CCSP – Certified Cloud Security Professional

Bharathi M – SSCP, CISSP

What is Cloud?

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

— *Source: NIST*

What is Cloud?

– Image source: internet

Cloud Computing Roles

- Cloud Service Provider – CSP
- Cloud Customer
- Cloud Service Partner
- Cloud Access Security Brokers – CASB

AWS Partner Network – https://aws.amazon.com/partners/

Azure Partner – https://azure.microsoft.com/en-us/partners/

Cloud – Essential Characteristics

1. On-demand self-service
2. Broad network access
3. Resource pooling
4. Repaid Elasticity
5. Measured Service

Cloud – Service Models

1. Software as a Service (SaaS)
2. Platform as a Service (PaaS)
3. Infrastructure as a Service (IaaS)

Cloud – Deployment Models

1. Private
2. Public
3. Hybrid
4. Community

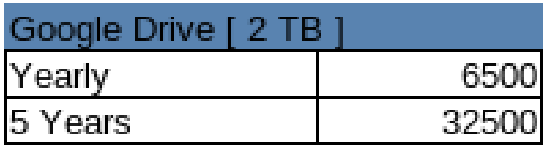
Cloud – Multitenancy

Multitenancy is a type of computing architecture in which one or more logical software instances are created and executed on top of primary software

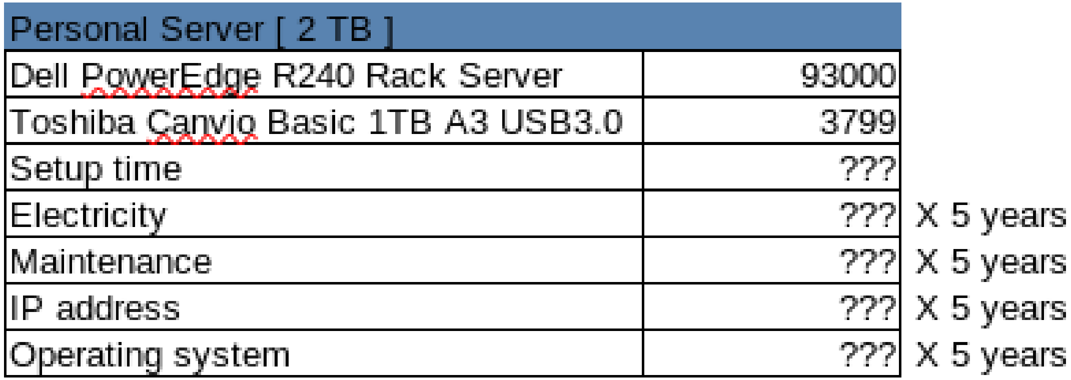
— *Source: techopedia*

– *Image source: internet*

CBA – Cost Benifit Analysis



Google Drive [2 TB]	
Yearly	6500
5 Years	32500



Personal Server [2 TB]		
Dell PowerEdge R240 Rack Server	93000	
Toshiba Canvio Basic 1TB A3 USB3.0	3799	
Setup time	???	
Electricity	???	X 5 years
Maintenance	???	X 5 years
IP address	???	X 5 years
Operating system	???	X 5 years

Virtualization

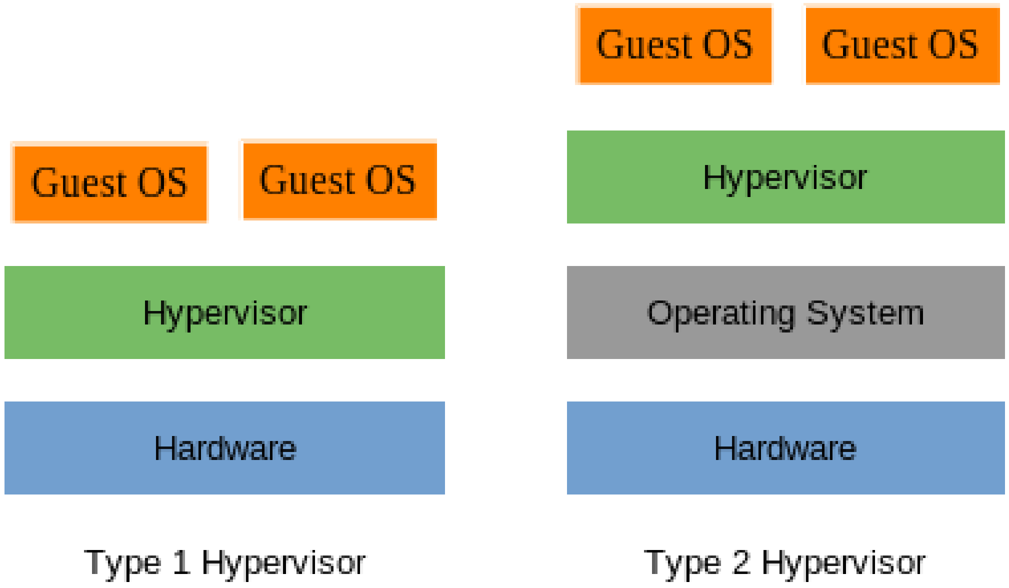
Virtualization is the act of creating a virtual version of something, including virtual computer hardware platforms, storage devices, and computer network resources.

— *Source: Wikipedia*

– Image source: internet

Virtualization – New Terms

1. Host Machine
2. Guest Machine
3. Hypervisor
   - Bare-metal hypervisor (Type – 1)
   - Hosted hypervisor (Type – 2)



Virtualization – Security Issues

1. VM Escape
2. VM Sprawl

Virtualization – Extra for the Experts

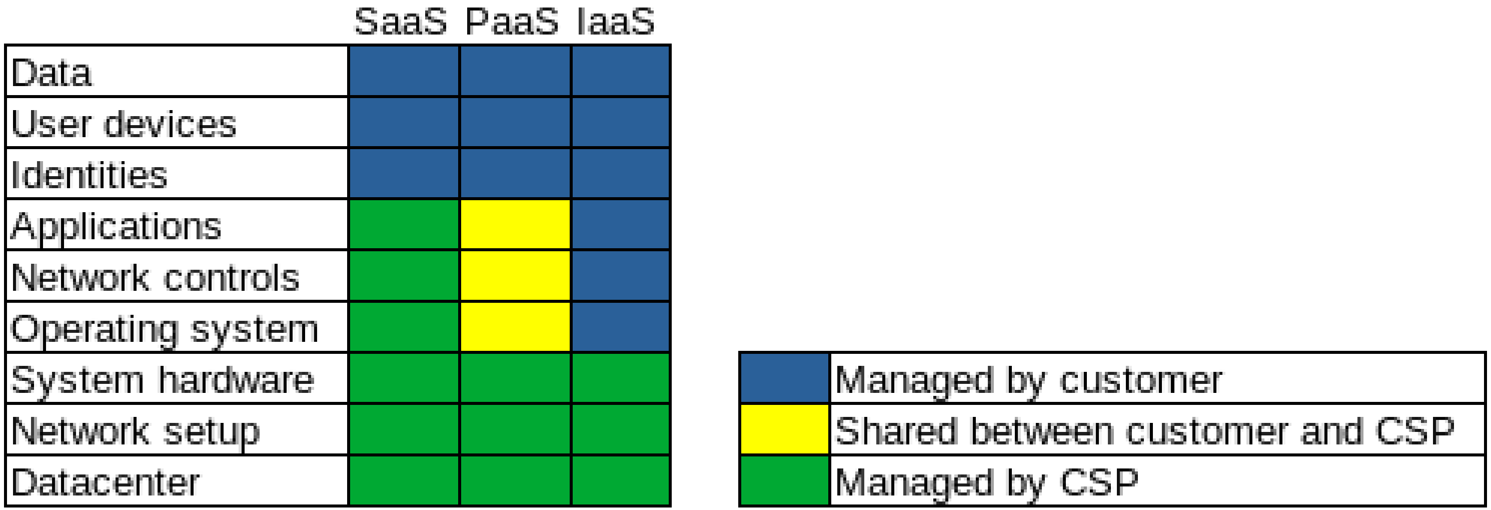
1. Desktop Virtualization
2. Application Virtualization

Cloud – Building Blocks

- Virtualization
- Storage
  - Block Storage (expensive)
  - Object Storage (Affordable)
- Networking
  - VPC – Virtual Private Cloud
- Database
  - Traditional Database
  - Managed Database
  - Cloud native Database

- Storage
  - Infrastructure as a Code
    - Vendor API
    - Third party API

Cloud – Shared Responsibility Model



	SaaS	PaaS	IaaS
Data	🟦	🟦	🟦
User devices	🟦	🟦	🟦
Identities	🟦	🟦	🟦
Applications	🟩	🟨	🟦
Network controls	🟩	🟨	🟦
Operating system	🟩	🟨	🟦
System hardware	🟩	🟩	🟩
Network setup	🟩	🟩	🟩
Datacenter	🟩	🟩	🟩

🟦	Managed by customer
🟨	Shared between customer and CSP
🟩	Managed by CSP

Cloud – Security Concerns

- Confidentiality
- Integrity
- Availability
- Privacy
- Legal and Regulatory compliance

✔ Governance must exist to address all the above and other concerns

Cloud – Operational Consideration

- Reversibility – Roll back plan
- Portability – Data
- Interoperability – Our solution / application

Cloud – Emerging Technologies

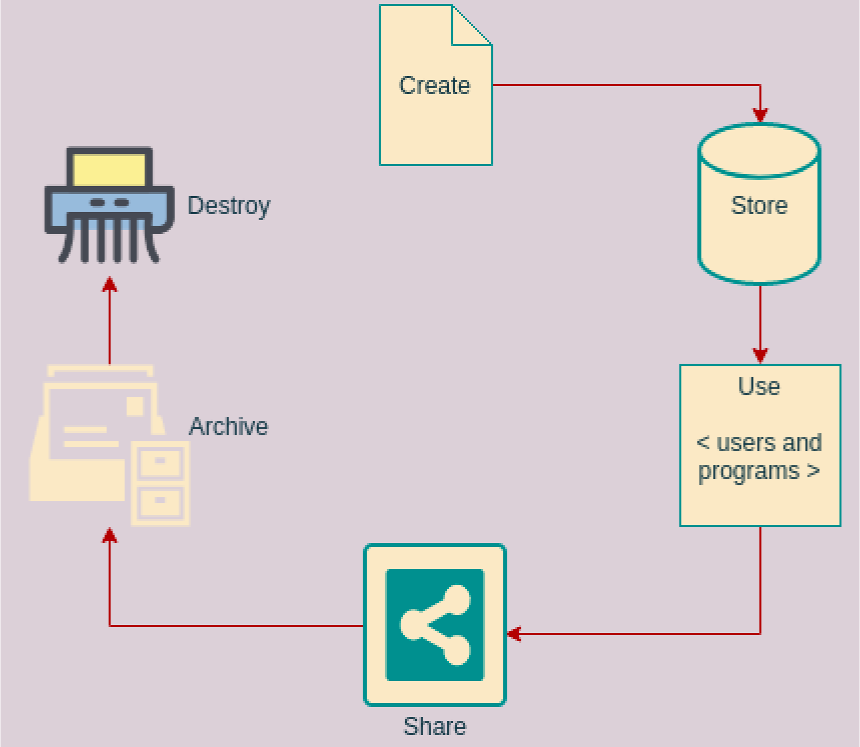
1. Machine Learning (ML)
2. Artificial Intelligence (AI)
3. Blockchain
4. Internet of Things (IoT)
    - ICS
    - SCADA
5. Containers
6. Quantum computing

Cloud – Evaluating CSPs

- ISO 27017
- PCI DSS
- FedRAMP – US Government cloud service certification

https://marketplace.fedramp.gov/#!/products?sort=productName

Cloud – Data Lifecycle



Cloud Storage

- Raw Disk Storage
  - Permenant & Indipendant
  - Virtual disk drives
- Ephemeral Storage
  - Temporary and attached to that perticular instance
  - Faster

Cloud Storage – New Terms

- Data Dispersion
  - Store data in multiple locations

Don't put all your eggs in one basket

– Image source: internet

Cloud Storage – Security

- Encryption
  - Data-in-transit
  - Data-at-rest
- Access Control

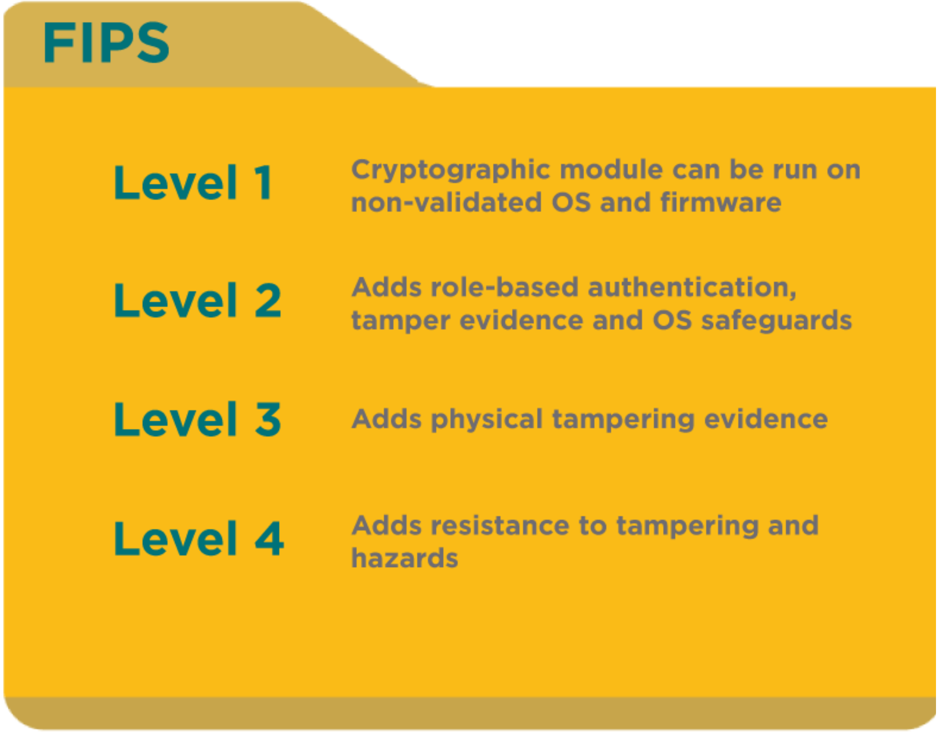
Cryptography 101

- Encryption
- Decryption
- Algorithm
- Key
- Symmetric Encryption – Faster
  - ➢ Shared secret key
- Asymmetric Encryption – Slower
  - ➢ Private Key
  - ➢ Public Key

- **Goals**
  - ✓ Confidentiality
  - ✓ Integrity
  - ✓ Authentication
  - ✓ Authorization
  - ✓ Non-repudiation
- **Key Exchange**
  - ✓ In-band vs out of band key exchange
  - ✓ Key Escrow

Cryptography 101 – Key Storage

- HSM – Hardware Security Module
  - A hardware security module is a physical computing device that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, strong authentication and other cryptographic functions
  - FIPS 140-2
    - Level 2 – CC EAL 2 certified
    - Level 3 – CC EAL 4 certified



FIPS

Level 1	Cryptographic module can be run on non-validated OS and firmware
Level 2	Adds role-based authentication, tamper evidence and OS safeguards
Level 3	Adds physical tampering evidence
Level 4	Adds resistance to tampering and hazards

– Image source: internet