5.1 Cloud Storage
Storage-as-a-Service (StaaS)

Cloud Storage

- Cloud storage is a cloud computing model that stores data on the Internet through a cloud computing provider who manages and operates **data storage as a service**.
- It’s delivered **on demand** with **just-in-time capacity and costs**, and eliminates buying and managing your own data storage infrastructure.
- This gives you **agility, global scale and durability**, with **“anytime, anywhere”** data access.

Cloud Storage

- Cloud storage is a model of computer data storage in which the digital data is stored in logical pools said to be on “the Cloud”.
- The physical storage spans multiple servers (sometimes in multiple locations), and the physical environment is typically owned and managed by a hosting company.

Cloud Storage

- These cloud storage providers are responsible for keeping the data **available and accessible**, and the physical environment **secured, protected, and running**.
- People and organizations buy or lease storage capacity from the providers to store user, organization, or application data.

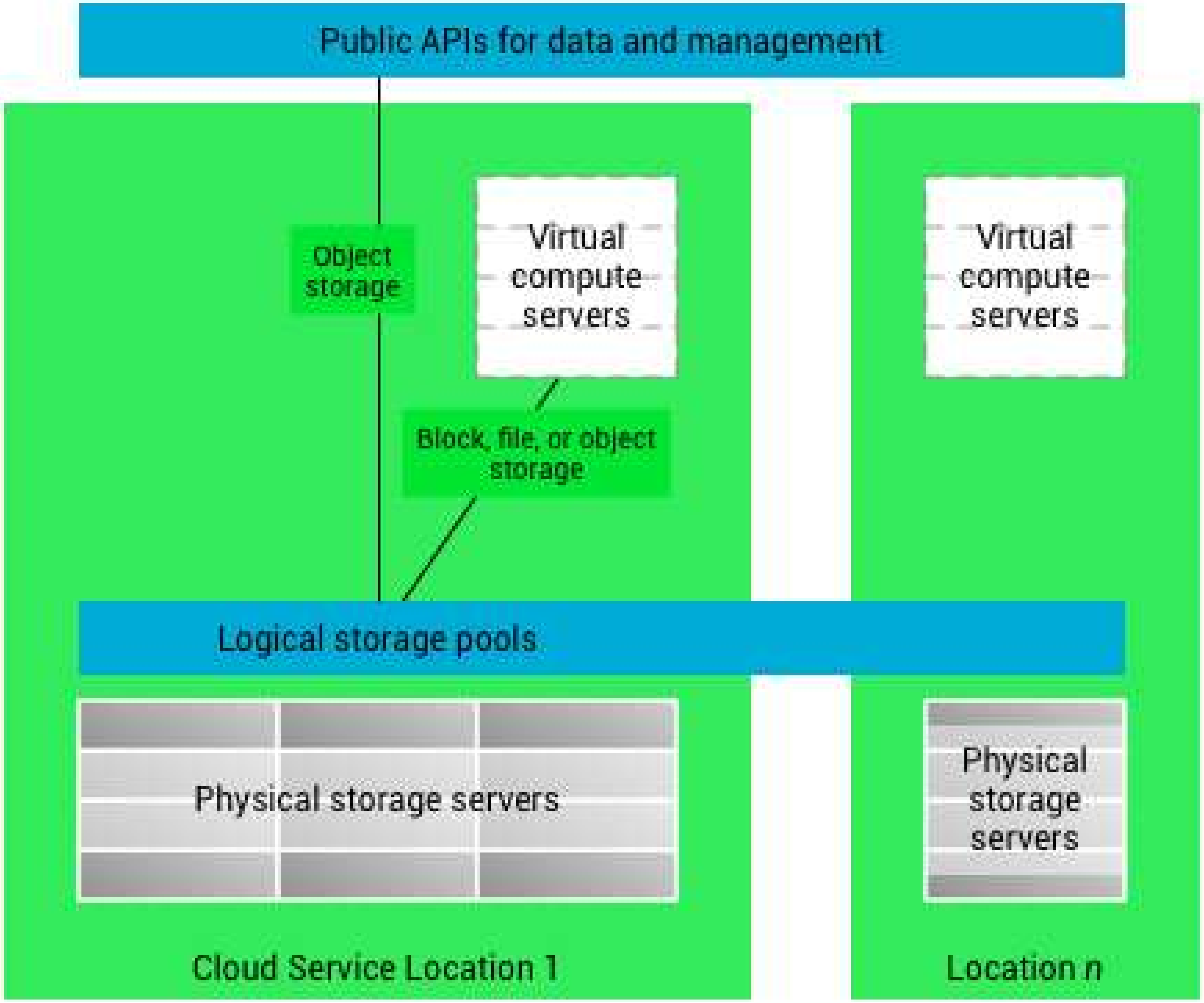
Durability, Availability and Security

- Durability
  - Data should be redundantly stored, ideally across multiple facilities and multiple devices in each facility.
  - Natural disasters, human error, or mechanical faults should not result in data loss.
- Availability
  - All data should be available when needed, but there is a difference between production data and archives.
  - The ideal cloud storage will deliver the right balance of retrieval times and cost.
- Security
  - All data is ideally encrypted, both at rest and in transit.
  - Permissions and access controls should work just as well in the cloud as they do for on premises storage.

Cloud Storage

- Cloud storage services may be accessed through a
  - Colocated cloud computing service
  - A web service application programming interface (API)
  - Applications that use the API
    - Cloud desktop storage
    - A cloud storage gateway
    - Web-based content management systems

High level cloud storage architecture



Cloud Storage

- There are three types of cloud storage:
  - A hosted object storage service
  - File storage
  - Block storage
- Each of these cloud storage types offer their own unique advantages.

File

- File-based storage is a simple, straightforward approach to data storage.
- File-based storage works well for organizing data in a hierarchical, simple, and accessible platform.
- The key to successful file-based storage is a documented nomenclature (naming) strategy and regular clean-up.
- Also known as shared file system, file storage is good for file sharing, archiving, and data protection.
- The architecture has its drawbacks, though; unlimited scalability means an unlimited number of files to comb through when searching for something you need.

Block

- Primarily deployed in SAN (storage area network) architectures, block storage references the individual block of raw storage that is then filled with files of equal size.
- Block storage allows a server-based operating system to use the blocks as individual hard drives.
- Although it may be a little less straightforward, the system's management of metadata enables more efficient storage, making block storage a high-performing system.
- Block storage is typically used for databases, email servers, and virtual machines.

Object

- Object-based storage is deployed to solve for unstructured data (videos, photos, audio, collaborative files, etc.).
- Basically, when data is big or shared, object storage works by storing data in containers or “buckets”.
- Collaborative software utilizes object storage because it works across multiple levels, from the device level to the interface.

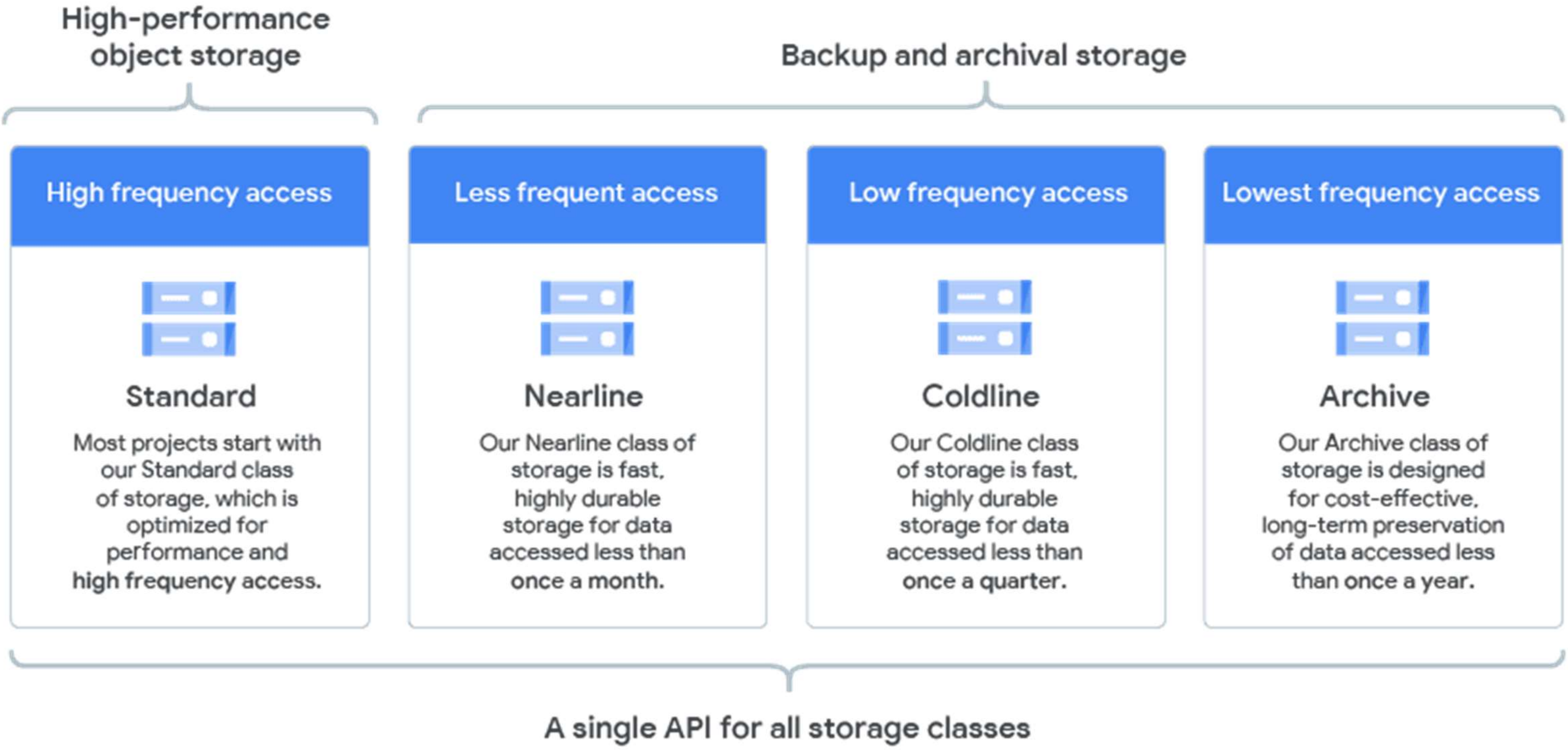
Object

- With the explosive growth of data highlighted in the news practically every day, it makes sense a new kind of storage that allows for greater flexibility and scalability would flourish.
- Object-storage’s reliance on REST APIs enables access to objects via HTTP, creating a greater ease of access for authentication, permissions, and properties.

Types of Cloud Data Storage

- Object Storage
  - Applications developed in the cloud often take advantage of object storage's vast scalability and metadata characteristics.
- File Storage
  - Some applications need to access shared files and require a file system.
  - This type of storage is often supported with a Network Attached Storage (NAS) server.
- Block Storage
  - Other enterprise applications like databases or ERP systems often require dedicated, low latency storage for each host.
  - This is analogous to direct-attached storage (DAS) or a Storage Area Network (SAN).

Cloud Storage Classes



High-performance object storage

Backup and archival storage

High frequency access

Standard

Most projects start with our Standard class of storage, which is optimized for performance and high frequency access.

Less frequent access

Nearline

Our Nearline class of storage is fast, highly durable storage for data accessed less than once a month.

Low frequency access

Coldline

Our Coldline class of storage is fast, highly durable storage for data accessed less than once a quarter.

Lowest frequency access

Archive

Our Archive class of storage is designed for cost-effective, long-term preservation of data accessed less than once a year.

A single API for all storage classes

Cloud Storage – Usages

- Backup and Recovery
  - Backup and recovery is a critical part of ensuring data is protected and accessible, but keeping up with increasing capacity requirements can be a constant challenge.
  - Cloud storage brings low cost, high durability, and extreme scale to backup and recovery solutions.

Cloud Storage – Usages

- Software Test and Development
  - Software test and development environments often requires separate, independent, and duplicate storage environments to be built out, managed, and decommissioned.
  - In addition to the time required, the up-front capital costs required can be extensive.

Cloud Storage – Usages

- Compliance
  - Easily deploy and enforce compliance controls on individual data vaults
- Media content storage and delivery
- Backups and archives
- Integrated repository for analytics and machine learning

Benefits of Cloud Storage

- Total Cost of Ownership
  - With cloud storage, there is no hardware to purchase, storage to provision, or capital being used for "someday" scenarios.
  - You can add or remove capacity on demand, quickly change performance and retention characteristics, and only pay for storage that you actually use.
  - Less frequently accessed data can even be automatically moved to lower cost tiers in accordance with auditable rules, driving economies of scale.

Benefits of Cloud Storage

- Time to Deployment
  - When development teams are ready to execute, infrastructure should never slow them down.
  - Cloud storage allows IT to quickly deliver the exact amount of storage needed, right when it's needed.
  - This allows IT to focus on solving complex application problems instead of having to manage storage systems.

Benefits of Cloud Storage

- Information Management
  - Centralizing storage in the cloud creates a tremendous leverage point for new use cases.
  - By using cloud storage lifecycle management policies, you can perform powerful information management tasks including automated tiering or locking down data in support of compliance requirements.

Amazon

- Amazon Simple Storage Service (Amazon S3)
  - A service that provides scalable and highly durable object storage in the cloud.
- Amazon Glacier
  - A service that provides low-cost highly durable archive storage in the cloud.
- Amazon Elastic File System(Amazon EFS)
  - A service that provides scalable network file storage for Amazon EC2 instances.

Amazon

- Amazon Elastic Block Store (Amazon EBS)
  - A service that provides block storage volumes for Amazon EC2 instances.
- Amazon EC2 Instance Storage
  - Temporary block storage volumes for Amazon EC2 instances.
- AWS Storage Gateway
  - An on-premises storage appliance that integrates with cloud storage.

Amazon

- AWS Snowball
  - A service that transports large amounts of data to and from the cloud.
- Amazon CloudFront
  - A service that provides a global content delivery network (CDN).

Amazon Web Services

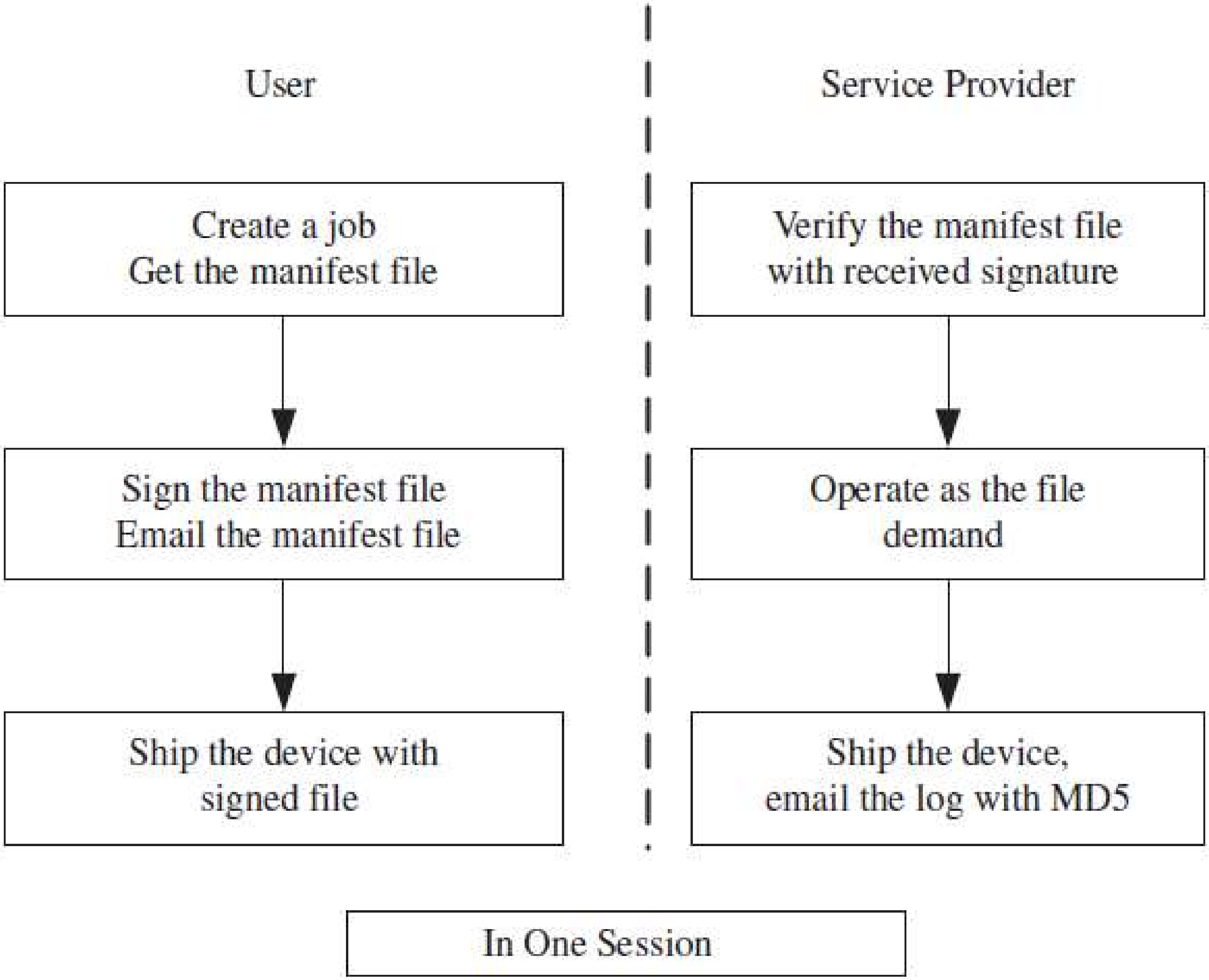


FIGURE 8.2. AWS data processing procedure.

Microsoft Azure

- There are three basic data items: blobs (up to 50 GB), tables, and queues (<8k)

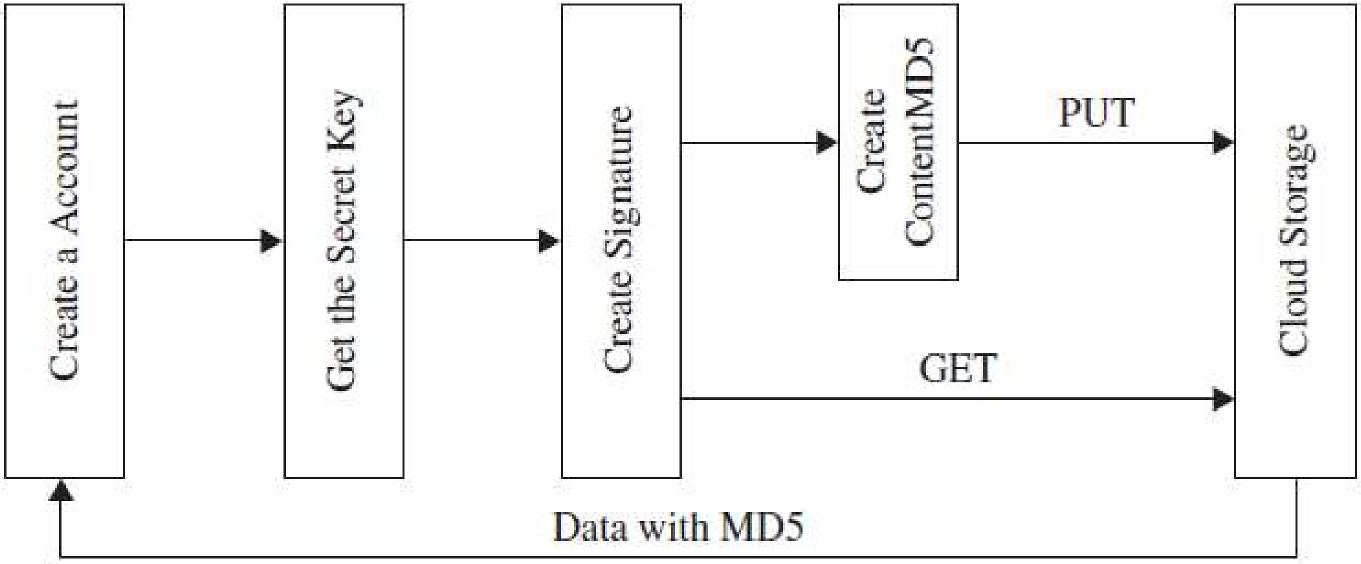


FIGURE 8.3. Security data access procedure.

Google App Engine

- The SDC constructs an encrypted connection between the data source and Google Apps.

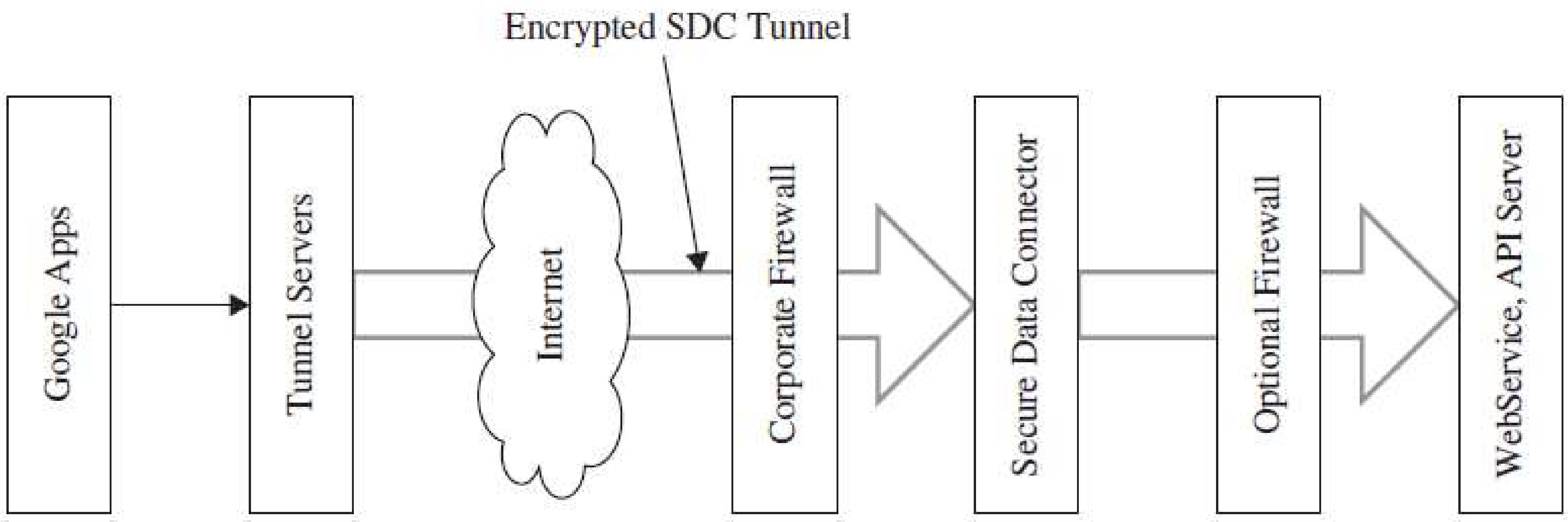


FIGURE 8.5. Illustration of Google SDC working flow.

Examples

- Object storage services that can be hosted and deployed with cloud storage characteristics include
  - Amazon S3,
  - Oracle Cloud Storage and
  - Microsoft Azure Storage
- Object storage software like Openstack Swift,
- Object storage systems like EMC Atmos, EMC ECS and Hitachi Content Platform
- Distributed storage research projects like OceanStore and VISION Cloud

5.2 Data Security in the Cloud

Data Security in the Cloud

- **Most important resource** in the cloud is the **user data**.
- It is painful to replace data if **lost or corrupted**.

Threats to data stored in cloud

- Data Availability
  - A software or hardware fault or data integrity problem or data storage unit impact entire environment.
  - Data integrity and availability are **critical** for the cloud to function.

Threats to data stored in cloud

- Data Performance
  - Data is located at various data centre, **far** from the user.
  - Higher distance induce **latency**.
  - **Low performance** with synchronous write, mirroring, and parallel read and write operations.
  - Provider must introduce **caching** techniques and pre-emptive read-ahead.

Threats to data stored in cloud

- Price
  - Storage space and bandwidth to access the data must be **low**.
- Flexibility
  - In a multi-tenant cloud, some tenant applications or activity causes **high utilization**.
  - Which impacts other user groups.
  - Need to adjust storage access speed to meet **load requirement**.

Threats to data stored in cloud

- Underlying Complexity
  - Storage hardware can be **heterogeneous**.
  - But it must be presented as a simple storage device and as a virtual storage pool to the end user.

Threats to data stored in cloud

- Data Security
  - The data must be **encrypted**.
  - Kept **safe** with a highly-monitored and regulated access.
- Data Integrity
  - With ease of access by varied user types, it is critical to **manage data integrity**.

Threats to data stored in cloud

- It is important for the cloud provider to understand the challenges and build in measures to resolve these issues because of all the data related problems.

Challenges with Cloud Data

Challenges with Data Redundancy

- **Copies of data** stored at various **locations** and **replicated in synchronous or asynchronous mode**.
- The system must be aware of **data location**, **latency**, user **workload and activity** such as backup, report generation, application testing etc.
- Following requirements must be met:
  - **Different strategies** must be setup **to improve replication and data access**.

Challenges with Data Redundancy

- **Configure load balancing** of incoming data request so that users have ready access to geographically closest.
- **Data consistency** must be **maintained** despite of wide distribution of replicated data source.
- Each data set must have **internal redundancy**, which enabled the system to **rebuild the entire data set** even if some components are temporarily damaged, available, powered off, or inaccessible due to connectivity problems.

Challenges with Disaster Recovery

- DR is one of the important criteria when **evaluating cloud providers**.
- DR with cloud computing has several benefits such as cost effectiveness, ease of implementation, scalability, quick provisioning.
- Challenges:
  - **Initial data copy** for existing data – for large data set it takes time.

Challenges with Disaster Recovery

- Limited or no support for some **old** operating systems like Solaris, HPUX, AIX.
- Insufficient bandwidth – **incremental update** instead of full at once.
- **Financial consideration** – small or mid size data DR Vs vast amount of data.
- Supplier issues – providers do not take the effort and time to understand the **customer specific need**.

Challenges with Data Backup

- For downloading data from cloud, **pay for the bandwidth**.
- Requires safe place to store the data and **regularly check media integrity**.
- **Harden the security** to protect from hackers and malwares.
- Data recovery from cloud is tough, slow, and prone to **transfer interruptions**.

Challenges with Data Replication

- Creating copies of user data and applications to protect from primary site failure.
- Two types of replications:
  - Synchronous replication
    - Always in **sync** with primary site.
    - Distance within **100 kms** due to latency otherwise impact the performance.

Challenges with Data Replication

- Asynchronous replication
  - Replicated data **lags** behind the primary data by a time period of **10 minutes to a few hours**.
  - This is common in cloud, but it impact performance.

Challenges with Data Residency or Location

- Location of data can pose a compliance or **legal problem**.
- For your data you need to know legal requirements you must comply with.
- Certain gov. restrict access of data according to country laws.
- For certain data you must keep the data within the region or country.

Challenges with Data Reliability

- Service reliability in cloud is concern because of:
  - **Heterogeneous hardware and software components**
  - **Connectivity over multi-vendor WAN**
  - **Massive user base sharing** the same resource pool
  - **Ease of access** for users
- The cloud providers must implement measures to guarantee service uptime and an acceptable performance in the SLA.
- Reliability, hard to analyze due to varying cloud conditions.

Challenges with Data Fragmentation

- **Numerous users** simultaneously working on different datasets in the cloud.
- User **data is split or fragmented** into many pieces and stored at different locations.
- As it is fragmented, **overhead of keeping tracks** of different part of data, file location, lead to inefficiency and degrades read-write performance.
- Provider must have to **use data management technique** to reduce user-data fragmentation.

Challenges with Data Integration

- Content distribution
  - Content of a file reside in **different datacenters** and various storage **subsystem** in same datacenter
- Exchange of data
  - Data interact with application which resides on **other public/private clouds**
  - This poses challenge in **compatible** data format and application interface

Challenges with Data Integration

- Speed of change
  - **Continuous change and keeping track** of the data poses a tough challenge for integration.
- Distributed control
  - **Control** over data is shared between **consumer and provider** increases challenge
- Connectivity
  - Accessed only when user and service are **online**.
  - Integration required **bandwidth**, **amount** of transaction and **work at hand.**

Challenges with Data Transformation

- In cloud various application use the same data.
- Different data formats used by different cloud application – need to convert – transformation – so that used by several applications.
- Challenges:
  - – Run-time issues
    - Run-time environments in the cloud may not be compatible with new transformed data.

Challenges with Data Transformation

- Redundancy issues
  - Transformation creates multiple copies.
  - Keeping track of location and changes in the various set are a challenge.
- Implementation issues
  - Transformation can be expensive.
  - It must be automated.

Challenges with Data Migration

- After taking decision to move to cloud you may need to migrate user login, profile, data and corporate information to cloud.
- Cloud provider must have templates and procedures to conveniently migrate in-house data to public cloud.

Challenges with Data Migration

- Challenges:
  - Liability concerns
    - Provider have a max data value for damage claims in SLA.
    - It is much less than the data value or efforts needed to fix data loss or integrity problem.
  - Compliance concerns
    - Provider must comply with various regulatory and legal requirement
  - Connectivity concerns
    - Connectivity providers are outside the control of the consumer or the provider

Challenges with Data Security

- Security risks: Due to inherent **multi-tenancy** and ease of access within a cloud, the data is subjected to various security risks.
  - Snooping
    - The access of each tenant should be limited to his/her own data.
    - Any mechanism to **connect to another tenant's data**, such as mounts, shares and symbolic links, should be limited to their own data set.

Challenges with Data Security

- Unauthorized discovery
  - Data should be **invisible** to all tenants except the owner.
- Spoofing
  - **Implement authentication mechanism** to make sure that no cloud tenant can assume the identity of another tenant.

Challenges with Data Security

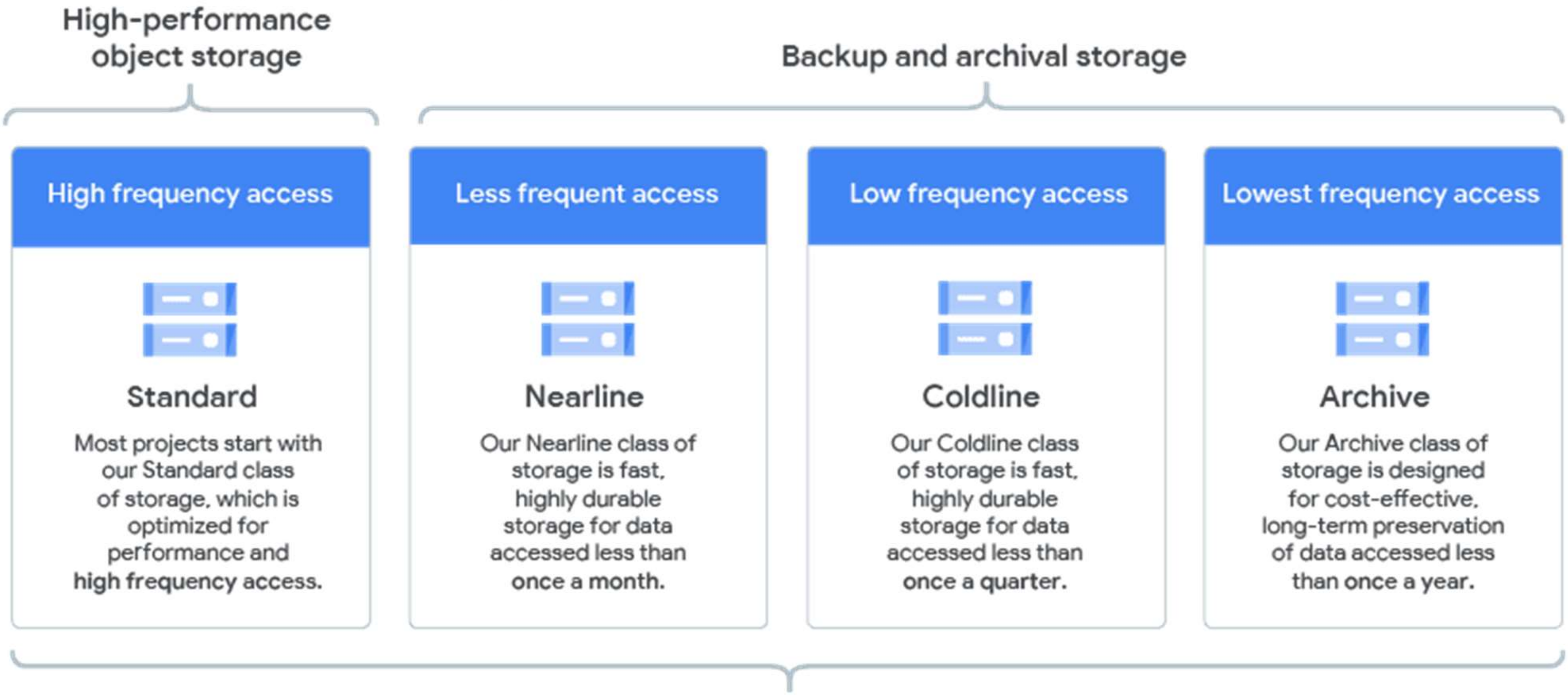
- Accidental or malicious deletion
  - No user should be able to delete the data belonging to another tenant
- Denial-of-Service attacks
  - Other cloud user should not able to do DoS attacks on the shared storage volumes.

Challenges with Data Security

- Quality of service
  - Concern after security is QoS.
  - Apprehensions(worries) about long response time, WAN-Induced latency, inhibit many potential customers from accepting cloud services.
  - To improve performance cloud provider:
    - Implement and offer storage tiers.
    - Premium tiers with higher cost can be used for real-time computation and provide better response.

Challenges with Data Security

- Lower storage tiers can be used just for backups and archiving.
- The cloud must assign priority such that lower storage tiers do not impede(obstruct) the performance of the higher storage tiers.



Standard

Most projects start with our Standard class of storage, which is optimized for performance and high frequency access.

Nearline

Our Nearline class of storage is fast, highly durable storage for data accessed less than once a month.

Coldline

Our Coldline class of storage is fast, highly durable storage for data accessed less than once a quarter.

Archive

Our Archive class of storage is designed for cost-effective, long-term preservation of data accessed less than once a year.

Challenges with Data Security

- Data availability
  - 3rd concern after security and quality of service is data availability.
  - Chances of unexpected downtime.
  - Several outage despite of redundancy and replication.
  - 100% uptime: No guarantees

Data Confidentiality and Encryption

- According to Wikipedia,
  - In information security, confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes."

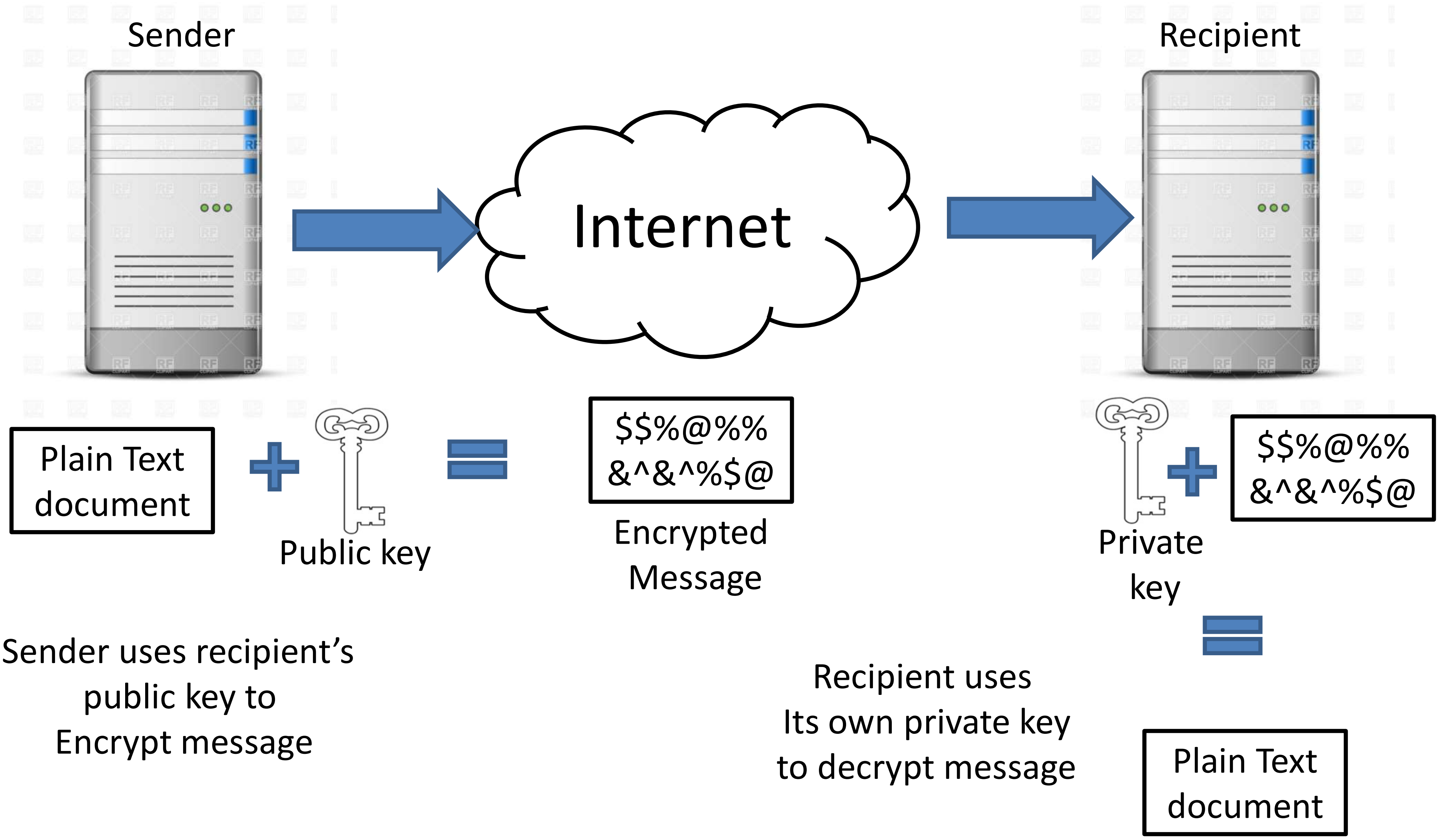
Data Confidentiality and Encryption

- A common way to achieve data confidentiality is to encrypt data.

- Encryption algorithm + Key

- Two common ways to encryption
  - Symmetric Encryption
  - Asymmetric Encryption

Asymmetric Encryption



Sender

Recipient

Internet

Plain Text document

Public key

$$%@%%
&^&^%$@

Encrypted Message

Private key

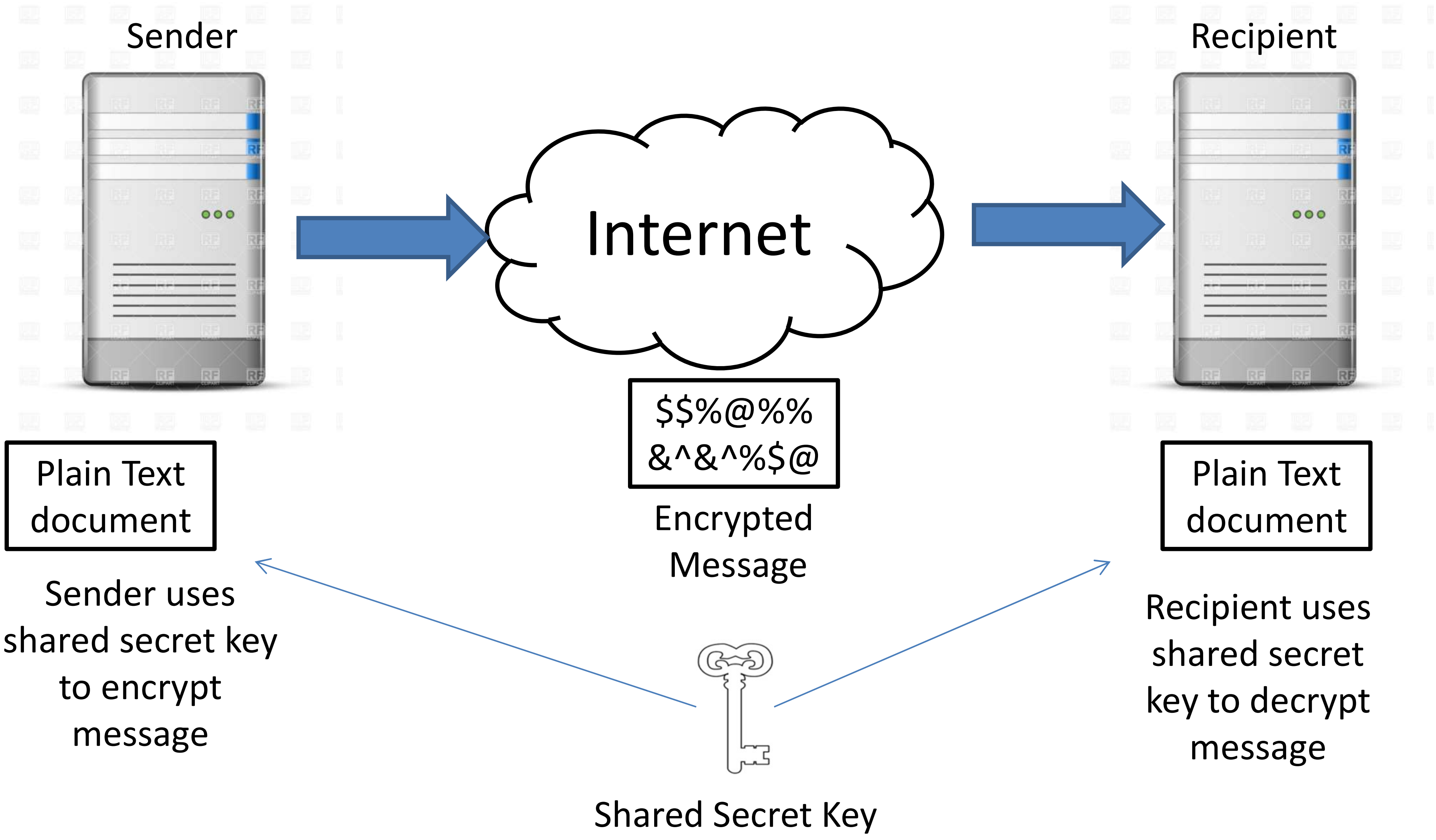
$$%@%%
&^&^%$@

Plain Text document

Sender uses recipient’s public key to Encrypt message

Recipient uses Its own private key to decrypt message

Symmetric Encryption



Sender

Internet

Recipient

Plain Text document

$$%@%% &^&^%$@

Encrypted Message

Plain Text document

Sender uses shared secret key to encrypt message

Recipient uses shared secret key to decrypt message

Shared Secret Key

Data Confidentiality and Encryption

- Key Protection
  - The sender uses the recipient’s public key to encrypt the shared key.
  - The encrypted shared key is sent to the recipient.
  - The recipient uses its own private key to decrypt the key.

Data Confidentiality and Encryption

- Algorithms used for cloud data encryption
  - RSA (1977)
    - Developed by three mathematician Ron Rivest, Adi Shamir and Len Adleman.
    - Product of two large prime numbers used to form required keys
    - Widely used, especially for digital signature
  - DES/3DES (1977)
    - Data Encryption Standard developed by US government.
    - New version 3DES encrypts data three times

Data Confidentiality and Encryption

- – IDEA (International Data Encryption Algorithm)
  - Uses same secret key for encryption and decryption.
  - 128 bit key, , symmetric key
  - Fast and can be used for cloud data
  - Operates on 64 bit blocks at a time
- – Blowfish (1993)
  - Symmetric block-cipher algorithm
  - 32 to 448 bit key length
  - Strong and fast therefore suitable for use in cloud

Data Confidentiality and Encryption

- RC4
  - Fast, strong, use key up to 2048 bits
  - Creates a stream of random bytes and XOR it with the text
  - New key for each message
- SEAL (Software Optimized Encryption Algorithm)
  - Stream cipher – data is continuously encrypted
  - Uses 160 bit key
  - Longer initialization phase

Data Confidentiality and Encryption

- Encryption algorithm process data in the following ways:
  - Stream Ciphers
    - Encrypts the bits of a message, one at a time, and as a stream of bits.
    - Require too much processing hence not advisable
  - Block Ciphers
    - Encrypts certain number of bits as a single unit
    - Example: AES uses 128 bits
    - Recommended for cloud data

Data Confidentiality and Encryption

- Key Length
  - The keys are usually 128, 196, 256 bits.
  - Longer the key – complicated it is to derive
  - Example:
    - multiple door – single/multiple key
    - Similarly different part of cloud data must be encrypted using different keys
    - Keep two sets of key to prevent loss of data
- Backup Data
  - Need to encrypt backup data too

Data Confidentiality and Encryption

- Best practises for cloud data encryption
  - Deploy encryption
    - secure all critical data and store keys and encrypted data on different servers
  - Use Data-origin Authentication
    - When encrypted data in transit – man in the middle attack change packet-Decrypt result in different than original
  - Use Session-based Encryption Keys with Short Life Span
    - If too much data encrypted using same key result into decoded key
    - Use different key at regular interval

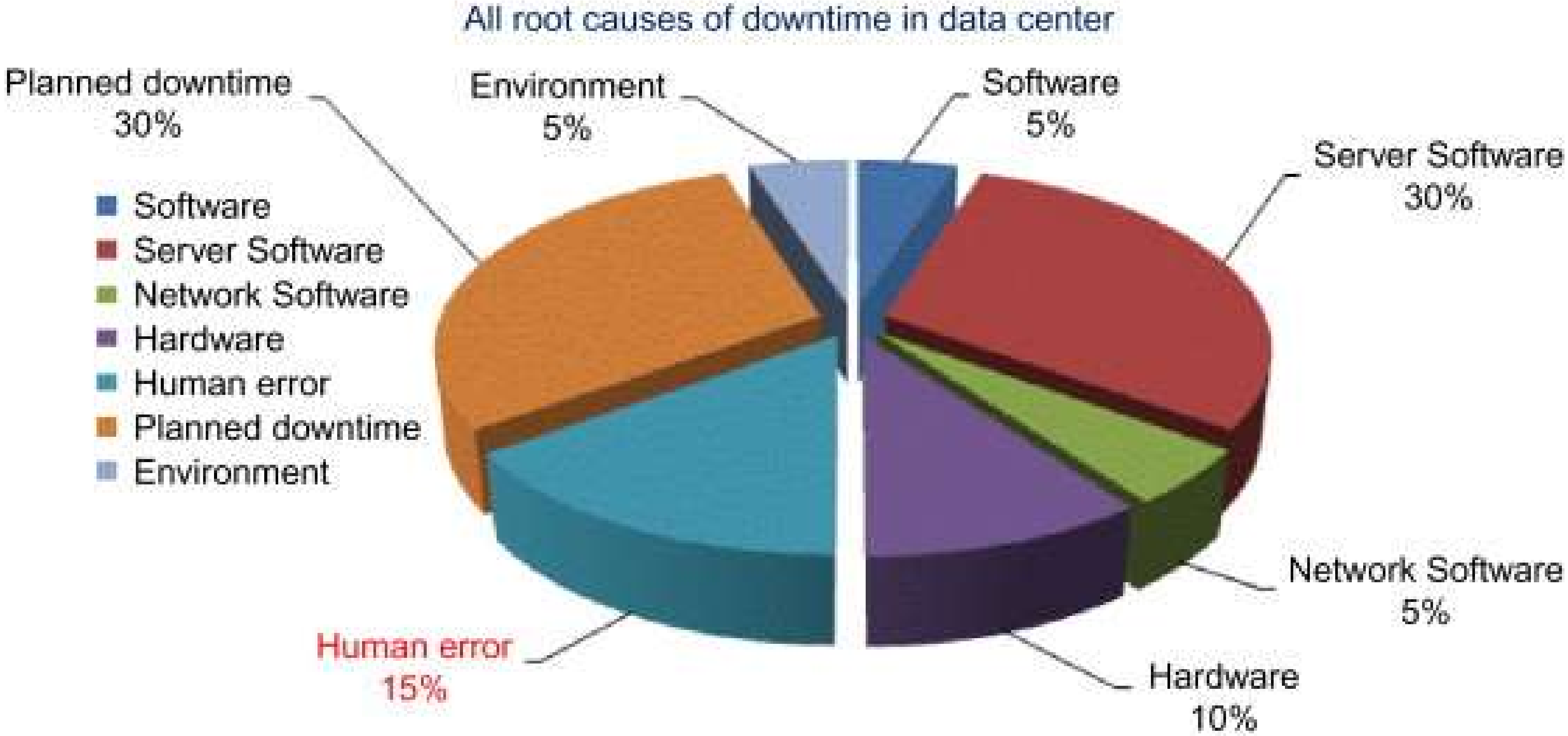
Data Confidentiality and Encryption

- Use Strong Encryption Algorithms
  - Strength of symmetric key encryption algorithm relies on randomness of their key.
  - If not sufficiently random, attacker may narrow down the number of possible values for the encryption key.
  - Easy for brute force attack
- Use Published, Well-known Encryption Algorithms
  - User algorithm which pass through rigorous review process
- Implement Compliance
- Implement Role-Based Access Control (RBAC)

Data Confidentiality and Encryption

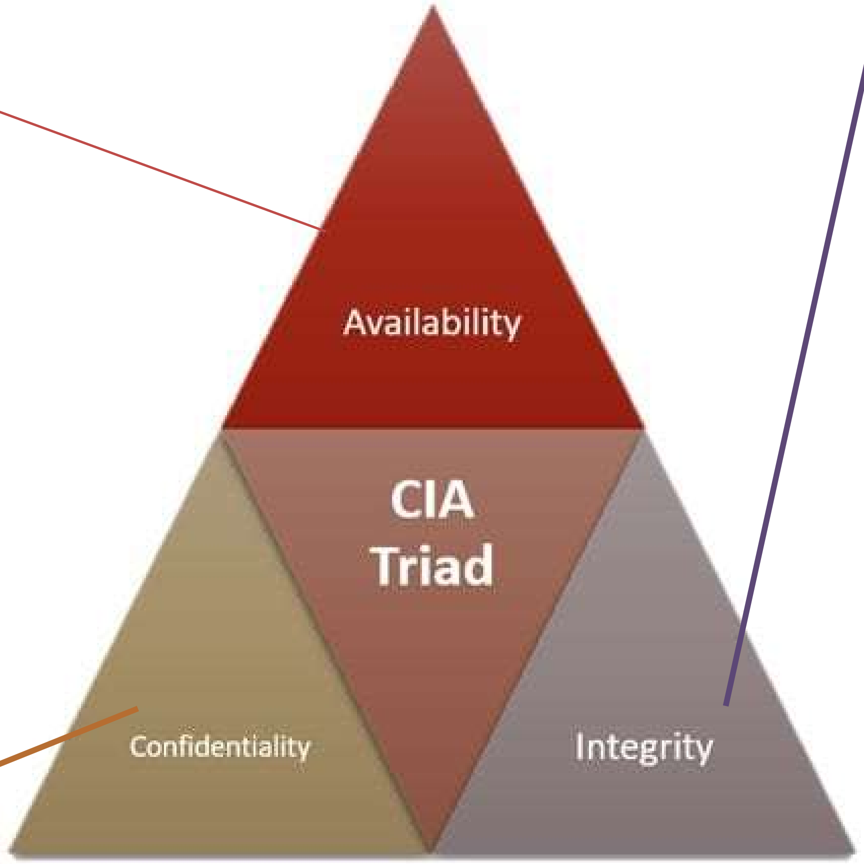
- Data Availability
  - Data must ne available to user as and when needed
  - Downtime as a cost
    - Soft cost: Loss in customer confidence and employee morale
    - Hard cost: Loss due to employee productivity and customer revenue during the outage window

Availability %	Downtime per month	Downtime per year
99	7.20 hours	3.65 days
99.5	3.60 hours	1.83 days
99.9	43.2 minutes	8.76 hours
99.99	4.32 minutes	52.56 minutes
99.999	25.9 seconds	5.26 minutes
99.9999	2.59 seconds	31.5 seconds



All root causes of downtime in data center

Makes sure that users can access data when they want to



Makes sure data is protected.

Makes sure that the data in the cloud cannot be read or understood by unauthorized parties

Data Confidentiality and Encryption

- Data Integrity
  - Malicious attempts by other tenants or user
  - Errors by the administrators who work for the cloud service provider
  - Hardware or software errors, bugs, or malfunctioning

Data Confidentiality and Encryption

- Data Integrity
  - Ask following to cloud provider
    - Are there know loopholes to comprise data integrity?
    - What processes does the provider follow to assure data integrity?
    - How does the provider report the success or failure of data integrity?
    - What is the maximum loss that can occur to you if your data in the cloud lacks integrity?

Data Confidentiality and Encryption

- Data Integrity
  - Measures for ensure data integrity
    - They must control the access to data using mechanism such as Role Based Access Control (RBAC)
    - They must design implement user interfaces that prevent input of invalid data.
    - They must use error detection and correction software when transmitting data.
    - Data storage is protected using techniques such as new Data Integrity Field (DIF)

Cloud Data Management Interface

- **Cloud Data Management Interface** (CDMI) from **Storage Networking Industry Association** (SNIA) is a standard to protect data.
- CDMI allows users to tag the data with special metadata (code services that must be provided such as encryption, backup, replication, compression, archiving).

Cloud Data Management Interface

- CDMI enables inter-operable cloud storage implementations from various cloud service providers and storage vendors.

Cloud Data Management Interface

- Objects
  - Objects are similar to files in a traditional file system, but are enhanced with an increased amount and capacity for metadata.
  - Accessed by either name or OID
- Containers
  - Similar to a traditional file system directory structure

Cloud Data Management Interface

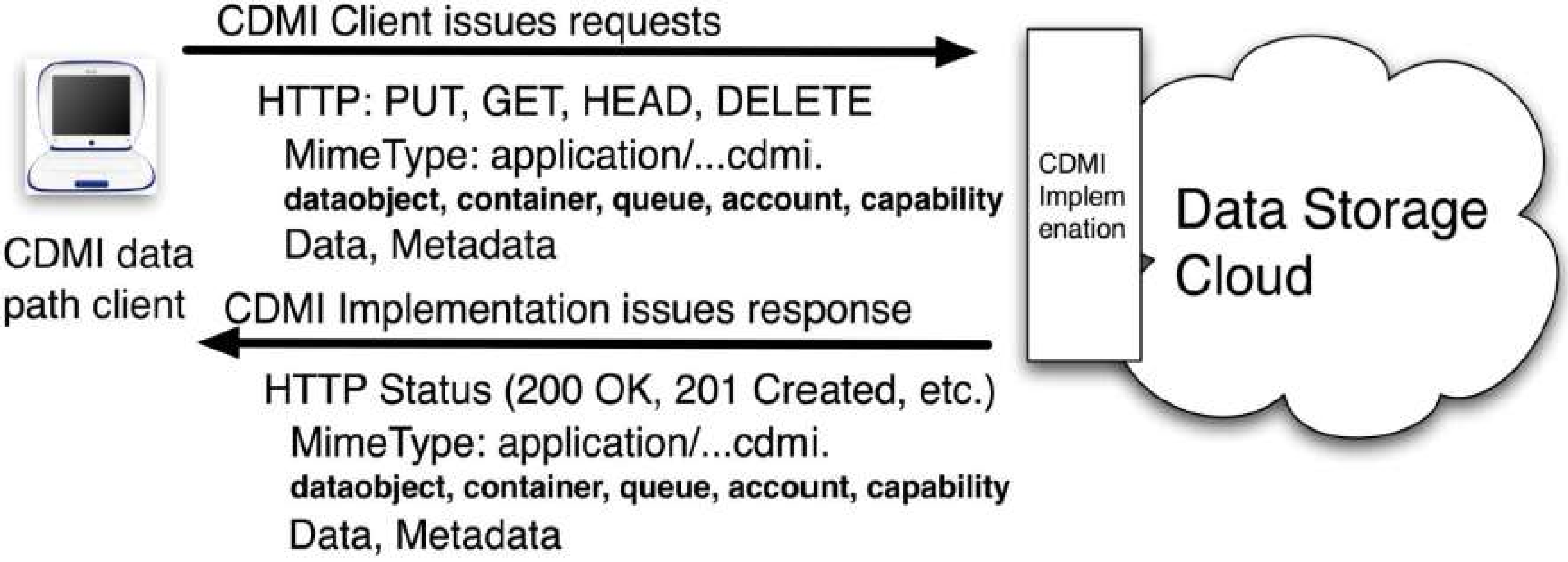
- Capabilities
  - Compliant implementations must provide access to a set of configuration parameters known as capabilities.
- Domains, Users and Groups
  - Like LDAP, Active directory
- Queues
  - FIFO useful for job scheduling, order processing and other tasks

Cloud Data Management Interface

- Access Control
  - Follows the ACL and ACE model used for file authorization operations by NFSv4
- Queries
  - queries against CDMI containers, with a rich set of comparison operators
- Metadata
  - Objects and containers have "storage system metadata", "data system metadata" and arbitrary user specified metadata

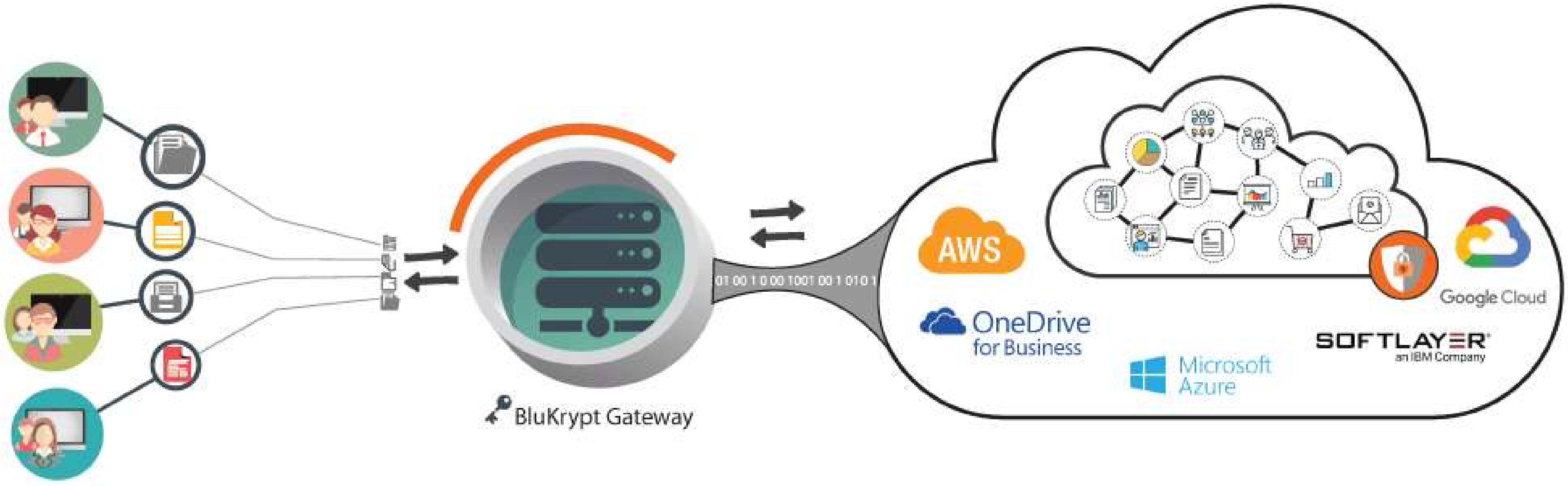
Cloud Data Management Interface

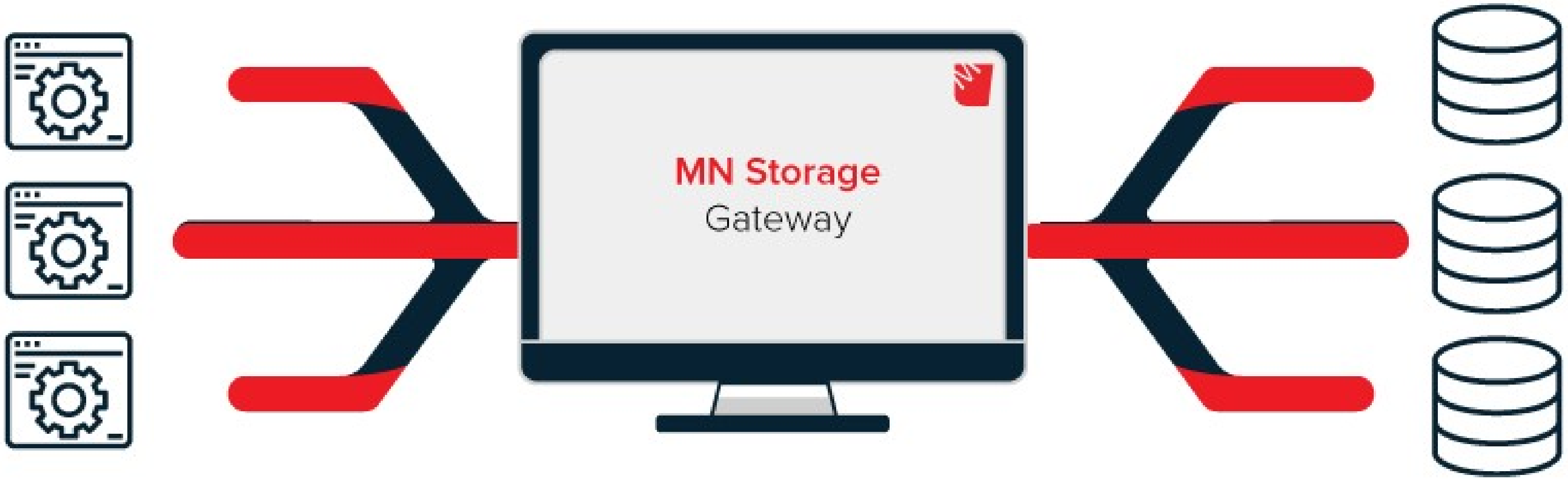
- CDMI Basic flow:



CDMI Client issues requests
HTTP: PUT, GET, HEAD, DELETE
MimeType: application/...cdmi.
dataobject, container, queue, account, capability
Data, Metadata
CDMI data path client
CDMI Implementation issues response
HTTP Status (200 OK, 201 Created, etc.)
MimeType: application/...cdmi.
dataobject, container, queue, account, capability
Data, Metadata
CDMI Implemenation
Data Storage Cloud

Cloud Storage Gateways (CSGs)





Cloud Storage Gateway

- To address the performance and security issues in public clouds, organizations can use CSGs.
- CSG is an appliance residing in the customer’s premises and provides data protection by encrypting, compressing, and archiving data sets before moving the data to a cloud.
  - CSG is a storage appliance, installed in a customer datacenter.
  - It intercepts all the I/O between the customer datacenter and all the public clouds.

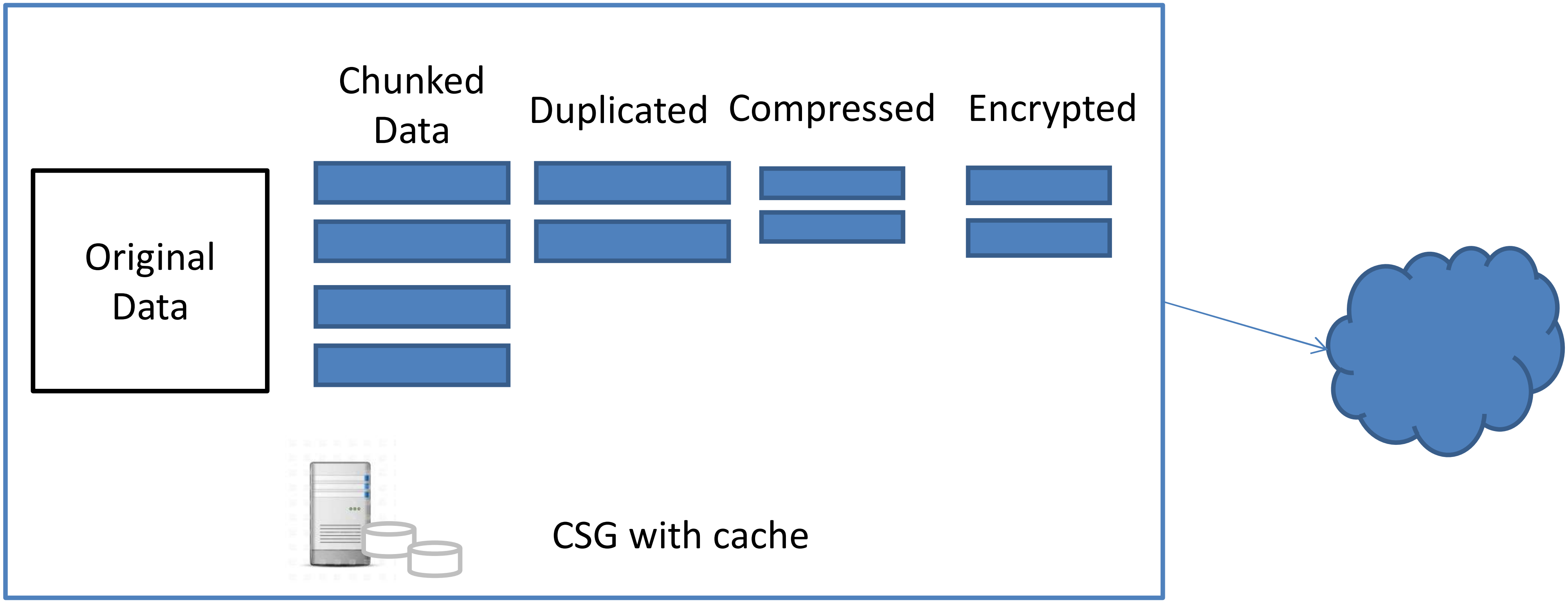
Cloud Storage Gateway

- CSG provides data protection in 4 steps:
  - The CSG cache accelerates I/O rates and enables a convenient replication procedure.
  - Files that are to-be-copied to the cloud are first stored in the CSG cache.
  - After a certain pre-set time interval, the cache data is pushed to the cloud.
  - Data that is read from the cloud is copied to the cache.

Cloud Storage Gateway

- CSG must provide following features/benefits:
  - Caching algorithms
  - Intelligent pre-fetching algorithms
  - Caching time periods
  - Synchronous snapshots
  - Data replication process

Cloud Storage Gateway



Original Data

Chunked Data

Duplicated

Compressed

Encrypted

CSG with cache

Use of CSG to copy and save data in a cloud

Cloud Storage Gateway

- End-to-end encryption
- Secure channels
- Data compression
- CSG tuning parameters

Cloud Firewall

- A cloud firewall is a network firewall appliance, explicitly built to work with other cloud based security solutions.
- Serves the same purpose as traditional firewall but differences are:
  - Scalability
    - Scalable as per customer bandwidth or hardware upgrade
  - Availability
    - Extremely high availability through an infrastructure
  - Extensibility
    - Are available in locations where the network manager can provide a protected communication path

Virtual Firewall

- A VF is a network firewall service running entirely within a virtualized environment.
- Like physical firewall, it provides the usual packet filtering and monitoring.
- Easy way to decrease investment by consolidating multiple logical firewalls onto a single platform.

Virtual Firewall

- Depending on the point of deployment VF can operate in two different modes:
  - Bridge mode
    - Act like physical firewall work with physical or virtual switch to intercept network traffic.
  - Hypervisor mode
    - Resides in the virtualization hypervisor, can capture, monitor and filter all the activities of all virtual machines and logical resources.

5.3 Host Security in Cloud

Need of Host Security

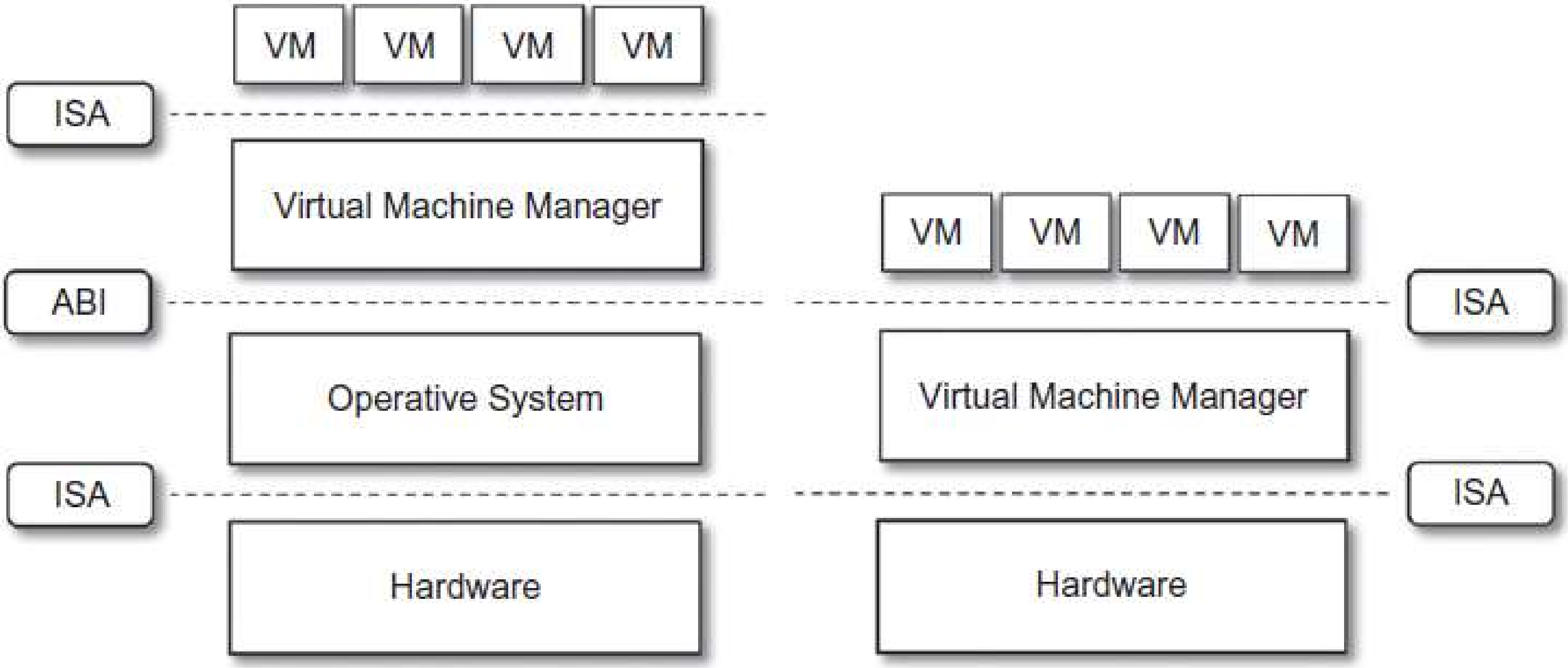
- Security for a cloud host is to some extent similar for traditional, non-virtualized on-premise servers.
- Every cloud resource (in public/private) is virtualized and shared by diverse business units.
- The amount of resources in a public cloud is usually 10/100s of times more than any corporate server farm or private cloud.

Introduction

- With several users and applications in a cloud, malwares can magnify damages faster then in any dedicated environment.
- Users need to deploy tools to identify and resolve malware, data integrity and authentication problems.
- SLA is also important to share responsibilities between cloud provider and consumers.

Security for the Virtualization Product

- In public cloud, the cloud provider is responsible for the security of the virtualization software.
- Provider/consumer can create and delete VM.
- It enables several VM or OS instances to share the same underlying server resources – CPU, network cards, bandwidth, memory and storage).
- OS and user data located on SAN, NAS or iSCSI storage devices connected to the server.


VM
VM
VM
VM
ISA
Virtual Machine Manager
ABI
Operative System
ISA
Hardware
VM
VM
VM
VM
ISA
Virtual Machine Manager
ISA
Hardware

Security for the Virtualization Product

- In PaaS and SaaS, the VM are shared by several customers.
- In an IaaS, each VM is owned by a customer.
- The VM come with different variant of an OS.
- Need to keep Virtualization layer secure.

Security for the Virtualization Product

- There are several attacks on the hypervisor level and these are known as bugs where a guest machine can gain access to the host OS.
- A zero day vulnerability is a flaw(/problem) that is found and exploited by hackers on the release day.
- Zero day signifies that hackers have tools to launch attack on the same day the flaw is found.

Security for the Virtualization Product

- A zero-day vulnerability is particularly dangerous as the provider and software vendor may not have a ready remedy to fix it.
- Example:
  - Virtualization software: HyperVM
  - S/w used by: VAServ – UK based hosting provider
  - Hacker obtained root access to the OS and deleted large portion of user data.

Security for the Virtualization Product

- Provider need to deploy measures to protect against any unknown weakness:
  - Early problem detection techniques, **IPS and IDS** to protect against intrusion,
  - virtual LANs(vLANS) with IPsec to protect in-transit messages, and

Security for the Virtualization Product

- Network Access Control(NAC) to prevent rouge users or machines from gaining access to underlying infrastructure.
- WiFi Protected Access (WPA) for mobile users to defend against wireless baseed attacks on the hypervisor, OS and applications.

Security for the Virtualization Product

- Historically, there are several problems in industry-standard virtualization software.
- There are also vulnerabilities that allow attackers to find out where a VM instance is running and start new VM on same hardware in quick succession.
- It uses resources CPU, RAM, and hard disk – launch side-channel attack.

Security for the Virtualization Product

- Before WPA, original wireless security standard called Wired Equivalent Privacy (WEP) was deficient in may ways.
- Access to WEP encrypted data can be decrypted easily.
- **Cloud providers must implement necessary controls to enable tighter security for the hypervisor, the foundation for its servers and services.**

Host Security of SaaS

Architecture

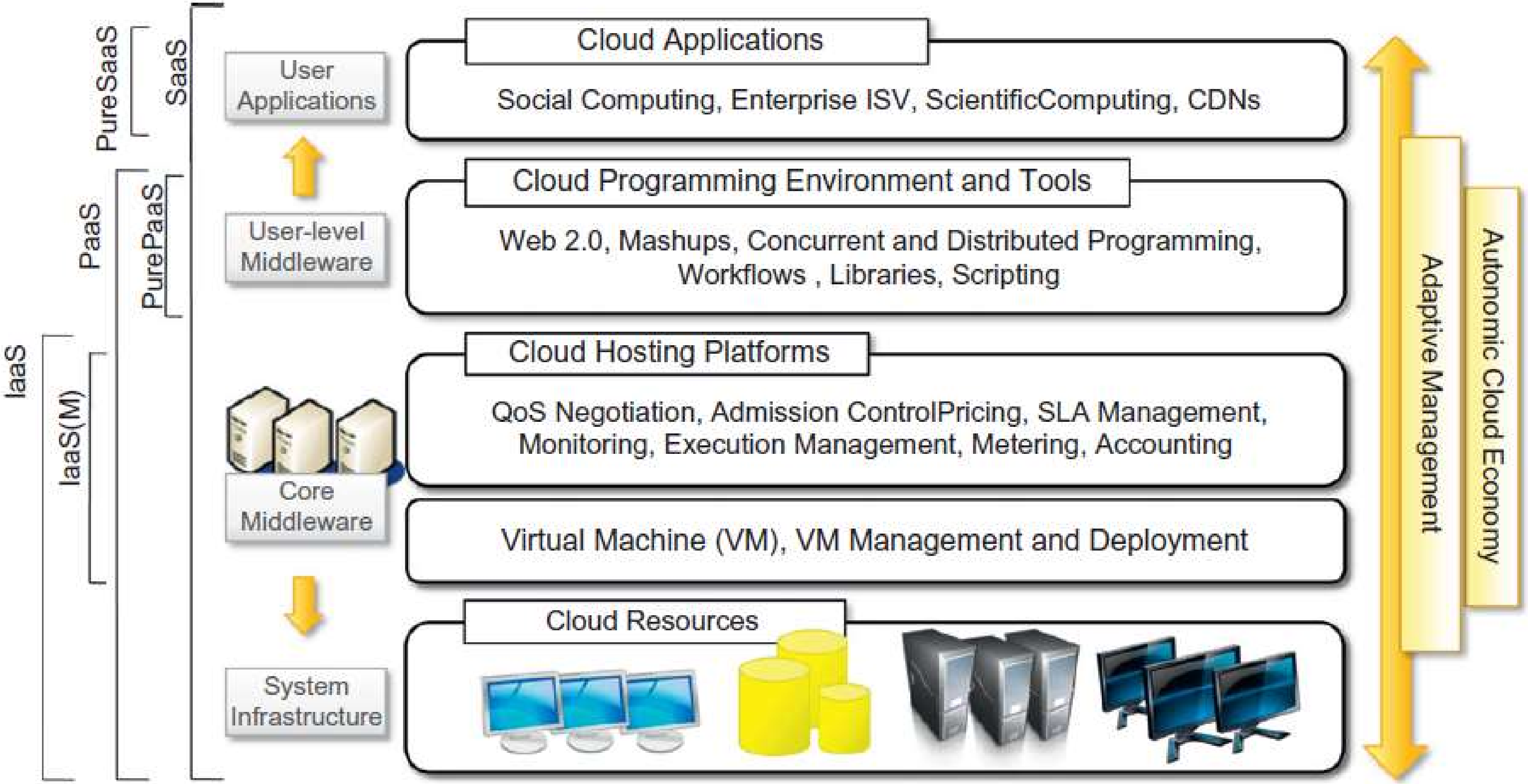

PureSaaS
SaaS
PaaS
PurePaaS
IaaS
IaaS(M)
User Applications
User-level Middleware
Core Middleware
System Infrastructure
Cloud Applications
Social Computing, Enterprise ISV, ScientificComputing, CDNs
Cloud Programming Environment and Tools
Web 2.0, Mashups, Concurrent and Distributed Programming, Workflows , Libraries, Scripting
Cloud Hosting Platforms
QoS Negotiation, Admission ControlPricing, SLA Management, Monitoring, Execution Management, Metering, Accounting
Virtual Machine (VM), VM Management and Deployment
Cloud Resources
Adaptive Management
Autonomic Cloud Economy

FIGURE 4.1

The cloud computing architecture.

Host Security for SaaS

- For SaaS services, the provider owns and manages the servers, network and applications.
- As customer you will get little or no information about host.
- Provider refuse to provide details on OS, patches, implemented security measures, hypervisor etc.

Host Security for SaaS

- Way to get assurance of the degree of security implemented by the SaaS provider, Customer can ask for:
  1. detailed security status after signing a Non-Disclosure Agreement (NDA) with the provider.
  2. provider has security assessment report such as SAS 70 or SysTrust.
  3. Security certification such as ISO 27002

Host Security for SaaS

- SaaS providers are not obligated to give information.
- They can give a high-level SLA for the service availability or type of data backup and disaster recovery.

Host Security for PaaS

Architecture

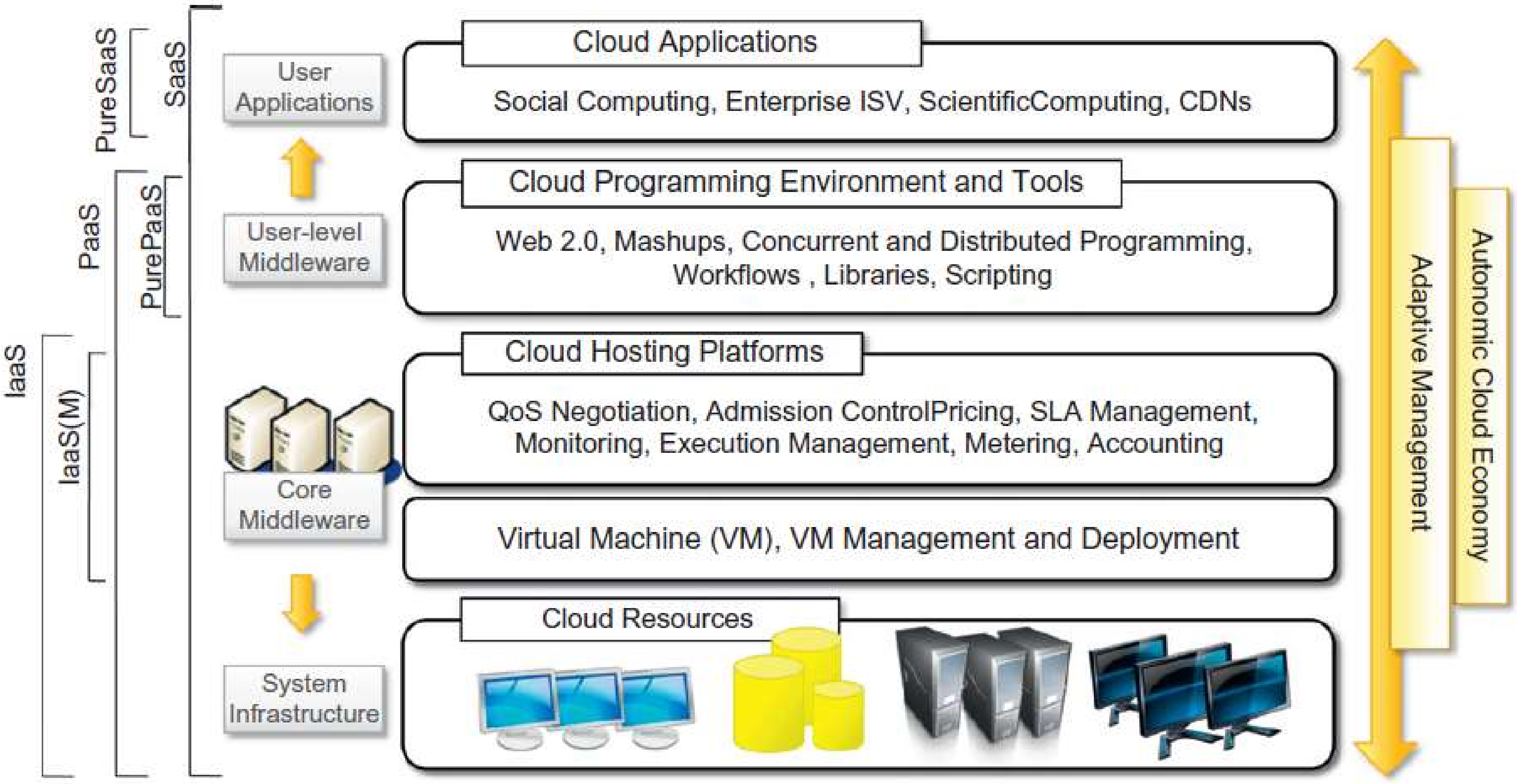

PureSaaS
SaaS
PaaS
PurePaaS
IaaS
IaaS(M)
User Applications
User-level Middleware
Core Middleware
System Infrastructure
Cloud Applications
Social Computing, Enterprise ISV, ScientificComputing, CDNs
Cloud Programming Environment and Tools
Web 2.0, Mashups, Concurrent and Distributed Programming, Workflows , Libraries, Scripting
Cloud Hosting Platforms
QoS Negotiation, Admission ControlPricing, SLA Management, Monitoring, Execution Management, Metering, Accounting
Virtual Machine (VM), VM Management and Deployment
Cloud Resources
Adaptive Management
Autonomic Cloud Economy

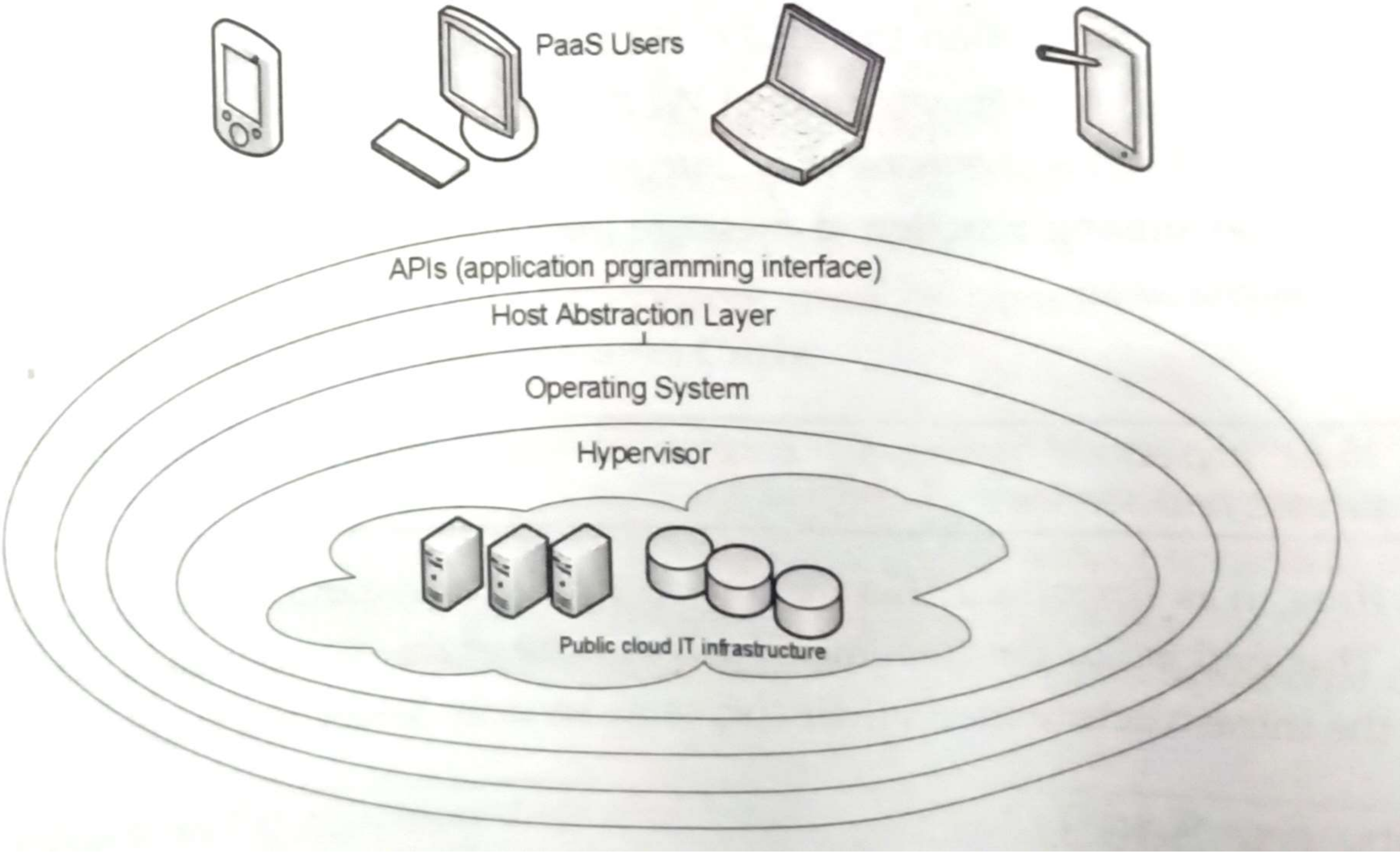
FIGURE 4.1

The cloud computing architecture.

Host Security for PaaS

- Similar to SaaS as far as providing server information to customer.
- Customer do have access to libraries and kernel level parameters as PaaS provides an environment to develop products.
- Server is shared by other developers, customer don’t have root or administrator level privileges.

Host Security for PaaS


PaaS Users
APIs (application prgramming interface)
Host Abstraction Layer
Operating System
Hypervisor
Public cloud IT infrastructure

Host Security for PaaS

Similar to SaaS

+

access to libraries and kernel-level parameters.

No root or administrator-level privileges

Host administration is the responsibility of cloud provider

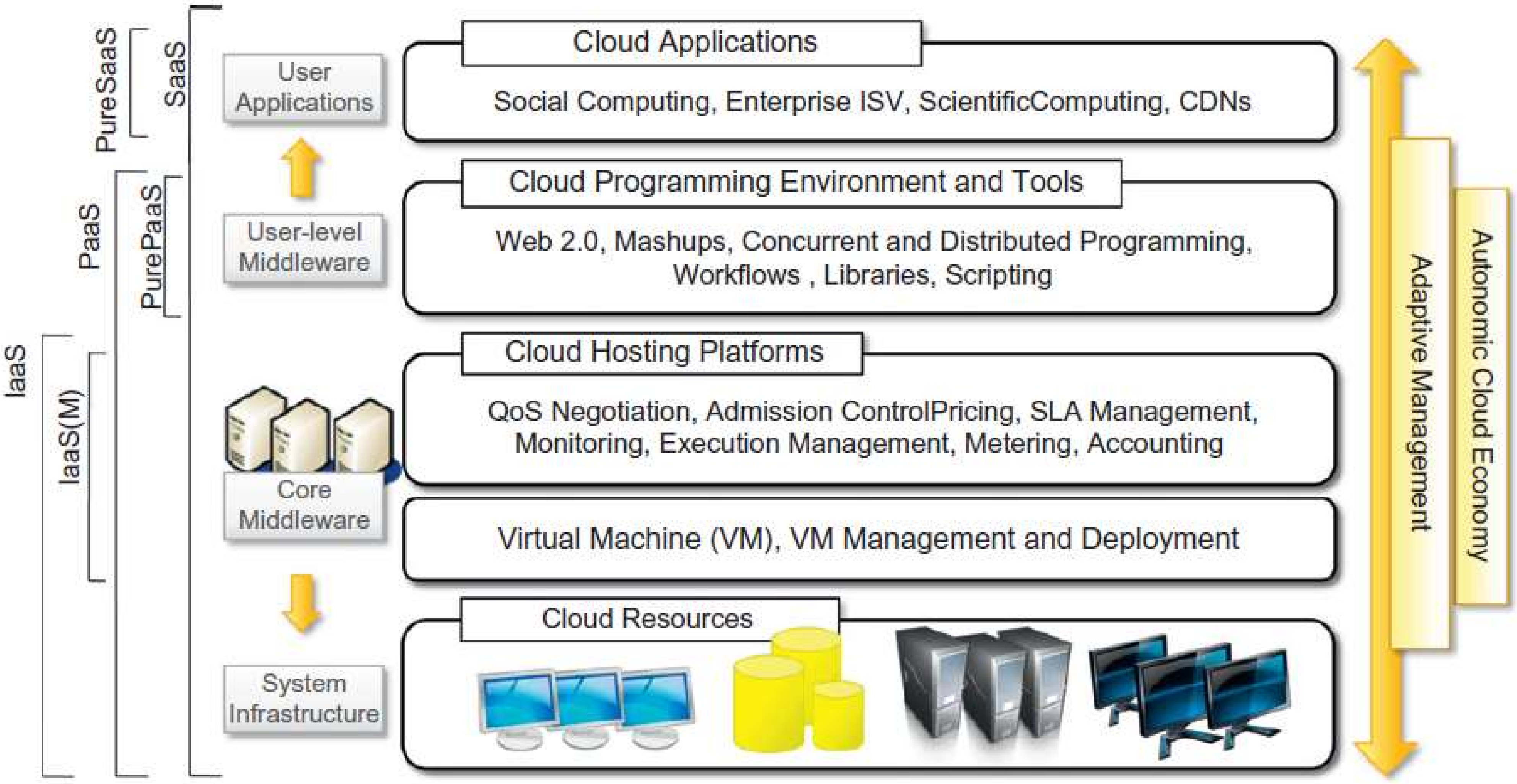

PureSaaS
SaaS
PaaS
PurePaaS
IaaS
IaaS(M)
User Applications
User-level Middleware
Core Middleware
System Infrastructure
Cloud Applications
Social Computing, Enterprise ISV, ScientificComputing, CDNs
Cloud Programming Environment and Tools
Web 2.0, Mashups, Concurrent and Distributed Programming, Workflows , Libraries, Scripting
Cloud Hosting Platforms
QoS Negotiation, Admission ControlPricing, SLA Management, Monitoring, Execution Management, Metering, Accounting
Virtual Machine (VM), VM Management and Deployment
Cloud Resources
Adaptive Management
Autonomic Cloud Economy

FIGURE 4.1

The cloud computing architecture.

Host Security for IaaS

- Users have complete access to
  - – the server OS
  - – its resources such as
    - CPU,
    - memory,
    - network,
    - ports,
    - bandwidth and
    - storage,
  - – along with root or administrator password.

Host Security for IaaS

- User decides the OS modules to be installed and services to be activated on the server.
- IaaS providers offers APIs to provision, replicate, add or remove resources or decommission virtual hosts.
- It is recommended that users automate as many virtual host operations as possible including growing or shrinking so as to dynamically meet workloads.
- If not automated, their management will soon become burdensome and resources will not be optimized to the workload.

Host Security for IaaS

- Virtual host in cloud are accessible to everyone.
- Hence user must implement strategies to limit the access.

Host Security for IaaS

- Some ways to tighten the host level security in an IaaS

  1. to be ts the
  2. by the e attack surface and number of OS patches required.
  3. Block unused ports. User must open only one port at a time, as and when required.

Service	Port number
FTP	20, 21
telnet	23
NetBIOS	139
SMTP	25

Host Security for IaaS

4. Install host based IPS and IDS services to monitor and analyse the OS and log files. i.e. tripwire, OSSEC and Verisys
5. Enable event logging for all security and user activities to a dedicated log server. Set up automated alerts for malicious events. Review log files regularly for security breaches.
6. Protect the encryption keys. Keep the key separate from the cloud where data is stored.
7. Use sudo access to gain root-level rights for Unix hosts.
8. Enforce strong passwords for user.

Host Security for IaaS

- Products for cloud host and data security
  - Secure Cloud – encrypts and controls data in public and private cloud environment.
  - Deep Security – provide security for virtual hosts in a private or public cloud.