Course: Cloud Computing

Week 6: Cloud Infrastructure and Architecture

Lecturer: Ikwap Flavia Agatha
MSc. Computer Forensic
PHD in IT (Candidate)
University: Kumi University

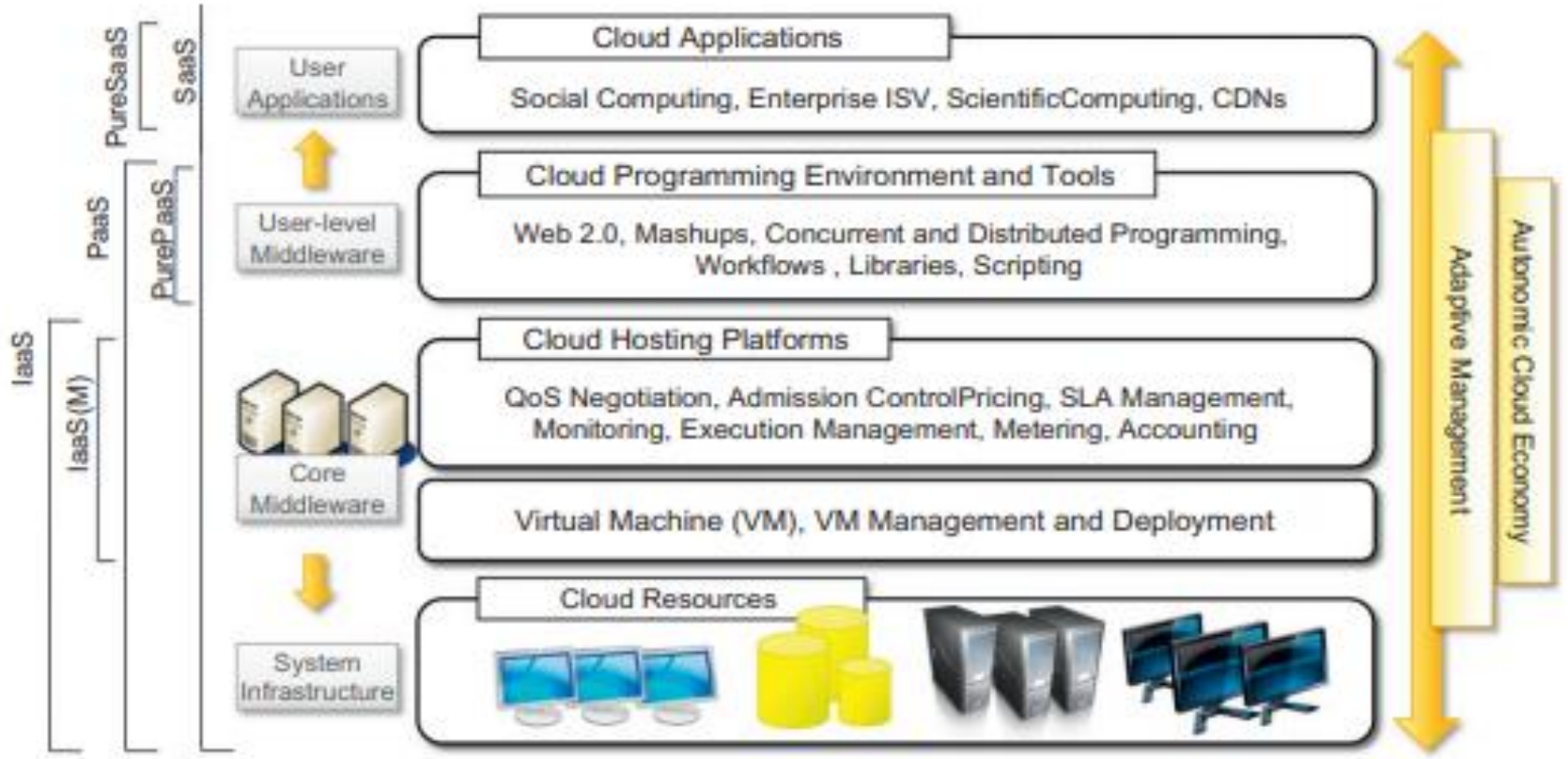
Lecture Learning out come

- At the end of these lecture you will be able to:
- Understand cloud infrastructure and Architecture
- Understand Cloud design objectives
- Understand infrastructure Components
- Understand Architecture Principles
- Understand Design considerations

Cloud Infrastructure and Architecture

- Cloud computing infrastructure and architecture consist of all physical and virtual components that make up a cloud computing environment.
- The physical infrastructure is managed by the core middleware, the objectives of which are to provide an appropriate runtime environment for applications and to best utilize resources. At the bottom of the stack, virtualization technologies are used to guarantee runtime environment customization, application isolation, sandboxing, and quality of service.

Physical infrastructure



- (Buyya, 2013)

Cloud Design Objectives:

- **Shifting Computing from Desktops to Datacenters:** The shift of computer processing, storage, and software delivery away from desktop and local servers to datacenters over the Internet.
- **Service Provisioning and Cloud Economics:** Provider supply cloud services by signing SLAs (Service Level Agreements) with consumers and end users. The services must be resource economic with efficiency in computing, storage, and power consumption, etc.

Cloud Design Objectives:

- **High Quality of Cloud Services:** The QoS of cloud computing must be standardized to remove doubt over services provided to users. Cloud interoperability is required across multiple providers. New Standards and Interfaces: This refers to solving the data lock-in problem associated with datacenters or cloud providers, universally accepted APIs and access protocols are need to provide high portability and flexibility of virtualized applications.

Infrastructure Components:

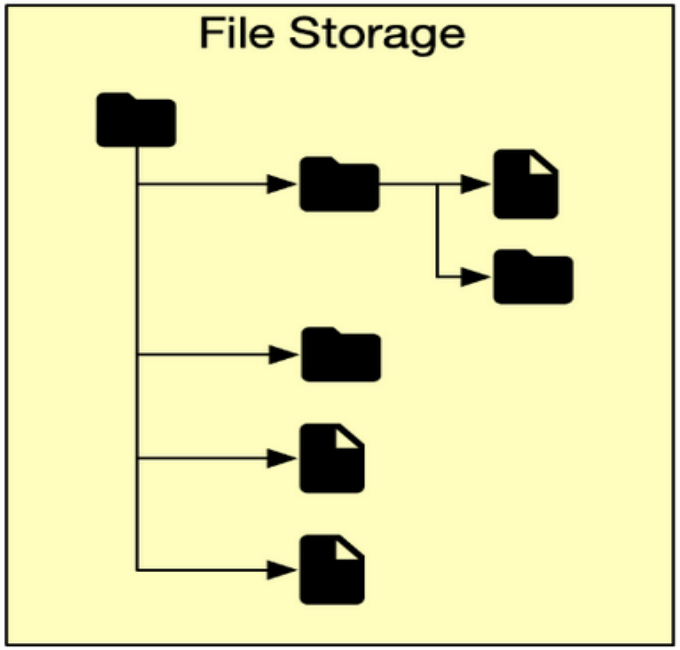
- Some of the infrastructure Components include:
  - **Virtualization**: Very Core enabler of cloud computing, allowing multiple virtual instances to run on a single physical (hardware) machine.
  - **Compute**: Virtual machines (VMs), containers, and server less functions provide the processing power to run applications.

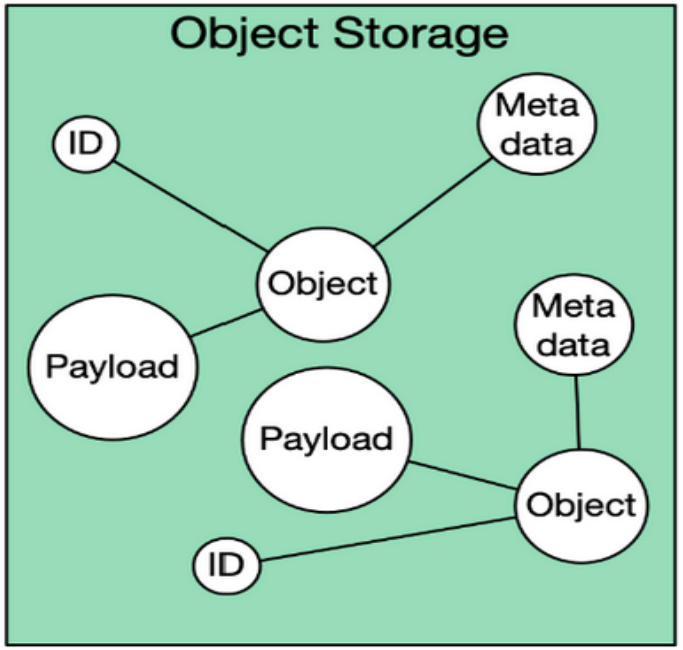
Infrastructure Components: Storage:

Facilities that support data storage in the cloud;

- Object storage (Object storage is a storage architecture that manages data as Objects rather than as blocks or files)
- File storage - (Data is stored in one single unit of the information under the hierarchy of folders. Accessible over standard network protocols such as NFS (Network File System) or SMB (Server Message Block)
- Bock storage (Block storage is a data storage approach in which each storage block acts as an independent hard drive).

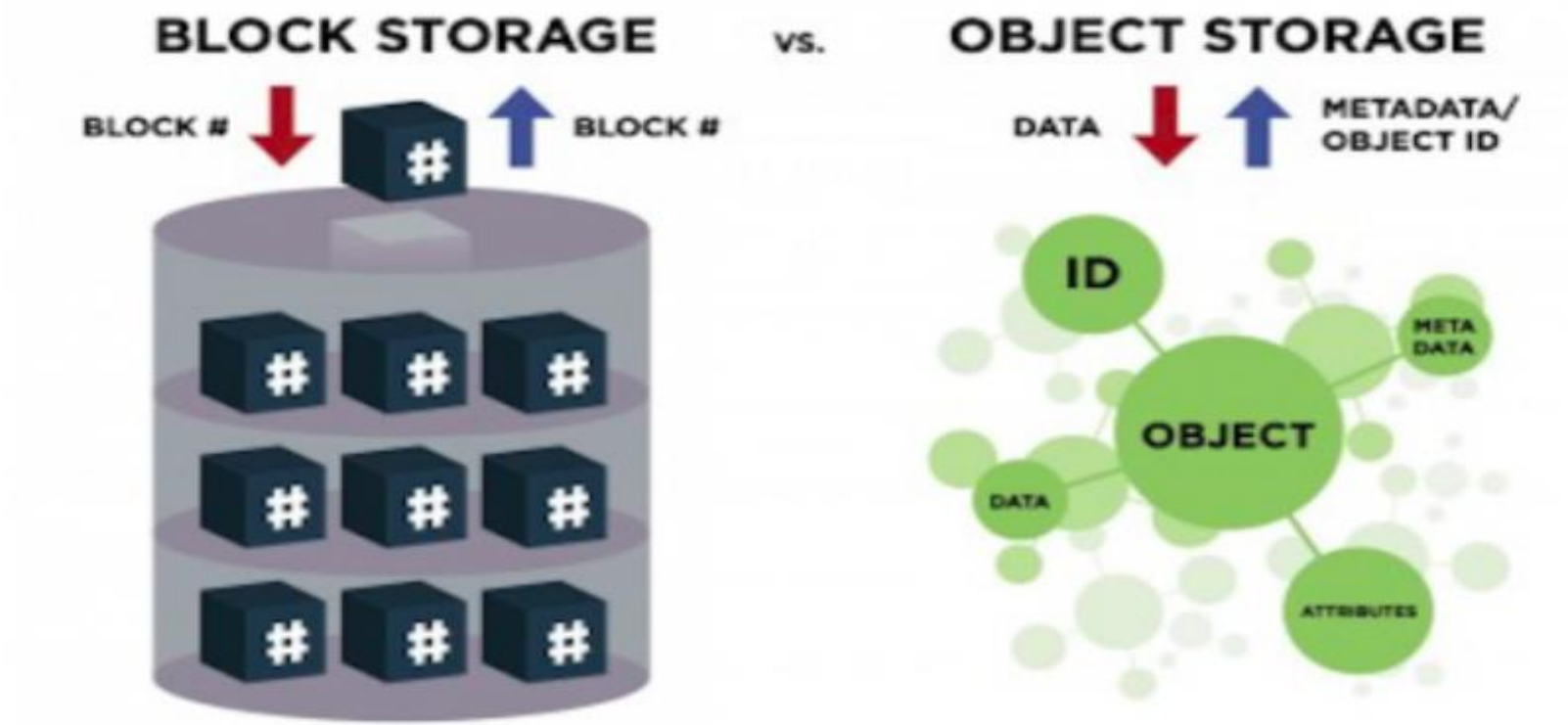
File and Object storage





- https://forum.huawei.com/enterprise/en/characteristics-of-computer-storage-devices/thread/694722873471680512-6672138597332541144

Object and Block storage



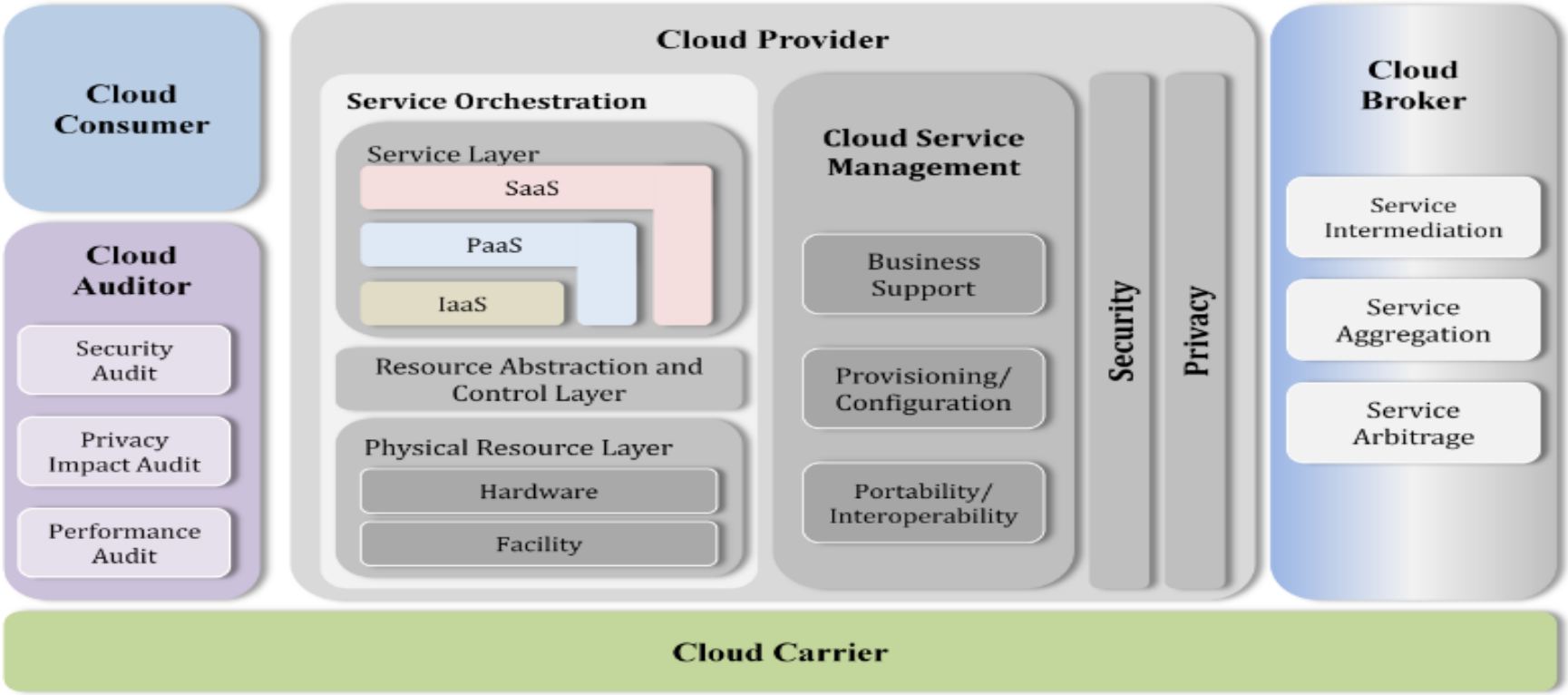
- https://www.druva.com/blog/object-storage-versus-block-storage-understanding-technology-differences

Infrastructure Components:

- **Networking**: Virtual networks, load balancers, and content delivery networks (CDNs) facilitate communication between cloud resources and users.
- **Security**: Access controls, Identity, Authentication, encryption, firewalls, and other security measures implemented to protect cloud environments from threats.

Infrastructure Components: Various players:

NIST cloud computing reference architecture



- (Liu, 2011)

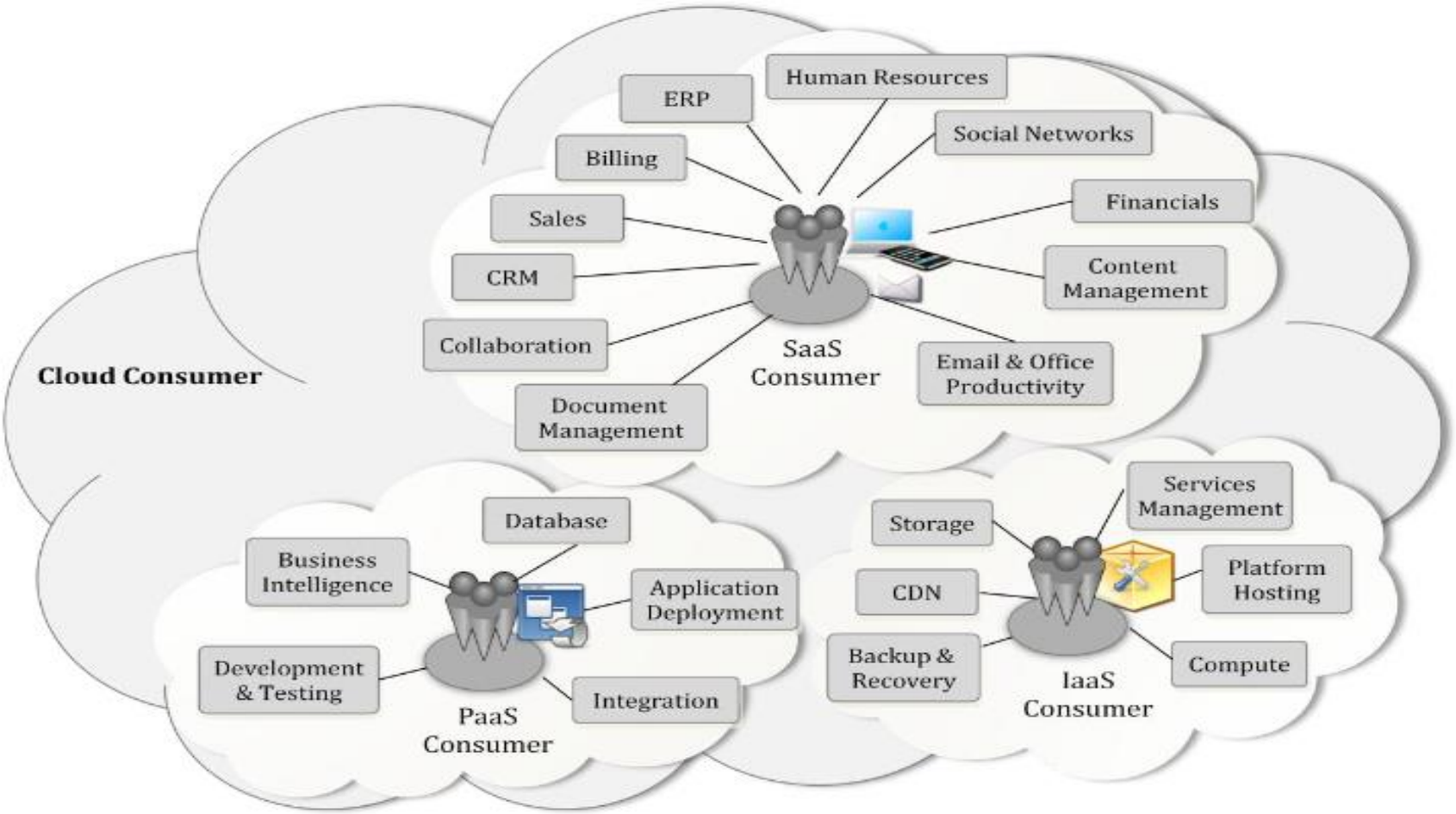
Infrastructure Components:

- NIST cloud computing reference architecture defines five major actors: cloud consumer, cloud provider, cloud carrier, cloud auditor and cloud broker. **Cloud Consumer**
- The cloud consumer is the principal stakeholder for the cloud computing service. A cloud consumer represents a person or organization that maintains a business relationship with, and uses the service from a cloud provider.

Cloud Consumer

- A cloud consumer browses the service catalog from a cloud provider, requests the appropriate service, sets up service contracts with the cloud provider, and uses the service. The cloud consumer may be billed for the service provisioned, and needs to arrange payments accordingly.

Infrastructure Components: :



- (Liu, 2011)

Cloud Provider

- A cloud provider is a person, an organization; it is the entity responsible for making a service available to interested parties. A Cloud Provider acquires and manages the computing infrastructure required for providing the services, runs the cloud software that provides the services, and makes arrangement to deliver the cloud services to the Cloud Consumers through network access.

Cloud Provider

- For Software as a Service, the cloud provider deploys, configures, maintains and updates the operation of the software applications on a cloud infrastructure so that the services are provisioned at the expected service levels to cloud consumers.
- For PaaS, the Cloud Provider manages the computing infrastructure for the platform and runs the cloud software that provides the components of the platform, such as runtime software execution stack, databases, and other middleware components.

Cloud Provider

- They also supports the development, deployment and management process of the PaaS Cloud Consumer by providing tools such as integrated development environments (IDEs), development version of cloud software, software development kits (SDKs), deployment and management tools.

Cloud Auditor

- A cloud auditor is a party that can perform an independent examination of cloud service controls with the intent to express an opinion thereon. Audits are performed to verify conformance to standards through review of objective evidence. A cloud auditor can evaluate the services provided by a cloud provider in terms of security controls, privacy impact, performance, etc.

Cloud Broker

- As cloud computing evolves, the integration of cloud services can be too complex for cloud consumers to manage. A cloud consumer may request cloud services from a cloud broker, instead of contacting a cloud provider directly. A cloud broker is an entity that manages the use, performance and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers.

Cloud Broker

- Service Intermediation: A cloud broker enhances a given service by improving some specific capability and providing value-added services to cloud consumers. The improvement can be managing access to cloud services, identity management, performance reporting, enhanced security, etc.

A cloud broker provide services in three categories:

- Service Aggregation: A cloud broker combines and integrates multiple services into one or more new services. The broker provides data integration and ensures the secure data movement between the cloud consumer and multiple cloud providers.

A cloud broker provide services in three categories:

- Service Arbitrage: Service arbitrage is similar to service aggregation except that the services being aggregated are not fixed. Service arbitrage means a broker has the flexibility to choose services from multiple agencies. The cloud broker, for example, can use a credit-scoring service to measure and select an agency with the best score.

Cloud Carrier

- A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers. Cloud carriers provide access to consumers through network, telecommunication and other access devices. For example, cloud consumers can obtain cloud services through network access devices, such as computers, laptops, mobile phones, mobile Internet devices

Cloud Service Management

- Cloud Service Management includes all of the service-related functions that are necessary for the management and operation of those services required by or proposed to cloud consumers

Cloud Service Management

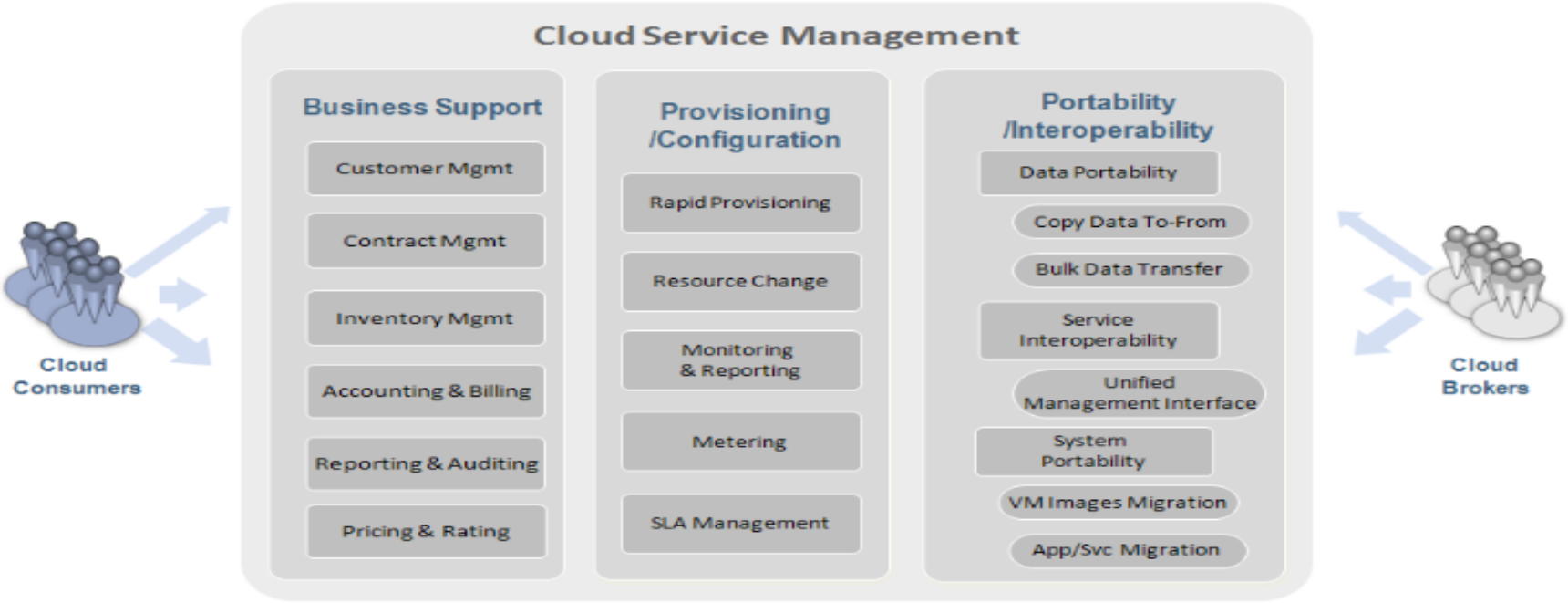


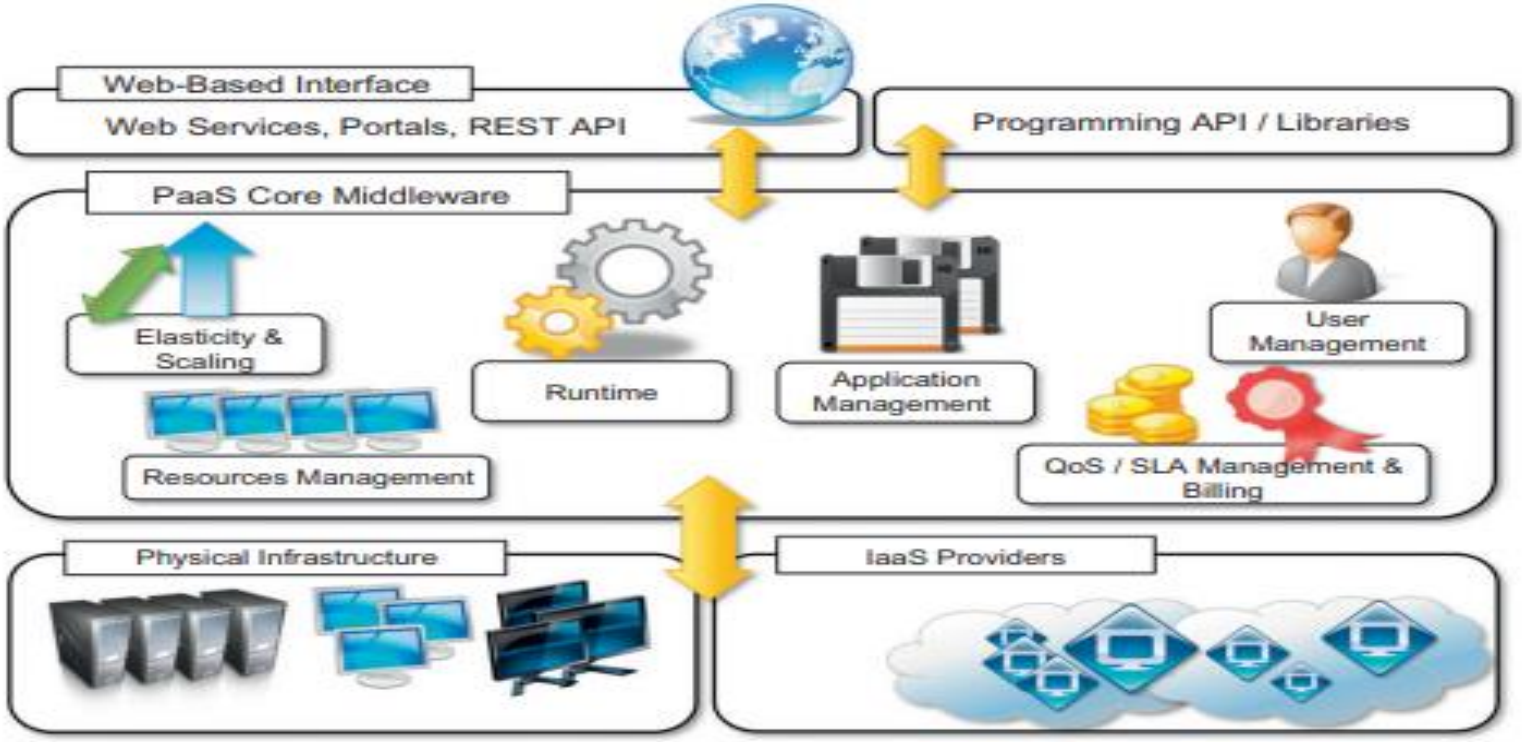
Figure 16: Cloud Provider - Cloud Service Management

- (Liu, 2011)

Cloud Service Architecture

- **Platform as a service**
- Platform-as-a-Service (PaaS) solutions provide a development and deployment platform for running applications in the cloud. They constitute the middleware on top of which applications are built.

Cloud Service Architecture



- (Buyya, 2013)

Cloud Service Architecture

- Characteristics that identify a PaaS solution:
- Application management is the core functionality of the middleware. PaaS implementations provide applications with a runtime environment
- They automate the process of deploying applications to the infrastructure, configuring application components, provisioning and configuring supporting technologies such as load balancers and databases, and managing system change based on policies set by the user.

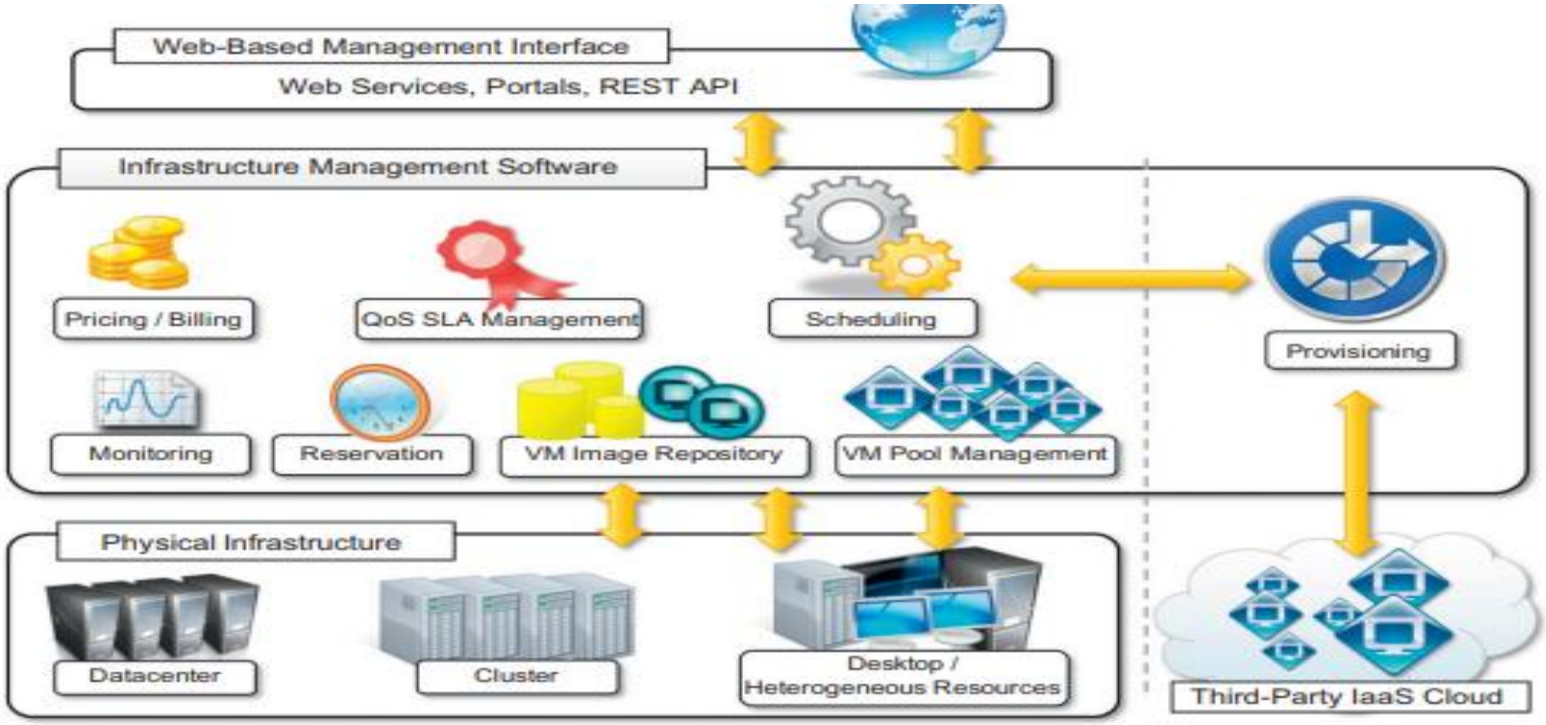
Cloud Service Architecture

- Managing the resources and scaling applications on demand or automatically, according to the commitments made with users. From a user point of view, the core middleware exposes interfaces that allow programming and deploying applications on the cloud. These can be in the form of a Web-based interface or in the form of programming APIs and libraries.
- The runtime framework executes end-user code according to the policies set by the user and the provider.

Cloud Service Architecture

- Automation. PaaS environments automate the process of deploying applications to the infrastructure, scaling them by provisioning additional resources when needed
- Cloud services. PaaS offerings provide developers and architects with services and APIs, helping them to simplify the creation and delivery of elastic and highly available cloud applications.
- Another essential component for a PaaS-based approach is the ability to integrate third-party cloud services offered from other vendors by leveraging service-oriented architecture. Such integration should happen through standard interfaces and protocols.

Architecture of Hardware as service



- (Buyya, 2013)

Architecture of Hardware as service

- The main technology used to deliver and implement these solutions is hardware virtualization:
- Web services, RESTful APIs, and mash-ups- enable applications or users to access the services exposed by the underlying infrastructure.
- Scheduler-allocates execution of virtual machine instances.
- The pricing and billing component takes care of the cost of executing each virtual machine instance and maintains data that will be used to charge the user.

Architecture of Hardware as service

- The monitoring component tracks the execution of each virtual machine instance and maintains data required for reporting and analyzing the performance of the system.
- The reservation component stores the information of all the virtual machine instances that have been executed or that will be executed in the future.

Architecture of Hardware as service

- QoS/SLA(Quality of Service) management component will maintain a repository of all the SLAs made with the users; ensures that a given virtual machine instance is executed with the desired quality of service
- The VM repository component provides a catalog of virtual machine images that users can use to create virtual instances. Some implementations also allow users to upload their specific virtual machine images.
- A VM pool manager component is responsible for keeping track of all the live instances.

Architecture Principles:

- **Scalability**: Is important for the cloud eco system, Cloud architectures should be designed to handle different workloads by automatically scaling resources up or down as needed. The following are types of scaling:
- Horizontal Scaling – scaling out and scaling in
- Vertical Scaling – scaling up and scaling down (Erl, 2013)

Architecture Principles:

- **Availability**: Security mechanisms, Redundancy, fault tolerance, backup and disaster recovery mechanisms ensure that cloud services remain available even in the event of failures.
- **Resilience**: Architectures should be resilient to failures and disruptions, with components distributed across multiple availability zones or regions.

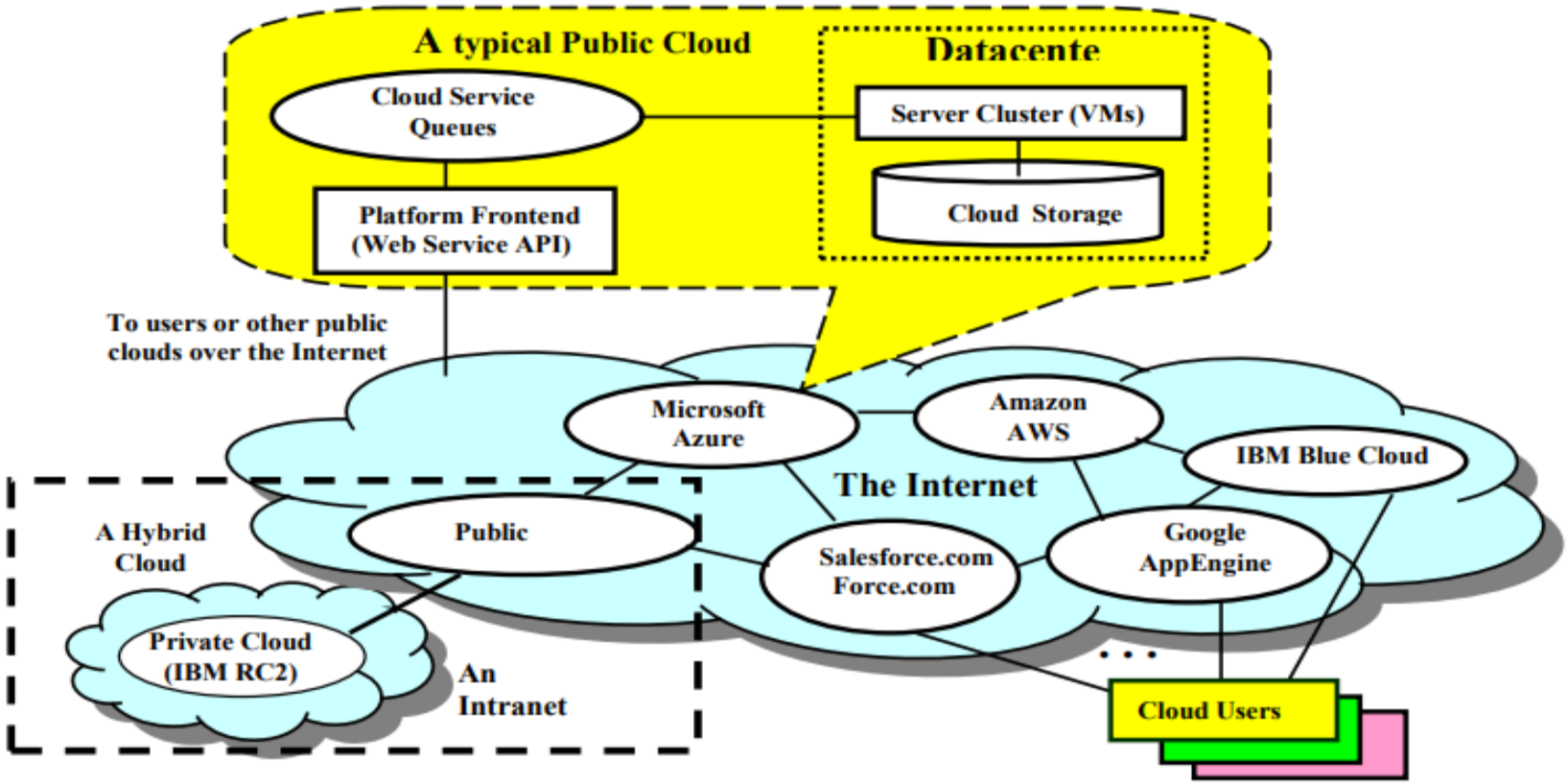
Architecture Principles:

- **Elasticity**: Cloud resources should be elastic, allowing them to quickly adapt to changes in demand without manual intervention.
- **Cost Optimization**: Designing cost-effective architectures by leveraging on-demand pricing, resource utilization optimization, and efficient workload management.
- **Security and Compliance**: Cloud must implement security best practices and compliance measures to protect data and meet regulatory requirements.

Types of Cloud Architectures:

- **Public Cloud**: Services are provided by third-party cloud providers over the internet, accessible to multiple organizations or individuals.
- **Private Cloud**: Cloud infrastructure is dedicated to a single organization, either hosted on-premises or by a third-party provider.
- **Hybrid Cloud**: Combines public and private cloud environments, allowing data and applications to move between them as needed.
- **Multi-Cloud**: Utilizes services from multiple cloud providers to avoid vendor lock-in, increase resilience, and optimize costs.

Using a hybrid Cloud to access cloud resources



- (Hwang, 2010)

Design Considerations

- Designing a suitable Cloud computing solution requires an organization to consider a number of factors as follows:
- **Define Requirements**:
  - Taking into consideration an organization's objectives, business goals, and technical requirements.
  - Identify the types of workloads and applications that will be migrated or developed for the cloud.
  - Determine performance, scalability, availability, security, and compliance requirements.

Design Considerations

- **Select Cloud Model**:
  - Choose the appropriate cloud deployment model (public, private, hybrid, or multi-cloud) based on security, compliance, and operational needs.
  - Decide whether to use Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS) offerings, or a combination thereof.

Design Considerations

- **Architectural Design**:
  - Design the overall architecture, including compute, storage, networking, security, and management components.
  - Consider scalability, fault tolerance, disaster recovery, and performance optimization.
  - Define data architecture, including data storage, databases, and data processing frameworks.
  - Determine the integration points with existing systems and services.

Design Considerations

- **Security and Compliance**:
  - Apply security mechanism, including identity and access control, encryption, network security, and threat detection.
  - Ensure compliance with relevant regulations and industry standards
- **Resilience and High Availability**:
  - Design for fault tolerance and high availability by distributing resources across multiple availability zones or regions.
  - Implement automated failover mechanisms and disaster recovery strategies to minimize downtime.

Design Considerations

- **Cost Optimization**:
  - Optimize resource utilization to minimize costs while meeting performance and availability requirements.
  - Leverage on-demand pricing, reserved instances, and spot instances to reduce expenses.
  - Monitor resource usage and adjust capacity as needed to avoid over-provisioning or underutilization.

Design Considerations

- **Performance Optimization**:
  - Optimize application and infrastructure performance through efficient resource allocation, load balancing, caching, and content delivery.
  - Consider factors such as latency, throughput, and response times to ensure a responsive user experience.

Design Considerations

- **Automation and Orchestration**:
  - Implement automation tools and workflows for provisioning, configuration management, monitoring, and scaling.
  - Use orchestration platforms like Kubernetes or cloud-native services to manage containerized workloads and microservices.

Design Considerations

- **Testing and Validation**:
  - Test the cloud design under various scenarios to validate performance, scalability, security, and reliability.
  - Conduct load testing, security testing, and disaster recovery drills to identify and address potential issues.

Design Considerations

- **Documentation and Governance**:
  - Document the cloud architecture, design decisions, and configurations for future reference and knowledge sharing.
  - Establish governance policies and procedures for managing cloud resources, access control, and compliance.

Next Lecture

- Cloud Deployment and Management

References

- Buyya, R. (2013). *Mastering Cloud Computing.* USA: MK.
- Erl, T. (2013). *Cloud Computing Concepts, Technology and Architecture.* Westford, Massachusetts: Prentice Hall.
- Hwang, K. (2010). *Cloud Architecture and Datacenter design.*
- Liu, F. (2011). *NIST Cloud Computing Reference Architecture.* USA: NIST Special Publication.