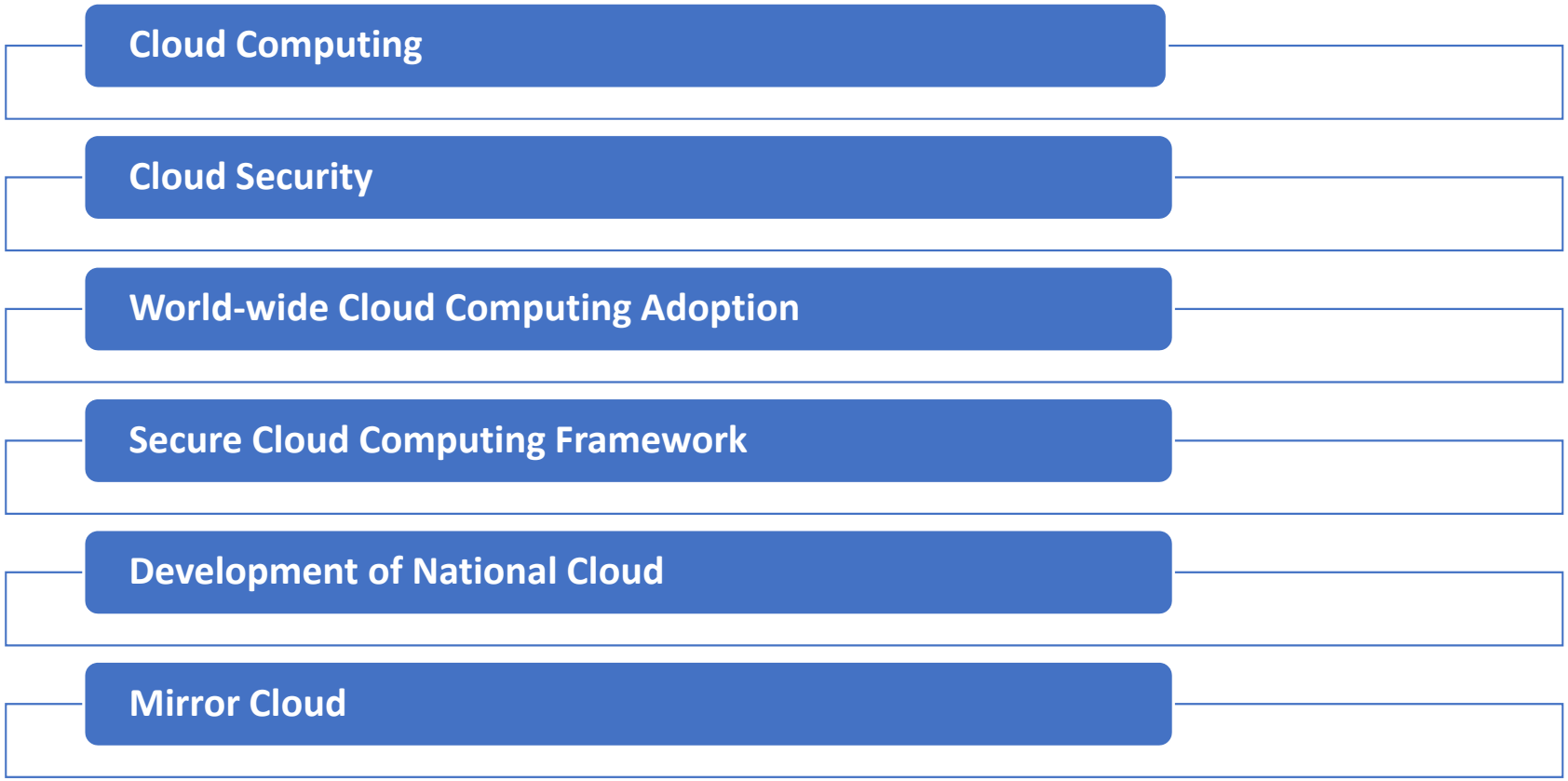

بسم الله الرحمن الرحيم

Emerging Trends in Cloud Security and their Standards

Dr. Syed Nasir Mehmood Shah
Deputy Director & Dean Sciences, KICSIT

16th International Bhurban Conference on Applied Sciences and Technology (IBCAST) 08-10 Jan 2018

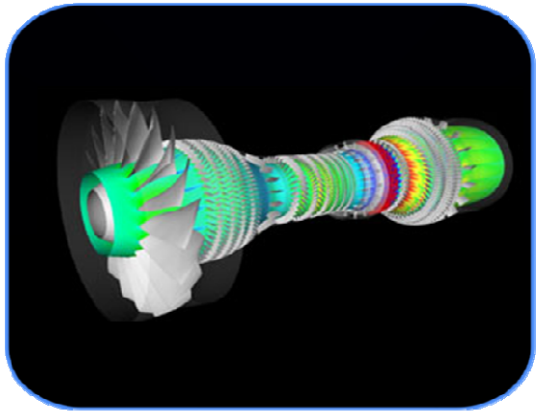
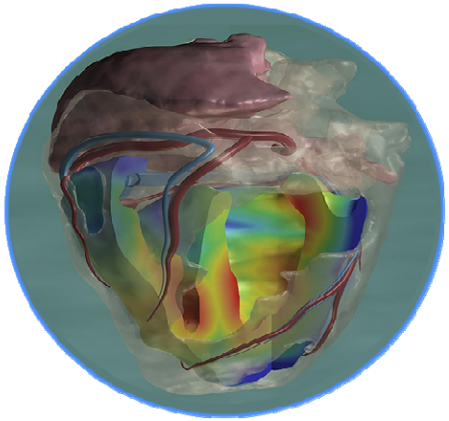
Goal of the Talk:

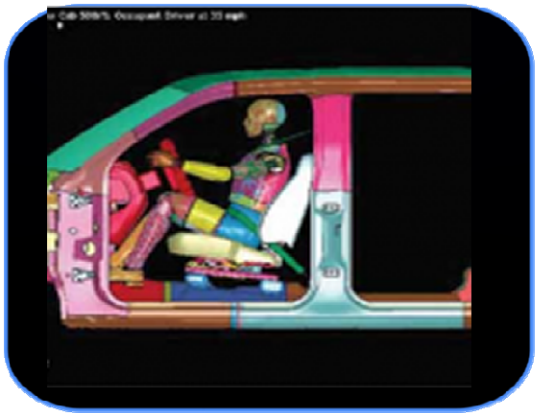
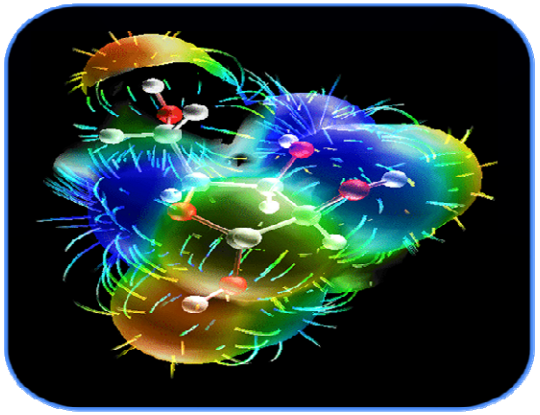
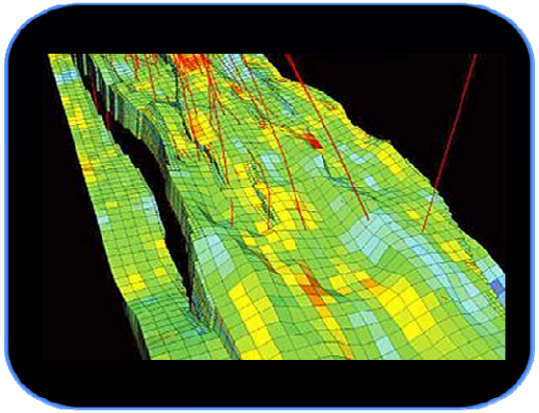


3

Cloud Computing

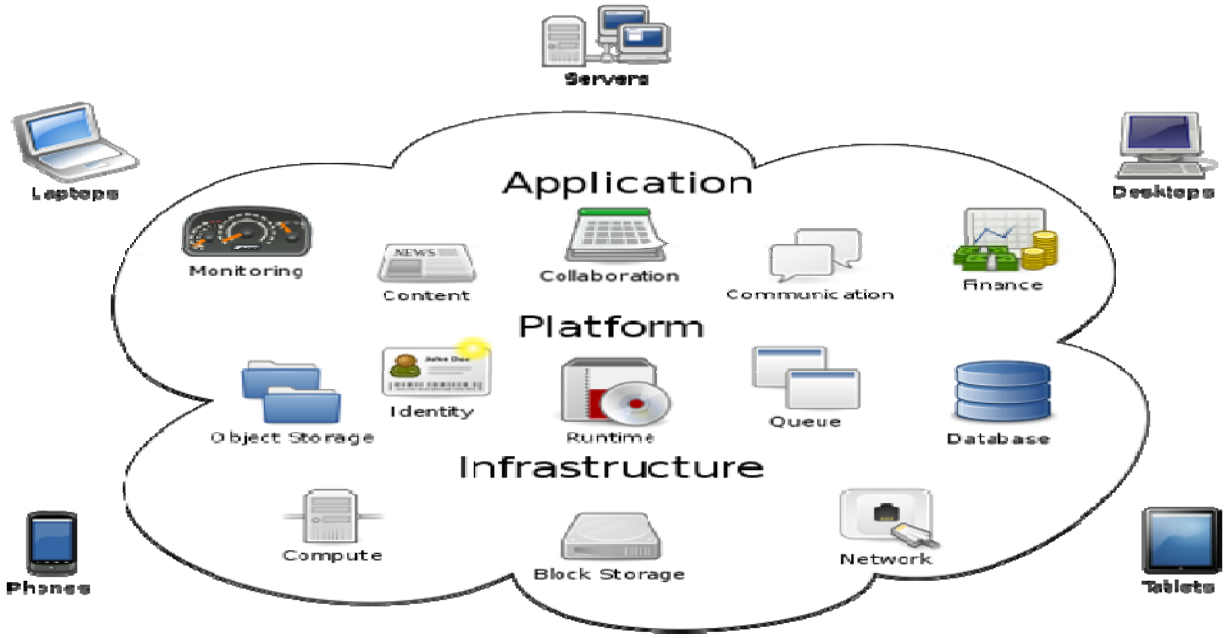
Real World

Cloud Computing

- Cloud computing is internet based computing, whereby shared resources, software and information are provided on-demand, like a public utility.



6

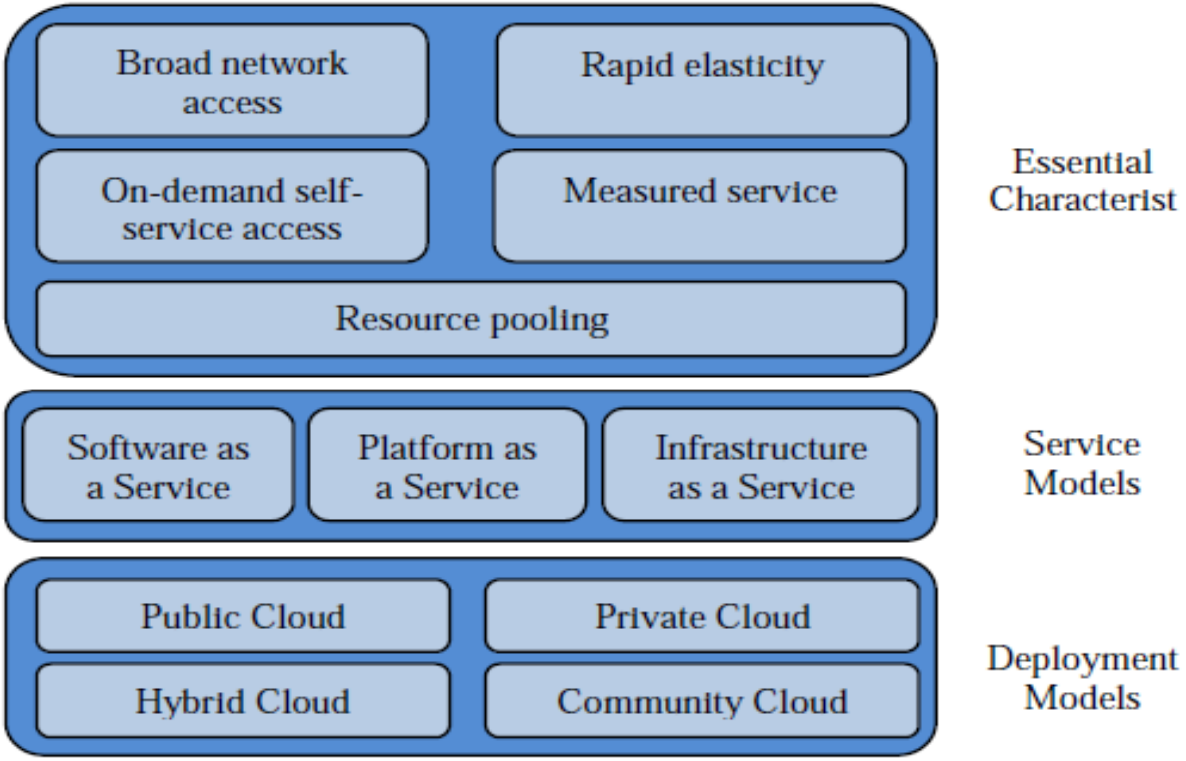
Cloud Computing

The European Network and Information Security Agency (ENISA) defines cloud computing as "an on-demand service model for IT provision, often based on virtualization and distributed computing technologies."

Cloud Computing

According to the U.S. National Institute of Standards and Technology's (NIST) definition, "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."

Cloud Computing



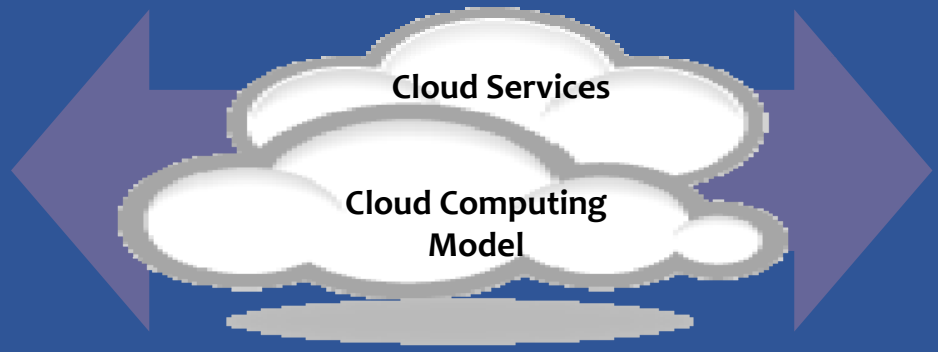
NIST visual model for cloud computing
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html

Cloud Computing Delivery Models

Flexible Delivery Models

Public ...

- Service provider owned and managed.
- Access by Subscription.
- Delivers select set of standardized business process, application and/or infrastructure services on a flexible price per use basis.
- E.g. **Amazon, Google**



Private ...

- Privately owned and managed.
- Access limited to client and its partner network.
- Drives efficiency, standardization and best practices while retaining greater customization and control
- e.g. **Mobilink, Banking Network**

Hybrid ...

- Access to client, partner network, and third party resources

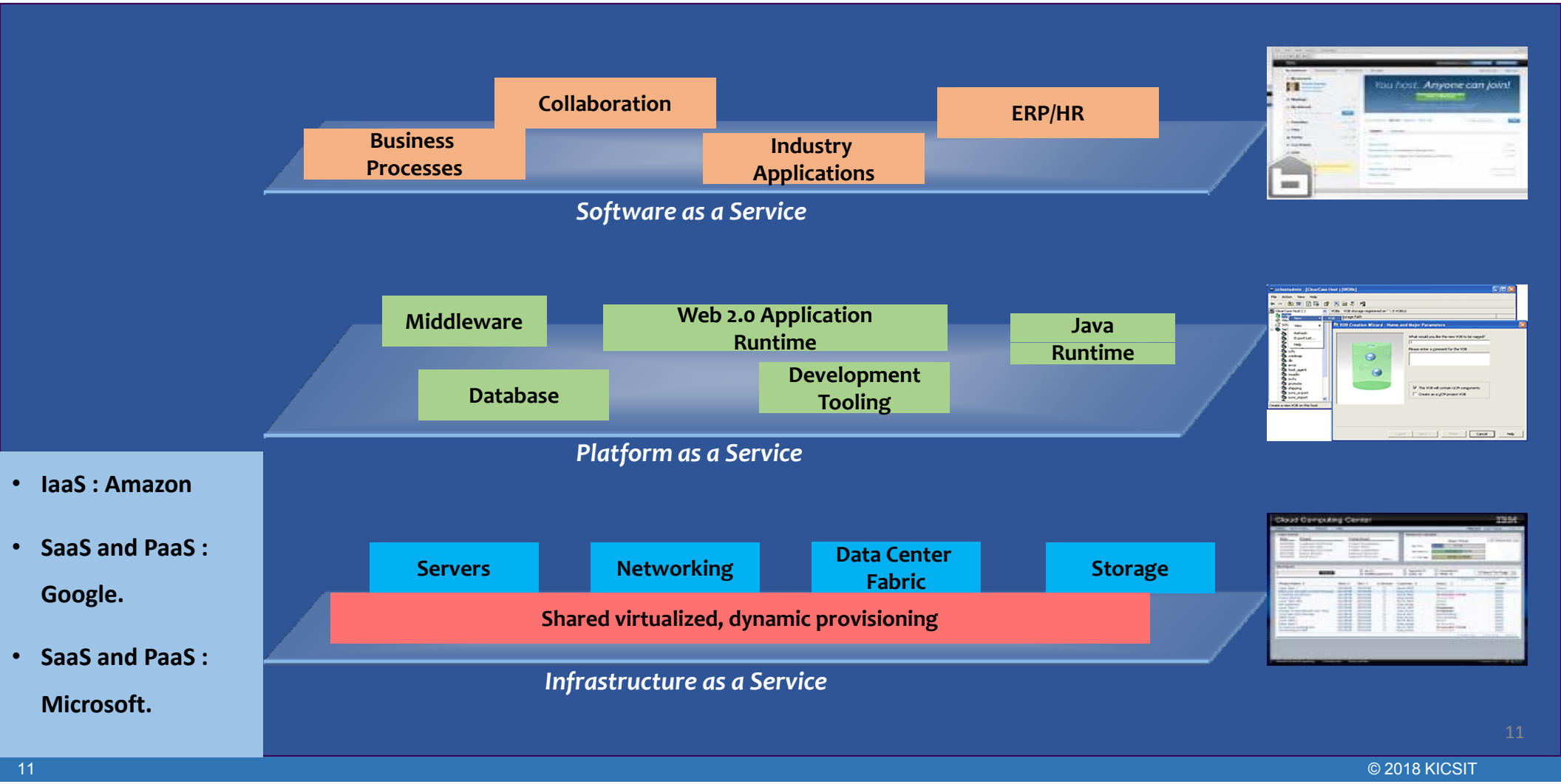
.... Standardization, capital preservation, flexibility and time to deploy

.... Customization, efficiency, availability, security and privacy

...service sourcing and service value

10

The layers of IT-as-a-Service



- IaaS : Amazon
- SaaS and PaaS : Google.
- SaaS and PaaS : Microsoft.

NCP Cloud Node of

CERN CLOUD

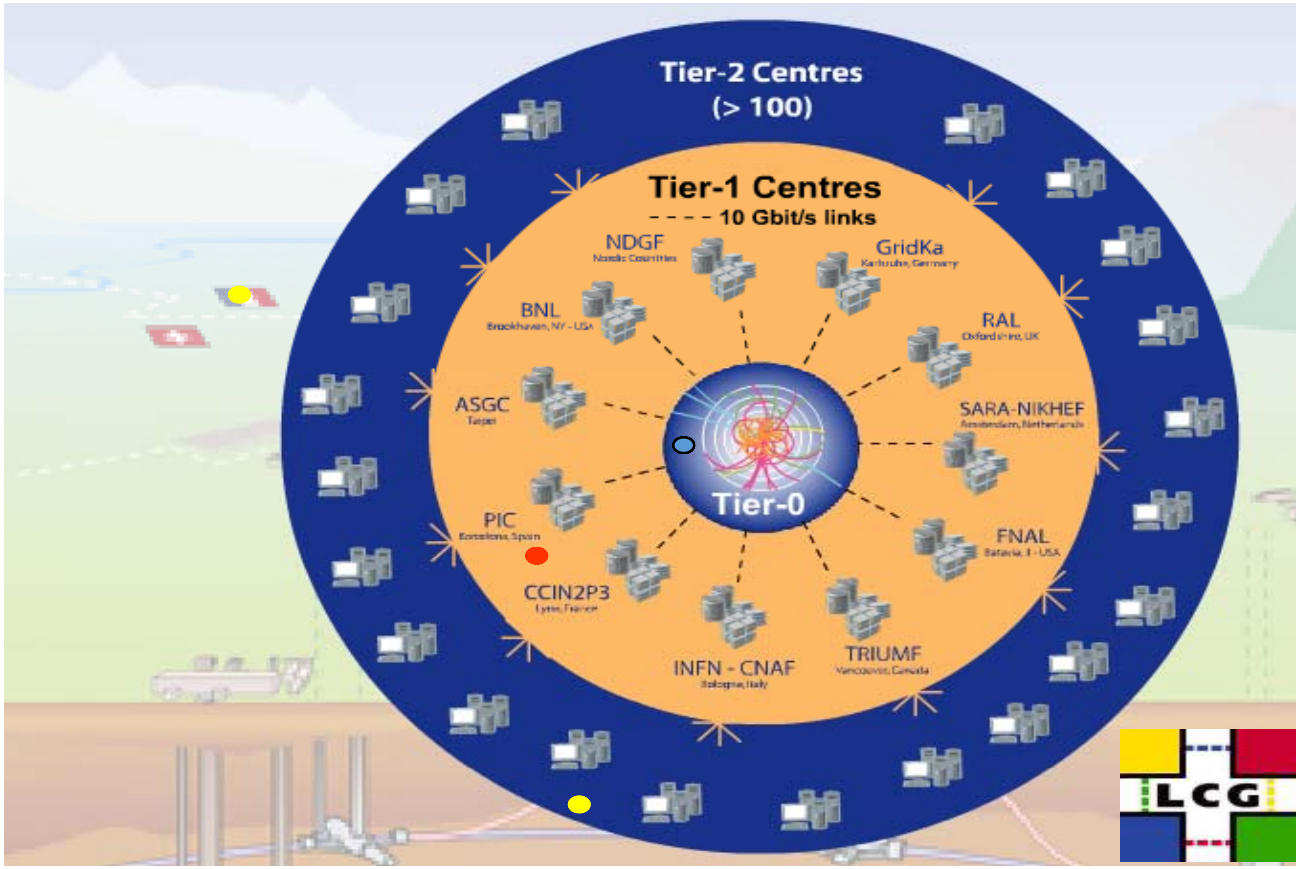
The LHC Data Challenge

- Once the accelerator is completed it will run for 10-15 years
- Experiments will produce about 15 Million Gigabytes of data each year
- LHC data analysis requires a computing power equivalent to ~100,000 of today's fastest PC processors
- Requires many cooperating computer centres, as CERN can only provide ~20% of the capacity

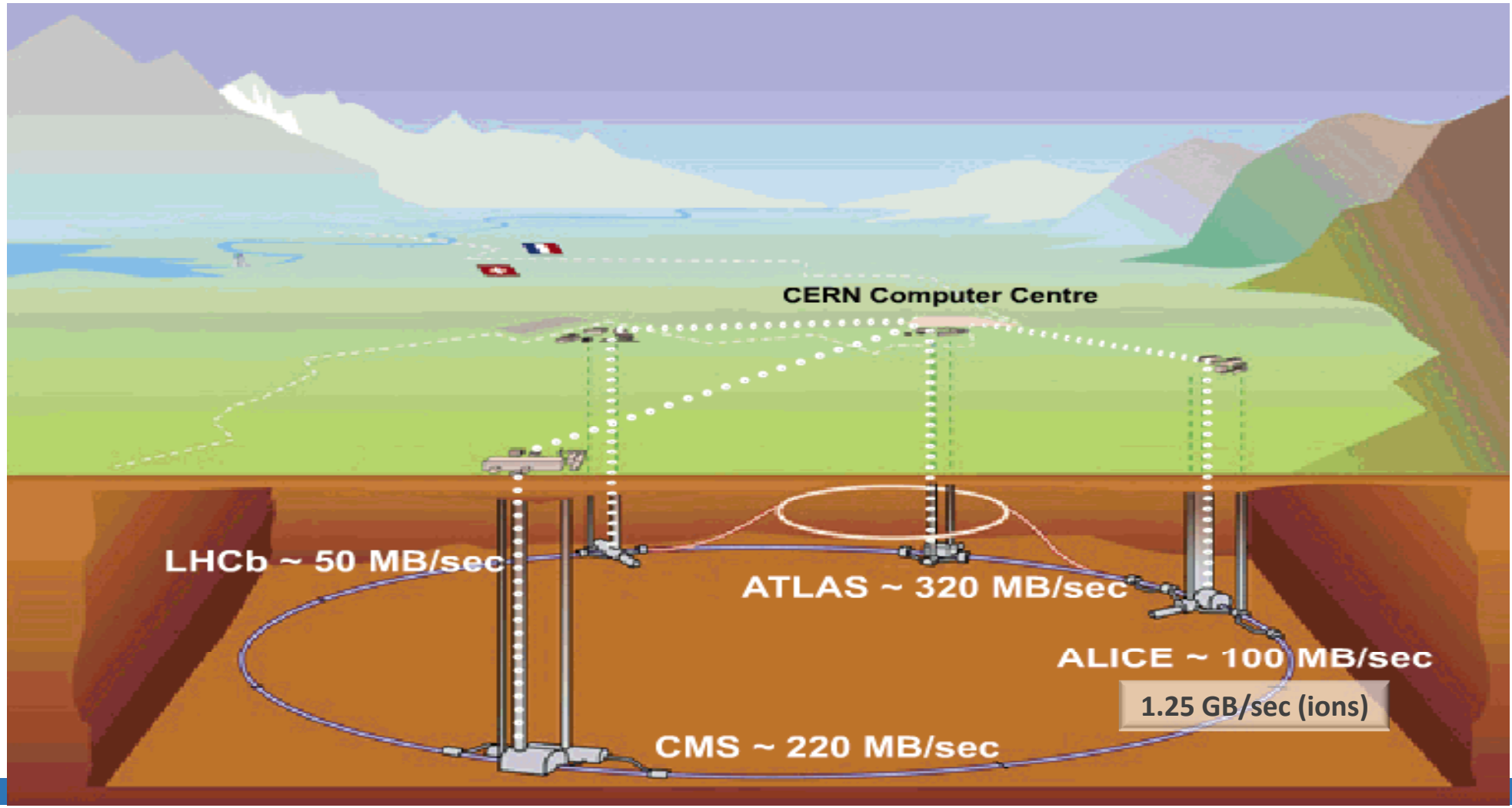
Solution: Cloud

LHC Computing Grid project (LCG)

- More than 140 computing centres
- 12 large centres for primary data management: CERN (Tier-0) and eleven Tier-1s
- 38 federations of smaller Tier-2 centres
  - 7 Tier 2 in Spain: supporting ATLAS, CMS, LHCb
- 35+ countries involved



Tier 0 at CERN: Acquisition, First pass reconstruction, Storage & Distribution



NCP Cloud

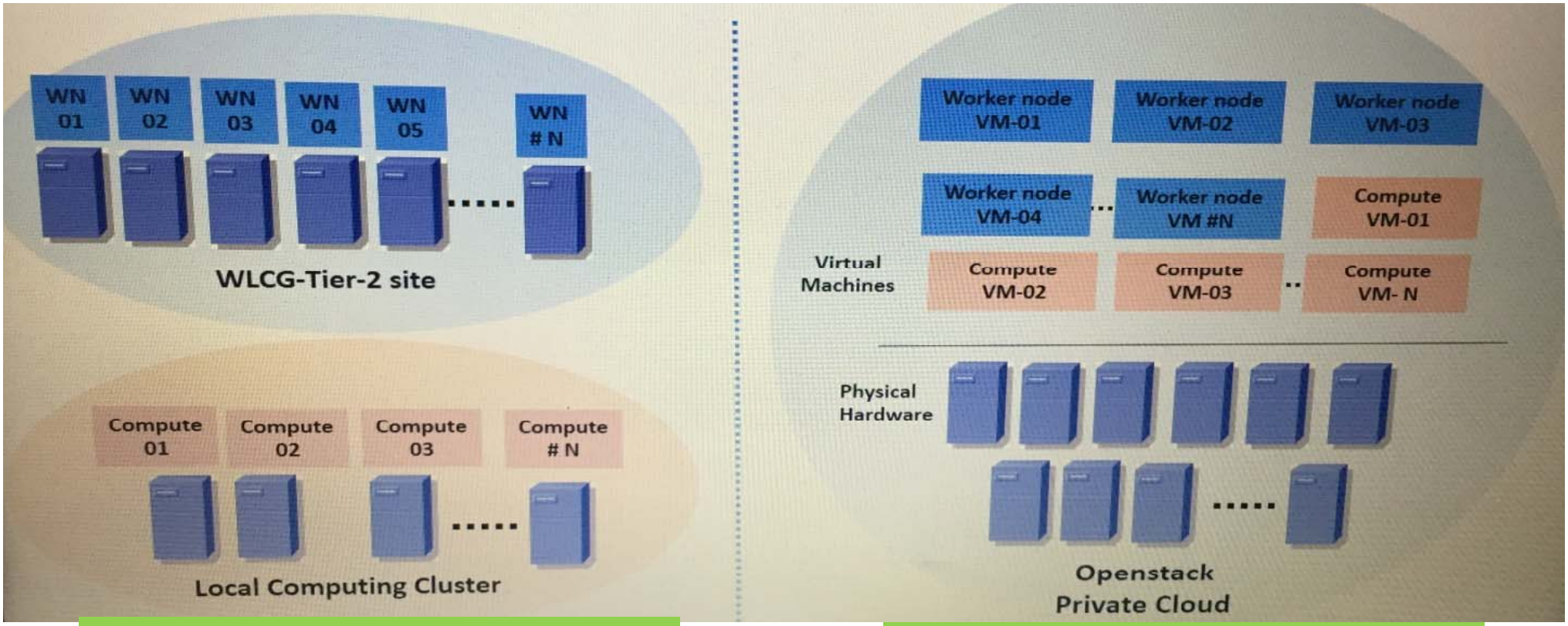
NCP is maintaining a large computing infrastructure:-

1. Hosted a **WLCG TIER-2 Site** comprising of 524 CPU Cores and 400 TB of Disk Storage
2. **HPC Cluster** of 96 CPU Cores installed for local scientific community

HPC Research areas @ NCP

- Computational Fluid Dynamics(CFD)
- Molecular Biology
- Bio Chemistry
- Physics
- Weather Forecasting
- Density Functional Theory (DTF)
- Ion channeling
- Multi-Particle Interaction

Cloud Deployment @ NCP



Traditional Computing Model

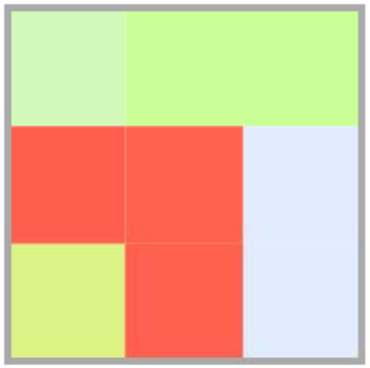
Migration to Cloud Computing Model

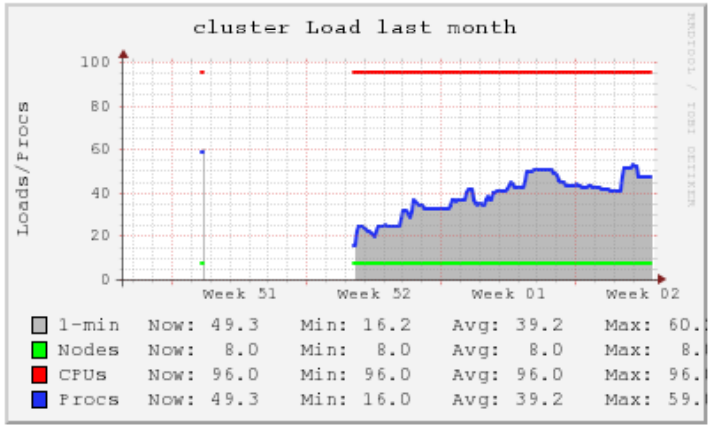
HPC Cluster@ NCP

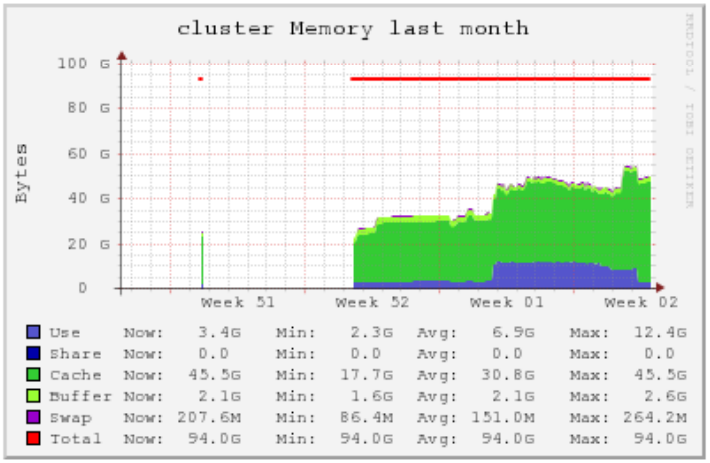
CPUs Total: **96**
Hosts up: **8**
Hosts down: **0**

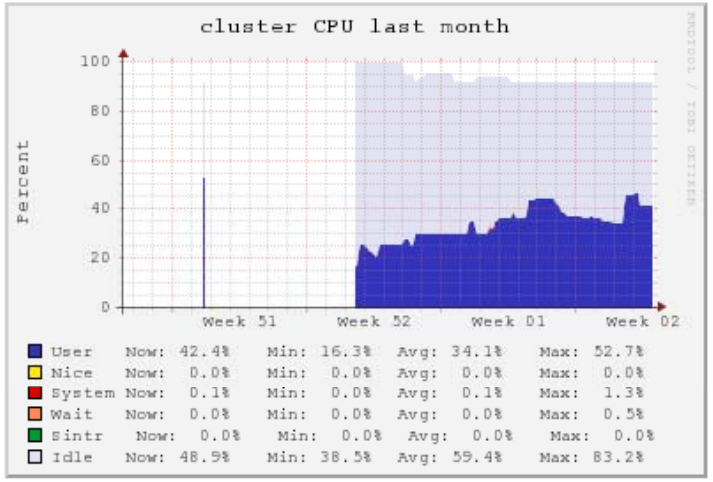
Current Load Avg (15, 5, 1m):
50%, 50%, 51%
Avg Utilization (last month):
41%

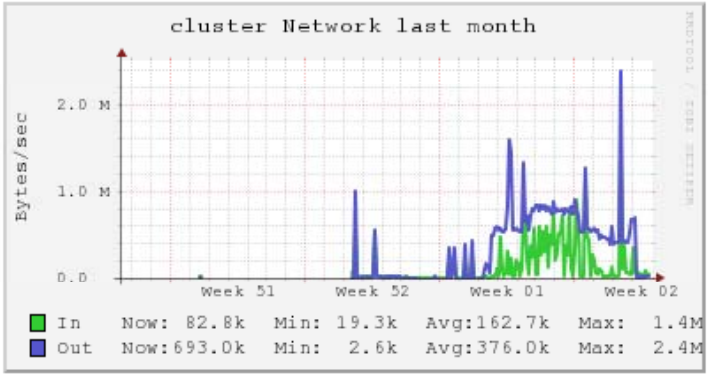
Server Load Distribution





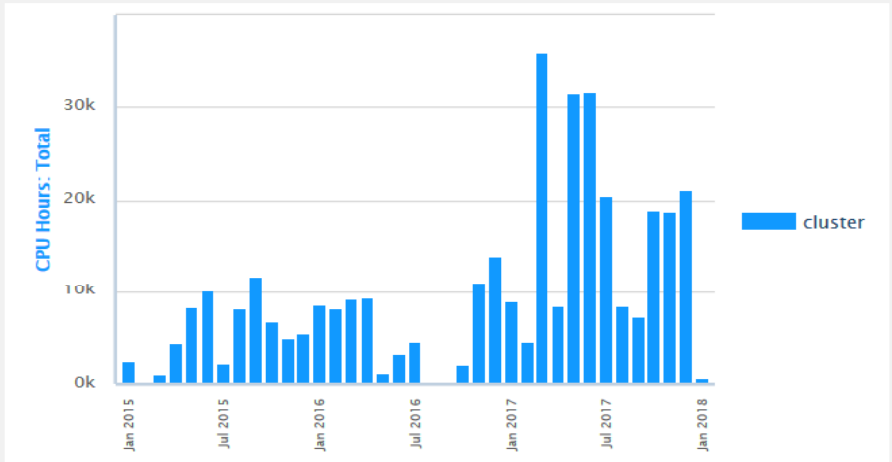




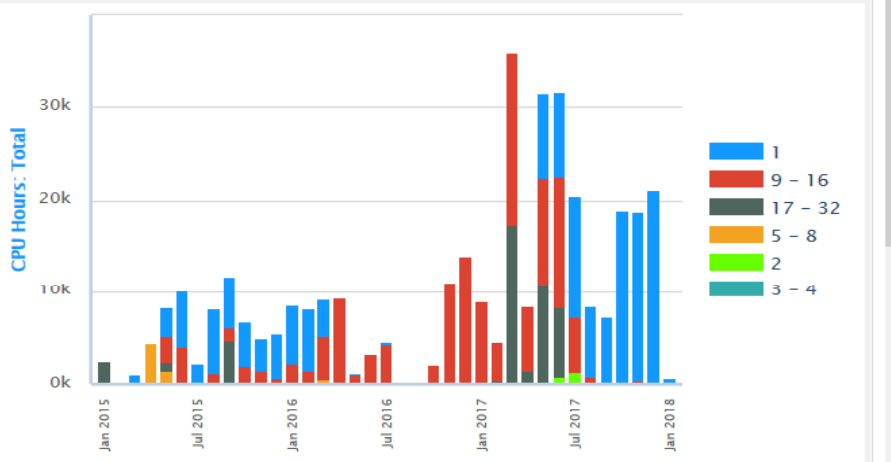


Activity		Jobs	CPU Time (h)		Wait Time (h)	Wall Time (h)		Processors	
Users:	Pls:	Total:	Total:	Avg (Per Job):	Avg (Per Job):	Total:	Avg (Per Job):	Max:	Avg (Per Job):
31	31	4,415	353,454.2	76.42	3.64	176,137.3	38.08	32	4

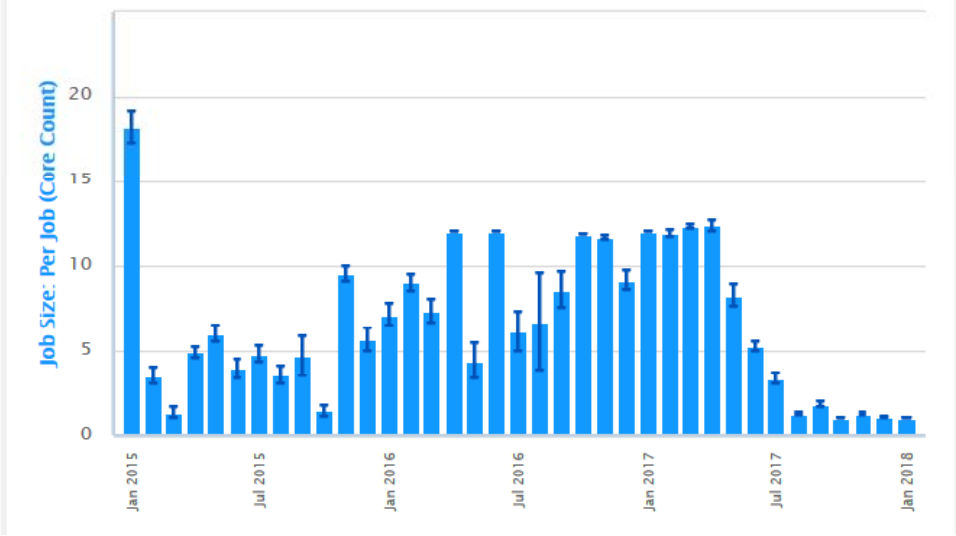
Total CPU Hours By Resource (Top 10)



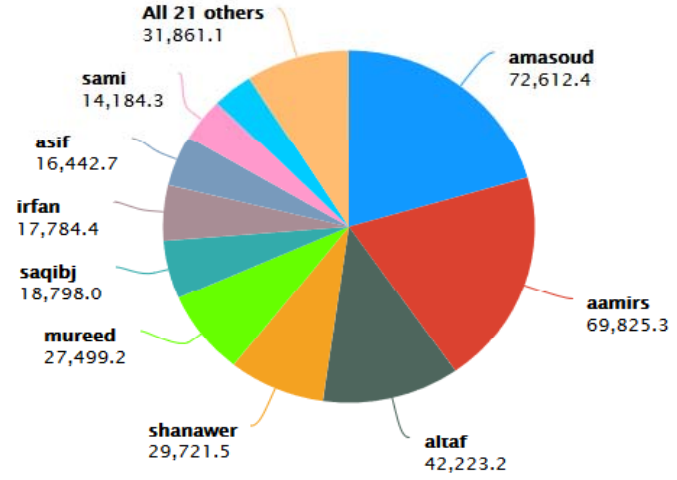
Total CPU Hours by Job Size



Avg Job Size (Core Count)



Total CPU Hours by PI



World-wide Cloud Computing Adoption

World wide Cloud Adoption

Japan

- Cloud market was worth 4.5 billion U.S. dollars (363 billion Yen) in 2010
- Smart Cloud Strategy (May 2010)
- Increased approximately seven times; 27.9 billion US $ by end 2015

Europe

- Every European Digital”
- 370 000 new businesses, over 5 years and over 450 000 over 10 years.
- Europe: Cloud Computing in Horizon 2020
- G-Cloud: Digital Market Place

US

- Estimated total of $20 billion of the Federal Government’s $80 billion budget of ICT for cloud computing
- Decision Framework for Cloud Migration: Select, Provision & Manage

Australia

- Three work directions known as “streams”
- Stream 1: provides agencies with guidance and documentation.
- Stream 2: Encourage agencies towards cloud.
- Stream 3: Strategic approach to Cloud

Microsoft Word Document

World wide Cloud Adoption

Brazil

- Brazil Internet Bill of Rights (2012)
- Cloud computing market growth from US $ 64 million in 2010 to 491 million US $

Asia & Asia Pacific

- Asia Cloud Computing Association(ACCA) and Asia Cloud Readiness Index
- Ever-ready leaders such as Japan, New Zealand, Australia, Singapore, Hong Kong and South Korea.
- The dedicated improvers such as Taiwan, Malaysia, Thailand and the Philippines.
- The steady developing countries including China, Indonesia, India and Vietnam.

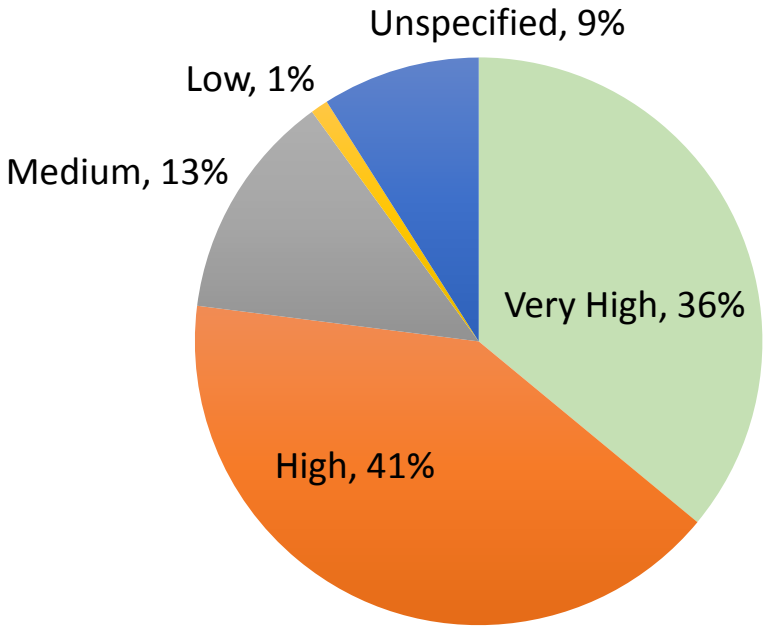
India

- Architectural Vision and the GI Cloud Environment
- Adoption Approach of GI Cloud
- Phase I: Strategy, policy and guidelines establishment
- Phase II: Implementation
- Phase III: Monitoring, management and ongoing improvement

Africa

- Almost 50% of ICT Organizations have moved to Cloud.
- Specific data centers in Tanzania and Rwanda
- Strategies being set up in Benin and Burundi
- 58 % of the ICT organizations in Namibia support cloud adoption
- Strategic plan formulated by Government for launching of data centers in Africa

Security: A Big Barrier to Cloud Adaption



Cloud Security

Security

- Security is the quality or state of being secure – to be free from danger
- Security is the safeguarding of assets from unwanted, illegitimate, unauthorized access

Cloud Security

Cloud Computing is **a security nightmare** and it can't be handled in traditional ways.

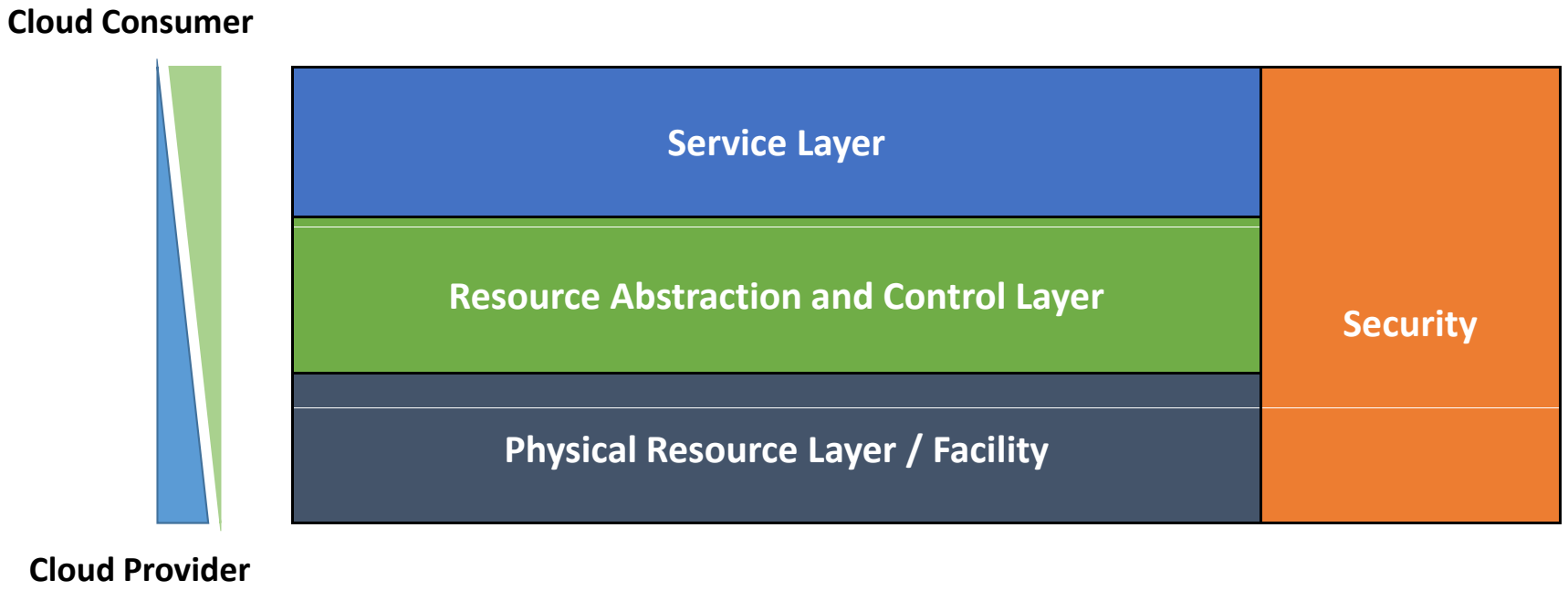
John Chambers
CISCO CEO

- Security is one of the most difficult task to implement in cloud computing.
  - Different forms of attacks in the application side and in the hardware components

(http://www.exforsys.com/tutorials/cloud-computing/cloud-computing-security.html)

28

Cloud Security



Octad of Information Security

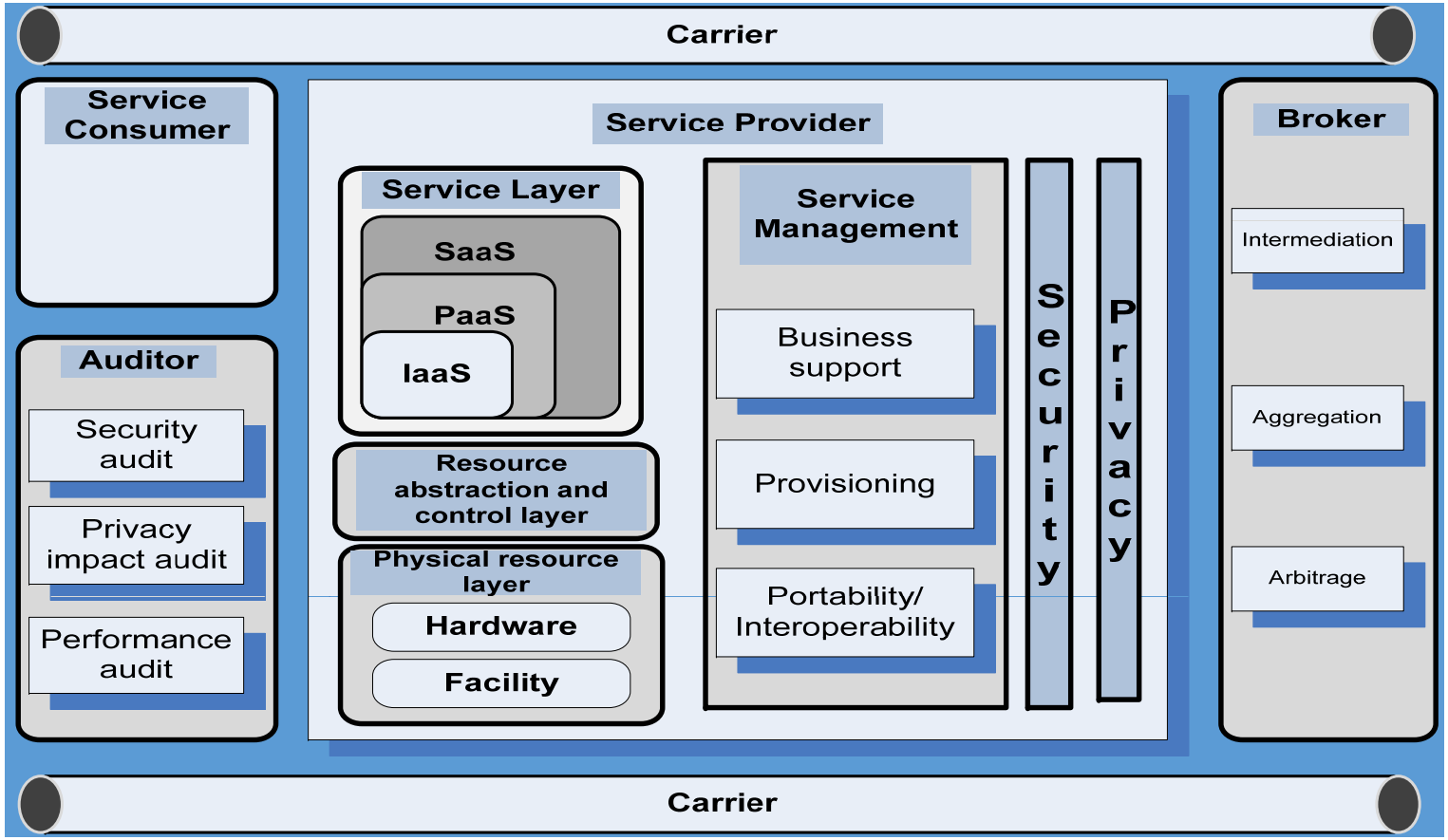
30

The standards in Cloud Computing

- ▶Cloud computing standards for interoperability and portability
- ▶Cloud computing standards for security
- ▶Cloud computing standards for performance
- ▶Cloud standards for service agreements
- ▶Cloud standards for monitoring
- ▶Cloud computing standards for accessibility

(Source: NIST, SP 500-292)

NIST Cloud Reference (CR) Model



(Source: NIST, SP 500-292)

Cloud Actors

Actor	Definition
Cloud Consumer	A person or organization that maintains a business relationship with, and uses service from, *Cloud Providers*.
Cloud Provider	A person, organization, or entity responsible for making a service available to interested parties.
Cloud Auditor	A party that can conduct an independent assessment of cloud services, information system operations, performance and security of the cloud implementation.
Cloud Broker	An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between *Cloud Providers* and *Cloud Consumers*.
Cloud Carrier	An intermediary that provides connectivity and transport of cloud services from *Cloud Providers* to *Cloud Consumers*.

(Source: NIST, SP 500-292)

Derivation of Cloud Security Issues from NIST CR Model

- **Cloud Broker:** Security composition challenge within composed clouds such as a software as a service built upon an infrastructure as a service.
- **On-demand:** Security challenges associated with the business user being able to easily and instantly obtain new computing resources that must be pre-secured on delivery.
- **Resource pooling:** From a cloud customer perspective, this characteristic reveals the possibility that attacks against one customer may inadvertently affect another customer using the same shared resources.

Source: https://cloudsecurityalliance.org

Derivation of Cloud Security Issues from NIST CR Model

- **Service Models:** The cloud definition service models reveal challenges with multi-tenancy in a resource pooled environment.
- **Infrastructure as a Service:** This service model reveals challenges with using virtualization as a front line security defense perimeter to protect against malicious cloud users.
- **Broad network access:** This cloud characteristic shifts the security model to account for possibly untrustworthy client devices that are fully reliant on the network for service.
- **Measured service:** This cloud characteristic reveals the need to measure cloud usage to promote overall availability of the cloud.

Cloud Security and NIST Standards

- **NIST SP 800-145 defines Infrastructure as a Service (IaaS) as follows:**

> The capability provided to the [cloud Consumer] is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The [cloud Consumer] does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Cloud Security and NIST Standards

- **NIST SP 800-145 defined Platform as a Service (PaaS) as follows:**

The capability provided to the [cloud Consumer] is to deploy onto the [cloud Provider] consumer-created or acquired applications created using programming language, libraries, services, and tools supported by the provider. The [cloud Consumer] does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Cloud Security and NIST Standards

- **NIST SP 800-145 defines Software as a Service (SaaS) as follows:**

The capability provided to the [cloud Consumer] is to use the [cloud Provider's] applications running [in a cloud Ecosystem managed by the Provider or Technical Broker]. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. [Cloud Consumers] do not manage or control the underlying cloud [Ecosystem] including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings

Cloud Security and NIST Standards

- As noted in **SP 800-146**, "the term **cloud computing** encompasses a variety of systems and technologies as well as service and deployment models, and business models".
- Cloud computing unique attributes such as elasticity, rapid provisioning and releasing, resource pooling, multi-tenancy, broad-network accessibility, and ubiquity bring many benefits to cloud adopters, but also entails specific security risks associated with the type of adopted cloud and deployment mode.
- To accelerate the adoption of cloud computing, and to advance the deployment of cloud services, solutions coping with cloud security threats need to be addressed.

39

Cloud Security and NIST Standards

- Many of the threats that cloud providers and consumers face can be dealt with through traditional security processes and mechanisms such as security policies, cryptography, identity management, intrusion detection/prevention systems, and supply chain vulnerability analysis.
- Risk management activities must be undertaken to determine how to mitigate the threats specific to different cloud models and to analyze existing standards for gaps that need to be addressed.
- Securing the information systems and ensuring the confidentiality, integrity, and availability of information and information being processed, stored, and transmitted are particularly relevant as these are the high-priority concerns and present a higher risk of being compromised in a cloud computing system.

40

Cloud Security and NIST Standards

- Cloud computing implementations are subject to local physical threats as well as remote, external threats.
- The complexity of the cloud computing architecture supporting three service types and four deployment models, and the cloud characteristics, specifically multi-tenancy, heighten the need to consider data and systems protection in the context of logical, physical boundaries and data flow separation.

41

Security Challenges for Cloud Computing

- Compromises to the confidentiality and integrity of data in transit to and from a cloud provider and at rest;
- Attacks which take advantage of the homogeneity and power of cloud computing systems to rapidly scale and increase the magnitude of the attack;
- A consumer's unauthorized access (through improper authentication or authorization, or exploit of vulnerabilities introduced maliciously or unintentionally) to software, data, and resources provisioned to, and owned by another authorized cloud consumer;
- Increased levels of network-based attacks that exploit software not designed for an Internet-based model and vulnerabilities existing in resources formerly accessed through private networks;

42

Security Challenges for Cloud Computing

- Limited ability to encrypt data at rest in a multi-tenancy environment;
- Portability constraints resulting from the lack of standardization of cloud services application programming interfaces (APIs) that preclude cloud consumers to easily migrate to a new cloud service provider when availability requirements are not met;
- Attacks that exploit the physical abstraction of cloud resources and exploit a lack of transparency in audit procedures or records;
- Attacks that take advantage of known, older vulnerabilities in virtual machines that have not been properly updated and patched;
- Attacks that exploit inconsistencies in global privacy policies and regulations;

43

Security Challenges for Cloud Computing

- Attacks that exploit cloud computing supply chain vulnerabilities to include those that occur while cloud computing components are in transit from the supplier to the cloud service provider;
- Insider abuse of their privileges, especially cloud provider's personnel in high risk roles (e.g. system administrators; and Interception of data in transit (man-in-the-middle attacks).

44

Security Objective for Cloud Computing

- Identity management and access control policies : To protect consumers' data from unauthorized access, disclosure, modification or monitoring.
- Implementation of security domains: To prevent unauthorized access to cloud computing infrastructure resources.
- Deploy in the cloud web applications designed and implemented for an Internet threat model.
- Protect internet-connected personal computing devices by applying security software, personal firewalls, and patch maintenance. To mitigate end-user security vulnerabilities.
- Design and develop IDPS in cloud computing implementations

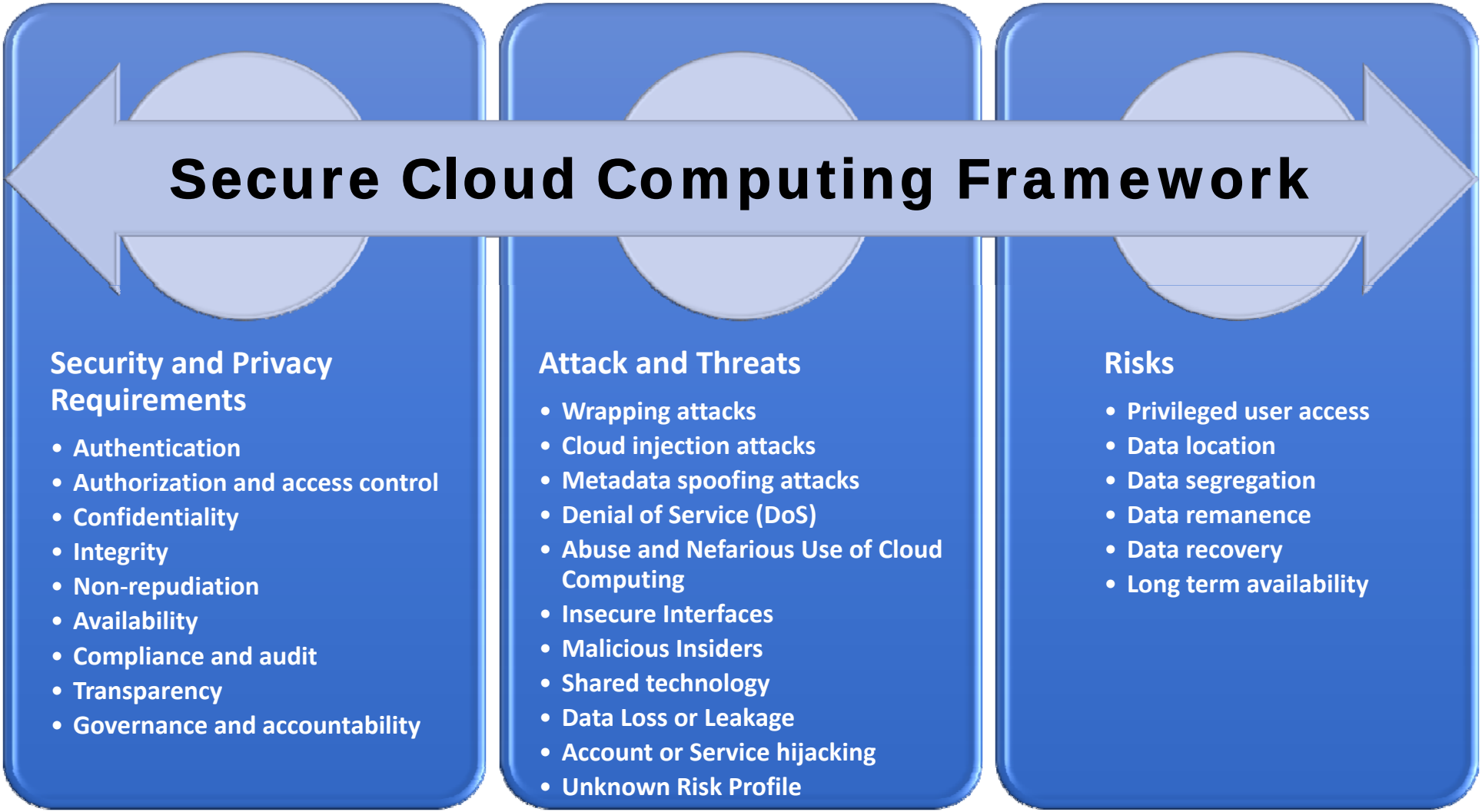
45

Security Objective for Cloud Computing

- Conduct audit process
- Define trust boundaries between cloud provider(s) and consumers to ensure that the responsibilities to implement security controls are clearly identified.
- Implement standardized APIs for interoperability and portability to support easy migration of consumers' data to other cloud providers when necessary.

46

Secure Cloud Computing Framework


Secure Cloud Computing Framework
Security and Privacy Requirements
• Authentication
• Authorization and access control
• Confidentiality
• Integrity
• Non-repudiation
• Availability
• Compliance and audit
• Transparency
• Governance and accountability
Attack and Threats
• Wrapping attacks
• Cloud injection attacks
• Metadata spoofing attacks
• Denial of Service (DoS)
• Abuse and Nefarious Use of Cloud Computing
• Insecure Interfaces
• Malicious Insiders
• Shared technology
• Data Loss or Leakage
• Account or Service hijacking
• Unknown Risk Profile
Risks
• Privileged user access
• Data location
• Data segregation
• Data remanence
• Data recovery
• Long term availability

Security and Privacy Requirements

Security & privacy req.	Implementation Strategy to achieve
Authentication	Username, Password, 2FA
Authorization and access control	Restrict cloud admins hiring process- Monitor activities of authorized users- Build trust between CSPs, cloud customers and admins.
Confidentiality	Employ strong authentication methods - Prevent unauthorized access - Use encryption techniques
Integrity	Use encryption and hash algorithms - Prevent unauthorized access
Non-repudiation	Digital signatures - Timestamps - Confirmation receipt services
Availability	Use backup and recovery schemes, fault tolerance and replication
Compliance and audit	Perform internal and external audits on a regular basis to monitor CSP's compliance to agreed terms, standards and regulations
Transparency	Provide customers with clear information on controls, security and operation of the cloud- Refer to SLA
Governance and accountability	Effective implementation and adherence of security policies and procedures to protect clouds from threats and data loss

Threats and their Mitigations

Attacks and threats	Mitigation
Wrapping attacks	Increase security during message passing from the web server to the web browser by using the SOAP message
Cloud injection attacks	Use hash algorithms
Metadata spoofing attacks	Use verification techniques
Denial of Service (DoS)	Provide more computational power and resources
Abuse and Nefarious Use of Cloud Computing	Improve credit card fraud detection-Apply strict registration and validation rules-Perform extensive examination of network traffic
Insecure Interfaces	Analyze the security model of the API- Employ strong authentication, access control and encryption techniques - Understand the dependency chain of the API

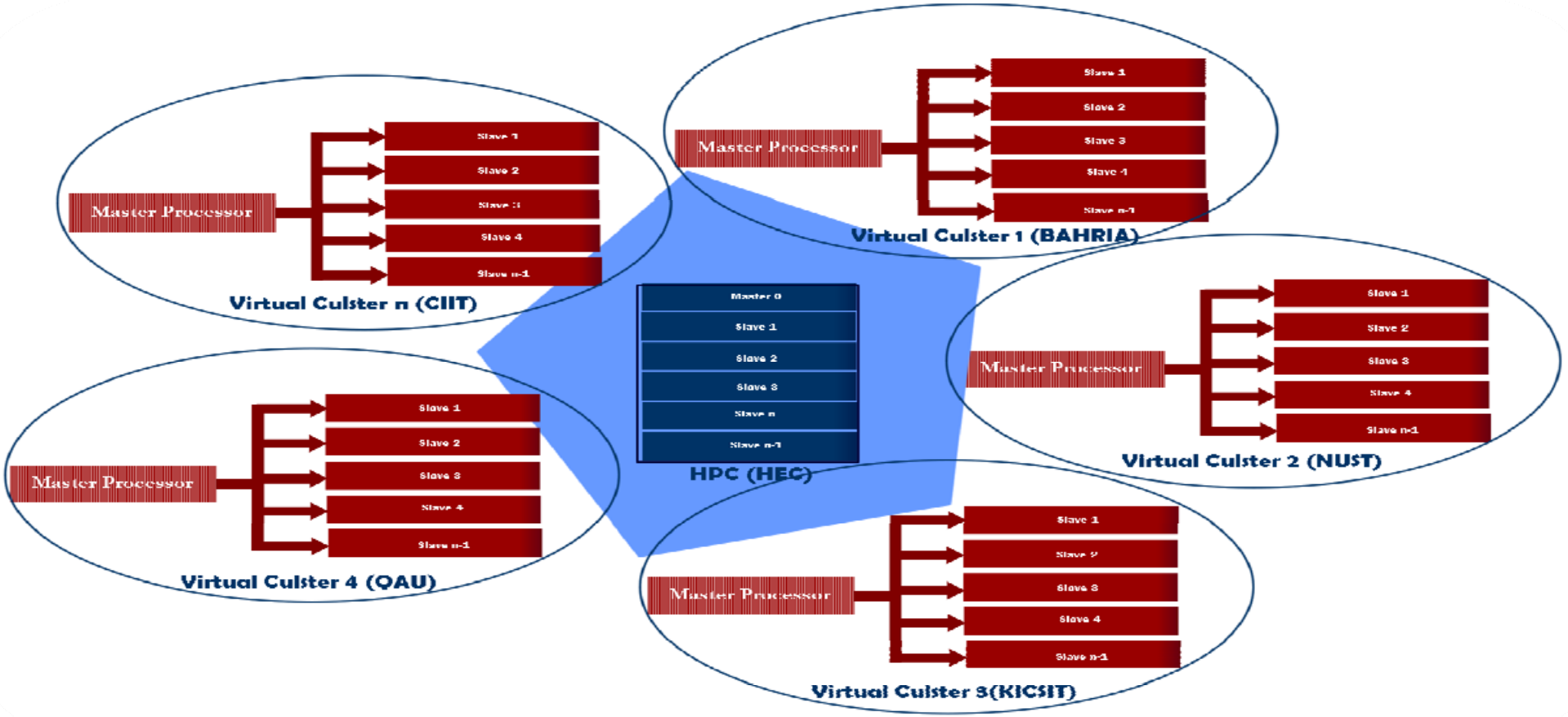
Threats and their Mitigations

Attacks and threats	Mitigation
Malicious Insiders	Require transparency in all information security issues- Define security breach notification processes- Enforce strict hiring requirements and HR assessment
Shared technology	Conduct vulnerability scanning and remediation- Promote strong authentication and monitor unauthorized activities - Implement security best practice for installation and configuration
Data Loss or Leakage	Implement strong API access control, key generation and encryption techniques- Provide backup and retention strategies- Analyze data protection at both design and run time.
Account or Service hijacking	security policies and SLAs-Forbid sharing of account credential employ 2FA- Understand CSPs
Unknown Risk Profile	Monitor on necessary information, Disclose applicable data, logs and infrastructure detail
Lack of governance	Carefully execute SLAs

Risks and their Counter Measures

Risks	Countermeasure
Privileged user access	Monitor authorized users activities, restrict admin hiring
Data location	Provide consumers with information about where their data stored and processed.
Data segregation	Use encryption to prevent data
Data remanence	Ensure the deletion of data after use of cloud service
Data recovery	Backup data at other data
Long term Availability	Apply insurance when cloud service no longer provided

National Cloud



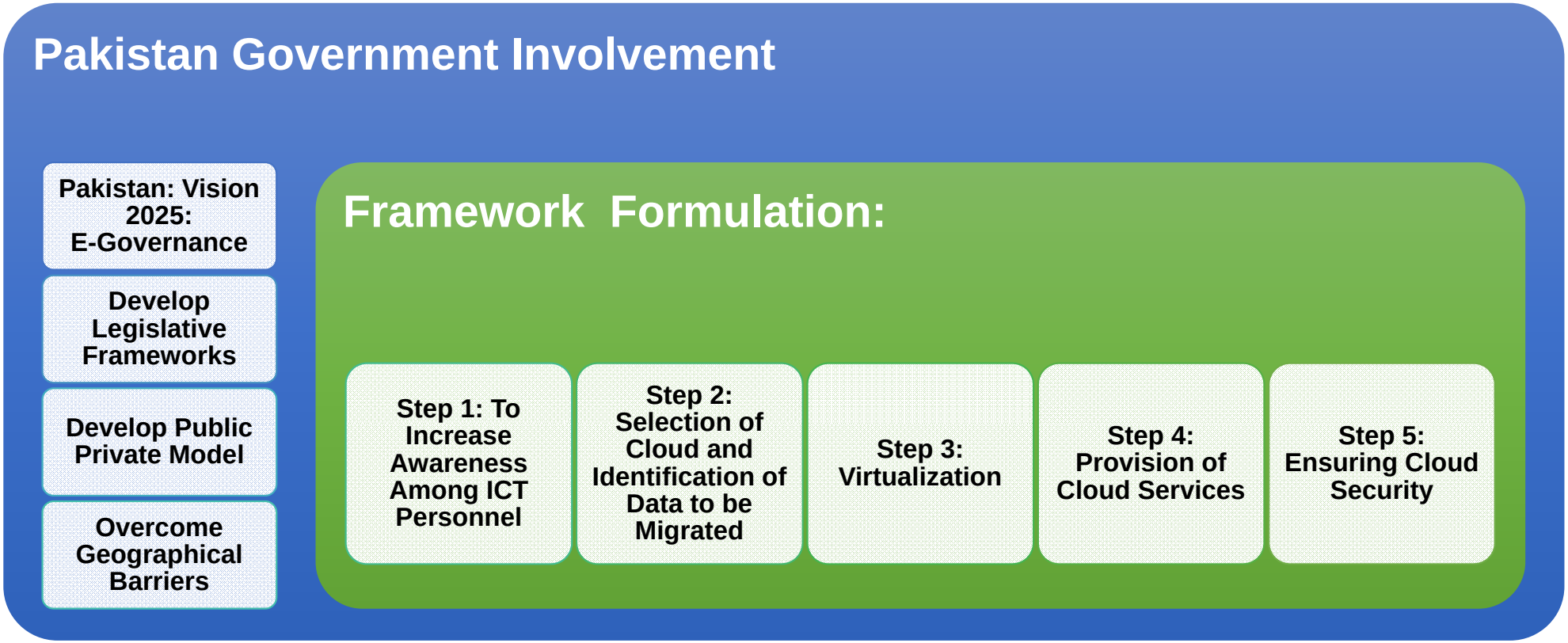
53

Objectives of National Cloud

- Promote the culture of collaboration among universities and R&D organization
- Promote the spirit of academic research in the field of computational sciences including computer science, computational biology, computational physics, computational chemistry and mathematics
- Provide an experimental and discussion forum for collaborative research among computational science students and industry people
- Promote the publication and presentation of scholarly works by students and young faculty members at conferences
- Assist each other academically in our individual and collective research
- Train our young scientific community with state of the art computational tools that they can apply in their research activities.

54

National Cloud



Step 1: To Increase Awareness

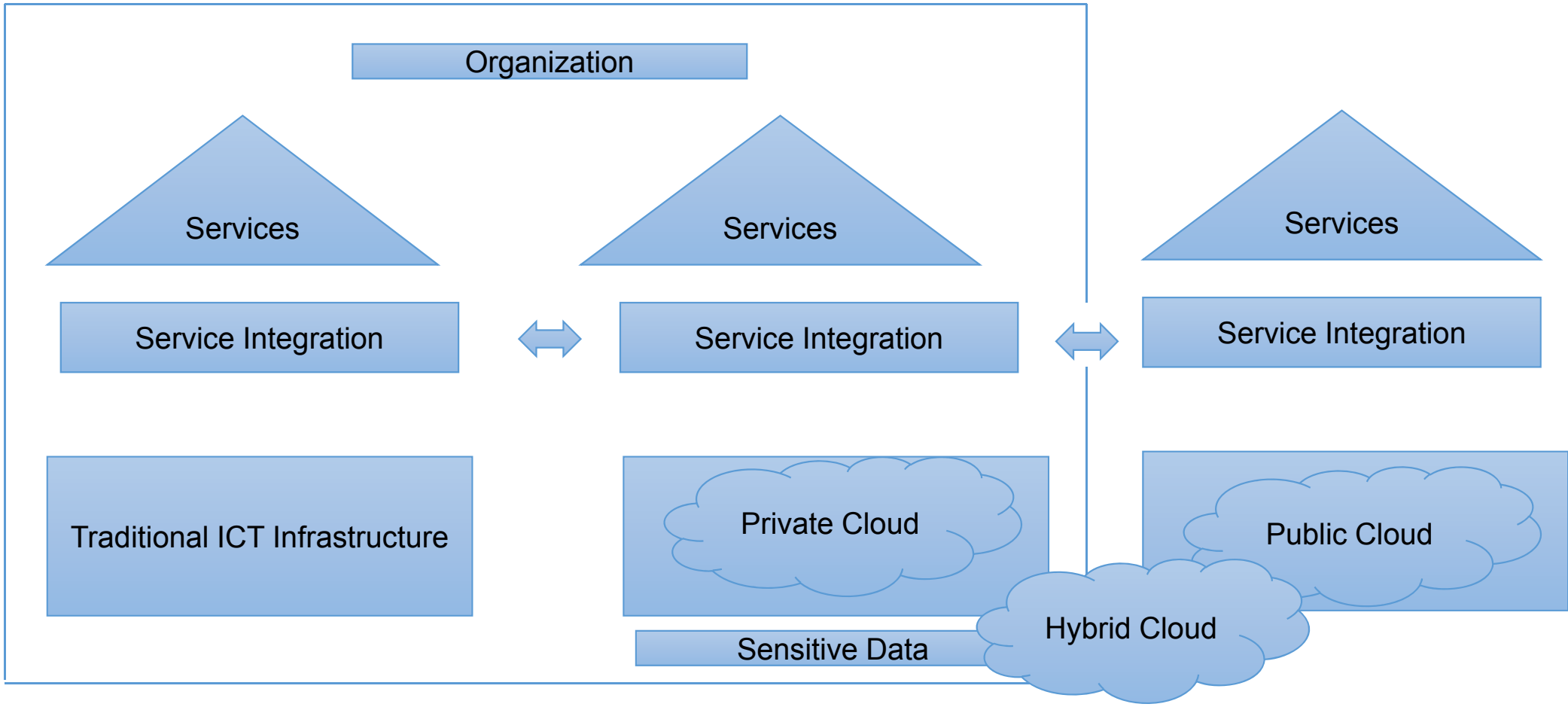
Proposed training modules for standardization and regulatory Process:

- Module 1: Cloud Computing Concepts, Definitions and Standards
- Module 2: Cloud Computing − Legal and Operational Challenges
- Module 3: The Contract Establishment

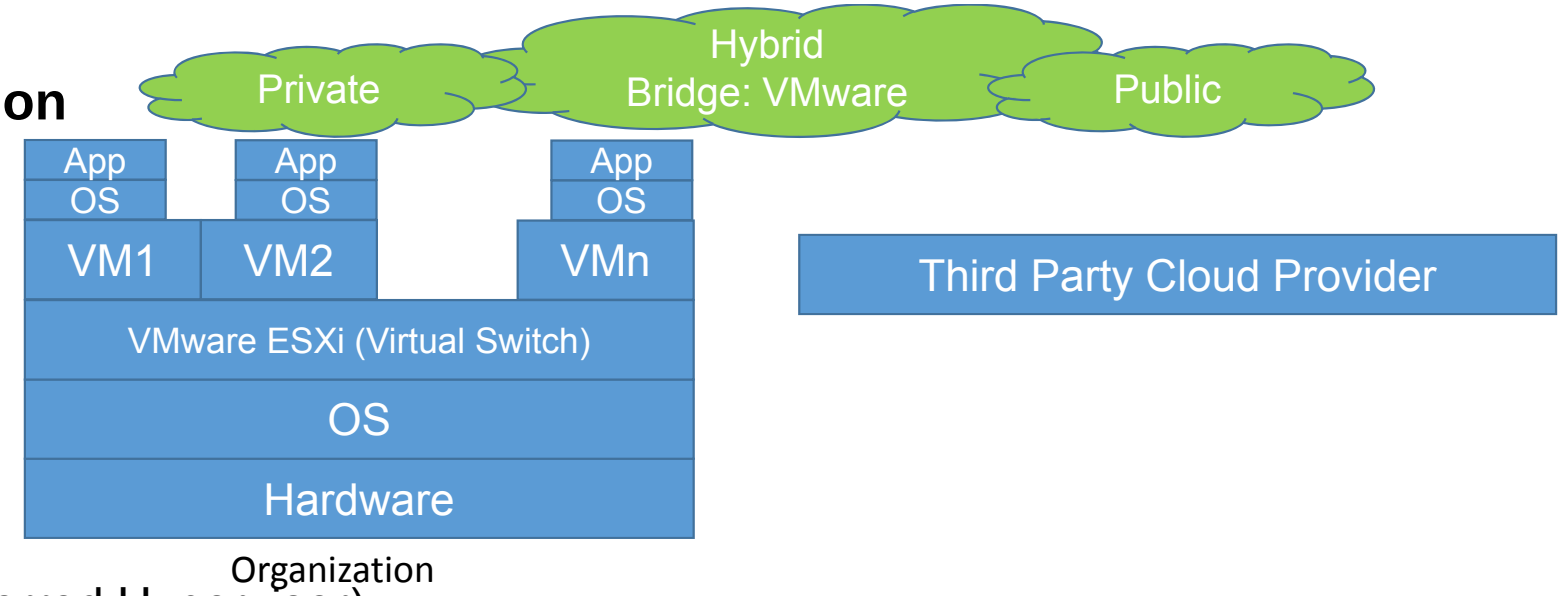
Proposed training modules for technical stakeholders:

- Module 1: An introduction to Cloud Computing
- Module 2: Data centers & Networks for the Cloud
- Module 3: Hypervisor: Installing, Configuration and Management
- Module 4: Creation of Virtual Networks, Storage Devices
- Module 5: Management of Resource Allocation and Utilization

Step 2: Selection of Cloud & Identification of Data to be Migrated

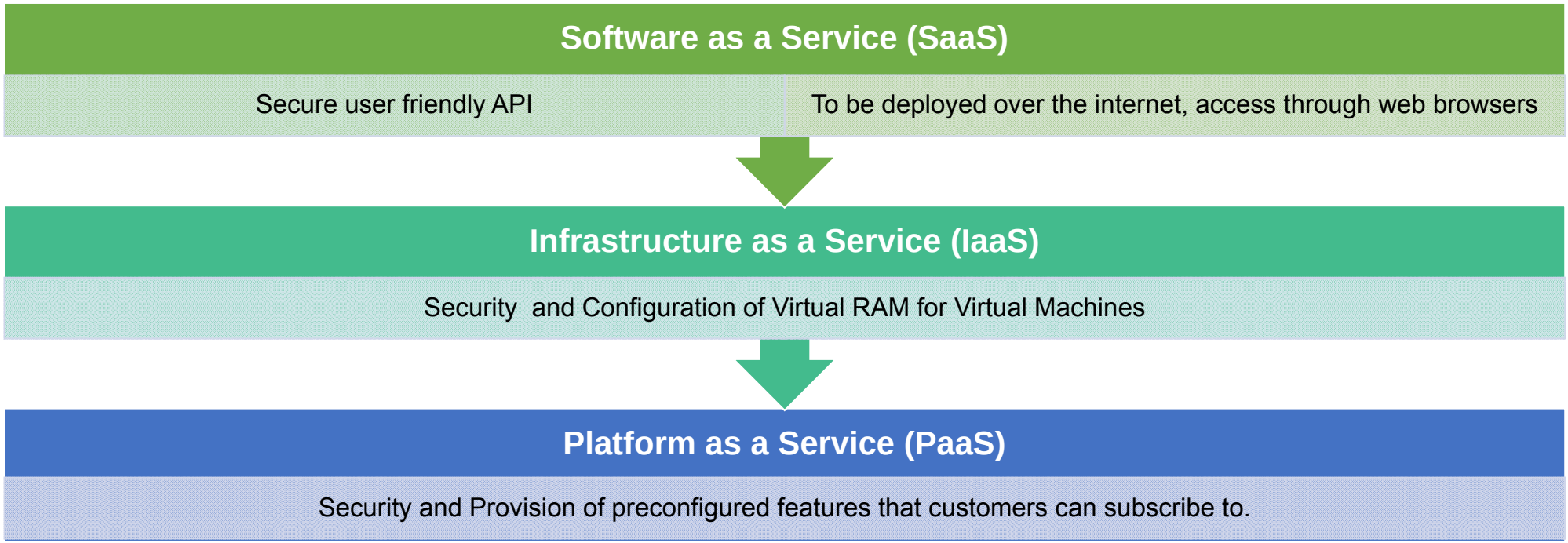


Step 3: Virtualization

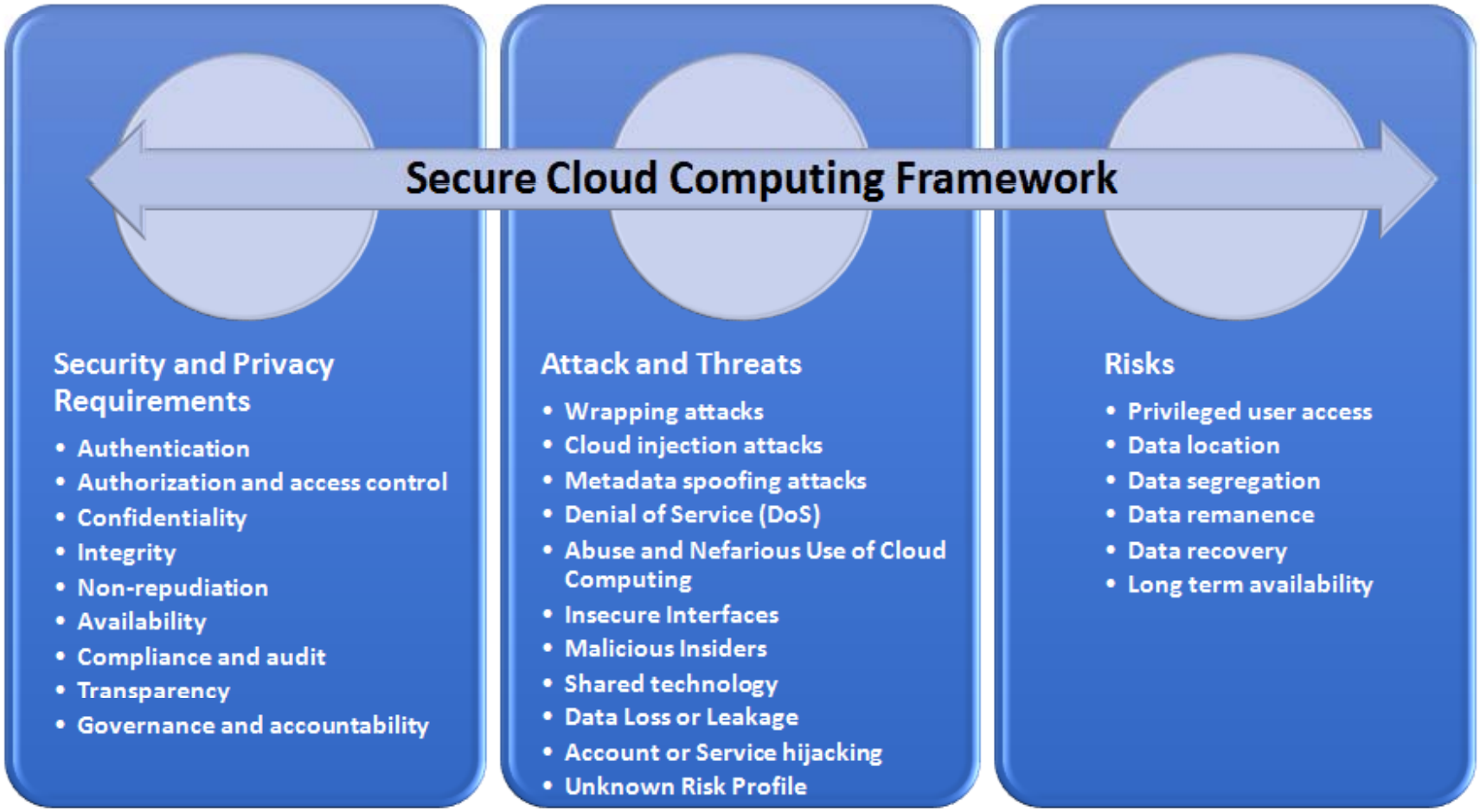


- VMware (Preferred Hypervisor)
- Installation of VMware
- Creation and Management of Virtual Machines
- Data Center Virtualization using vCenter Server
- Configuration of Virtual Networks using Virtual Switches with Security
- Configuring Virtual Storage Devices
- Implementing Security on Virtual Machines

Step 4: Provision of Cloud Services



Step 5: Ensuring Cloud Security



Mirror Cloud

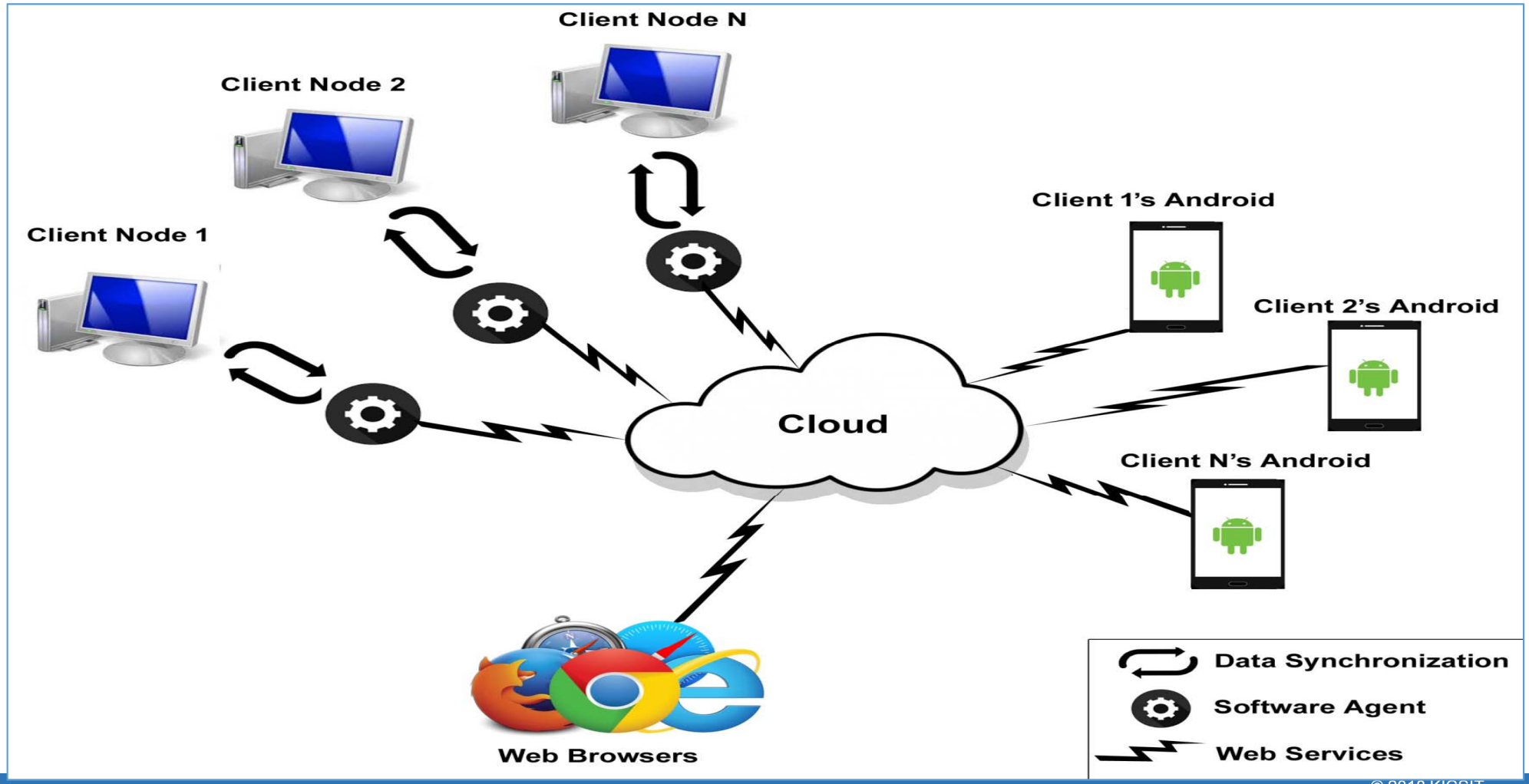
MIRROR CLOUD

Mirror Cloud is defined as the ‘File Management’ over the cloud in truly synchronized and secure manner to attain efficiency, reliability and security.

Mirror Cloud Provides

- Administrator level remote access of the data over the cloud.
- Autonomous data synchronization.
- Multi layers of security in secure file access i.e., file at rest security and file in motion security.

MIRROR CLOUD SYSTEM MODEL



FEATURES LIST

- Selection of files & Autonomous push.
- File Synchronization between cloud and local computers
- Data at rest encryption, Data in motion encryption
- File access over web and android with original file hierarchy
- File manipulation
- File sharing with access control
- Multiple PC files handling over single account
- Secure File / Directory Download with owner authentication
- Mitigation of cyber security threats.

Security and Privacy Requirements

Security & privacy req.	Implementation Strategy
Authentication	Multifactor Email authentication upon each login is used.
Authorization and access control	Access is specified for each and every user i.e. user can only access own files and not any other data.
Confidentiality	AES and RSA encryption techniques are used, reCaptcha upon signup and 2 Factor Email Authentication upon login are used.
Integrity	AES and RSA encryption technique is used, reCaptcha upon signup and 2 Factor Email Authentication upon login is used.

Cloud Attacks and their Mitigations

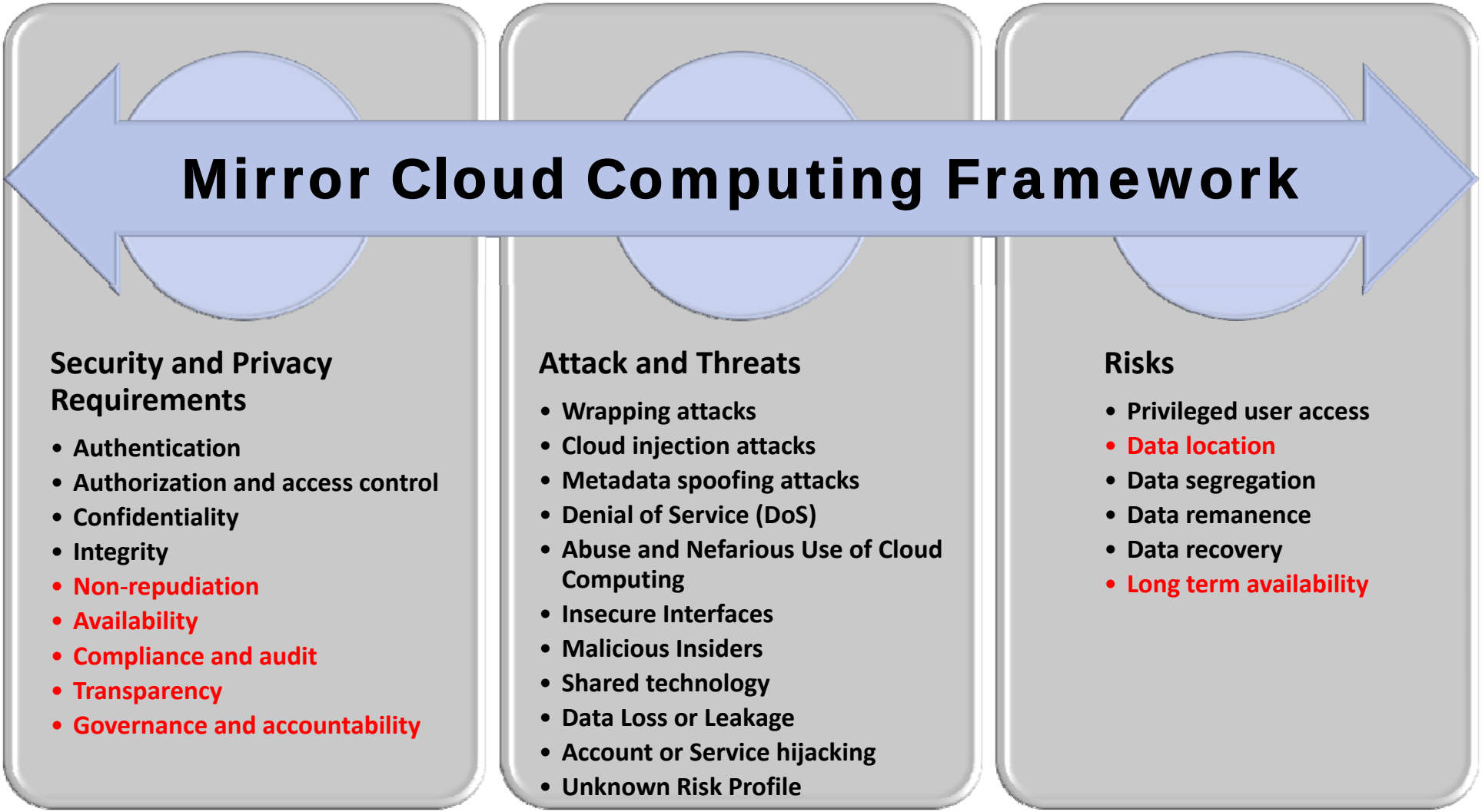
Attacks and threats	Mitigation
Wrapping attacks	Increased security during message passing from the web server to the web browser by using the SOAP message. System encrypts message for security purposes.
Cloud injection Attacks (SQL injection)	Prepared statements provided by the Java Core API for database interactions is used.
Metadata spoofing Attacks	The system verify each and every user and allows access only to the genuine users. Multifactor Authentication and reCaptcha is used for verification.
Denial of Service (DoS)	All the requests received by the system are saved in the databases with the request timing. A threshold of 100 requests in 30 seconds is defined in the system. All the requests are first compared with the saved records and if the number of requests from a specific host exceeds 30 per second, the host address is added to the block list and error pages are delivered to the host.
Abuse and Nefarious Use of Cloud Computing	Users activity log is maintained and monitored. Multifactor authentication is implemented and user access is defined in system.
Insecure Interfaces	Our user interface provides a user friendly experience allowing the user to interact with the system in a natural and intuitive way and it does not lead to any kind of unauthorized usage of data.

Cloud Attacks and their Mitigations

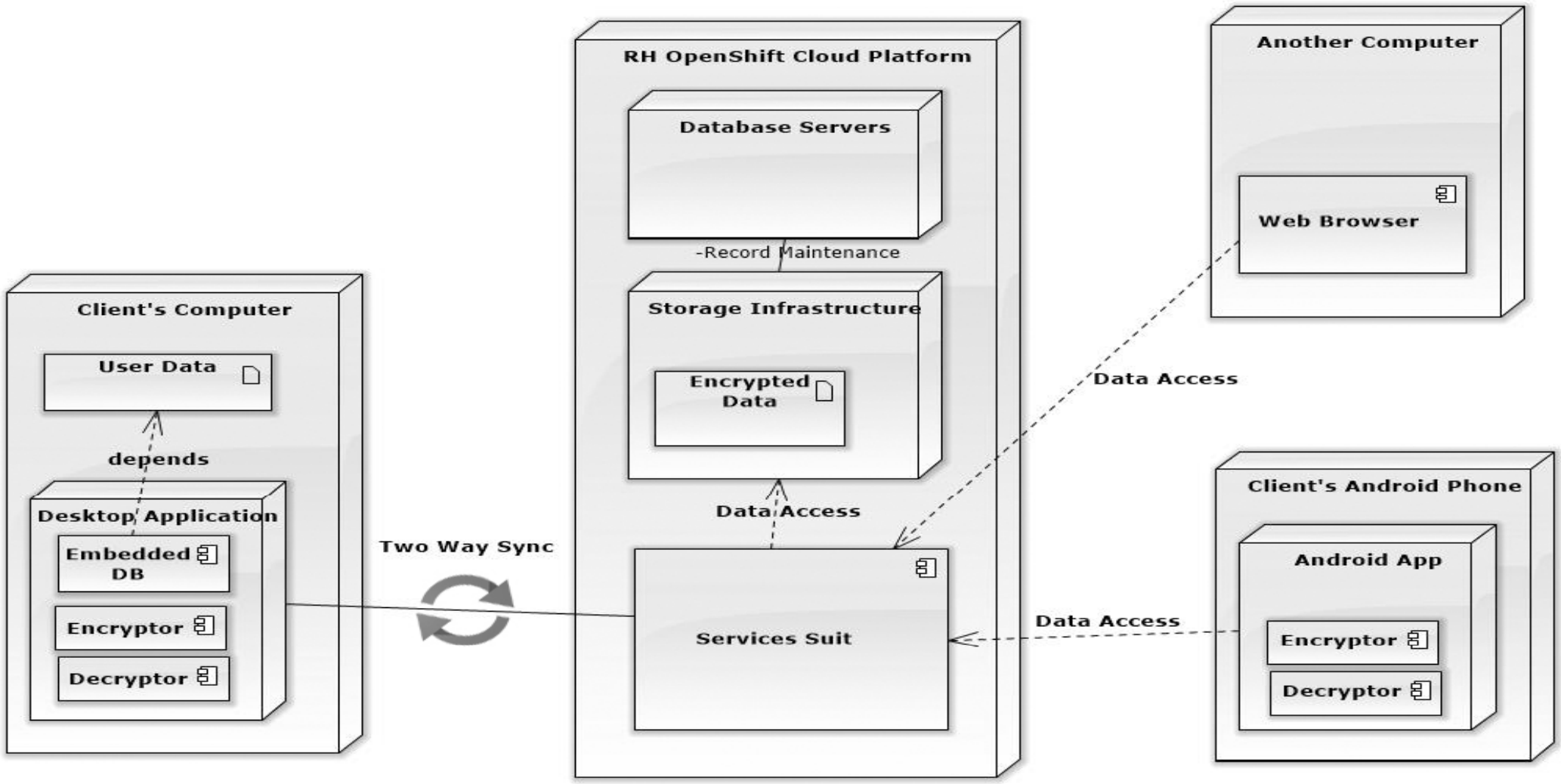
Attacks and threats	Mitigation
Malicious Insiders	Access to the files is only permitted to the data owner. User's data is secured by malicious insiders by using MD5 hashing technique.
Shared technology	Strong authentication is implemented by email verification, reCaptcha and monitored unauthorized activities using activity logs.
Data Loss or Leakage	Data residing in the cloud storage remains encrypted also cloud have a backup of user's data to use in case of accidental data loss.
Account or Service hijacking	Email verification upon every login attempt is implemented to prevent unauthorized user access in system.
Unknown Risk Profile	reCaptcha is used to distinguish genuine user from bots and Email verification authenticates user and specify access to system. Finally activity log is maintained and monitored.

Risks and their Counter Measures

Risks	Countermeasure
Privileged user access	Monitored authorized users activities.
Data segregation	Efficient Cryptography algorithms are used.
Data remanence	File is deleted without moving into trash folder.
Data recovery	User can recover deleted data within 30 days of deletion.

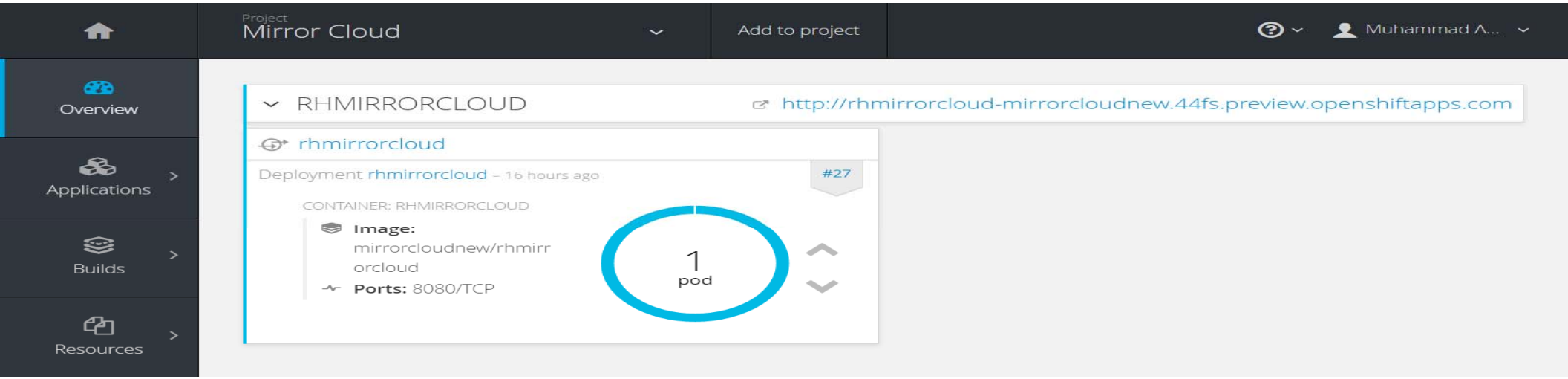

Mirror Cloud Computing Framework
Security and Privacy Requirements
• Authentication
• Authorization and access control
• Confidentiality
• Integrity
• Non-repudiation
• Availability
• Compliance and audit
• Transparency
• Governance and accountability
Attack and Threats
• Wrapping attacks
• Cloud injection attacks
• Metadata spoofing attacks
• Denial of Service (DoS)
• Abuse and Nefarious Use of Cloud Computing
• Insecure Interfaces
• Malicious Insiders
• Shared technology
• Data Loss or Leakage
• Account or Service hijacking
• Unknown Risk Profile
Risks
• Privileged user access
• Data location
• Data segregation
• Data remanence
• Data recovery
• Long term availability

DEPLOYMENT DIAGRAM

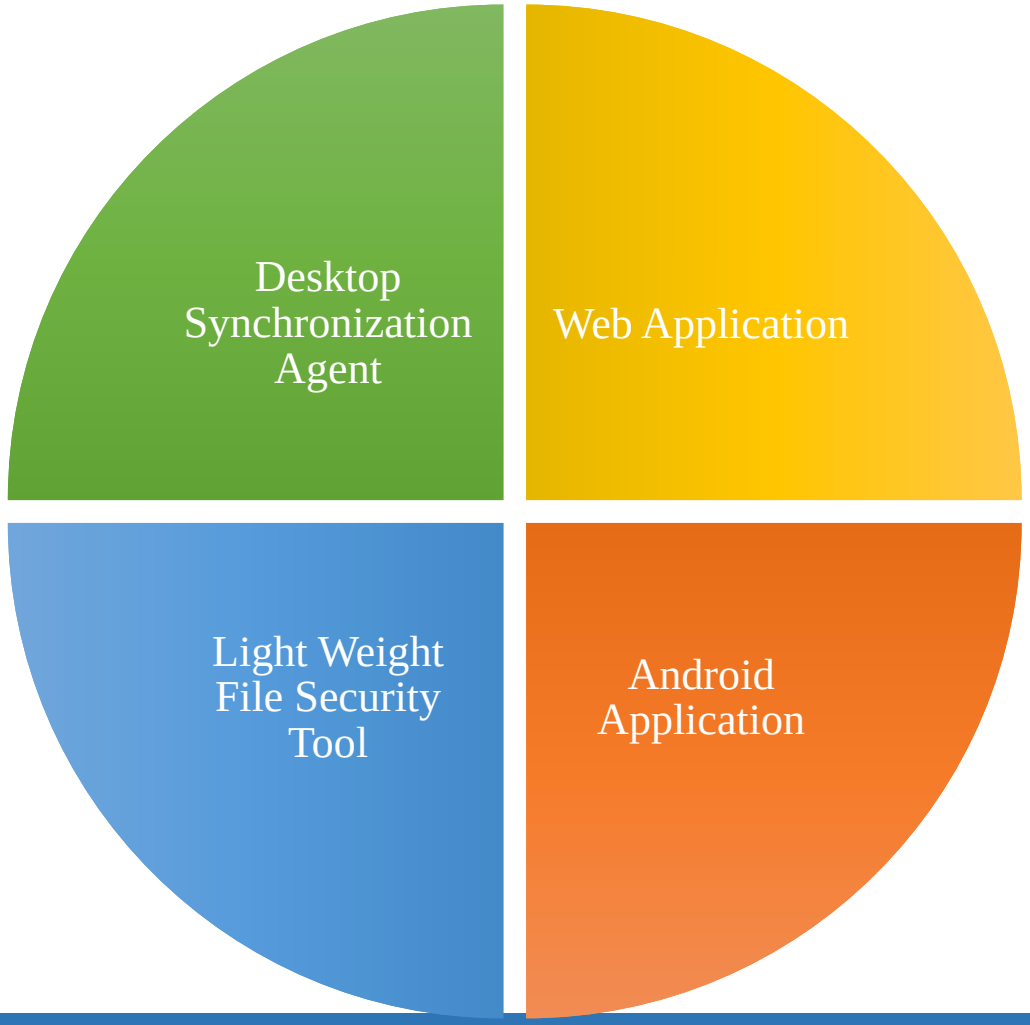


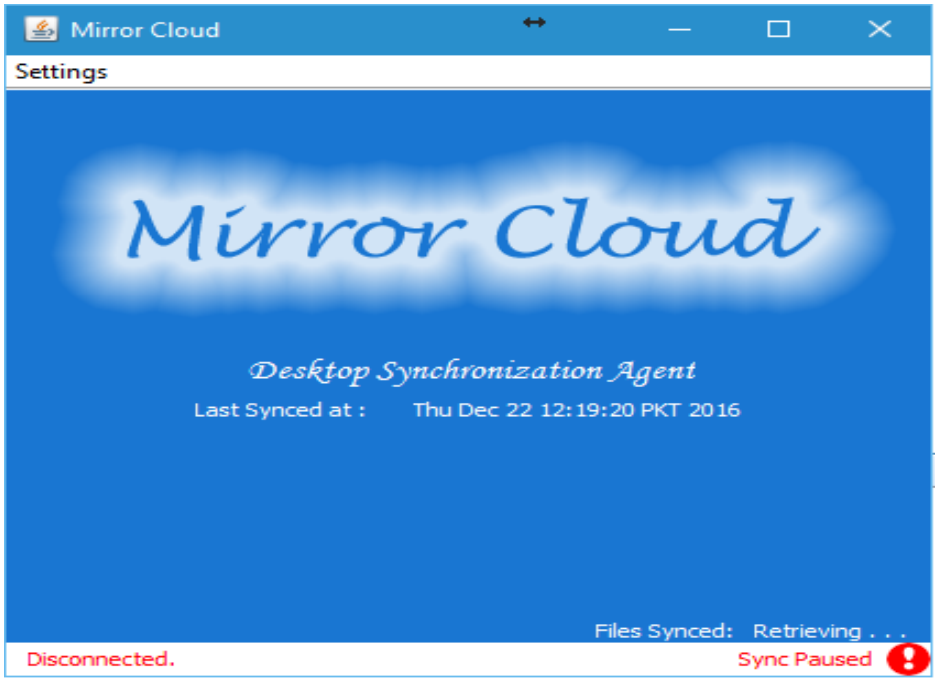
SYSTEM DEPLOYMENT

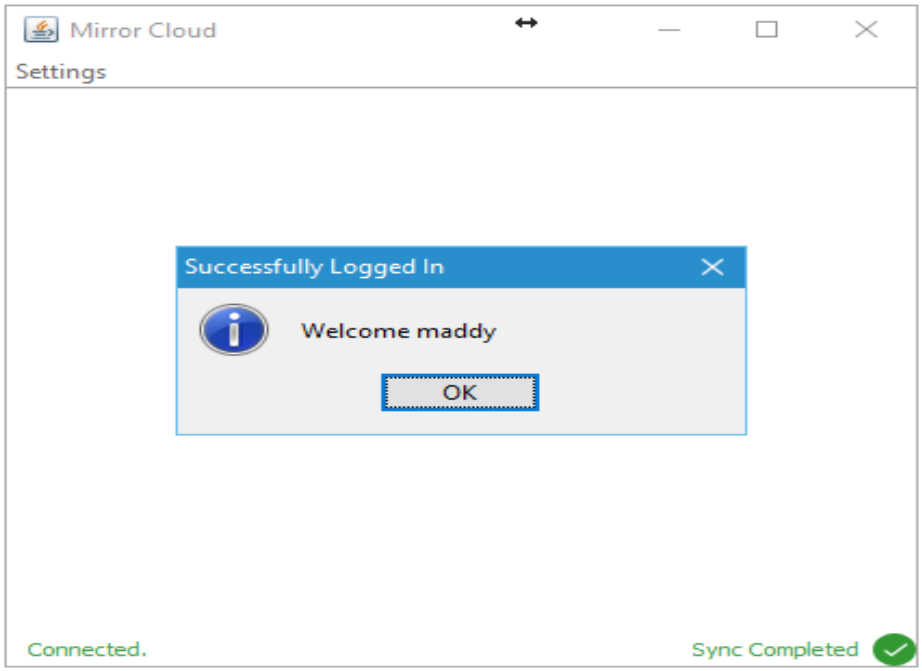
Deployed in Real Cloud Environment using Red Hat OpenShift v3 Next Gen Cloud PaaS Platform

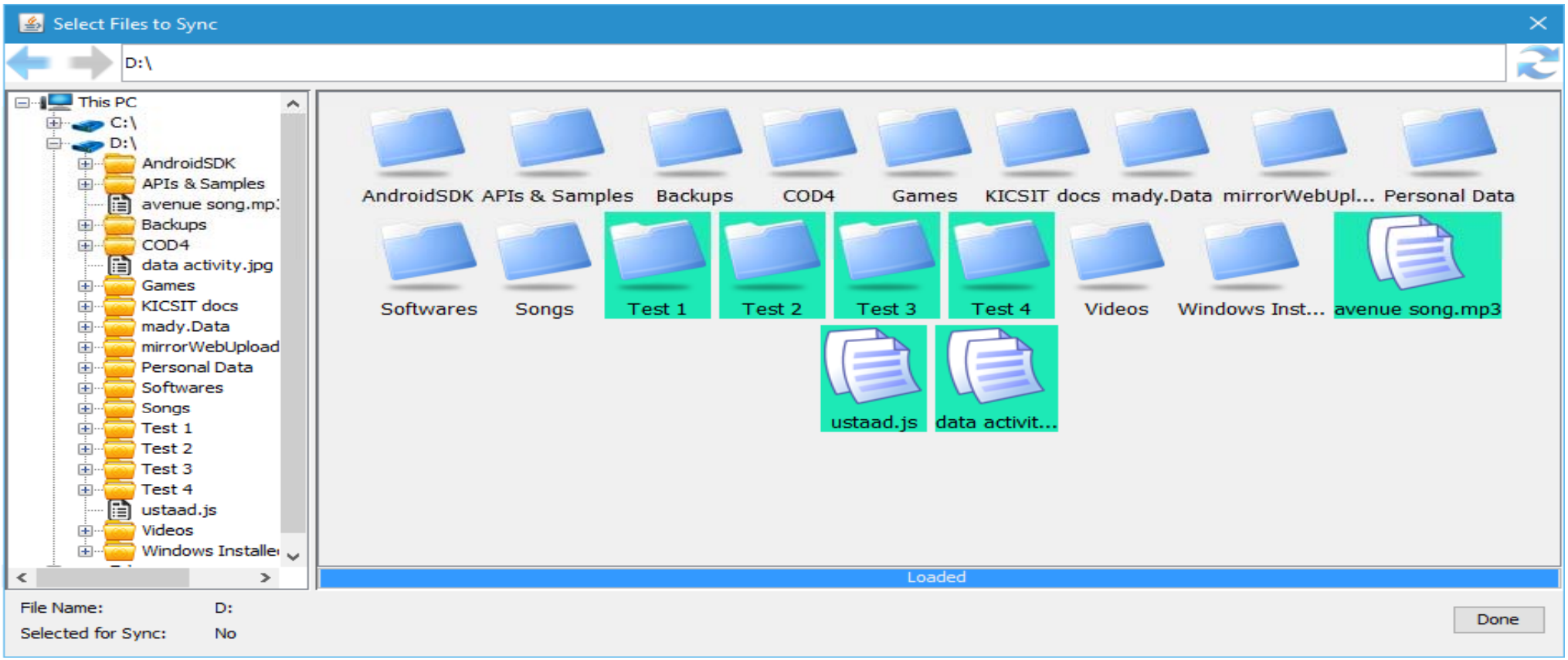


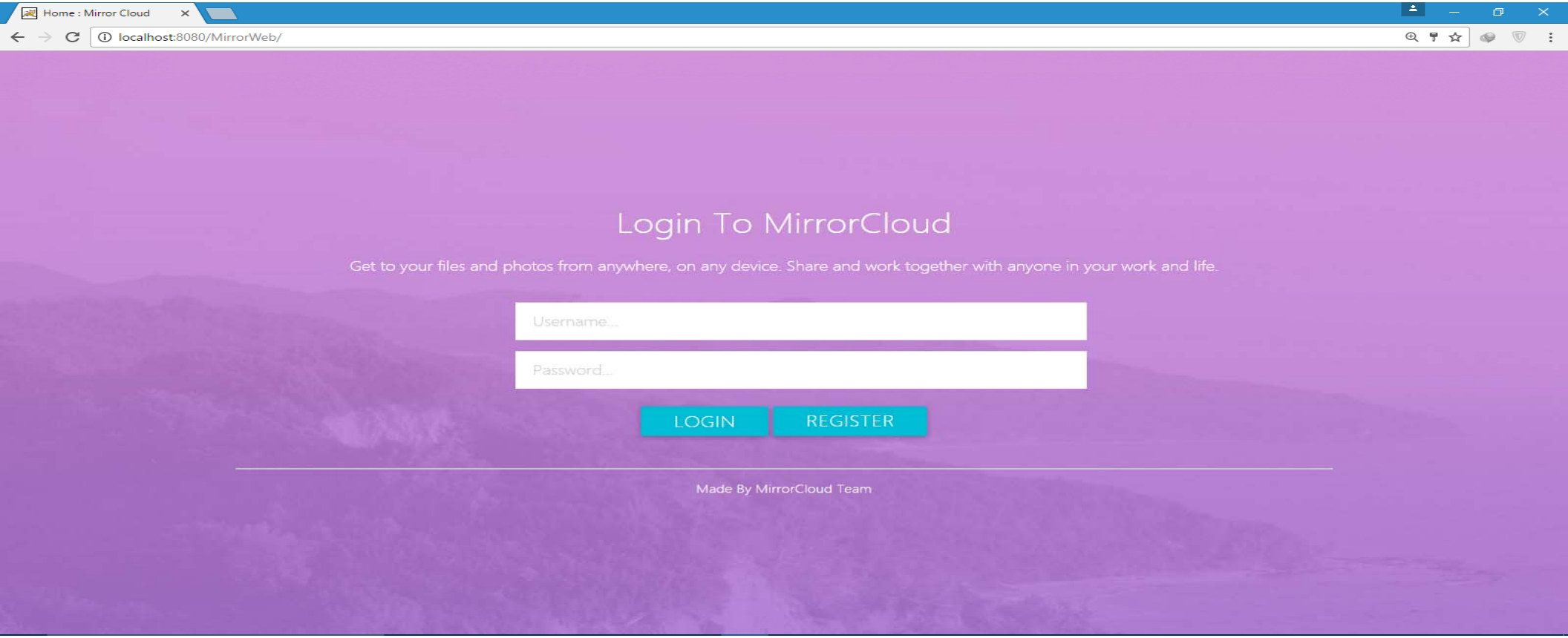
SOFTWARE COMPONENTS

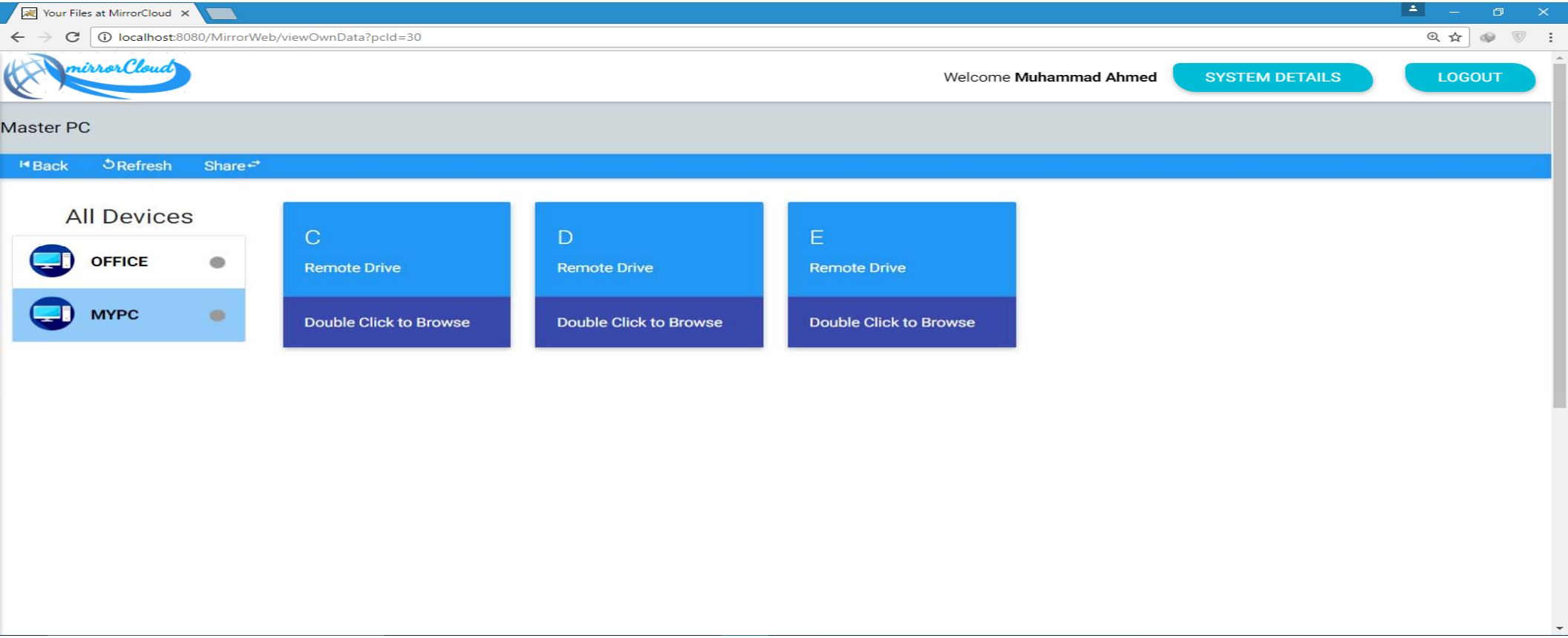


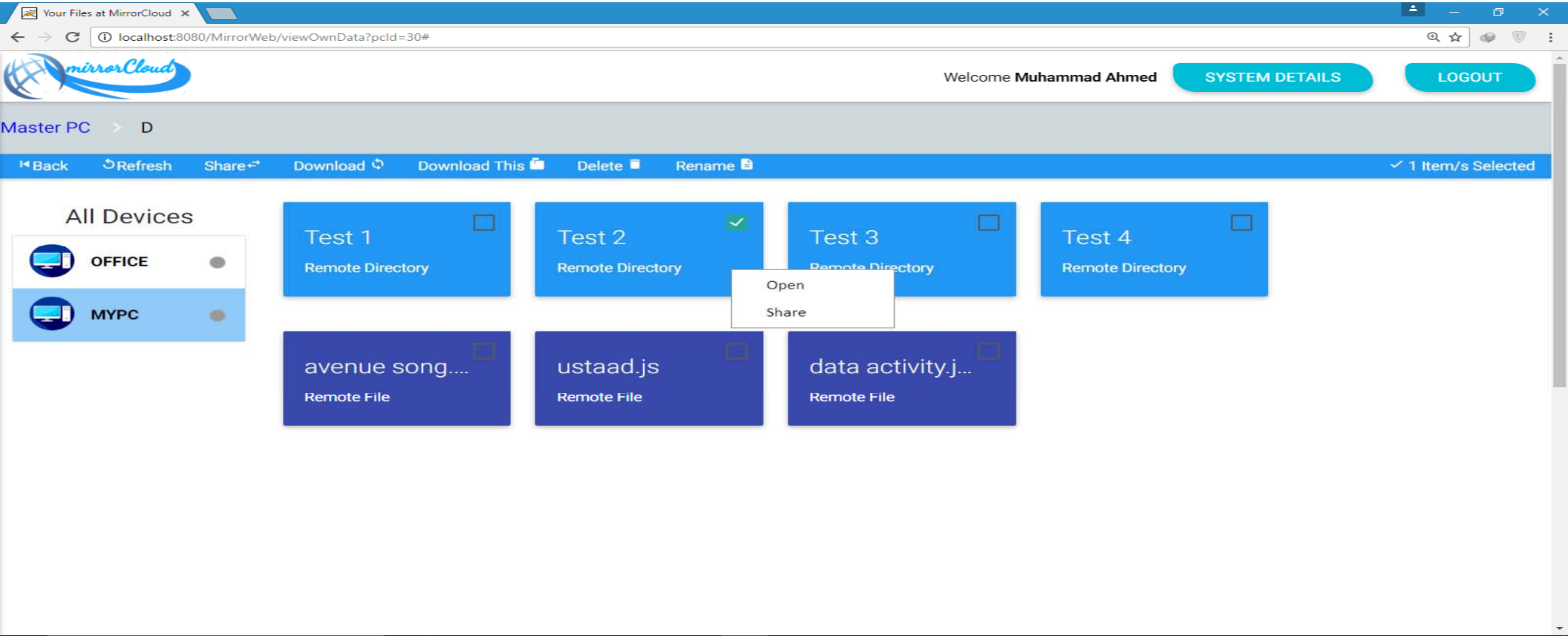

Mirror Cloud
Settings
Mirror Cloud
Desktop Synchronization Agent
Last Synced at : Thu Dec 22 12:19:20 PKT 2016
Files Synced: Retrieving . . .
Disconnected.
Sync Paused

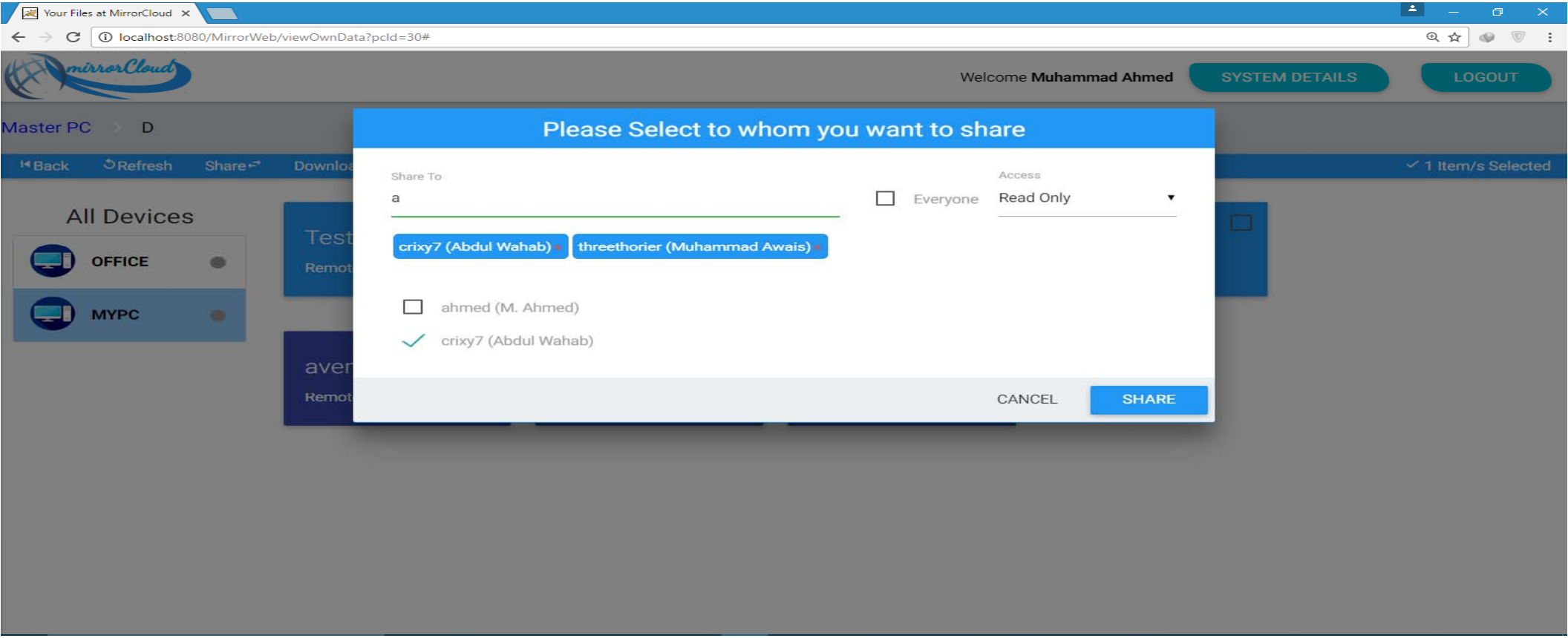

Mirror Cloud
Settings
Successfully Logged In
Welcome maddy
OK
Connected.
Sync Completed

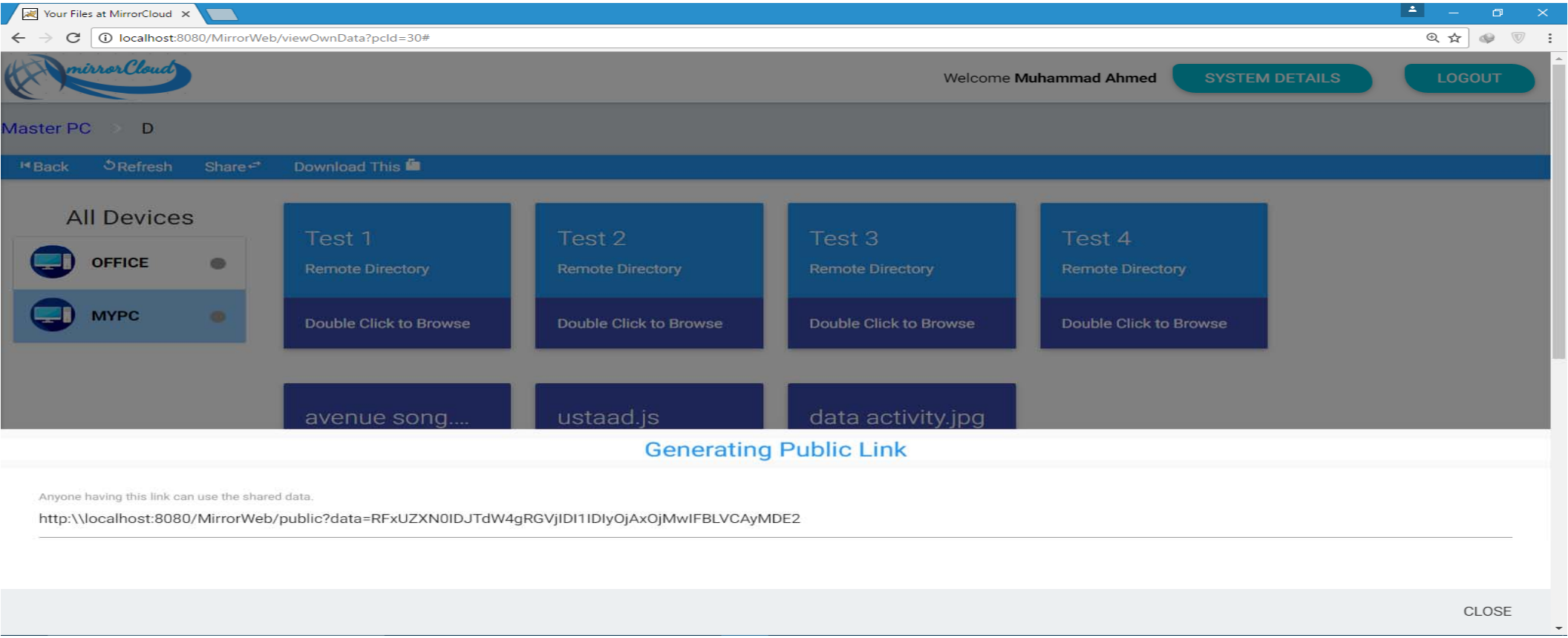

Select Files to Sync
D:\
This PC
C:\
D:\
AndroidSDK
APIs & Samples
avenue song.mp3
Backups
COD4
data activity.jpg
Games
KICSIT docs
mady.Data
mirrorWebUpload
Personal Data
Softwares
Songs
Test 1
Test 2
Test 3
Test 4
ustaad.js
Videos
Windows Installe
AndroidSDK
APIs & Samples
Backups
COD4
Games
KICSIT docs
mady.Data
mirrorWebUpl...
Personal Data
Softwares
Songs
Test 1
Test 2
Test 3
Test 4
Videos
Windows Inst...
avenue song.mp3
ustaad.js
data activit...
Loaded
File Name: D:
Selected for Sync: No
Done

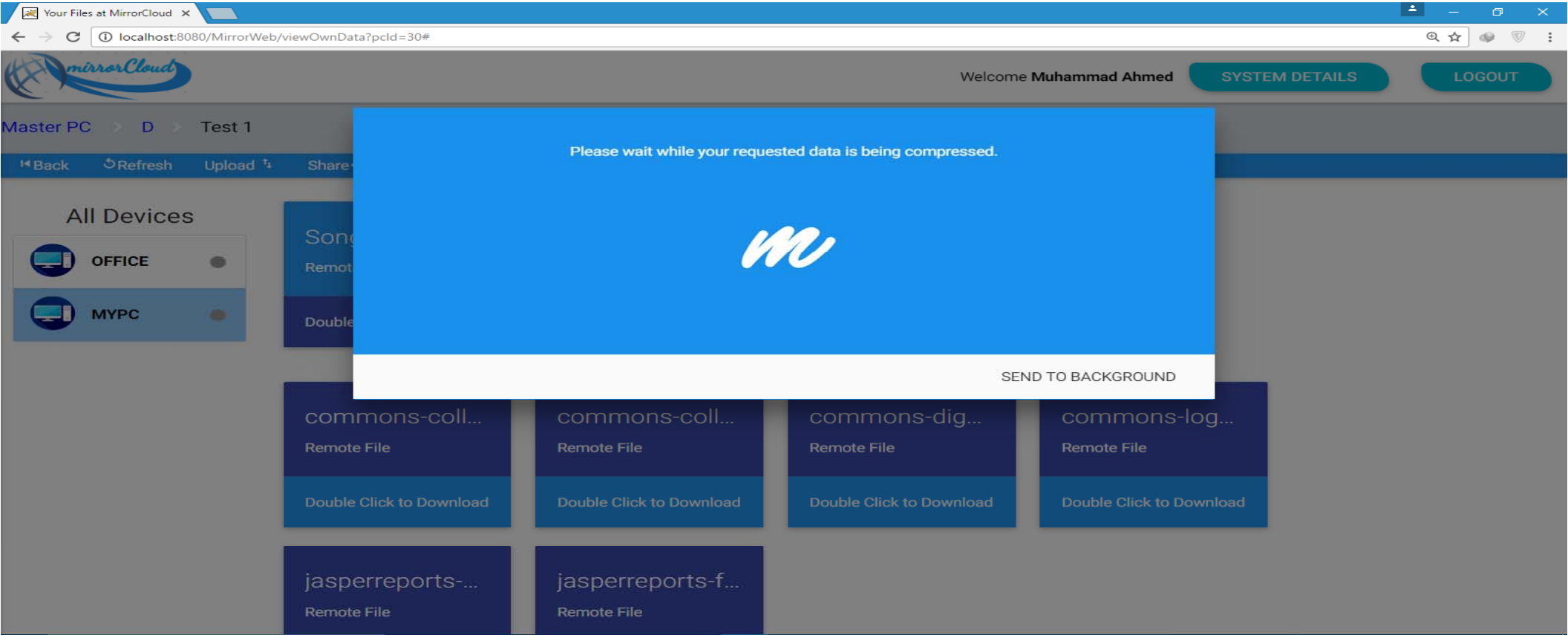

Home : Mirror Cloud
localhost:8080/MirrorWeb/
Login To MirrorCloud
Get to your files and photos from anywhere, on any device. Share and work together with anyone in your work and life.
Username...
Password...
LOGIN
REGISTER
Made By MirrorCloud Team


Your Files at MirrorCloud
localhost:8080/MirrorWeb/viewOwnData?pcId=30
mirrorCloud
Welcome Muhammad Ahmed
SYSTEM DETAILS
LOGOUT
Master PC
Back
Refresh
Share
All Devices
OFFICE
MYPC
C
Remote Drive
Double Click to Browse
D
Remote Drive
Double Click to Browse
E
Remote Drive
Double Click to Browse

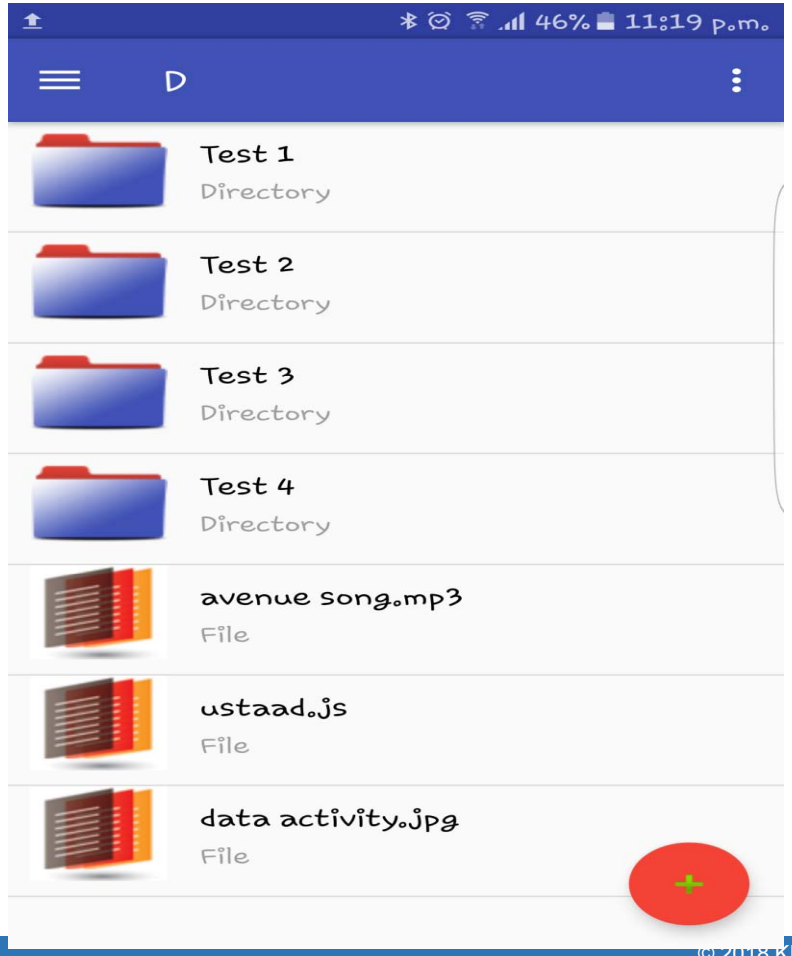

Your Files at MirrorCloud
localhost:8080/MirrorWeb/viewOwnData?pcId=30#
mirrorCloud
Welcome Muhammad Ahmed
SYSTEM DETAILS
LOGOUT
Master PC > D
Back
Refresh
Share
Download
Download This
Delete
Rename
1 Item/s Selected
All Devices
OFFICE
MYPC
Test 1
Remote Directory
Test 2
Remote Directory
Test 3
Remote Directory
Test 4
Remote Directory
Open
Share
avenue song....
Remote File
ustaad.js
Remote File
data activity.j...
Remote File

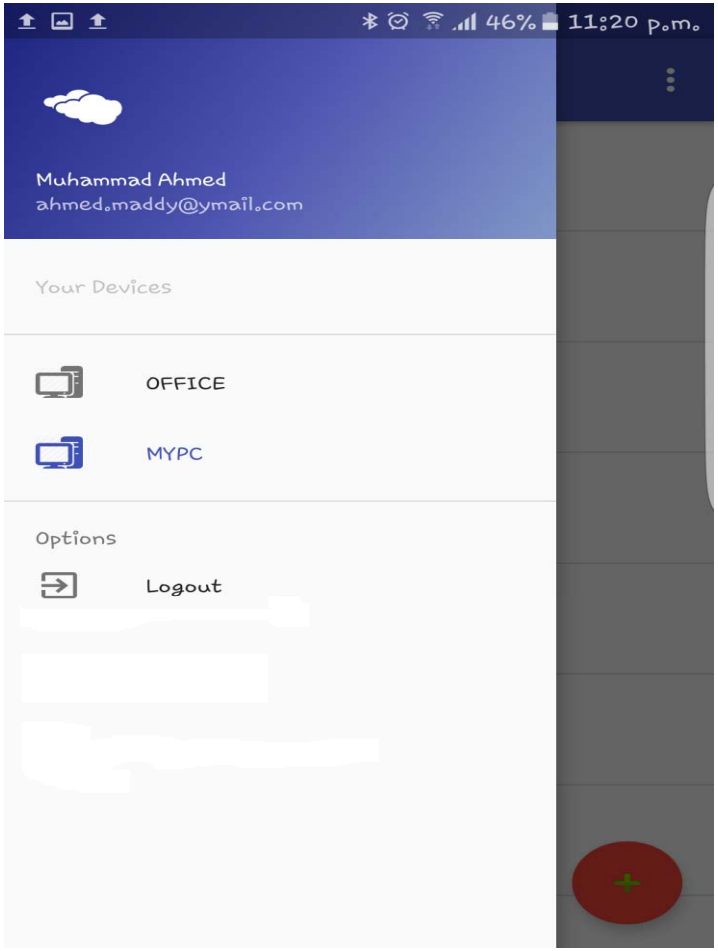

Your Files at MirrorCloud
localhost:8080/MirrorWeb/viewOwnData?pcId=30#
mirrorCloud
Welcome Muhammad Ahmed
SYSTEM DETAILS
LOGOUT
Master PC
D
Back
Refresh
Share
1 Item/s Selected
All Devices
OFFICE
MYPC
Please Select to whom you want to share
Share To
a
Everyone
Access
Read Only
crixy7 (Abdul Wahab)
threethorier (Muhammad Awais)
ahmed (M. Ahmed)
crixy7 (Abdul Wahab)
CANCEL
SHARE


Your Files at MirrorCloud
localhost:8080/MirrorWeb/viewOwnData?pcId=30#
mirrorCloud
Welcome Muhammad Ahmed
SYSTEM DETAILS
LOGOUT
Master PC > D
Back
Refresh
Share
Download This
All Devices
OFFICE
MYPC
Test 1
Remote Directory
Double Click to Browse
Test 2
Remote Directory
Double Click to Browse
Test 3
Remote Directory
Double Click to Browse
Test 4
Remote Directory
Double Click to Browse
avenue song....
ustaad.js
data activity.jpg
Generating Public Link
Anyone having this link can use the shared data.
http:\\localhost:8080/MirrorWeb/public?data=RFxUZXN0IDJTdW4gRGVjIDI1IDIyOjAxOjMwIFBLVCAyMDE2
CLOSE


Your Files at MirrorCloud
localhost:8080/MirrorWeb/viewOwnData?pcId=30#
mirrorCloud
Welcome Muhammad Ahmed
SYSTEM DETAILS
LOGOUT
Master PC > D > Test 1
Back
Refresh
Upload
Share
All Devices
OFFICE
MYPC
Please wait while your requested data is being compressed.
SEND TO BACKGROUND
commons-coll...
Remote File
Double Click to Download
commons-coll...
Remote File
Double Click to Download
commons-dig...
Remote File
Double Click to Download
commons-log...
Remote File
Double Click to Download
jasperreports-...
Remote File
jasperreports-f...
Remote File


MirrorCloud
Awaiting Connection


46% 11:19 p.m.
D
Test 1
Directory
Test 2
Directory
Test 3
Directory
Test 4
Directory
avenue song.mp3
File
ustaad.js
File
data activity.jpg
File


46%
11:20 p.m.
Muhammad Ahmed
ahmed.maddy@ymail.com
Your Devices
OFFICE
MYPC
Options
Logout

Potential Benefits of Secure Cloud Computing Framework

Way Forward

- ►Information and knowledge are growing exponentially
- ►People need high computing power
- ►Public –Private Model for National Cloud Development
- ►E-Governance
- ►eHealth Care, eEducational Clouds

National Cyber Secure Cloud is the demand of Today !

84

Thank You !!!