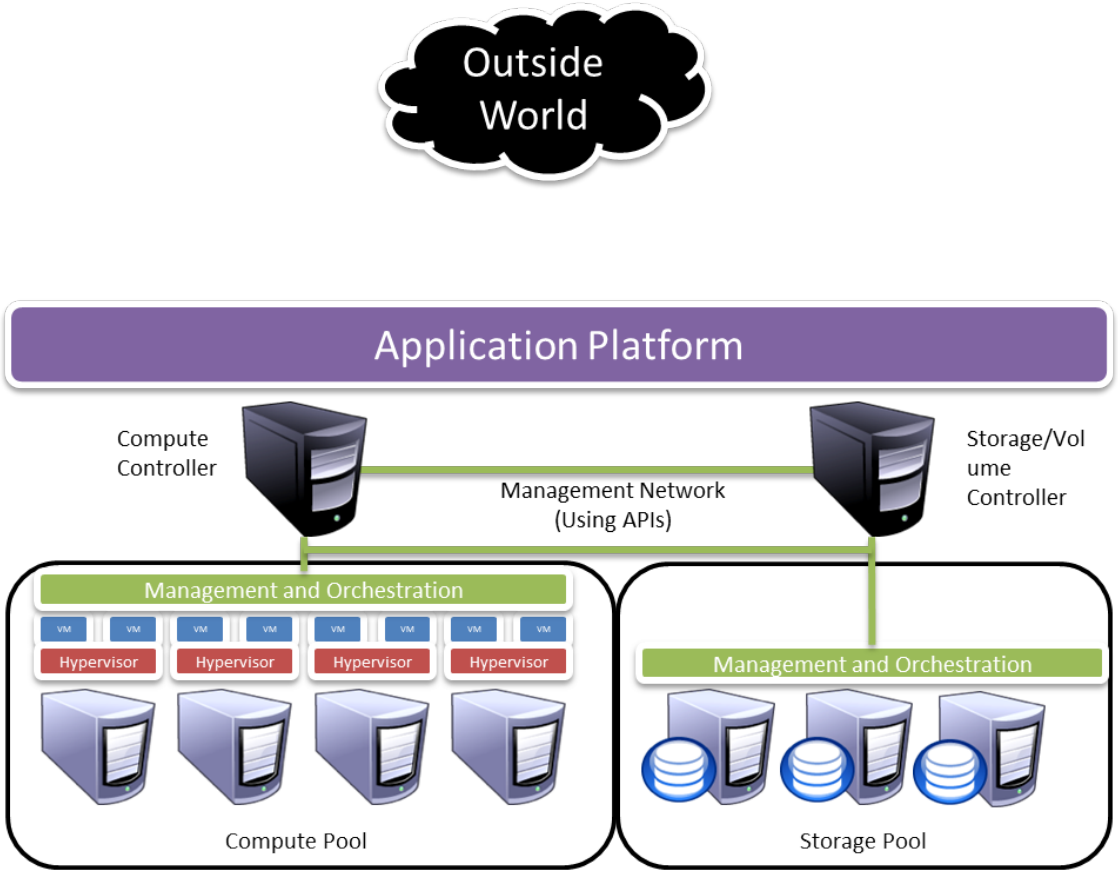
- Involves integrating all aspects of an application (DB, plug-ins, etc.)
- Responsible for all configurations implemented on the server (and in apps)
- Responsible to keep software up to date
- Multi-tenancy at hypervisor level

Src: *Securosis, L.L.C. / Cloud Security Alliance*

Cloud Service Models – PaaS

- It delivers a computing platform and solution stack as a service. PaaS offering facilitate deployment of applications without the cost and complexity of buying and managing the underlying hardware and software and provisioning hosting capabilities

What is PaaS?



Src: *Securosis, L.L.C. / Cloud Security Alliance*

PaaS

Benefits

- Packaged application "stack" reduces some complexity (configuration, components)
- If application vendor supports cloud APIs, streamlines implementation

Issues

- Still responsible to keep stack updated
- Locked into providers API (which can change)
- Multi-tenancy at platform layer

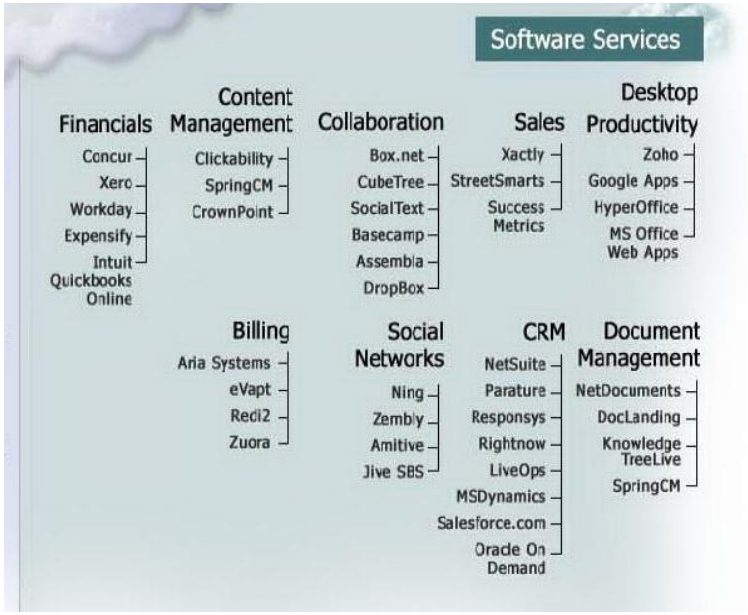
Src: *Securosis, L.L.C. / Cloud Security Alliance*

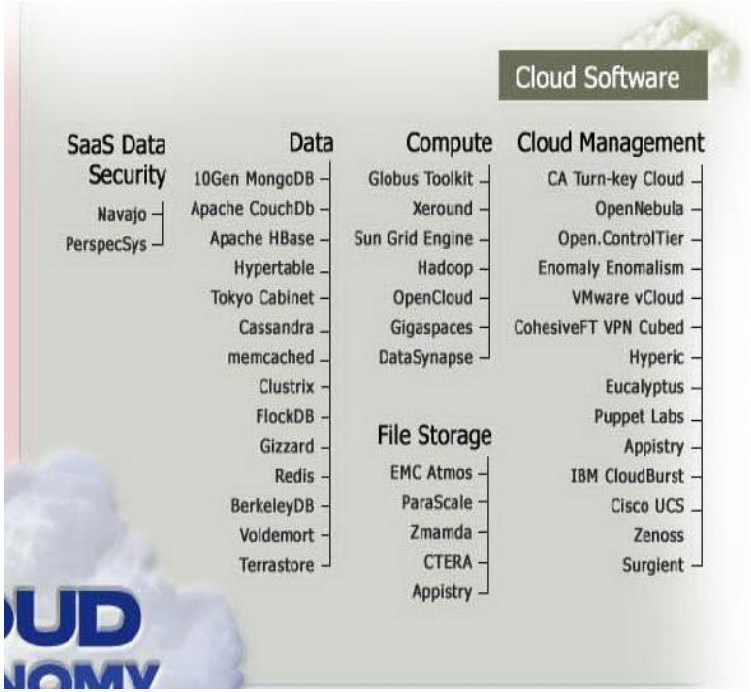
Software as a Service SaaS

- Cloud computing services, such as **Amazon's EC2** and **Google Apps**, are booming.
- With **Software as a Service**, you're not writing an app, just using someone else's.
- Changes the dynamic of pricing the software (pay on a per-use basis).
- 20% growth in SaaS products per year.

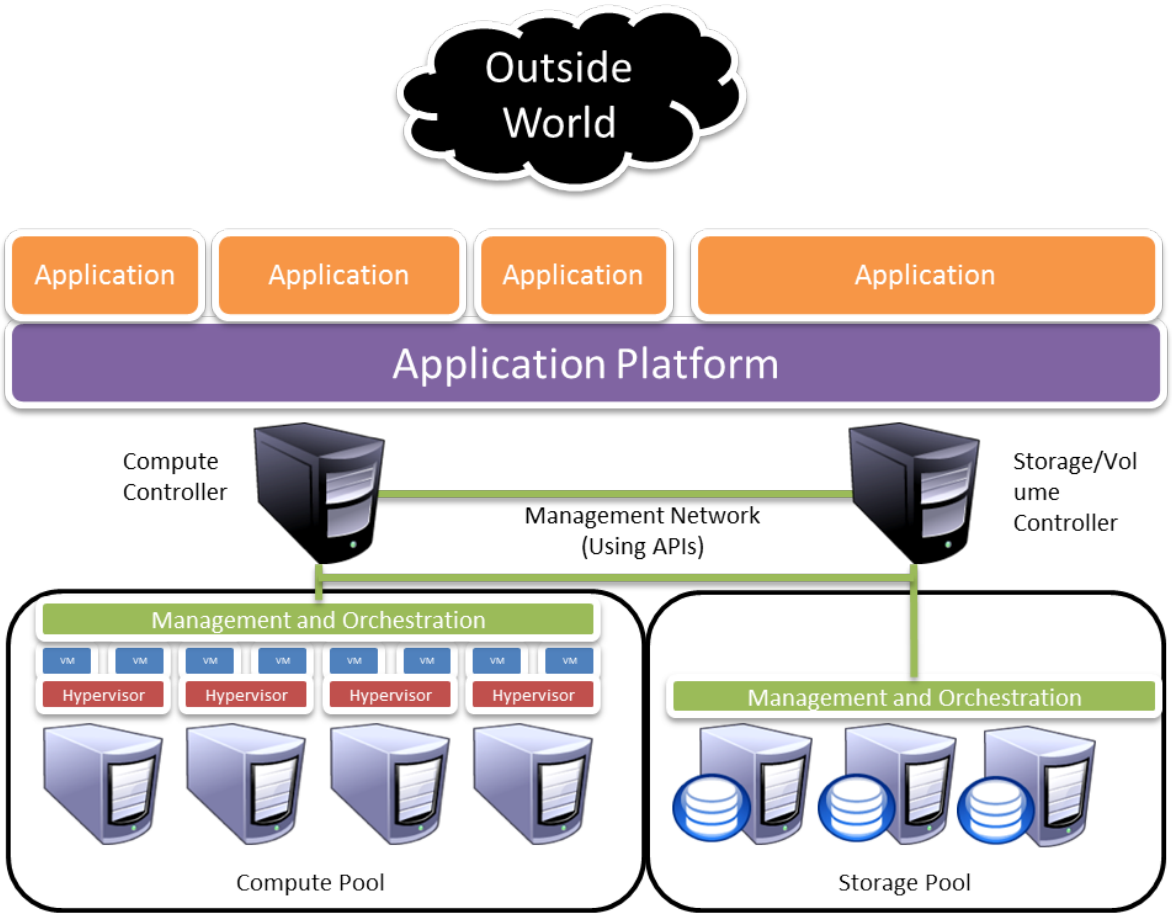
Cloud Service Models – SaaS

Software and data are hosted on the cloud and are typically accessed by users using a thin client (browser with internet access)





What is SaaS?



Src: *Securosis, L.L.C. / Cloud Security Alliance*

SaaS

Benefits

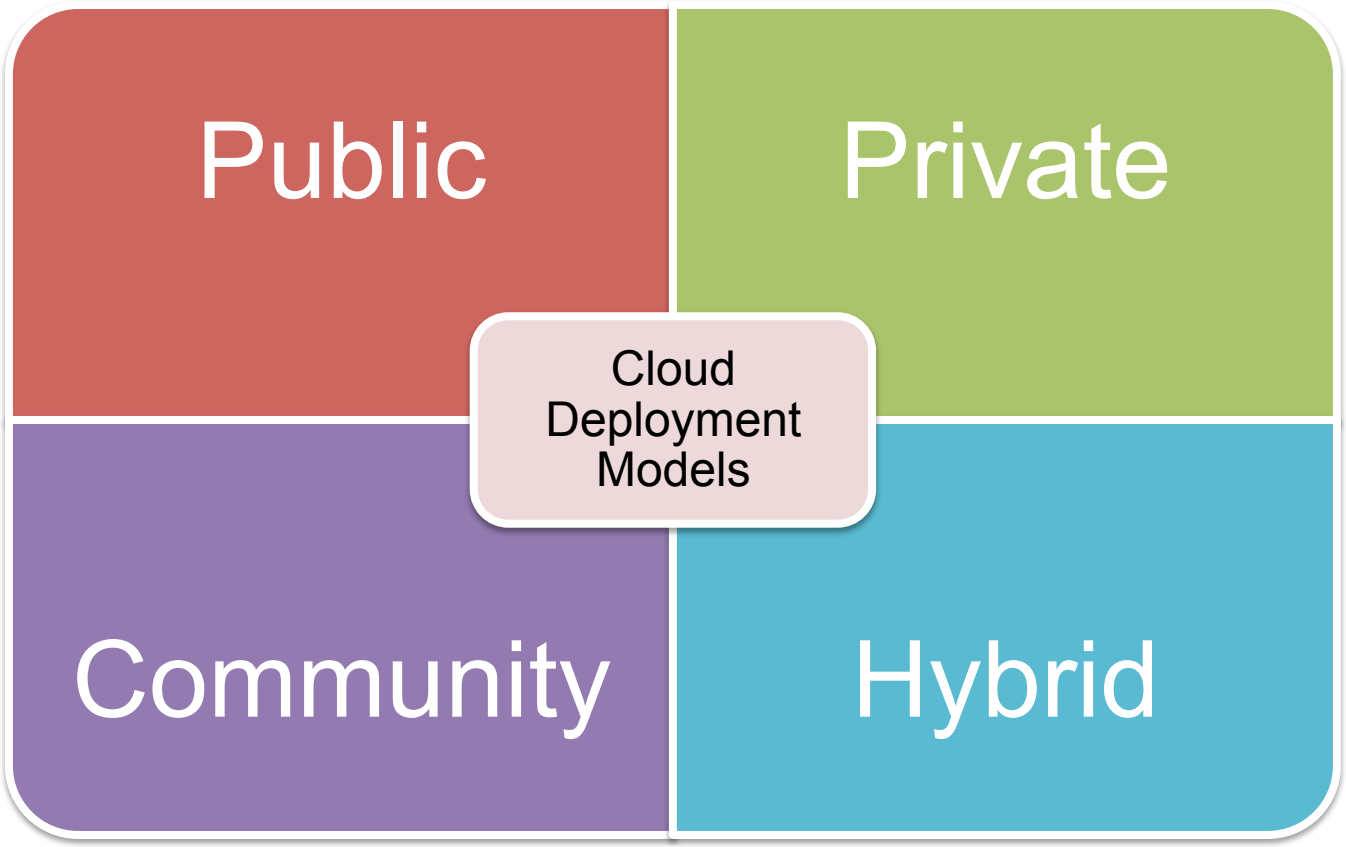
- Packaged solution reduces complexity
- Scaling environment isn't customer's problem.
- All updates/ configurations/security handled by provider.

Issues

- Very little app customization
- No control of components.
- No control of security (can only assess, not impact).
- Multi-tenancy issues at application layer.

Src: *Securosis, L.L.C. / Cloud Security Alliance*

Cloud Deployment Models

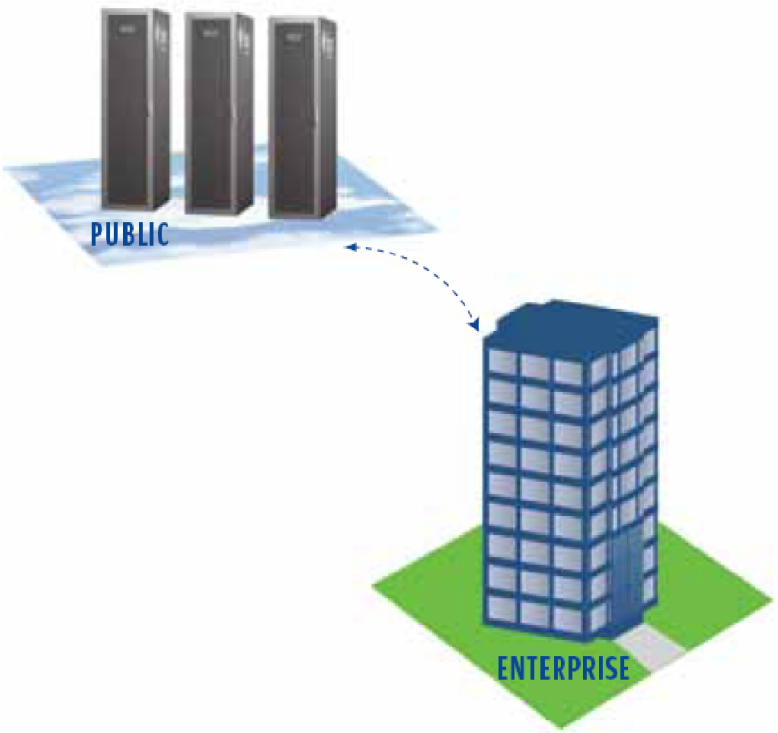


Src: *Securosis, L.L.C. / Cloud Security Alliance*

Cloud Deployment Models

- Deployment Options
  - Private
  - Public
  - Community
  - Hybrid
- Controlled/Owned By
  - Internal
  - External

Cloud Computing Infrastructures – Public Clouds



- Run by 3rd parties such as Amazon, Google or Microsoft.
- Employ statistical multiplexing to provide hardware and software resources.
- Are hosted away from user premises.
- For security, other applications running on the same clouds are transparent to cloud users.

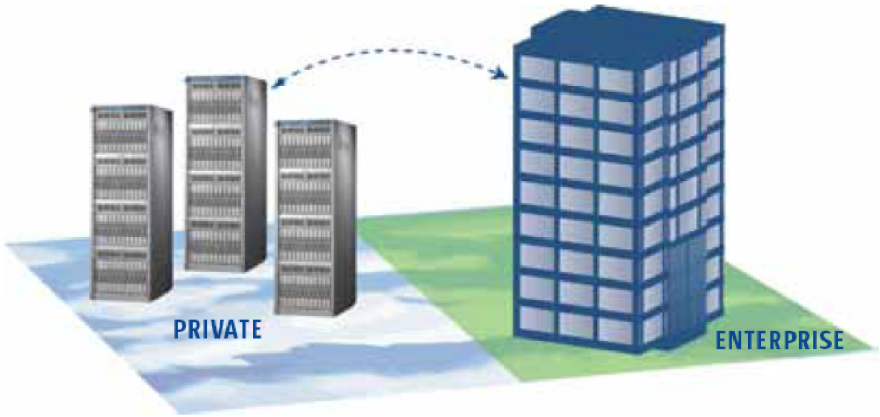
- Public clouds guarantee improved performance, considerable & scalable resources, and growth flexibility.

Public Cloud, Advantages, drawbacks

- Pros:
  - Reliability
  - Cost Efficiency
  - Scalability and Agility
- Cons:
  - Security
  - Control

Cloud Computing Infrastructures – Private Clouds

- Built for only one client.
- Provide complete control over data, security and QoS.
- Deployed on enterprise datacenter or co-location facility.



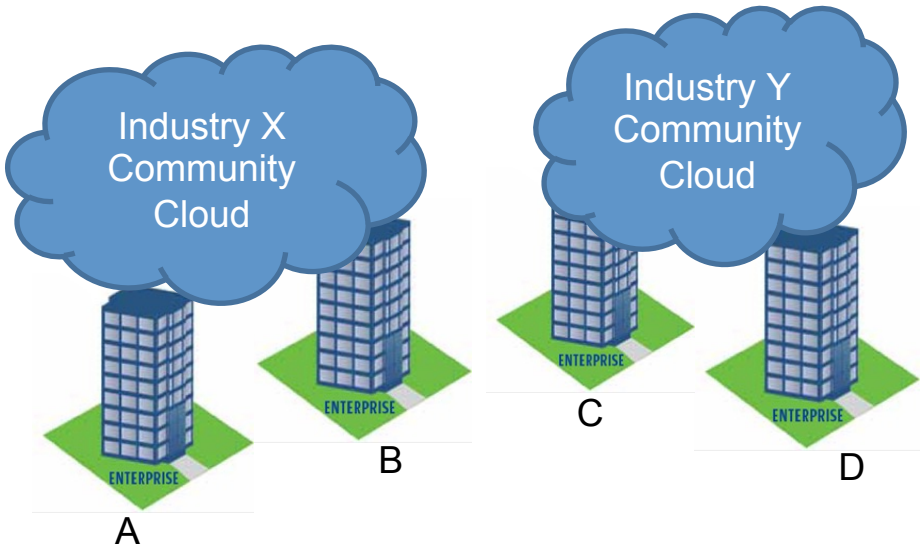
- Built by companies own IT organization or cloud service provider.
- Hosted private model- high level of control + technical expertise to establish and operate the cloud.

Private Cloud, Advantages, drawbacks

- Pros:
  - **Control / Security**
  - **Availability**
  - **Speed of Access**
- Cons:
  - **Scalability**
  - **Maintenance**

Community Cloud

- In a community cloud Multiple organizations and infrastructures from the same community share the cloud infrastructure.
- They all have similar concerns and goals which helps to agree on the same cloud policies.

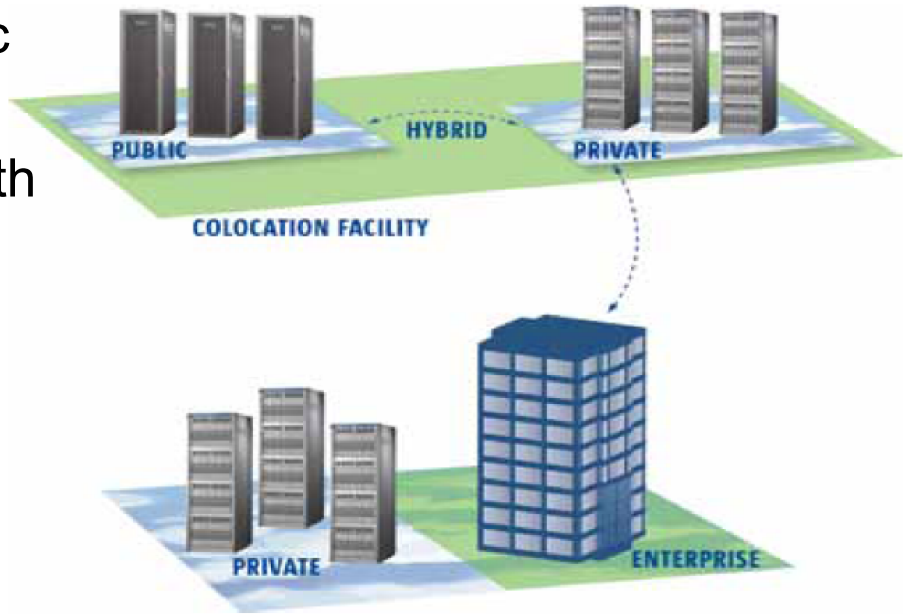


Community Cloud, Advantages, drawbacks

- Pros
  - Security
  - Legal/compliance
  - Same Policy and Concerns
- Cons
  - Development
  - Cost

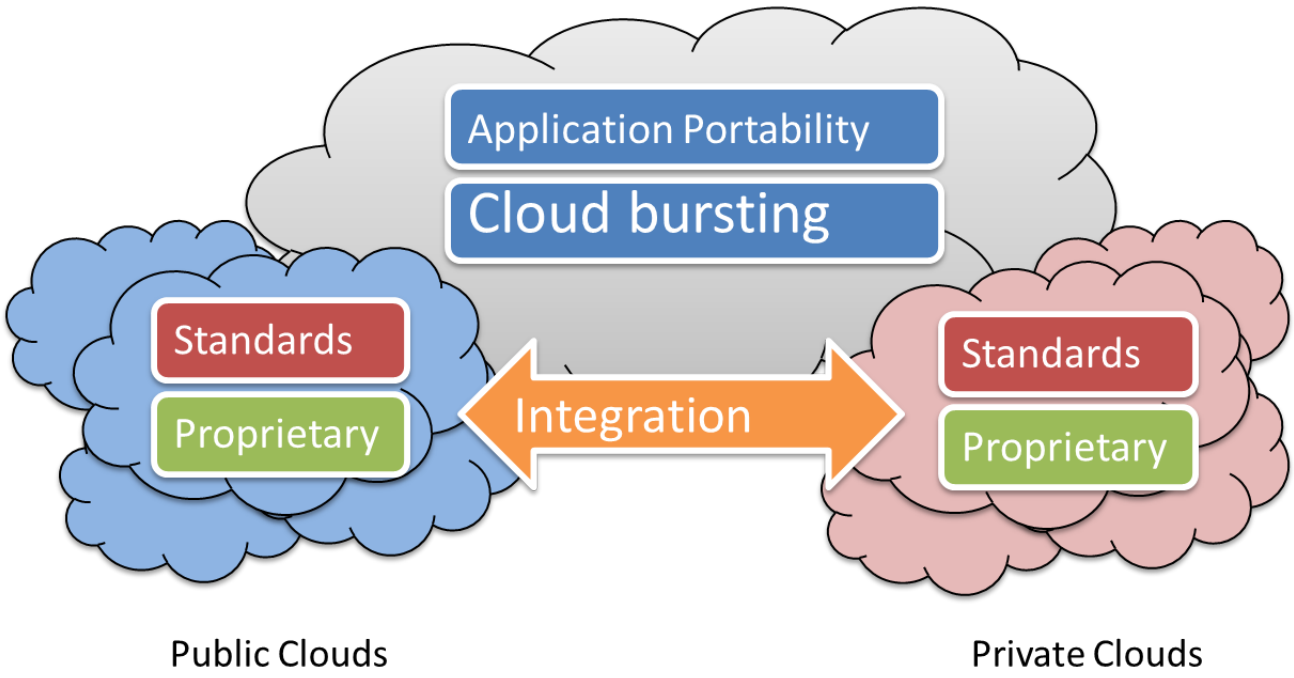
Cloud Computing Infrastructures – Hybrid Clouds

- Combines both private and public clouds.
- Private clouds are augmented with resources of public cloud.
- Are used to support Web 2.0 applications
- Also used to handle workload spikes, i.e. surge computing.



- More suitable for handling small data transfer or applications are stateless, than if large amount of data were transferred for small amount of processing.

Hybrid Clouds



Source: *Securosis, L.L.C. / Cloud Security Alliance*

Hybrid Cloud, Advantages, drawbacks

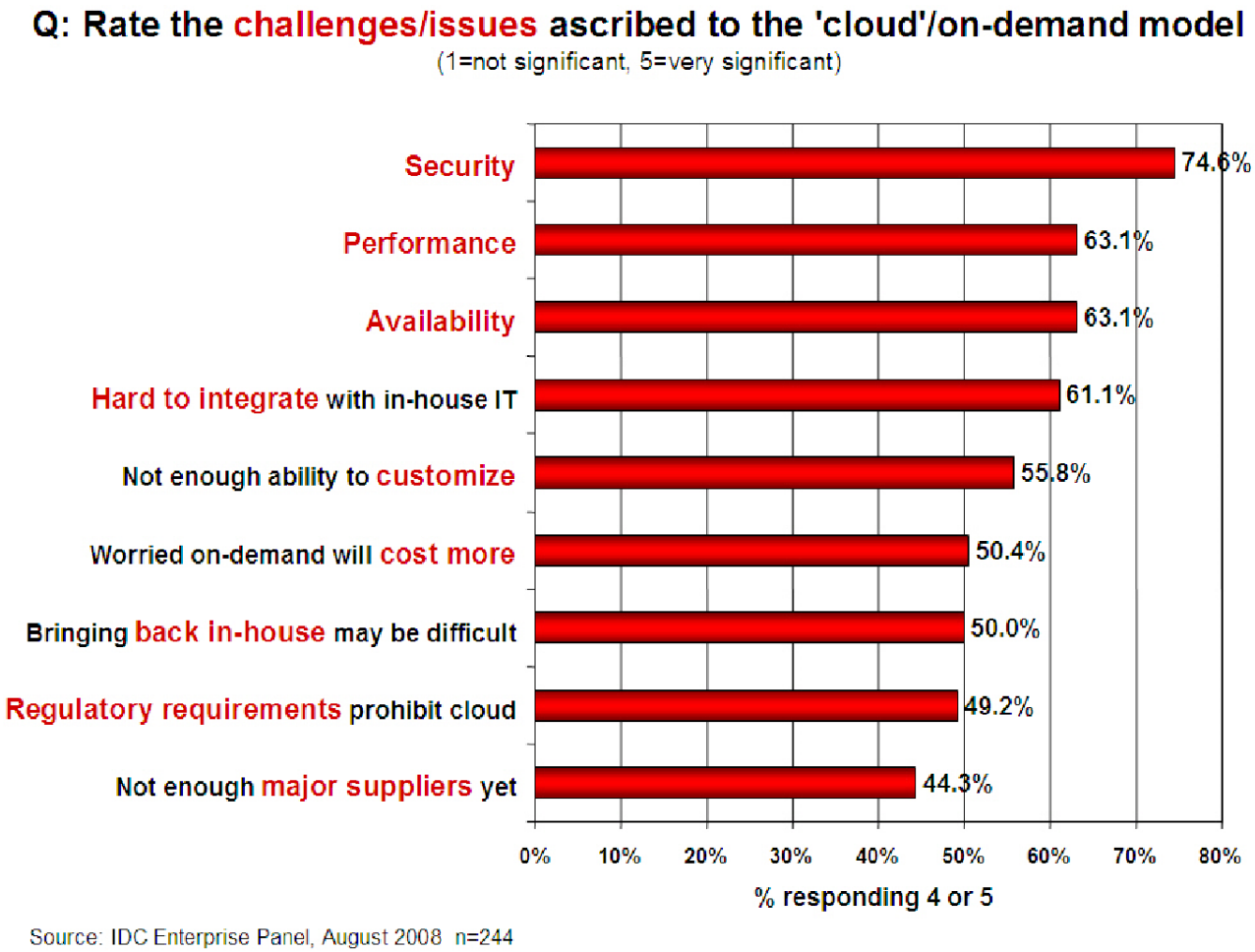
- Pros:
  - High performance:
  - Expanded capacity
  - Scalability
  - Security
  - Low cost:
- Cons:
  - Complex SLAs:
  - Complex networking

CLOUD SECURITY ISSUES

If cloud computing is so great, why isn't everyone doing it?

- The cloud acts as a big black box, nothing inside the cloud is visible to the clients
- Clients have no idea or control over what happens inside a cloud
- Even if the cloud provider is honest, it can have malicious system admins who can tamper with the VMs and violate confidentiality and integrity
- Clouds are still subject to traditional data confidentiality, integrity, availability, and privacy issues, plus some additional attacks

Companies are still afraid to use clouds



Top Cyberattacks in 2014 so far!

- Analysts, Hold Security, startlingly announced in February that it had managed to obtain a list of 360 million account credentials for web services from the black market. That's just after three weeks of research.
- According to research from Arbor Networks, the number of DDoS events topping 20Gbps in the first half of 2014, are double that of 2013.
- Akamai Technologies State of the Internet report also showed that hacker attacks on websites went up 75% in the final quarter of 2013, with hackers in China responsible for 43% of all attacks
- This incredible cybermap.kaspersky.com

interactive map from Antivirus software firm Kaspersky, which depicts all the current cyber attacks occurring around the world in real time, shows the growing intensity of hacks as the year progresses.

Top Cyberattacks in 2014 - continue

- In May, eBay revealed that hackers had managed to steal personal records of 233 million users, with usernames, passwords, phone numbers and physical addresses compromised.
- **Community Health Services (health care).** The personal data for 4.5 million patients were compromised between April and June. The sophisticated malware used in the attack reportedly originated in China. (September 2014)
- **Google (communications).** Reportedly, 5 million Gmail usernames and passwords were compromised.[23] About 100,000 were released on a Russian forum site. (September 2014)
- **Apple iCloud (technology).** Hackers reportedly used passwords hacked with brute-force tactics and third-party applications to access Apple user's online data storage, leading to the subsequent posting of celebrities' private photos online. (September 2014)
- **J.P. Morgan Chase (financial).** The contact information for 76 million households and 7 million small businesses was compromised. The hackers may have originated in Russia and may have ties to the Russian government. (October 2014)

Causes of Problems Associated with Cloud Computing

- Most security problems stem from:
  - Loss of control
  - Lack of trust (mechanisms)
  - Multi-tenancy
- These problems exist mainly in 3rd party management models
  - Self-managed clouds still have security issues, but not related to above

Loss of Control in the Cloud

- Consumer's loss of control
  - Data, applications, resources are located with provider
  - User identity management is handled by the cloud
  - User access control rules, security policies and enforcement are managed by the cloud provider
  - Consumer relies on provider to ensure
    - Data security and privacy
    - Resource availability
    - Monitoring and repairing of services/resources

Multi-tenancy Issues in the Cloud

- Conflict between tenants' opposing goals
  - Tenants share a pool of resources and have opposing goals
- How does multi-tenancy deal with conflict of interest?
  - Can tenants get along together and 'play nicely' ?
  - If they can't, can we isolate them?
- How to provide separation between tenants?

- Cloud Computing brings new threats
  - Multiple independent users share the same physical infrastructure
  - Thus an attacker can legitimately be in the same physical machine as the target

Taxonomy of Fear

- Confidentiality
  - Fear of loss of control over data
    - Will the sensitive data stored on a cloud remain confidential?
    - Will cloud compromises leak confidential client data
  - Will the cloud provider itself be honest and won't peek into the data?
- Integrity
  - How do I know that the cloud provider is doing the computations correctly?
  - How do I ensure that the cloud provider really stored my data without tampering with it?

www.cs.jhu.edu/~ragib/sp10/cs412

Taxonomy of Fear (cont.)

- Availability
  - Will critical systems go down at the client, if the provider is attacked in a Denial of Service attack?
  - What happens if cloud provider goes out of business?
  - Would cloud scale well-enough?

www.cs.jhu.edu/~ragib/sp10/cs412

Taxonomy of Fear (cont.)

- Privacy issues raised via massive data mining
  - Cloud now stores data from a lot of clients, and can run data mining algorithms to get large amounts of information on clients
- Increased attack surface
  - Entity outside the organization now stores and computes data, and so
  - Attackers can now target the communication link between cloud provider and client
  - Cloud provider employees can be phished

From [5] www.cs.jhu.edu/~ragib/sp10/cs412

Taxonomy of Fear (cont.)

- Auditability and forensics (out of control of data)
  - Difficult to audit data held outside organization in a cloud
  - Forensics also made difficult since now clients don't maintain data locally
- Legal quagmire and transitive trust issues
  - Who is responsible for complying with regulations?
    - e.g., SOX, HIPAA, PCI DSS ?
  - If cloud provider subcontracts to third party clouds, will the data still be secure?

www.cs.jhu.edu/~ragib/sp10/cs412

Cloud Computing: who should use it?

- Cloud computing definitely makes sense if your own security is weak, missing features, or below average.
- Ultimately, if
  - the cloud provider's security people are "better" than yours (and leveraged at least as efficiently),
  - the web-services interfaces don't introduce too many new vulnerabilities, and
  - the cloud provider aims at least as high as you do, at security goals,

  then cloud computing has better security.

CLOUD ATTACK MECHANISMS

Threat Model

- A threat model helps in analyzing a security problem, design mitigation strategies, and evaluate solutions
- Steps:
  - Identify attackers, assets, threats and other components
  - Rank the threats
  - Choose mitigation strategies
  - Build solutions based on the strategies

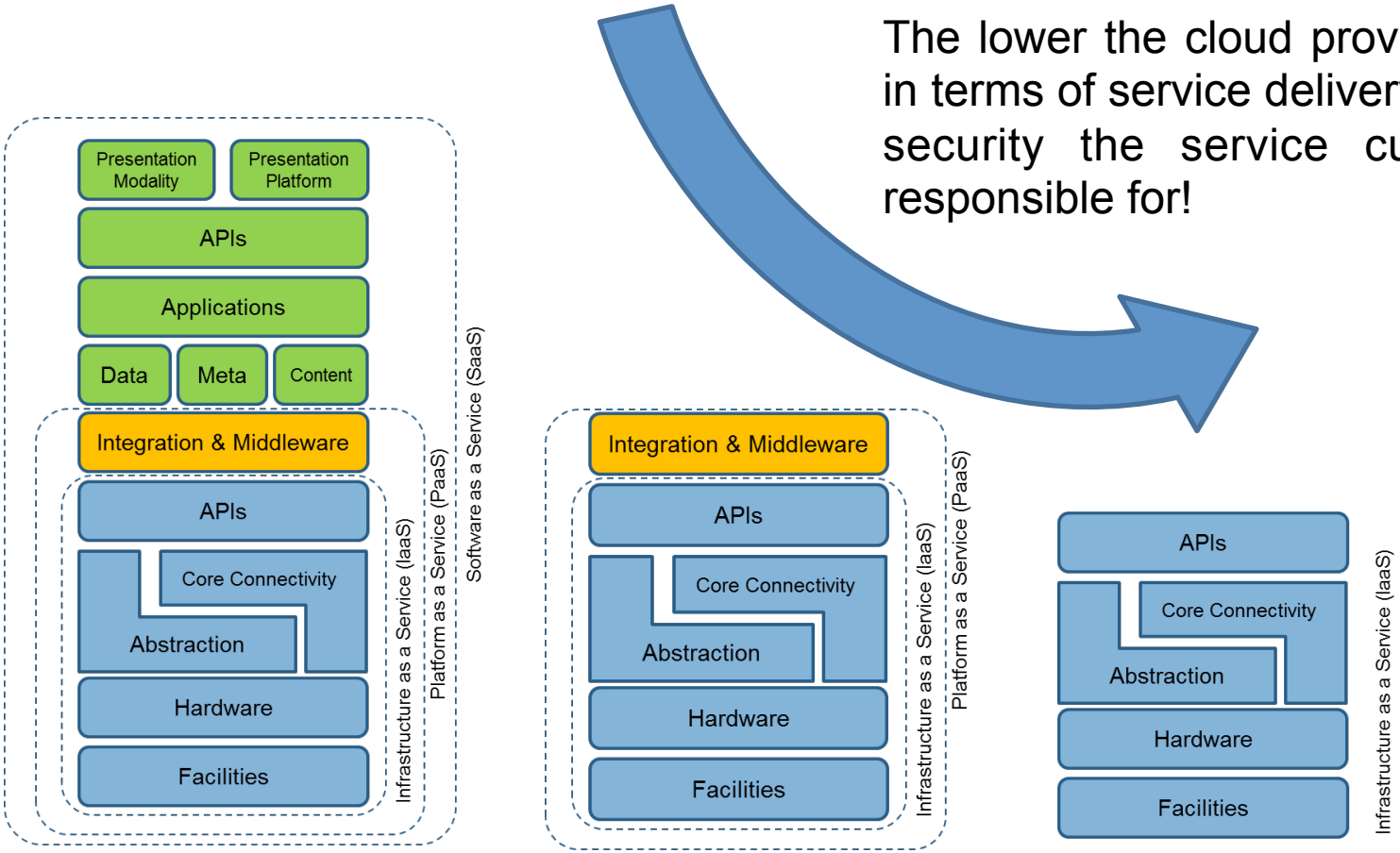
www.cs.jhu.edu/~ragib/sp10/cs412

Threat Model

- Basic components
  - Attacker modeling
    - Choose what attacker to consider
      - insider vs. outsider?
      - single vs. collaborator?
    - Attacker motivation and capabilities
  - Attacker goals
  - Vulnerabilities / threats

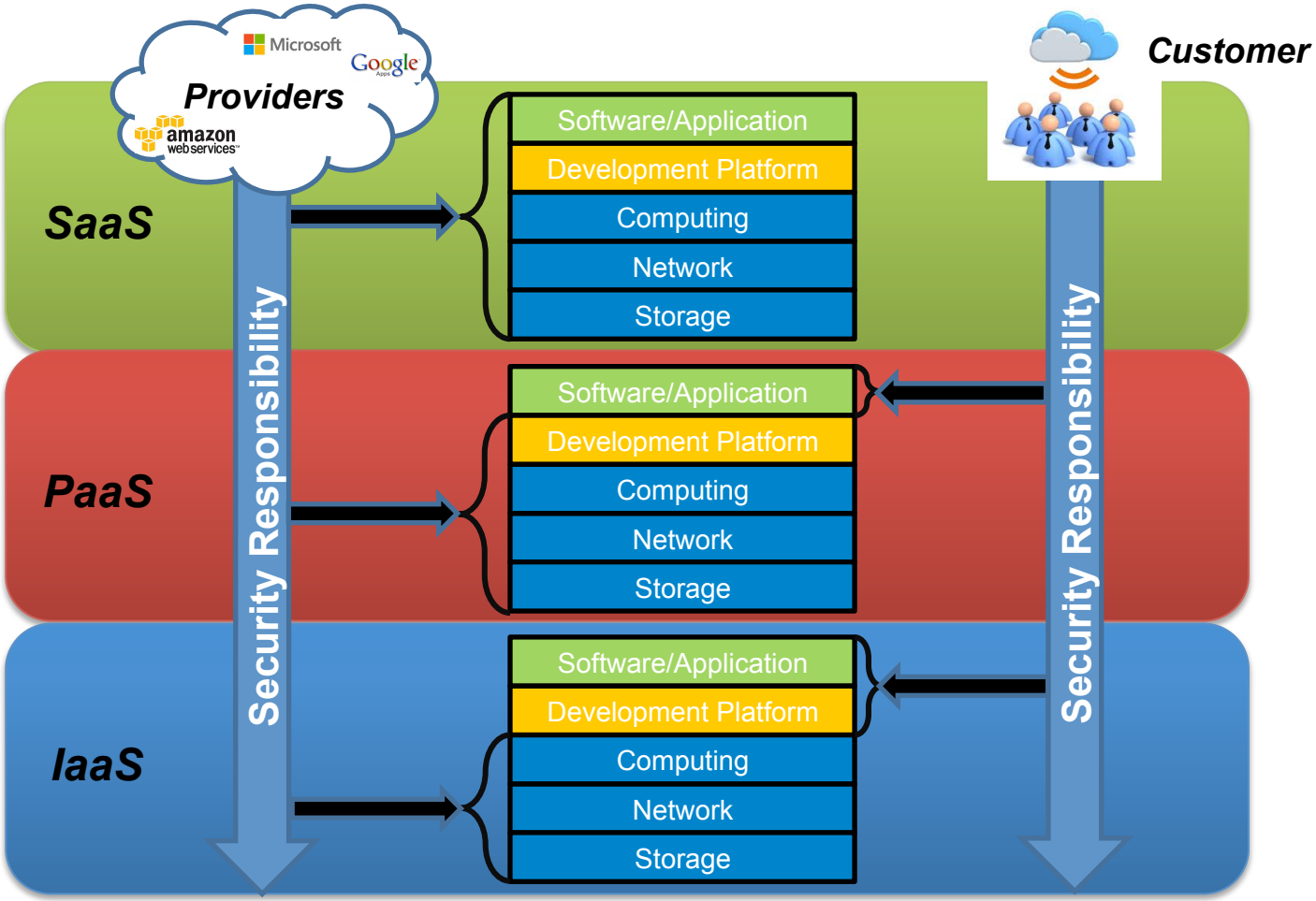
www.cs.jhu.edu/~ragib/sp10/cs412

Delivery model Security Issues



The lower the cloud provider stands in terms of service delivery, the more security the service customer is responsible for!

Delivery model Security Issues



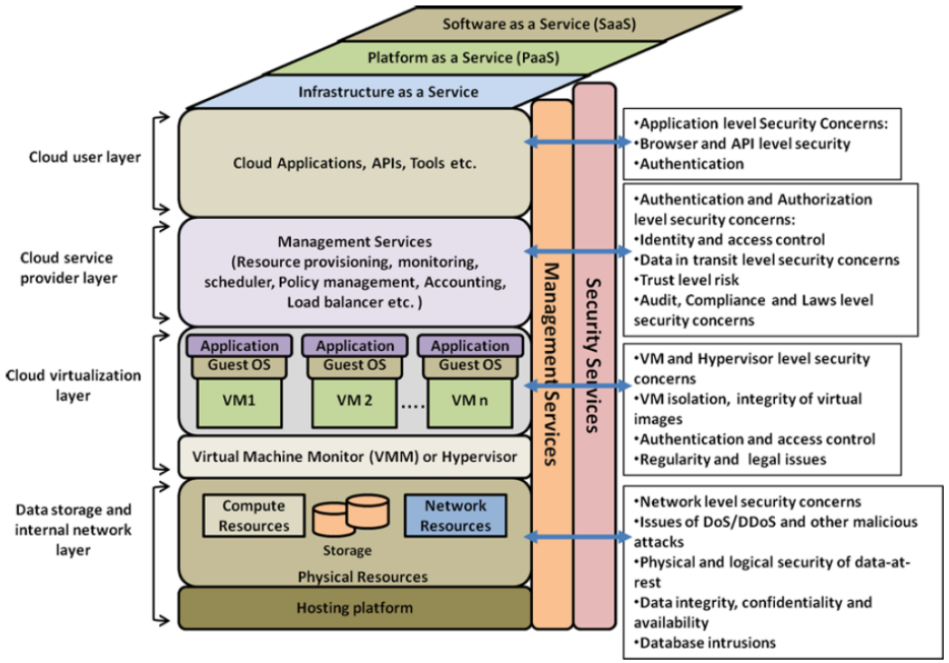
Cloud Security Taxonomy

Based on Service Models

- SaaS
  - -Cross Site Scripting
  - -Access Control Weaknesses
  - -SQL Injection Flaws
  - -Network Penetration
  - -Insecure SSL trust configuration
  - -Data Security
- PaaS
  - -Data Security Issues
- IaaS
  - -Data Reliability

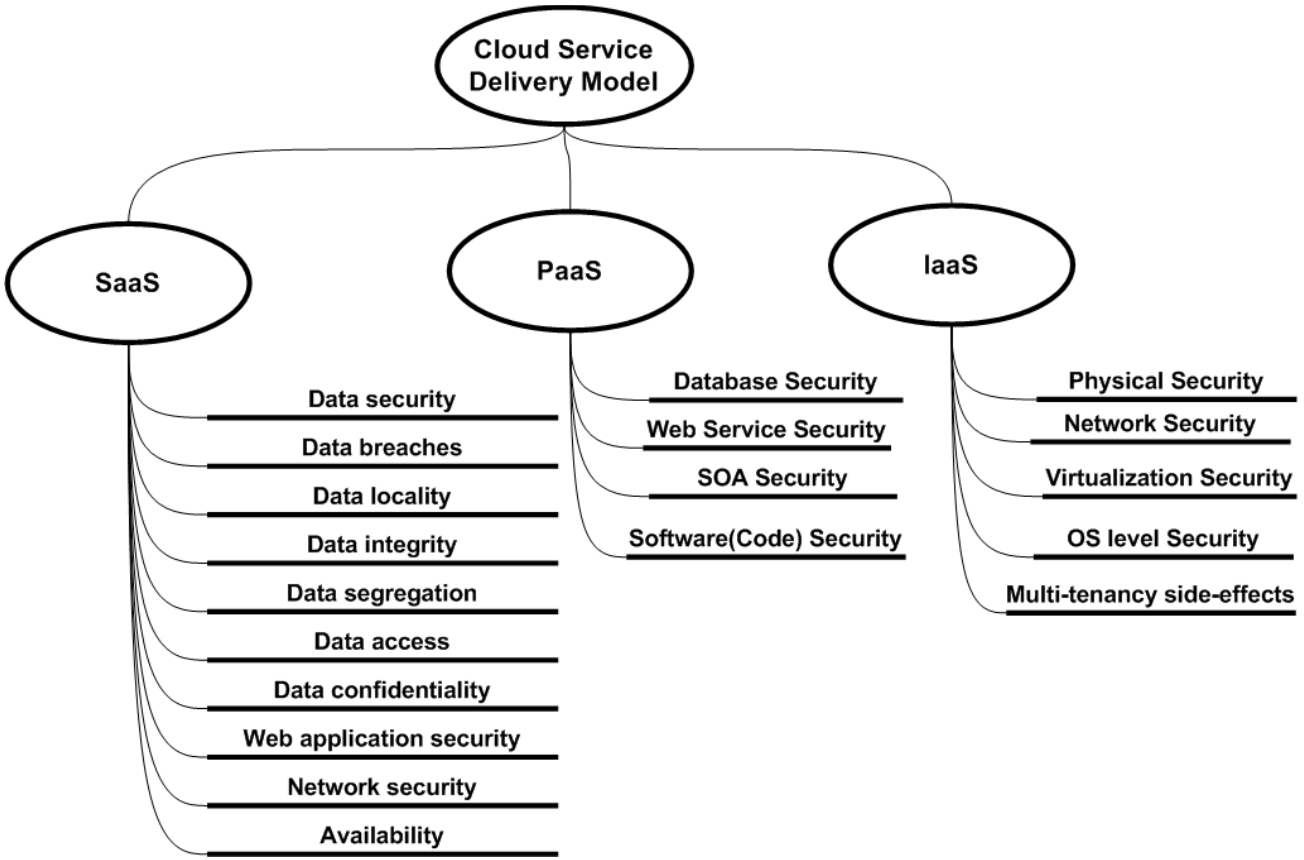
Source:V. S. Subashini, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. 34, pp. 1-11, 2011.

Based on Layers

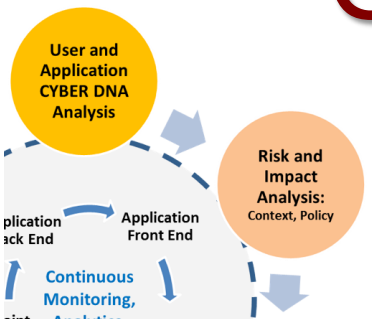


Source: C. Modi, D. Patel, B. Borisaniya, A. Patel and M. Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," The Journal of Supercomputing, pp. 1-32, 2012.

Delivery model Security Issues



Cloud Risk and Impact Analysis



Attacks	Attack Target	Impact
Cross Site Scripting SQL Injection Flaws Code malware, Worms Viruses, Flooding	**Cloud User Layer** Cloud Apps, APIs, Tools	Dollar and Reputation Loss, DoS, etc.
Identify and Access Control Insider Threats Insecure SSL trust configuration	**Cloud Service Provider Layer** Provisioning, Monitoring, Scheduling, Policy Management	Induced failures, availability, DoS, Inaccuracies, Reputation loss
VM and Hypervisor attacks VM integrity attacks Authentication and access control Backdoor implants	**Cloud Virtualization Layer** Applications, Guest OS, Virtual Machine Monitor,	VM privacy loss, Integrity of VM images
Dos/DDoS attacks Data integrity, confidentiality and availability Database intrusions	**Physical Resources Layer** Computing, Storage and Network Resources	Malfunctions, Data and Performance loss, Physical destruction

The Notorious Nine

- The CSA(Cloud Security Alliance) has identified "The Notorious Nine", the top 9 cloud computing threats for 2013.

1. Data Breaches
2. Data Loss
3. Account Hijacking
4. Insecure APIs
5. Denial of Service
6. Malicious Insiders
7. Abuse of Cloud Services
8. Insufficient Due Diligence
9. Shared Technology Issues

Data Breaches/Loss

- Deletion or alteration of records without a backup, Loss of an encoding key are some of the common examples which leads to data loss.
- As the data resides on the third parties data centers, security of data is becoming the main concern for cloud adoption.
- Thus it is the duty of Cloud security provider to prevent the unauthorized parties from gaining access to the sensitive data.

Data Loss Remediation

- Implementing strong access controls
- Strong encryption and decryption for data.
- Implement strong key generation, storage and management, and destruction practices.
- Maintaining back up for the data and updating the changes timely.

Data Breaches

SERVICE MODEL

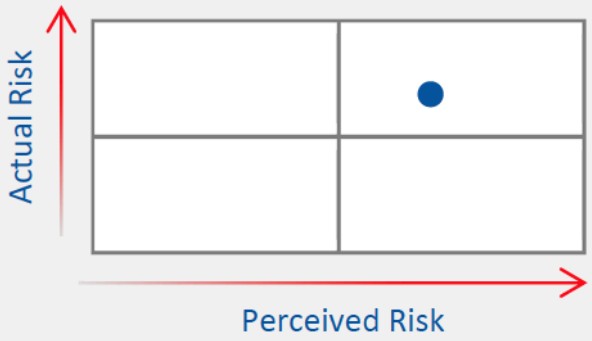
IaaS | PaaS | SaaS

RISK ANALYSIS

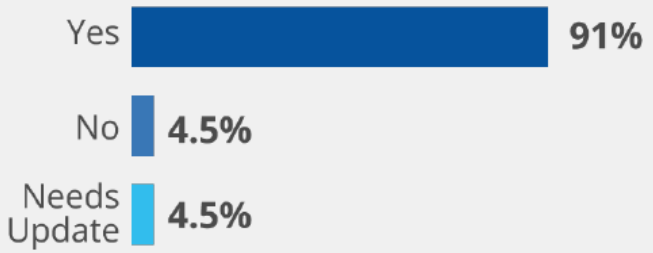
CIANA: Confidentiality

STRIDE: Information Disclosure

RISK MATRIX



IS THREAT STILL RELEVANT?



Source: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

Taxonomy of Security

- CIANA
  - stands for Confidentiality, Integrity, Availability, Non-Repudiation, and Authentication (Information Assurance, Information Security)
- **STRIDE** is a system developed by Microsoft threat analysis:

– **S**poofing of user identity
– **T**ampering
– **R**epudiation
– **I**nformation disclosure (privacy breach or data leak)
– **D**enial of service (D.o.S)
– **E**levation of privilege

Data Loss

SERVICE MODEL

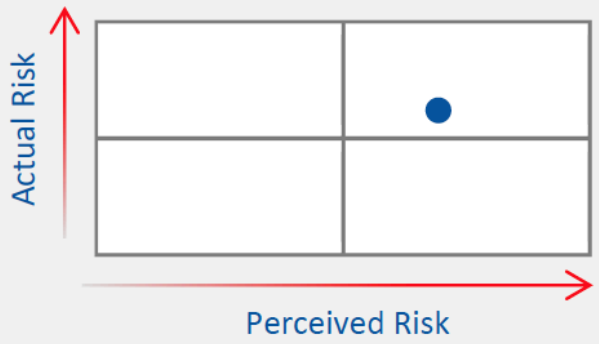
IaaS | PaaS | SaaS

RISK ANALYSIS

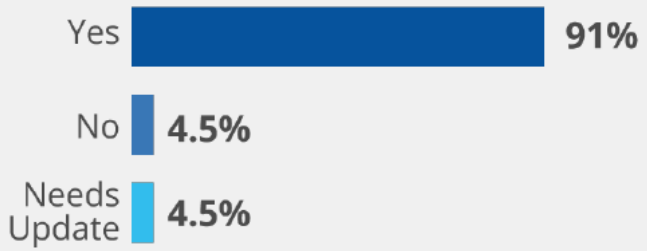
CIANA: Availability, Non-Repudiation

STRIDE: Repudiation, Denial of Service

RISK MATRIX



IS THREAT STILL RELEVANT?



Source: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

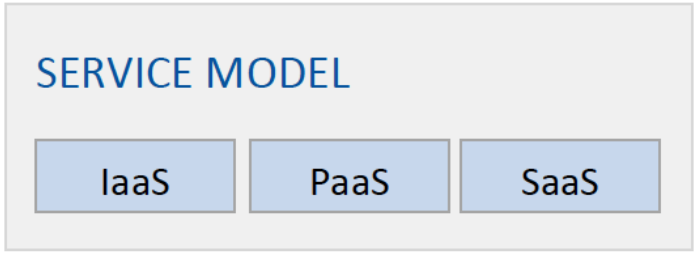
Account, Service and Traffic Hijacking

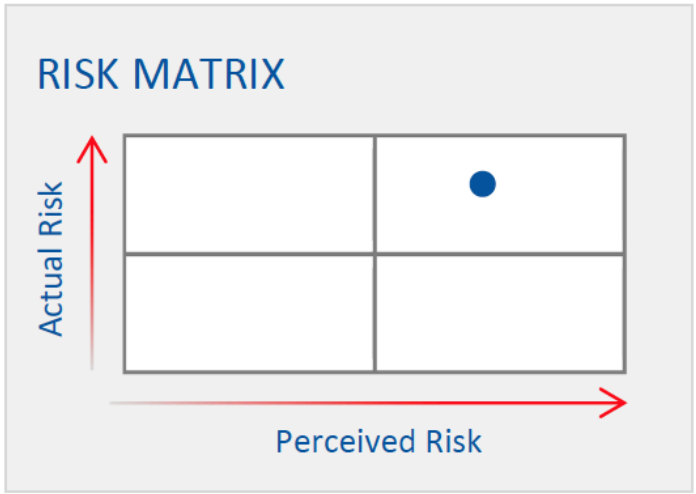
- If an attacker gains access to the credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites.
- Using the credentials and passwords for longer time without changing and reusing the same for different accounts makes this type of attack easy.

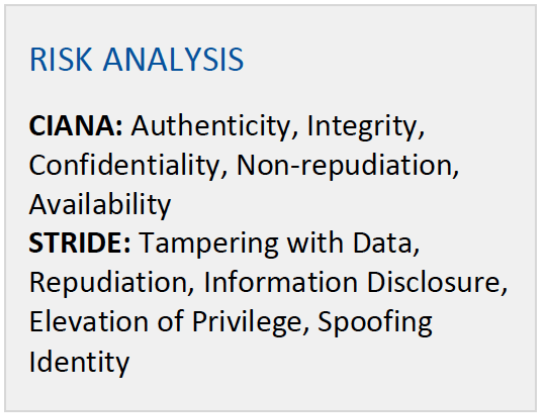
Remediation

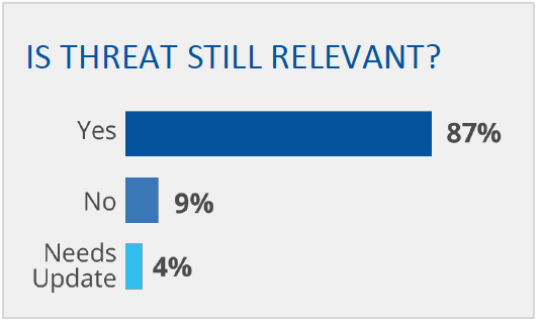
- Following the password rules to create strong passwords
- Changing the passwords timely
- Prohibiting the use of passwords on unknown machines and sharing of the passwords with other users

Account or Service Traffic Hijacking









Source: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

Insecure APIs

- The security of the cloud services is dependent on how secure is their API's
- accidental and malicious attempts must be taken into consideration when designing the APIs
- Organizations are facing a variety of authenticity, confidentiality, and integrity, issues due to their dependence on a weak set of APIs

Insecure APIs

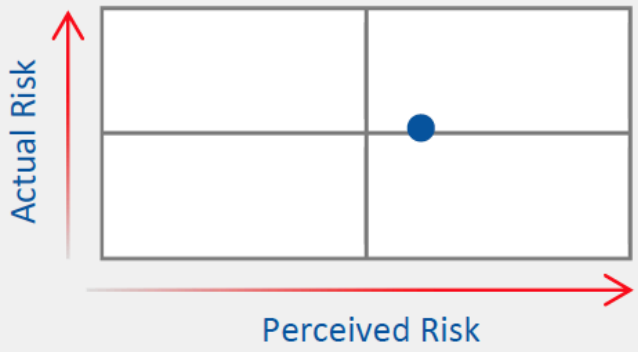
SERVICE MODEL

IaaS | PaaS | SaaS

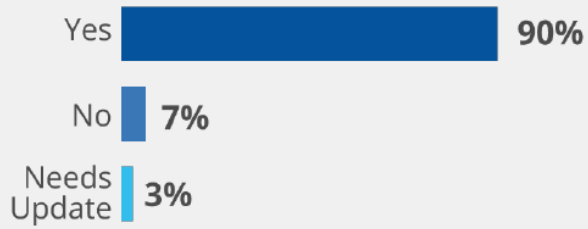
RISK ANALYSIS

CIANA: Authenticity, Integrity, Confidentiality
STRIDE: Tampering with Data, Repudiation, Information Disclosure, Elevation of Privilege

RISK MATRIX



IS THREAT STILL RELEVANT?



Source: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

Remediation

- Analyze the security model of cloud provider interfaces.
- Ensure strong authentication and access controls are implemented in concert with encrypted transmission.

Denial of Service

- Preventing users from accessing cloud services.
- Using resource exhaustion attacks or software vulnerability attacks.
- The cloud becomes irresponsive or legal users will pay more for using more resources.

Denial of Service

SERVICE MODEL

IaaS | PaaS | SaaS

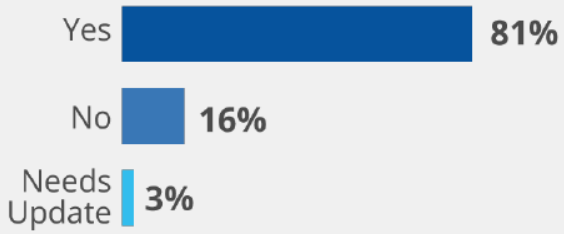
RISK ANALYSIS

CIANA: Availability

STRIDE: Denial of Service

RISK MATRIX

IS THREAT STILL RELEVANT?



Source: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

Remediation

- None is provided by CSA
- Anomaly Behavior Analysis (ABA)
- Intrusion Tolerance by using diversity and redundancy

Malicious Insiders

- Malicious insider threat is well-known to most organizations.
- A provider may not reveal how it grants employees access to physical and virtual assets, how it monitors these employees, or how it analyzes and reports on policy compliance.
- This kind of situation clearly creates an attractive opportunity for hobbyist hacker.

Malicious Insiders

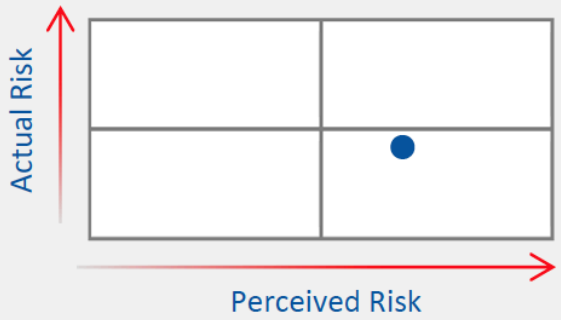
SERVICE MODEL

IaaS | PaaS | SaaS

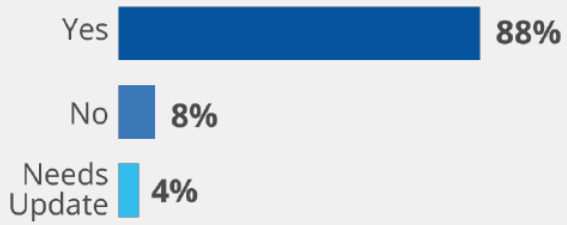
RISK ANALYSIS

STRIDE: Spoofing, Tampering, Information Disclosure

RISK MATRIX



IS THREAT STILL RELEVANT?



Source: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

Remediation

- Human resource required specifications should be part of legal contract.

- Cloud Service Provider should provide transparently all security and management practices.

Abuse of Cloud Services

- The registration process for cloud resources has become so easy that anyone with a valid credit card can register and immediately begin using services.
- Thus, spammers, malicious code authors, and other criminals have been able to conduct their activities with relative impunity
- Thus PaaS and IaaS providers are suffering from these kind of attacks.

Abuse of Cloud Services

SERVICE MODEL

IaaS | PaaS | SaaS

RISK ANALYSIS

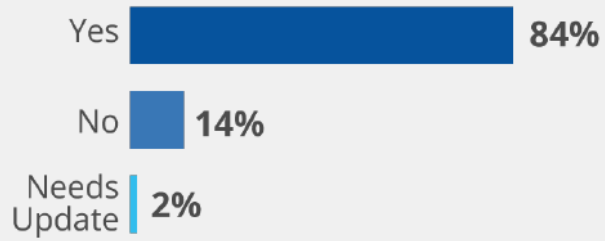
CIANA: N/A

STRIDE: N/A

RISK MATRIX

N/A

IS THREAT STILL RELEVANT?



Source: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

Impact

- Attackers are coming up with new technologies to improve their reach, avoid detection and improve the effectiveness of their activities.
- The reasons for this type of attacks are:
  - Weak registration systems that are facilitating the anonymity.
  - Limited capabilities of service providers to fraud detection capabilities

Remediation

- Strict initial registration and validation
- Enhanced credit card fraud monitoring and coordination
- Constant monitoring of customer network traffic.
- Monitoring public blacklists for one's own network blocks.

Insufficient Due Diligence

- Organizations moving fast toward the cloud for its cost reductions, operational efficiencies and improved security.
- However, without a full understanding of the cloud service provider environment and responsibilities, they are increasing their risk.

Insufficient Due Diligence

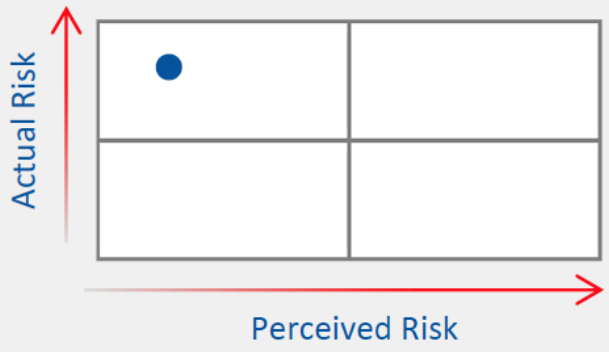
SERVICE MODEL

IaaS | PaaS | SaaS

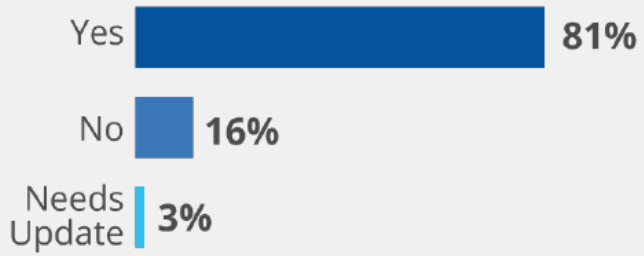
RISK ANALYSIS

STRIDE: All

RISK MATRIX



IS THREAT STILL RELEVANT?



Source: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

Remediation

- Organizations need to understand the risk of moving to the cloud.
- 24/7 Continuous Monitoring, Analysis, and Mitigation

Shared Technology Vulnerabilities

- Cloud Service Providers deliver their services in a scalable way by sharing infrastructure.
- Cloud services depend on utilizing virtualization.
- Virtualization Hypervisors, like any other software, have flaws that allow attackers with access to the guest operating system to attack the host.
- This impacts the operations of other cloud customers and allow attackers to gain access to unauthorized data.

Shared Technology Issues

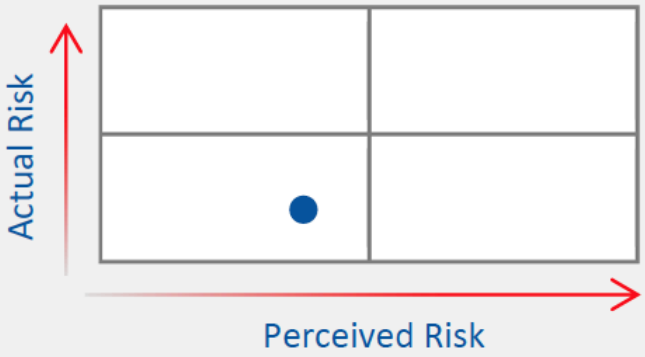
SERVICE MODEL

IaaS | PaaS | SaaS

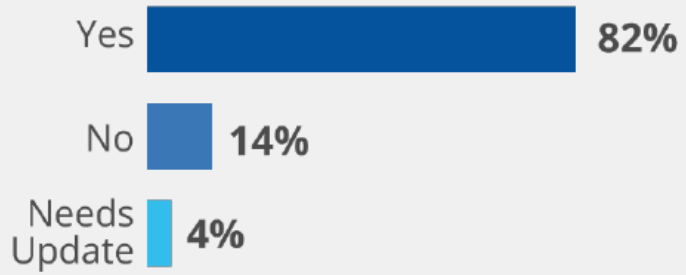
RISK ANALYSIS

STRIDE: Information Disclosure, Elevation of Privilege

RISK MATRIX



IS THREAT STILL RELEVANT?



Source: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

Remediation

- Implementing and applying security best practices for both the installation and configuration processes
- Continuously monitoring for the environment to detect unauthorized activities.
- Enforcing strict access control and strong authentication for all critical operations.
- Continuously searching for vulnerabilities and threats.

Unknown risk Profile

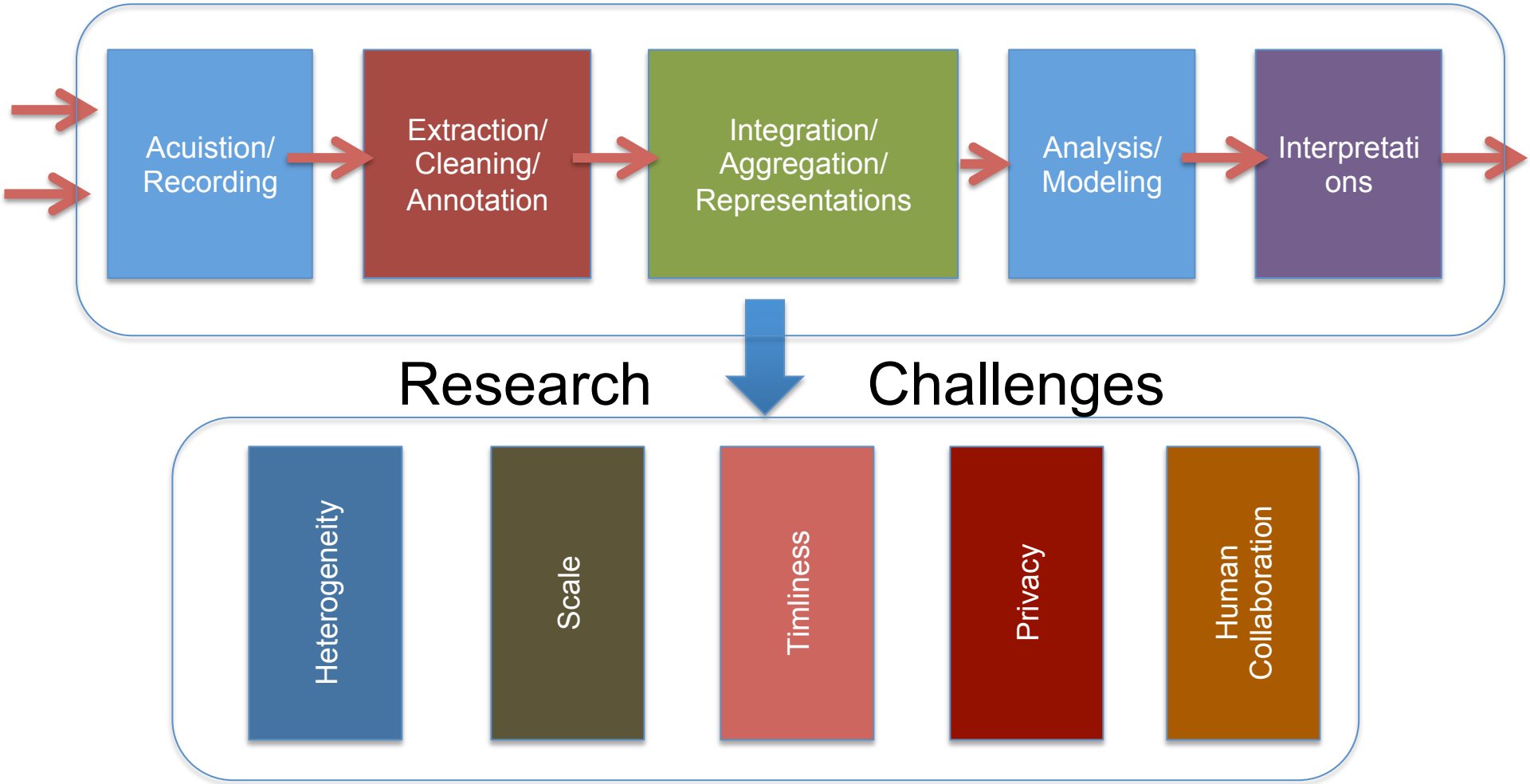
- The features and functionality of the cloud services are well informed to the customer, but the details of internal security procedures, auditing, logging, internal access control remains unanswered leaving customers with an unknown risk profile

General Security Issues

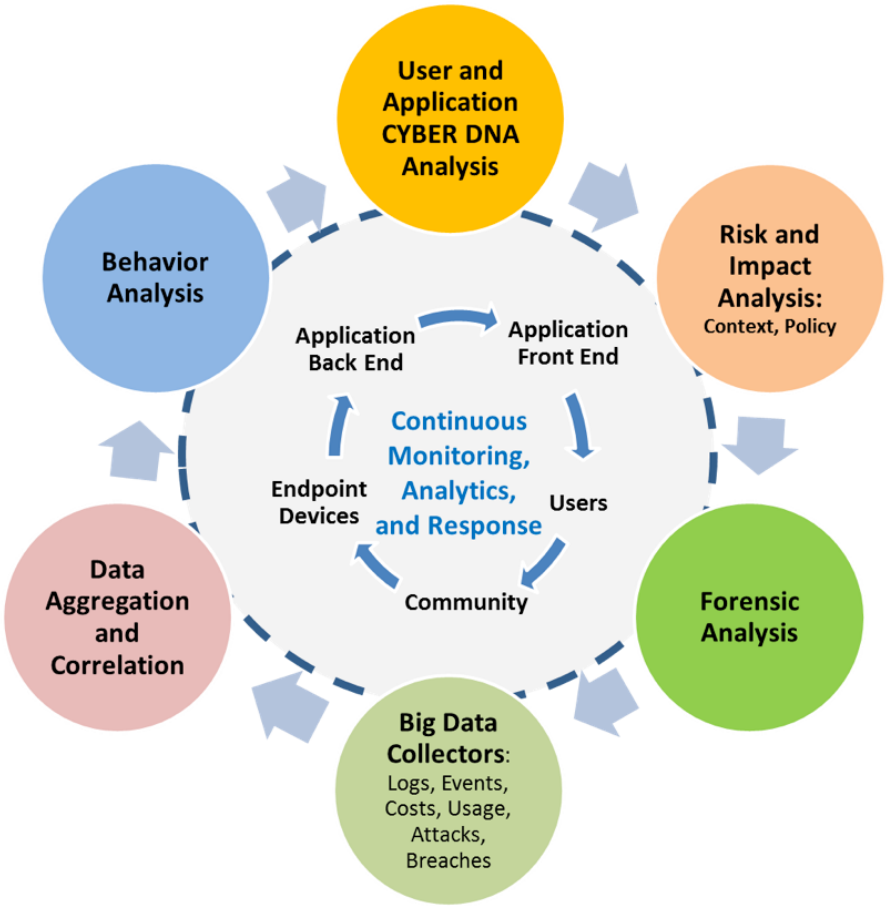
- In addition to the above mentioned top threats there are many other threats that are effecting cloud computing. They are:
- Insider Threats
- Hypervisor vulnerabilities
- Denial of Service attacks
- Malware Injection attacks
- Man-In-The Middle Cryptographic attacks

UA Ongoing Cybersecurity Research Projects

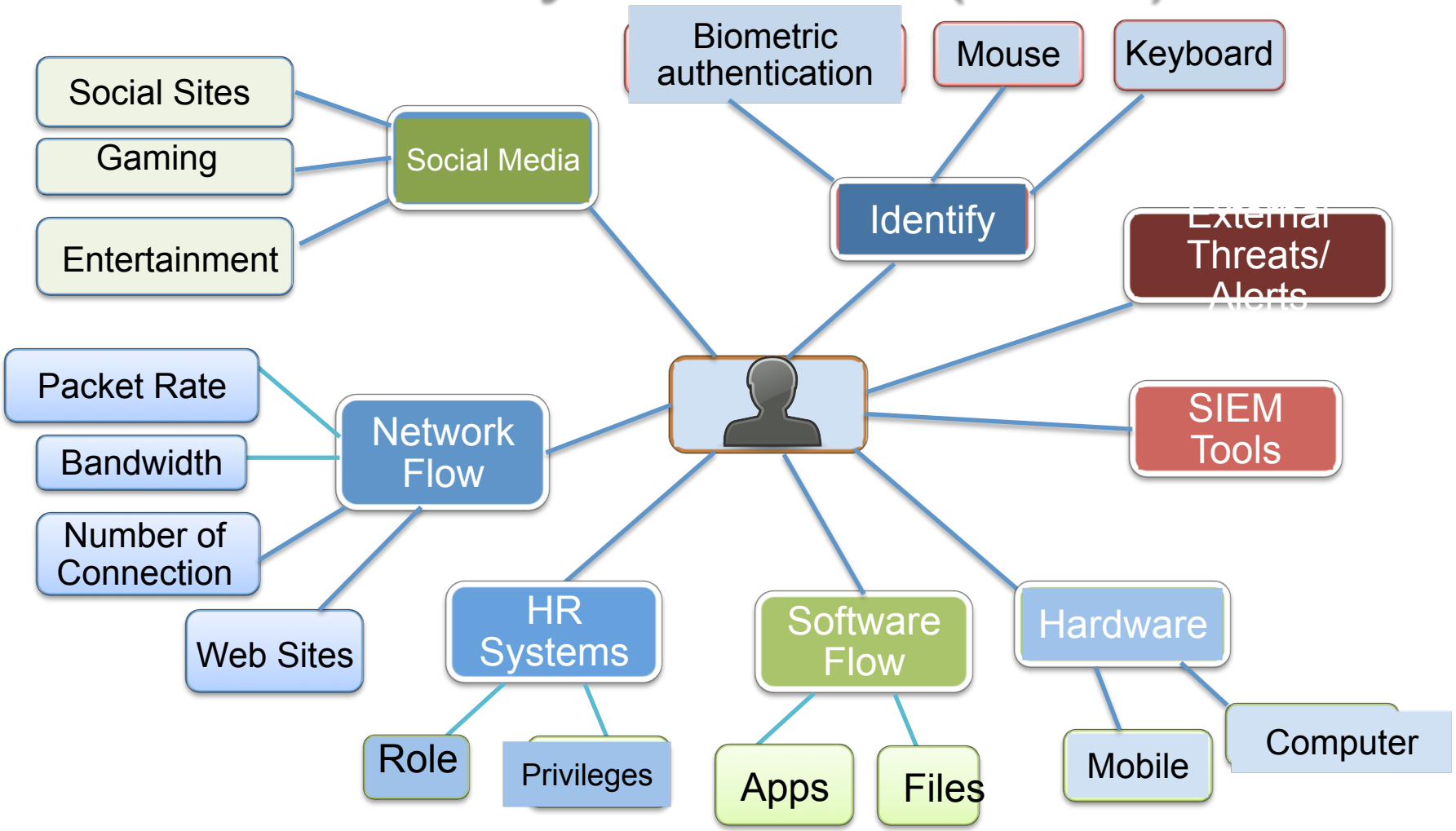
Big Data Analytics Pipeline



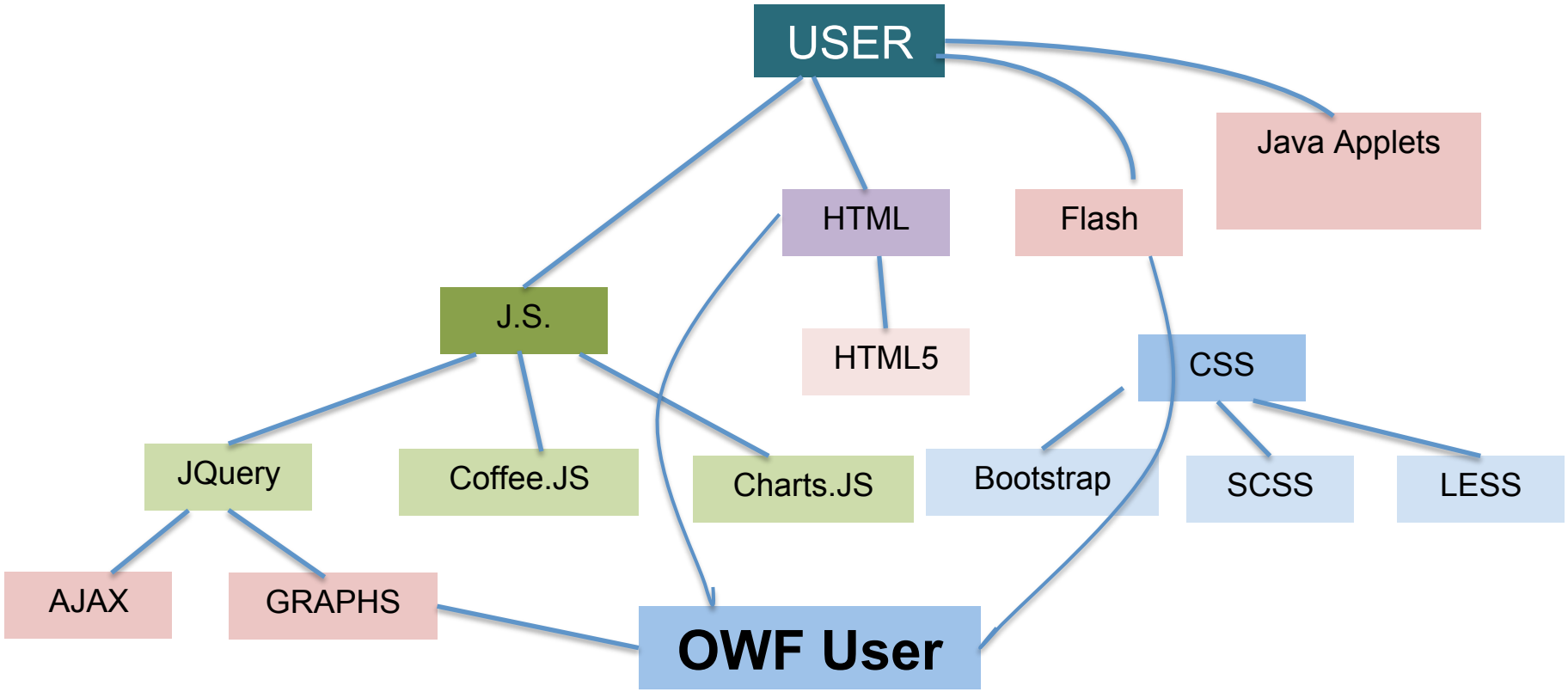
Big Data Analytics for Cyberecurity Architecture



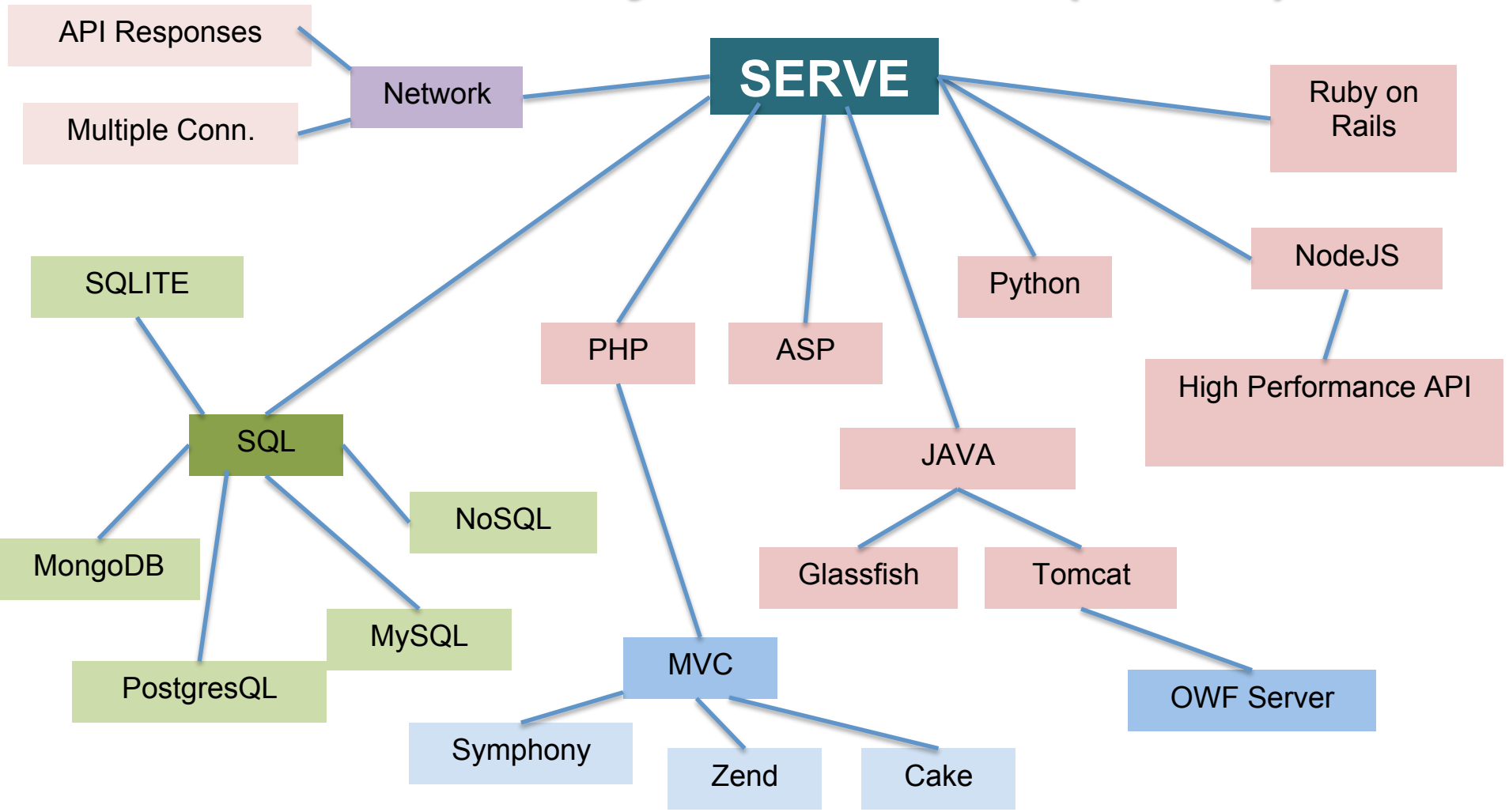
User Cyber Flow (UCF)



Application-Cyber Flow (ACF)

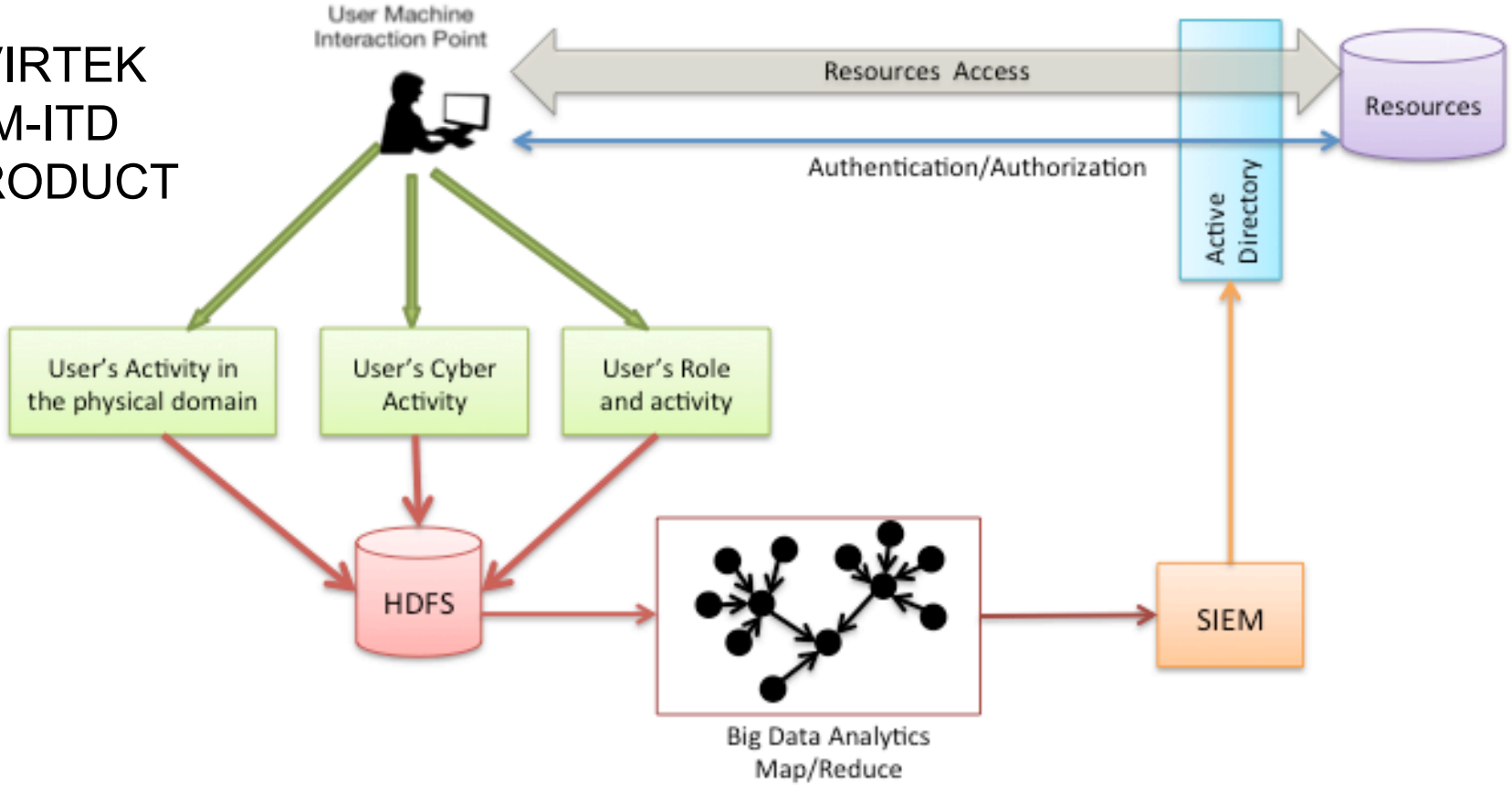


Server-Cyber Flow (SCF)



Insider Threat Detection (ITD) with Smart Big Data Analytics

AVIRTEK
AIM-ITD
PRODUCT



Conclusion

- Cloud computing is sometimes viewed as a reincarnation of the classic mainframe client-server model
  - However, resources are ubiquitous, scalable, highly virtualized
  - Contains all the traditional threats, as well as new ones
- In developing solutions to cloud computing security issues it may be helpful to identify the problems and approaches in terms of
  - Loss of control
  - Lack of trust
  - Multi-tenancy problems

Thank You