COSC130

Topic 10-2: Introduction to Cloud Security

Uday Tupakula
A/Prof in Cyber Security
School of Science and Technology
Faculty of Science, Agriculture, Business and Law
University of New England

Cloud Computing

- NIST Definition(SP 800-145): 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.

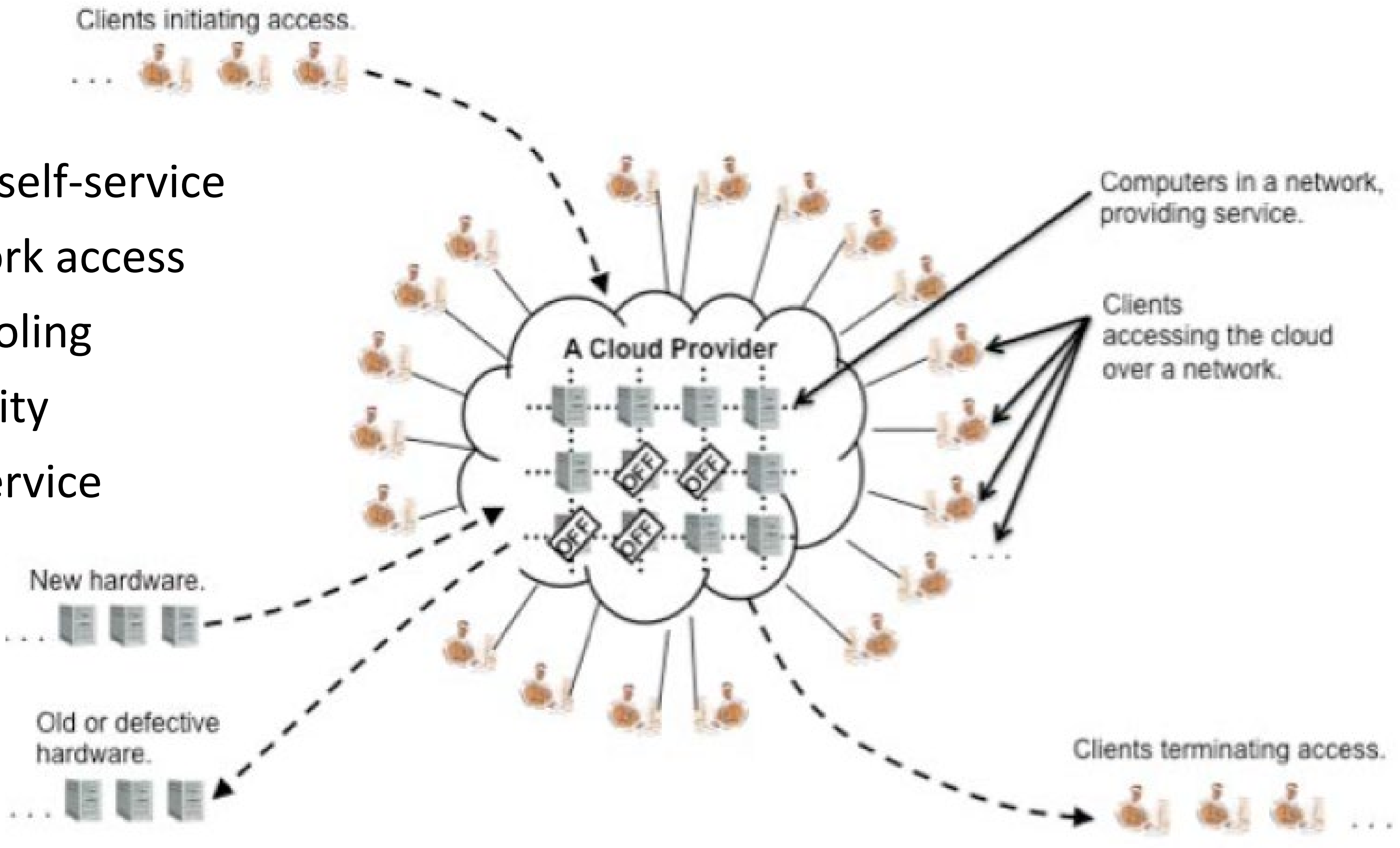
- Cloud model composed of
  - five essential characteristics
  - three service models
  - four deployment models

Cloud Computing: Essential Characteristics

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

General Cloud View

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

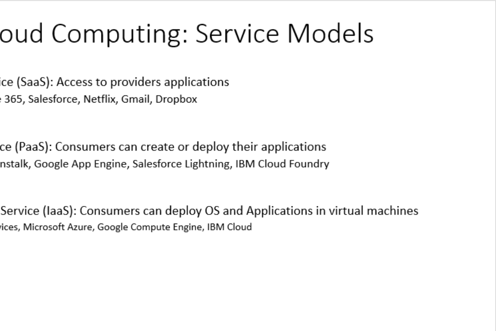

Clients initiating access.
A Cloud Provider
OFF
Computers in a network, providing service.
Clients accessing the cloud over a network.
New hardware.
Old or defective hardware.
Clients terminating access.

Cloud Computing: Typical Commercial Terms of Service

- Terms of service determined by legally binding agreement between providers and consumers
  - Service Agreement
  - Service Level Agreement

- Promises
  - Availability
  - Remedies for failure to perform: offer credits or refund
  - Data Preservation: service termination due to violation in acceptable usage policies
  - Legal care : do not sell or disclose customer information and/or data

- Limitations
  - Scheduled Outages not
  - Major Events: natural disasters
  - eement Changes
  - nerally security risks placed on consumers



oud Computing: Service Models

ice (SaaS): Access to providers applications
365, Salesforce, Netflix, Gmail, Dropbox

ce (PaaS): Consumers can create or deploy their applications
nstalk, Google App Engine, Salesforce Lightning, IBM Cloud Foundry

Service (IaaS): Consumers can deploy OS and Applications in virtual machines
vices, Microsoft Azure, Google Compute Engine, IBM Cloud

Cloud Computing: Typical Commercial Terms of Service

- Obligations
  - Acceptable Usage Policies
  - Licenced Software
  - Timely Payments

- Recommendations
  - Terminology: pay attention to some of the terms redefined by cloud provider
  - Compliance: service agreements should specify compliance with applicable laws and regulations
  - Security Criticality and Backup: check if provider recommends individual backup
  - Negotiated Service Agreements: discuss required modifications to terms of service prior to use
  - Service Agreement Changes: Provider may change terms of service with some notice period.

Cloud Computing: Service Models

- Software as a Service (SaaS): Access to providers applications
  - Microsoft Office 365, Salesforce, Netflix, Gmail, Dropbox

- Platform as a Service (PaaS): Consumers can create or deploy their applications
  - AWS Elastic Beanstalk, Google App Engine, Salesforce Lightning, IBM Cloud Foundry

- Infrastructure as a Service (IaaS): Consumers can deploy OS and Applications in virtual machines
  - Amazon Web Services, Microsoft Azure, Google Compute Engine, IBM Cloud

Cloud Computing: Deployment Models

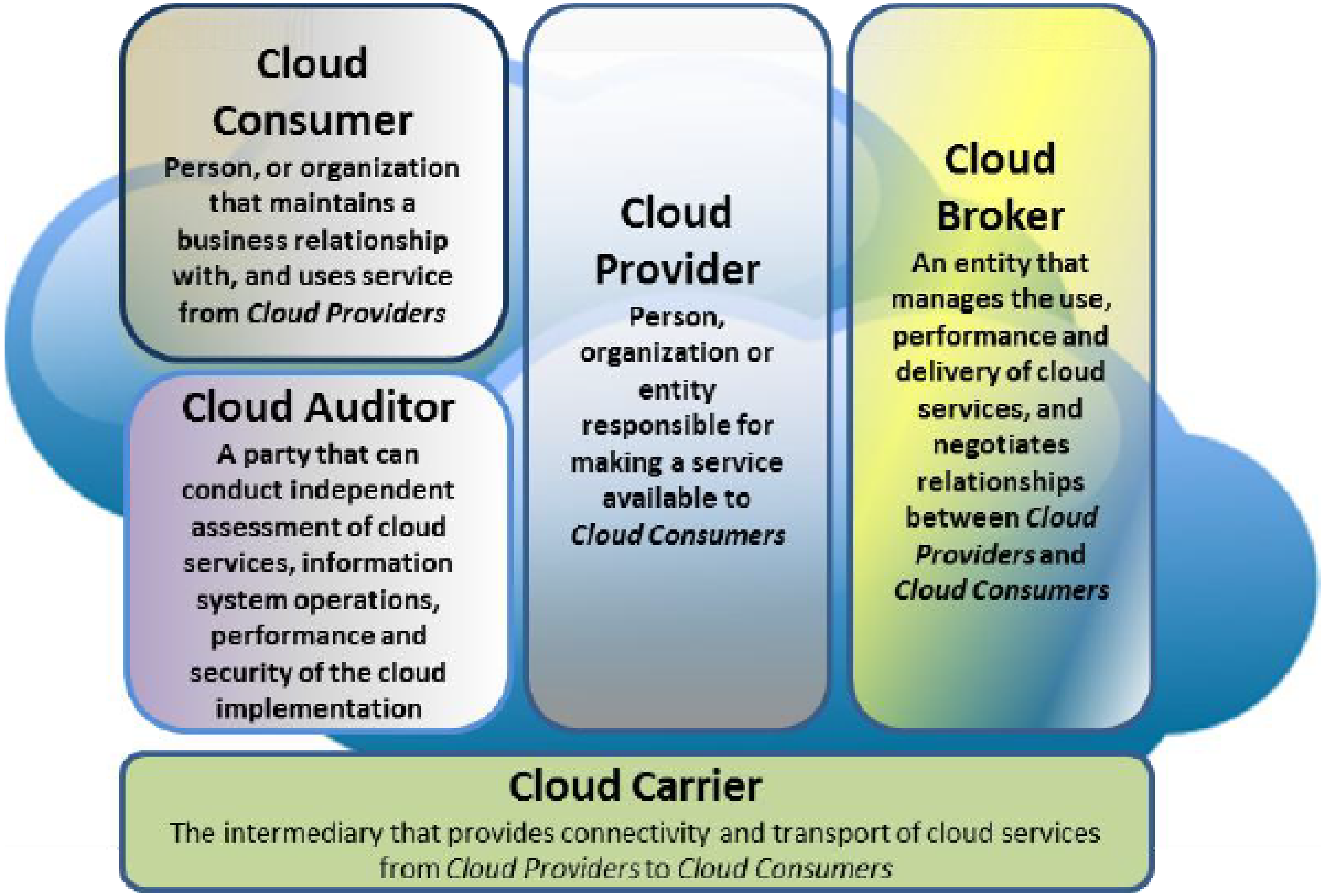
- Private Cloud: Provisioned for exclusive use by a single organisation
- Community Cloud: Provisioned for exclusive use by specific community of consumers
- Public Cloud: Provisioned for open use by the general public
- Hybrid Cloud: combination of two or more cloud infrastructures

NIST Cloud Reference Model (NIST CRM)

- High level conceptual model which is a logical extension to NIST Cloud Computing Definition
- Generic vendor neutral model
- Effective tool for discussing the requirements, structures, and operations of cloud computing
- Defines a set of actors, activities and functions that can be used in the process of developing cloud computing architectures
- Helps stakeholders to understand the overall view of roles and responsibilities in order to assess and assign risk
- Focuses on the requirements of “what” cloud services provide, not a “how to” design solution and implementation

NIST CRM: Cloud Actors

- Cloud Consumer
- Cloud Provider
- Cloud Auditor
- Cloud Broker
- Cloud Carrier



Cloud Consumer
Person, or organization that maintains a business relationship with, and uses service from *Cloud Providers*

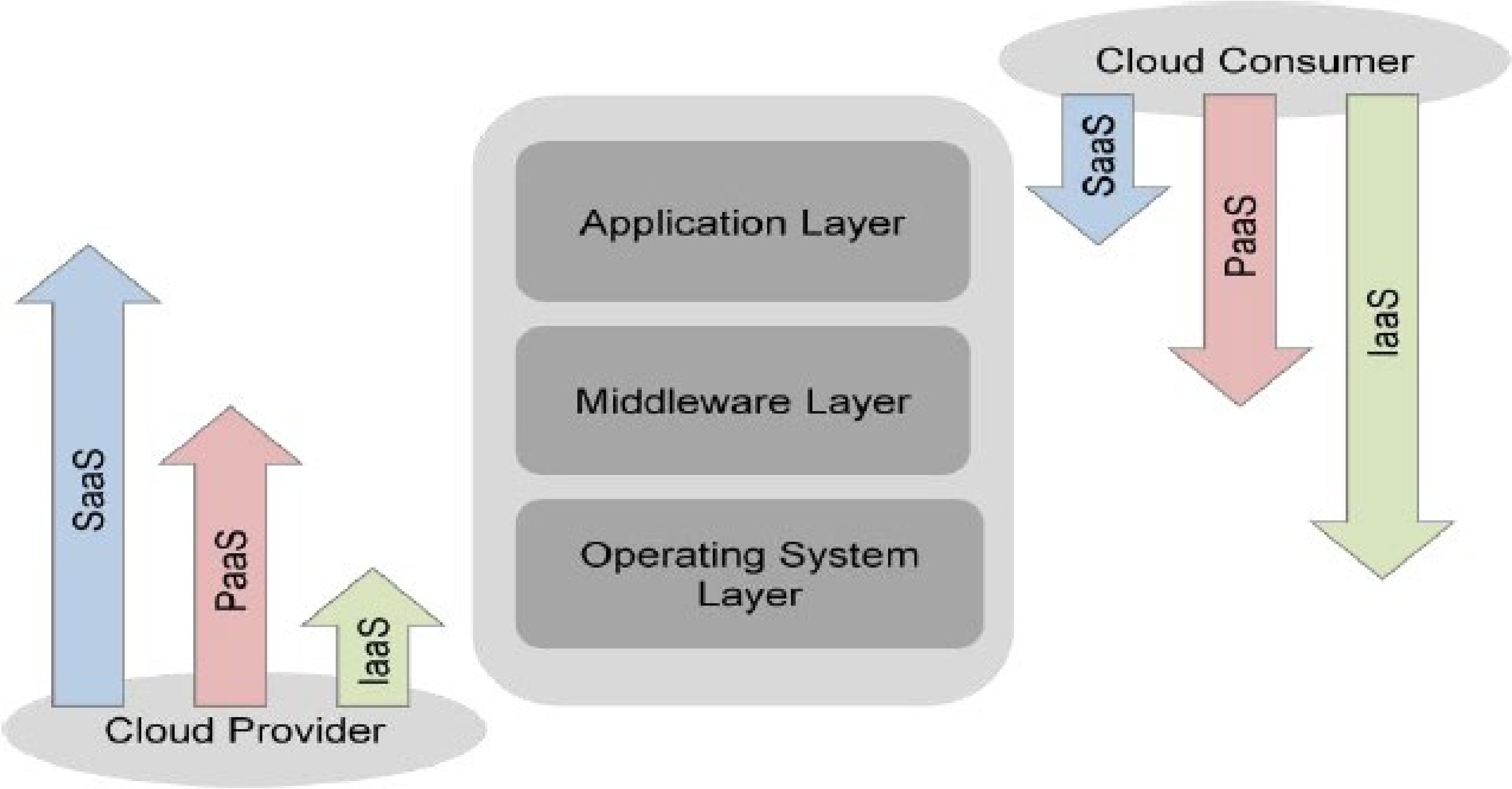
Cloud Auditor
A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation

Cloud Provider
Person, organization or entity responsible for making a service available to *Cloud Consumers*

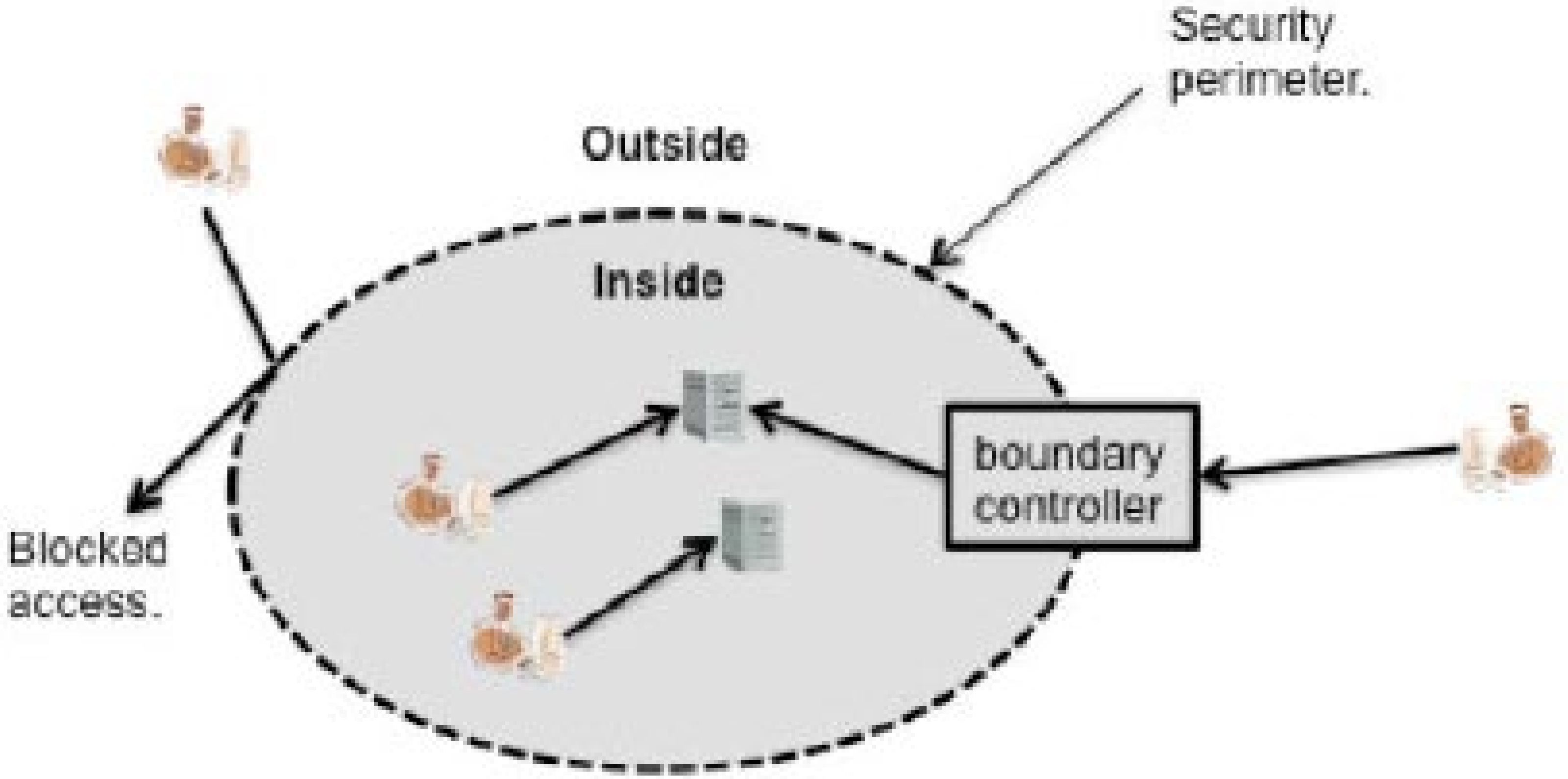
Cloud Broker
An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between *Cloud Providers* and *Cloud Consumers*

Cloud Carrier
The intermediary that provides connectivity and transport of cloud services from *Cloud Providers* to *Cloud Consumers*

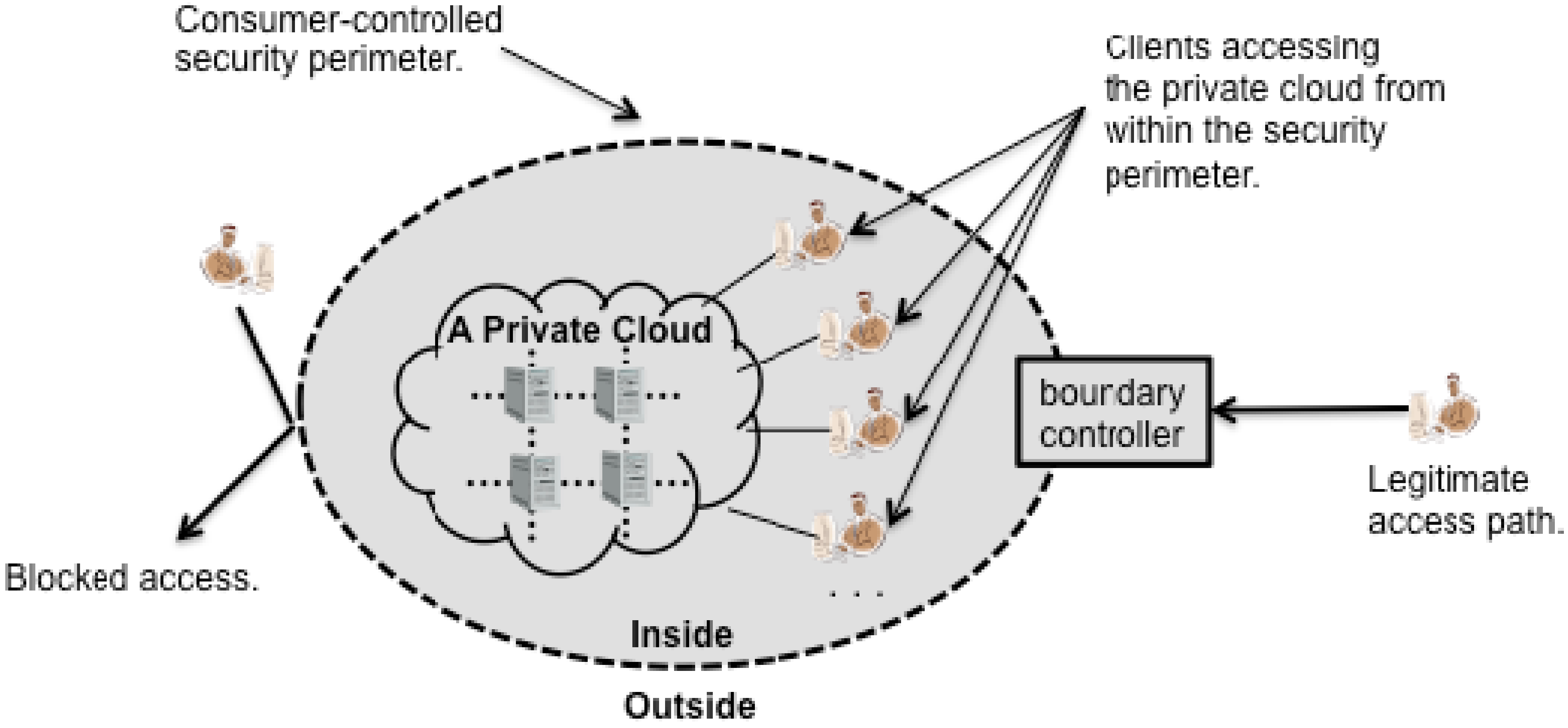
NIST CRM: Scope of control between customer and Provider



NIST CRM: Scope of control between customer and Provider



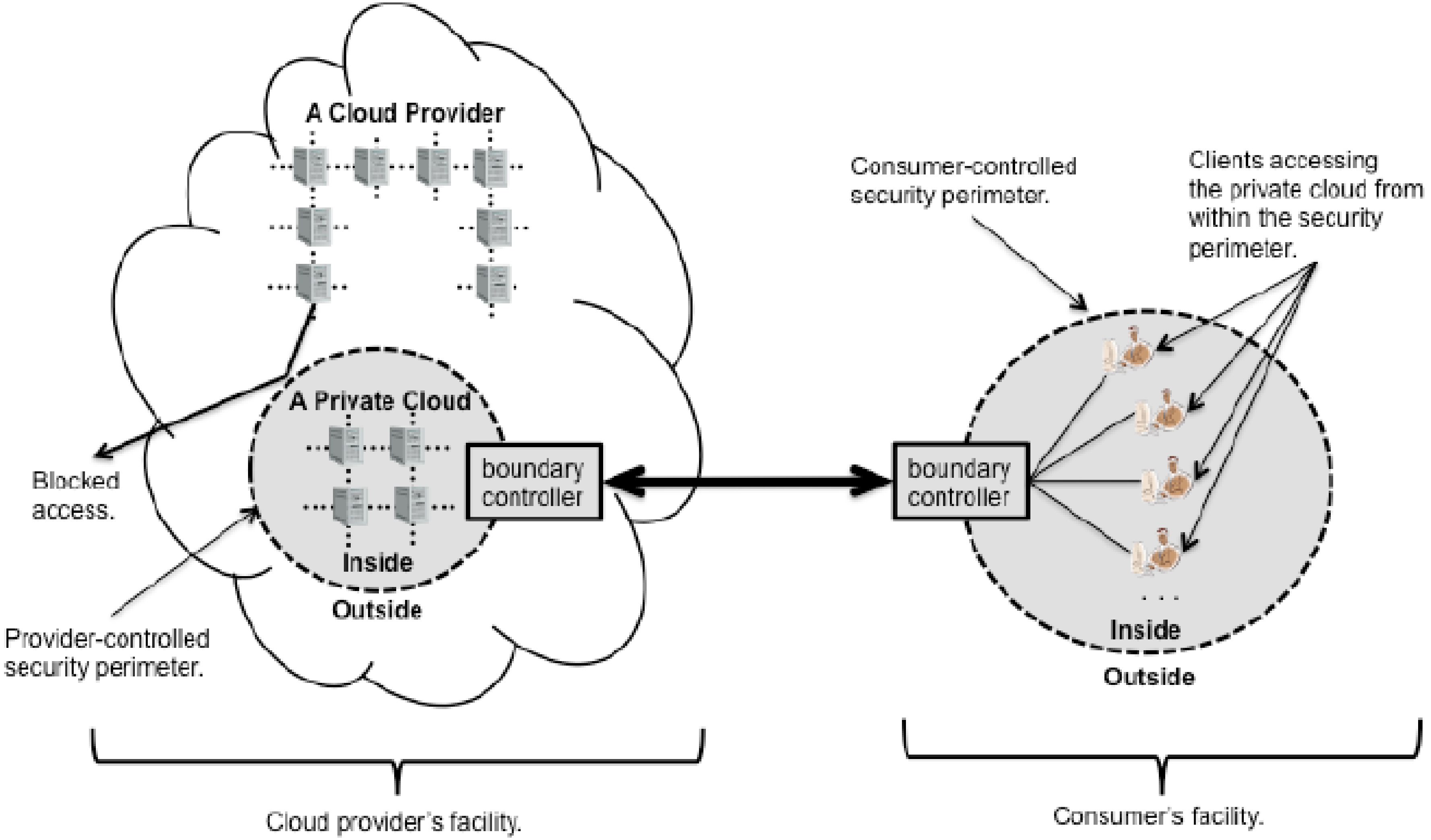
NIST CRM: Scope of control between customer and Provider- On-site Private Cloud


Consumer-controlled security perimeter.
Clients accessing the private cloud from within the security perimeter.
A Private Cloud
bourdary controller
Legitimate access path.
Blocked access.
. . .
Inside
Outside

NIST CRM: Scope of control between customer and Provider- On-site Private Cloud

- Network Dependency
- **Need additional skill for managing the private cloud**
- Workloads hidden from clients
- Data transfer and performance limitations
- Potentially strong security
- **Significant to high upfront costs to implement and migrate to cloud**
    - **New Data Centre, Converted Data Centre, Scavenged Resources**
- **Limited Resources**

NIST CRM: Scope of control between customer and Provider-Outsourced Private Cloud


A Cloud Provider
A Private Cloud
boundary controller
Blocked access.
Inside
Outside
Provider-controlled security perimeter.
Consumer-controlled security perimeter.
Clients accessing the private cloud from within the security perimeter.
boundary controller
. . .
Inside
Outside
Cloud provider's facility.
Consumer's facility.

NIST CRM: Scope of control between customer and Provider-Outsourced Private Cloud

- **Network Dependency**

- Workloads hidden from clients

- **Risks from multi-tenancy** (Depends on how separation is achieved)

- **Data transfer and performance limitations**

- Potentially strong security: Security applied at providers and consumers perimeter

- Modest costs to implement and migrate to cloud

- Extensive resources

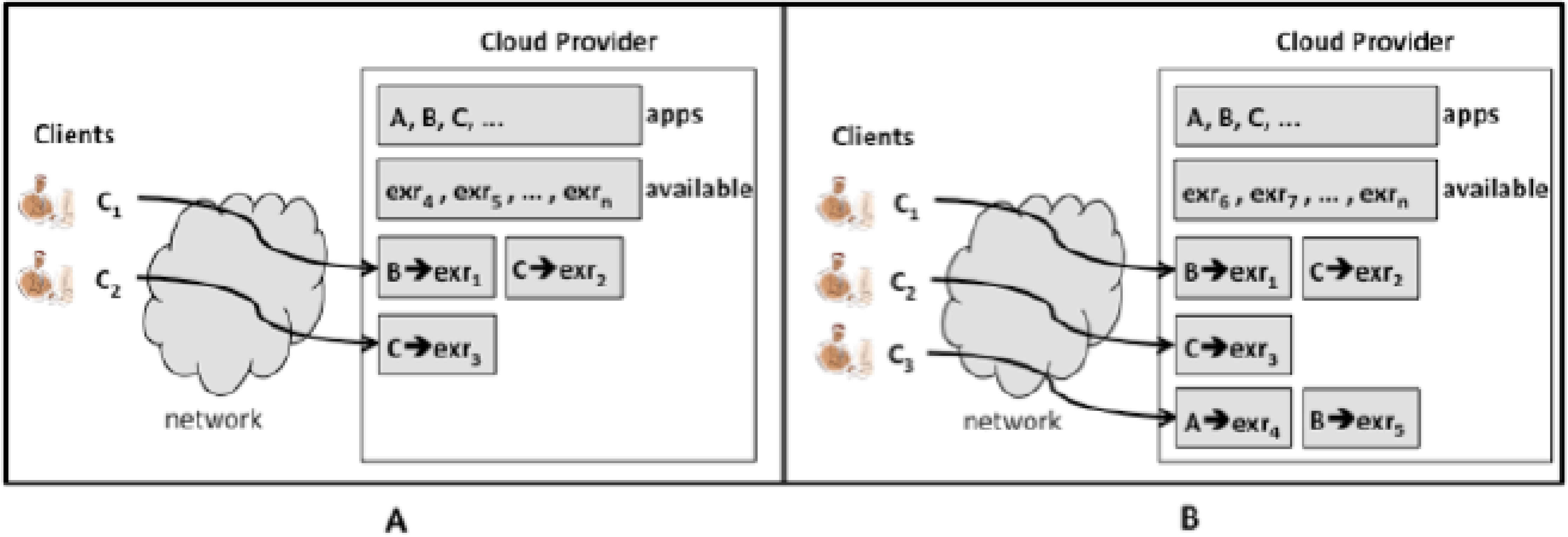
Software as a Service (SaaS) Environments

- Who are the consumers?
  - Organizations providing their users with access to typical software applications such as office productivity or email.
  - End users who directly use software applications.
  - Software application administrators who configure an application for end users.

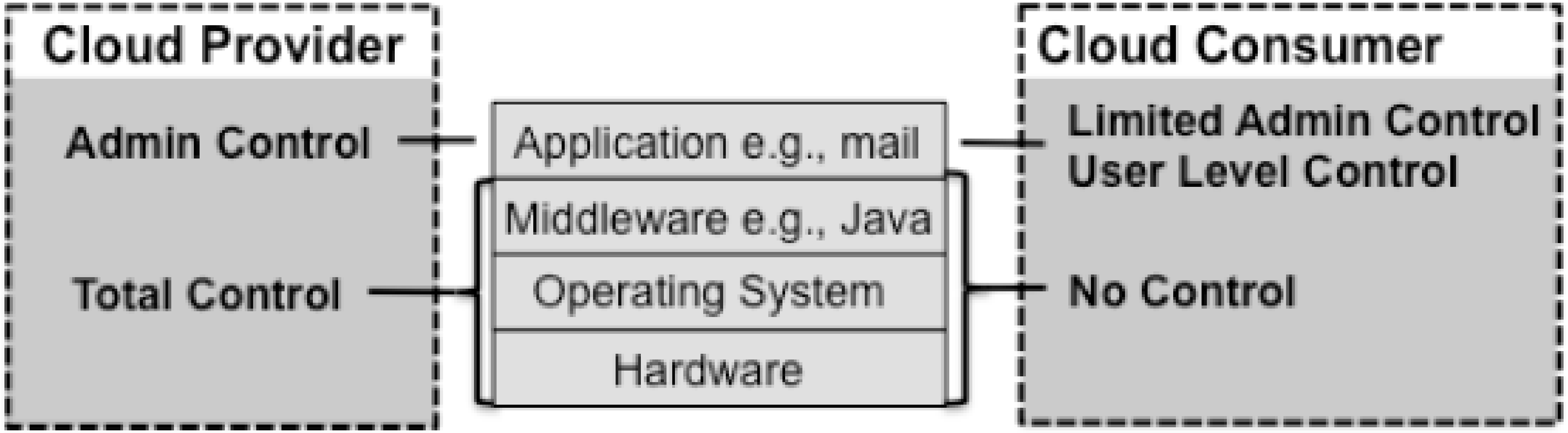
- What does a consumer get?
  - Use specific applications on demand.
  - application data management: backup and data sharing between consumers.

- How are usage fees calculated?
  - Based on different parameters: number of users, the time in use, per-execution, per-record-processed, network bandwidth consumed, and quantity/duration of data stored.

SaaS Environments: Abstract Interaction Dynamics



SaaS Environments: Scope of Control



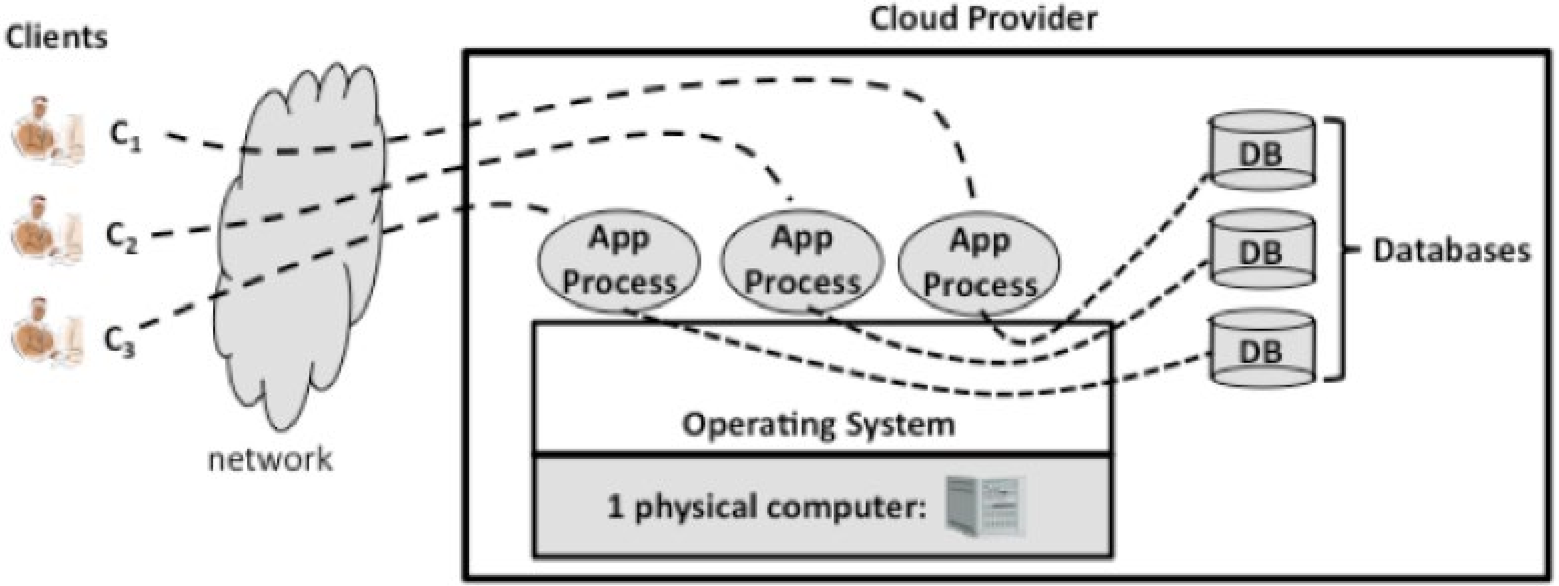
- Why limited admin control for consumer?
  - Manage application users: new staff, terminated staff, change of user roles

SaaS Environments

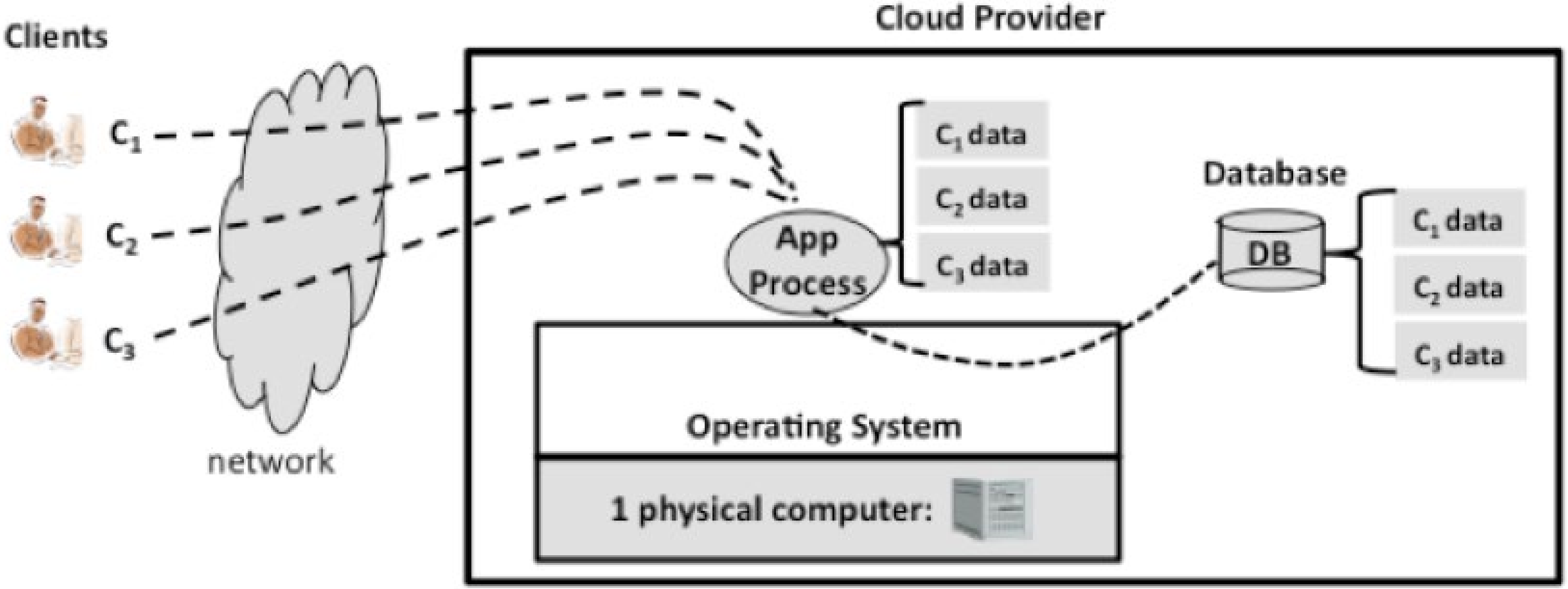
- Benefits
    - Modest software tool footprint
    - Efficient usage of software licences
    - Centralised management of data
    - Platform responsibilities managed by cloud providers
    - Savings in up-front costs

- Issues and Concerns
    - Browser based risks
    - Network dependence
    - Lack of portability between clouds
    - Isolation vs Efficiency

SaaS Environments: Isolation vs Efficiency



- Favouring Isolation



- Favouring Efficiency

SaaS Environments: Recommendations

- Data Protection
  - What mechanisms and configurations are being used?
  - Where is the data location?
  - CIA requirements for the data?

- Client Device Protection

- Encryption

- Secure Data Deletion

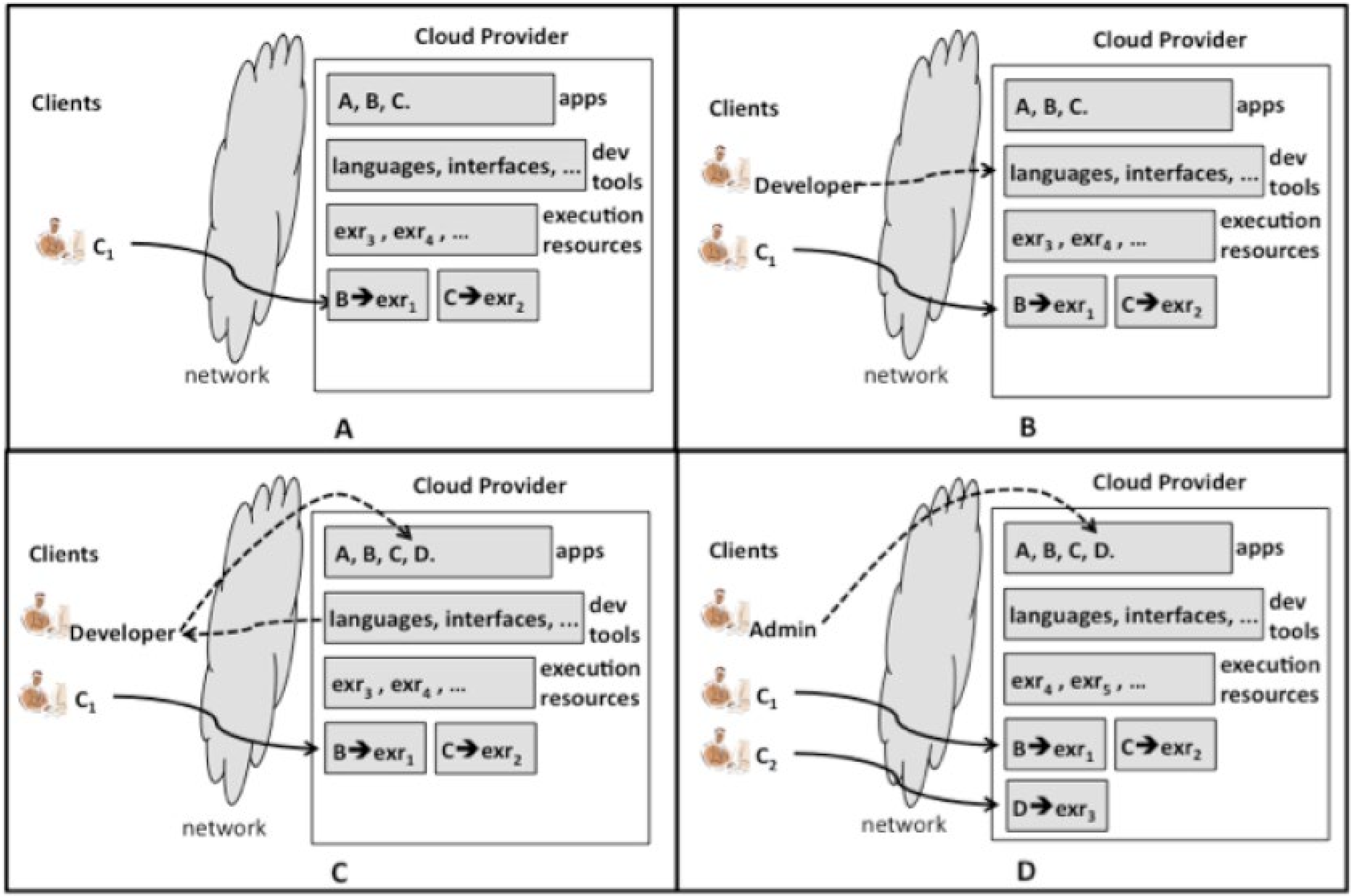
Platform as a Service(PaaS) Environments

- Who are the consumers?
  - Application developers to design and implement an application's software.
  - Application testers to run applications in various testing environments.
  - Application deployers who publish applications into the cloud and manage possible conflicts arising from multiple versions of an application.
  - Application administrators to configure, tune, and monitor application performance.
  - Application end users.

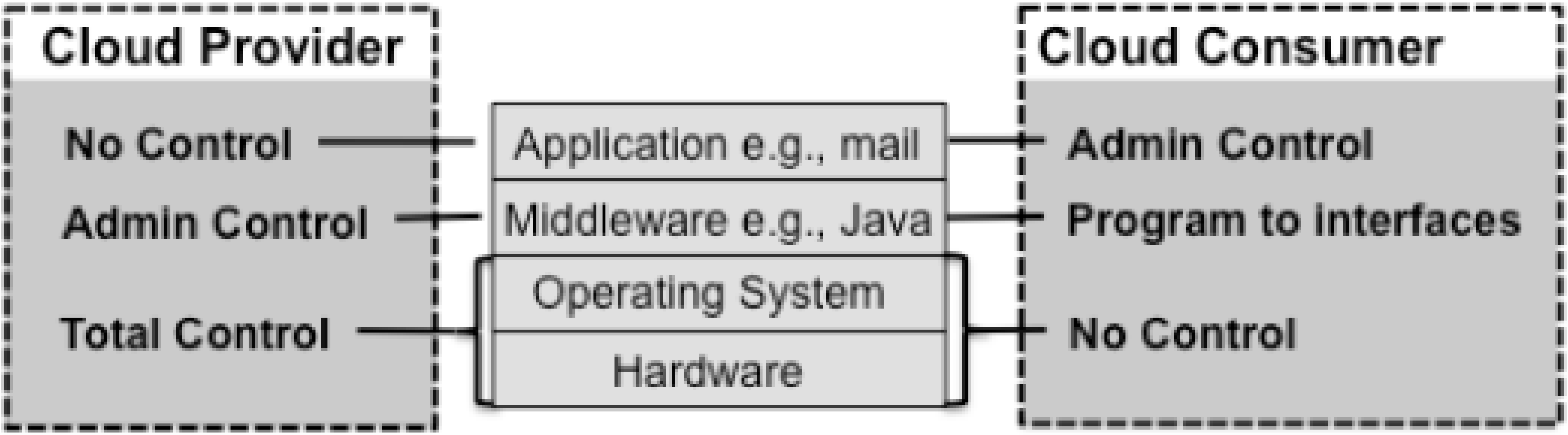
- What does a consumer get?
  - Usage of PaaS cloud provider's tools and execution resources to develop, test, deploy and administer applications

- How are usage fees calculated?
  - Based on different parameters: number of consumers, consumers types, storage, processing, or network resources consumed by the platform, requests serviced, and the time the platform is in use

PaaS Environments: Abstract Interaction Dynamics



PaaS Environments: Scope of Control



PaaS Environments

- Benefits
  - Modest software tool footprint
  - Efficient usage of software licences
  - Centralised management of data
  - Platform issues managed by cloud providers
  - Savings in up-front costs
  - Facilitated scalable application development and deployment

- Issues and Concerns
  - Browser based risks, Network dependence, Isolation vs Efficiency
  - Lack of portability between PaaS clouds
  - Security engineering of PaaS applications

PaaS Environments: Recommendations

- Generic Interfaces: to support portability and interoperability
- Standard language, tools and protocols
- Data Protection
- Application Framework: support for tools for mitigating security vulnerabilities
- Component Testing
- Security: ensure PaaS application can run in secure manner, can integrate with enterprise framework
- Data Deletion

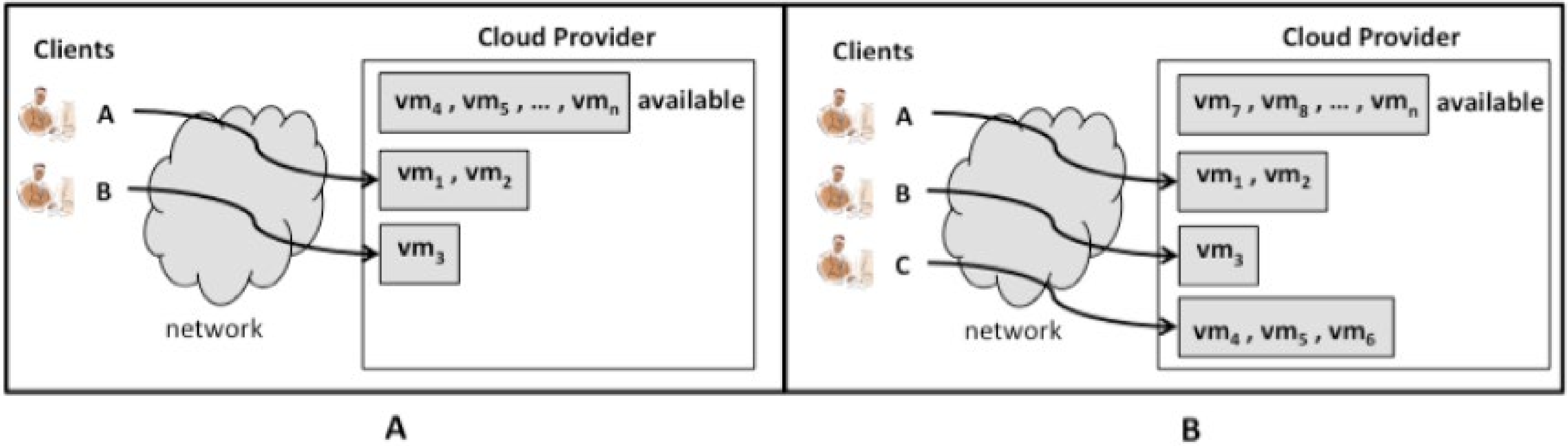
Infrastructure as a Service(IaaS) Environments

- Who are the consumers?
    - System Administrators

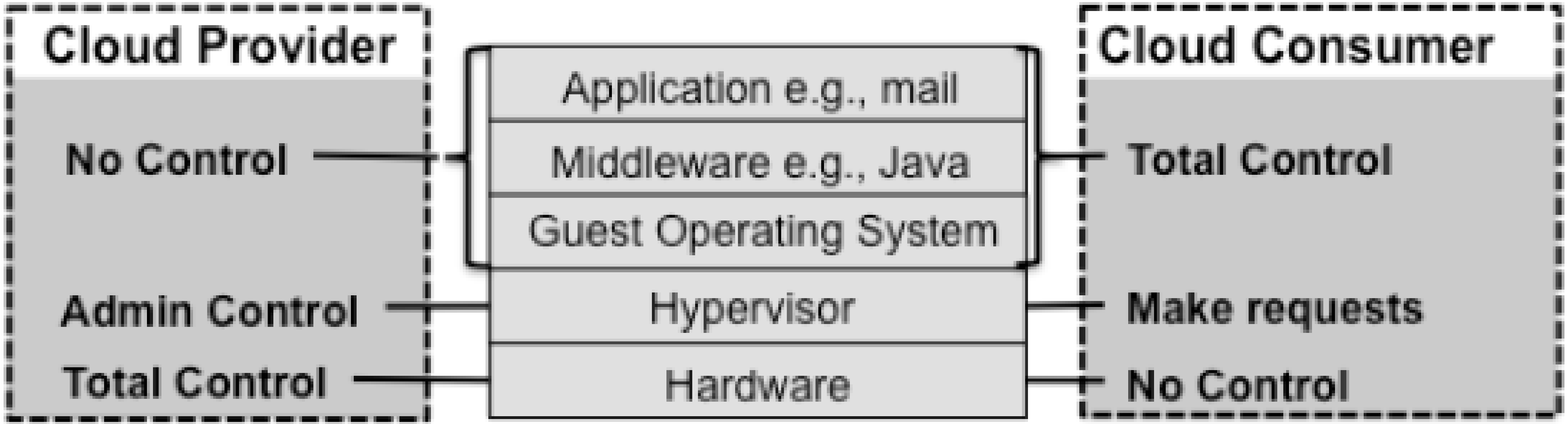
- What does a consumer get?
    - Access to virtual machines, network accessible storage, network infrastructure components

- How are usage fees calculated?
    - Based on different parameters: Resource allocation such as CPU, memory, storage, network bandwidth and the time in use

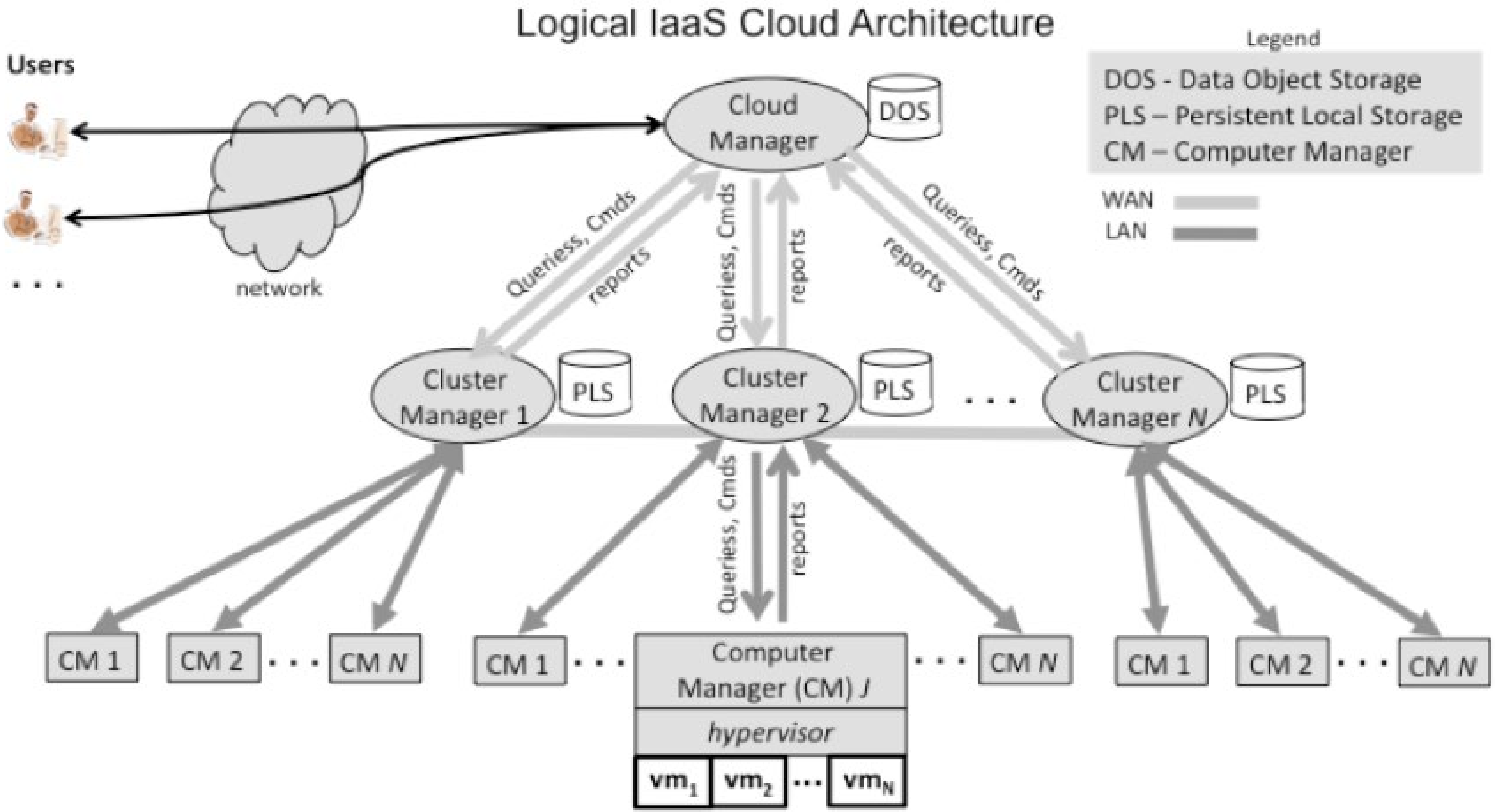
IaaS Environments: Abstract Interaction Dynamics



IaaS Environments: Scope of Control



IaaS Environments: Operational View



IaaS Environments

- Benefits
  - Savings in up-front cost
  - Full control of the virtual machine
  - Flexible and efficient renting of computing resources
  - Portable and interoperable

- Issues and Concerns
  - Browser based risks, Network dependence, Isolation vs Efficiency
  - Virtual machine sprawl
  - Robustness of VM-level isolation
  - Features for dynamic network configuration for providing isolation

IaaS Environments: Recommendations

- Multi-tenancy: Protection of Virtual Machines
- Data Protection
- Secure Data Deletion
- Admin Access to limited set of trained users
- Plan for VM migration