CLOUD COMPUTING AND SECURITY

Chapter 4

Dr.Mohammed Tawfik

CONTENT

- • Risks in cloud computing
- • Data security in cloud
- • Cloud security services
- • Tools and technologies for cloud
- • Cloud mashaps
- • Apache hadoop
- • Cloud tools

Risk Management

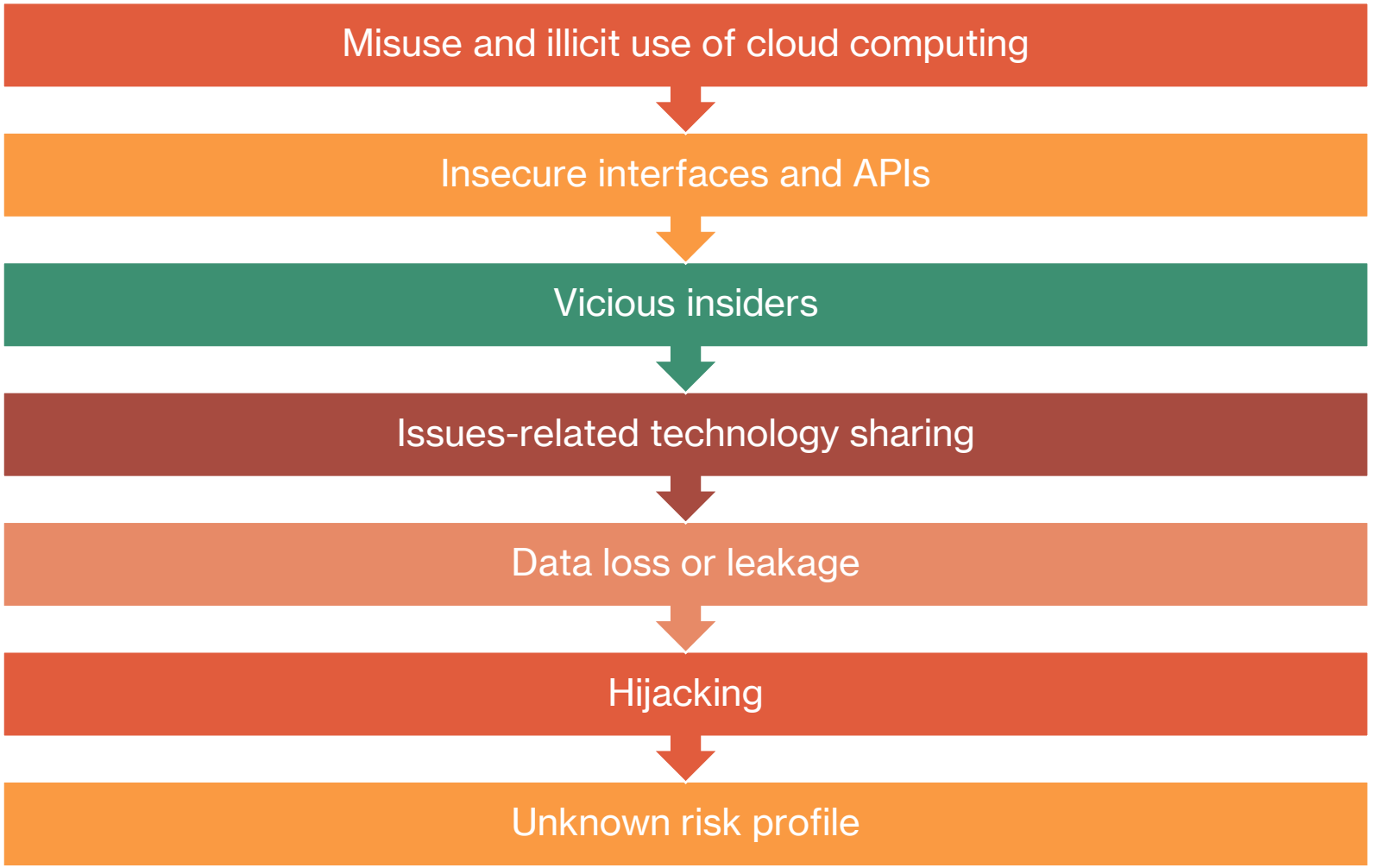
Risk management is a significant part of business planning.

It can also encompass legal risks like deception, robbery and sexual harassment lawsuits.

Cloud computing is somewhat new in its present pattern granted that it is best directed to reduce intermediate risk enterprise areas.

BUSINESS RISK IN CLOUD COMPUTING

Various Threat in cloud computing



Type of Risks in cloud computing

Internal Security Risk – Insider threats, misconfigurations, unauthorized access.

External Security Risk – Cyberattacks, hacking attempts, phishing threats.

Data Protection Risk – Unauthorized exposure, weak encryption, compliance issues.

Data Loss – Accidental deletion, hardware failure, inadequate backups.

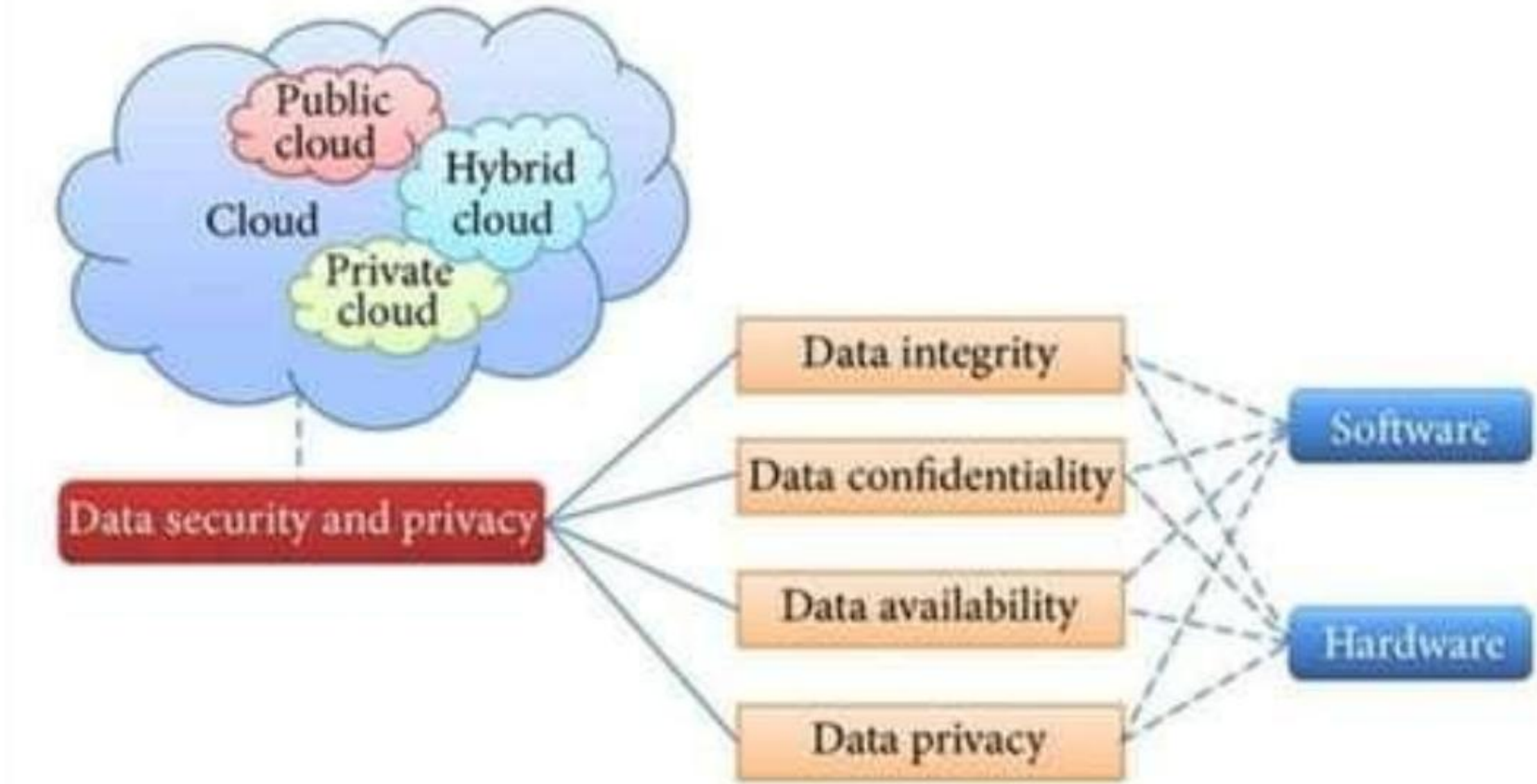
Security Advantages in Cloud Environment

- Data Centralization – Secure data storage, easier access control, better disaster recovery.

Incident Response – Faster threat detection, AI-driven security ops, automated responses.

Forensic Image Verification – Quick, reliable digital forensics, cryptographic verification, instant access.

Logging – Tracks user activity, detects threats, aids compliance audits.


Public cloud
Hybrid cloud
Cloud
Private cloud
Data security and privacy
Data integrity
Data confidentiality
Data availability
Data privacy
Software
Hardware

Security Disadvantages in Cloud Environment

Investigation – Limited access to physical evidence, complex forensic analysis.

Data Segregation – Risk of exposure due to shared infrastructure, weak isolation controls.

Long-Term Viability – Dependency on provider stability, potential service discontinuation.

Compromised Server – Vulnerability to breaches, unauthorized data modification, downtime risks.

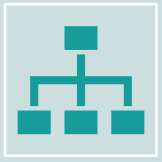
Regulatory Compliance – Challenges with legal requirements, cross-border data policies.

Recovery – Complex data restoration, reliance on provider backup efficiency.

Content Level Security(CLS)

1-Market Demand – CLS was developed to meet the needs of businesses and customers.

2-Data Organization – Helps organizations manage their data and content efficiently.



3-Better Control – Allows companies to secure and organize information at the organization level rather than the broader institutional level.

Data Confidentiality

- Access Control – Restricts data access to authorized users.
- Passwords – Secure login credentials to protect information.
- Biometrics – Uses fingerprints, facial recognition, or other unique traits for authentication.
- Encryption – Protects data by converting it into coded formats.
- Privacy – Ensures personal information is kept secure and undisclosed.
- Ethics – Encourages responsible handling of sensitive data.

Data Integrity

Definition – Ensures data is accurate, complete, and unchanged.

Protection – Prevents unauthorized or accidental modifications.

Reliability – Maintains data consistency in processing and storage.

Data Availability

Definition – Ensures data resources are accessible when needed.

Importance – A system must be available and functional at all times.

Access Control – Authorized users should have seamless access to data and assets when required.

Data Backup Plan

Data Backup Plan:

-Essential for security – Protects against data corruption and hardware failure.

-Restoration capability – Ensures organizations can recover lost or damaged data efficiently.

Disaster Recovery Plan (DRP):

- Rapid recovery strategy – Minimizes disruption after a disaster.

- Business continuity – Helps organizations resume operations with minimal impact.

Eras of Computing

Sequential & Parallel Eras – The two most significant phases in computing history.

Infinite Computing Resources – Cloud computing creates the illusion of unlimited resources on demand.

No Up-Front Commitment – Users avoid long-term obligations when utilizing cloud services.

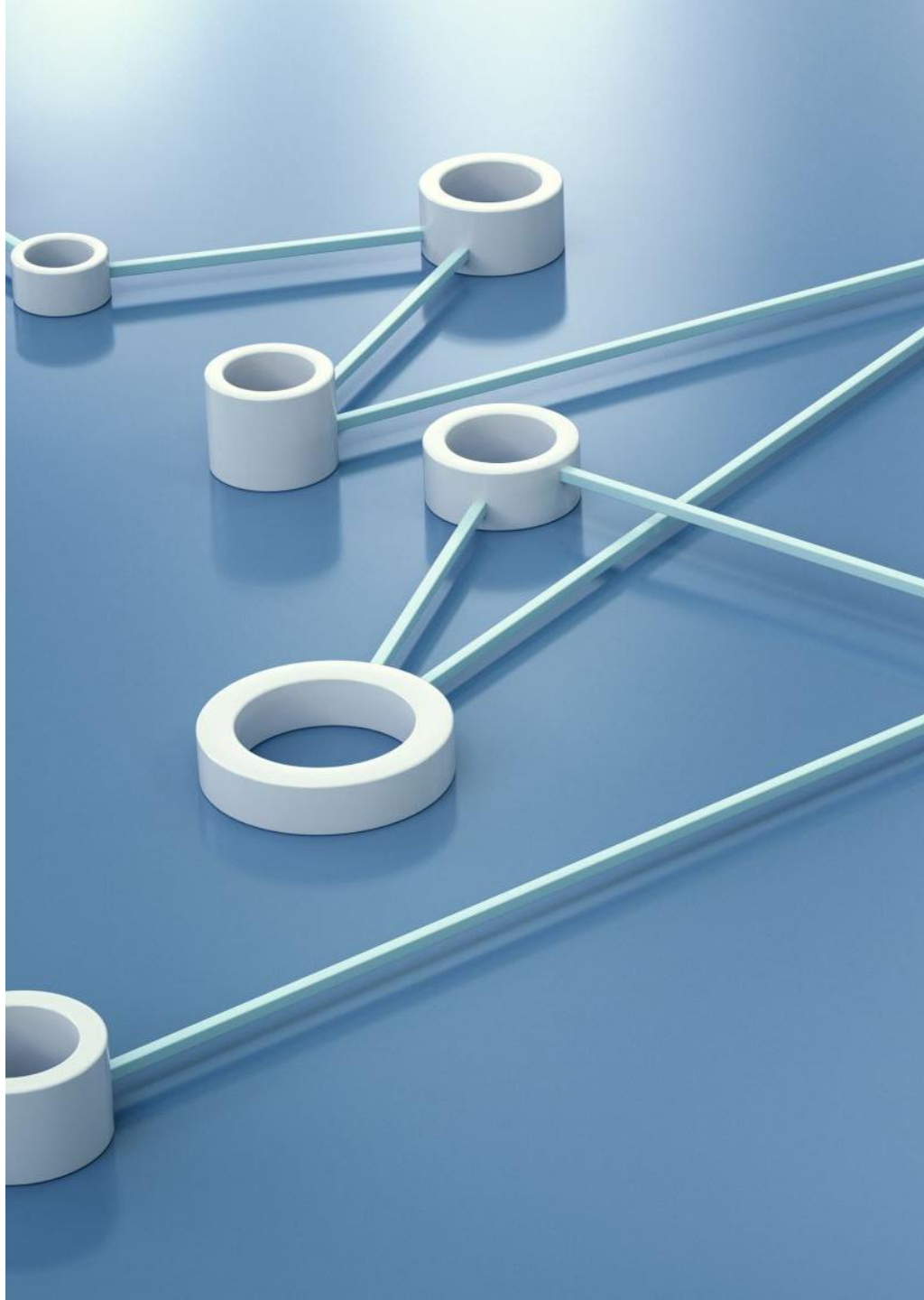
Pay-as-You-Go Model – Computing resources can be used temporarily and released as needed.

Cloud Computing Platforms

- **Abicloud** – A flexible cloud computing platform for managing resources.
- **Eucalyptus** – An open-source cloud solution for private and hybrid clouds.
- **Nimbus** – A cloud computing platform designed for scientific research.
- **OpenNebula** – A lightweight, open-source platform for managing virtualized data centers.

Key Elements of Cloud Infrastructure

- **Shared Infrastructure** – Resources are shared among multiple users for efficiency.
- **Self-Service Portal** – Automated platform for managing cloud services independently.
- **Scalable** – Easily expands or contracts based on demand.
- **Application Container** – Supports running and deploying applications flexibly.
- **Programmatic Control** – Enables automated cloud management through coding interfaces.
- **Virtual Hardware Abstraction** – Provides fully virtualized computing resources.
- **Multi-Tenancy** – Allows multiple users or organizations to use the same cloud securely.
- **Chargeback** – Tracks and bills cloud resource usage effectively.



cloud computing technologies and infrastructure

- Cloud computing enables **on-demand access** to computing resources, eliminating the need for physical servers. Key technologies like **virtualization (VMware), big data processing (Hadoop), and service integration (Mashups)** enhance scalability, efficiency, and flexibility in modern digital environments.

Mashups in Cloud Computing

Definition – Applications that combine and integrate data from multiple sources to create new functionalities.

Cloud Mashups – Vary in scope based on their purpose, such as combining web services, data feeds, or APIs to enhance user experience.

Hadoop

Hadoop is an open-source framework designed for distributed storage and processing of large datasets across multiple machines. It enables organizations to handle big data efficiently by distributing tasks across clusters of inexpensive servers.

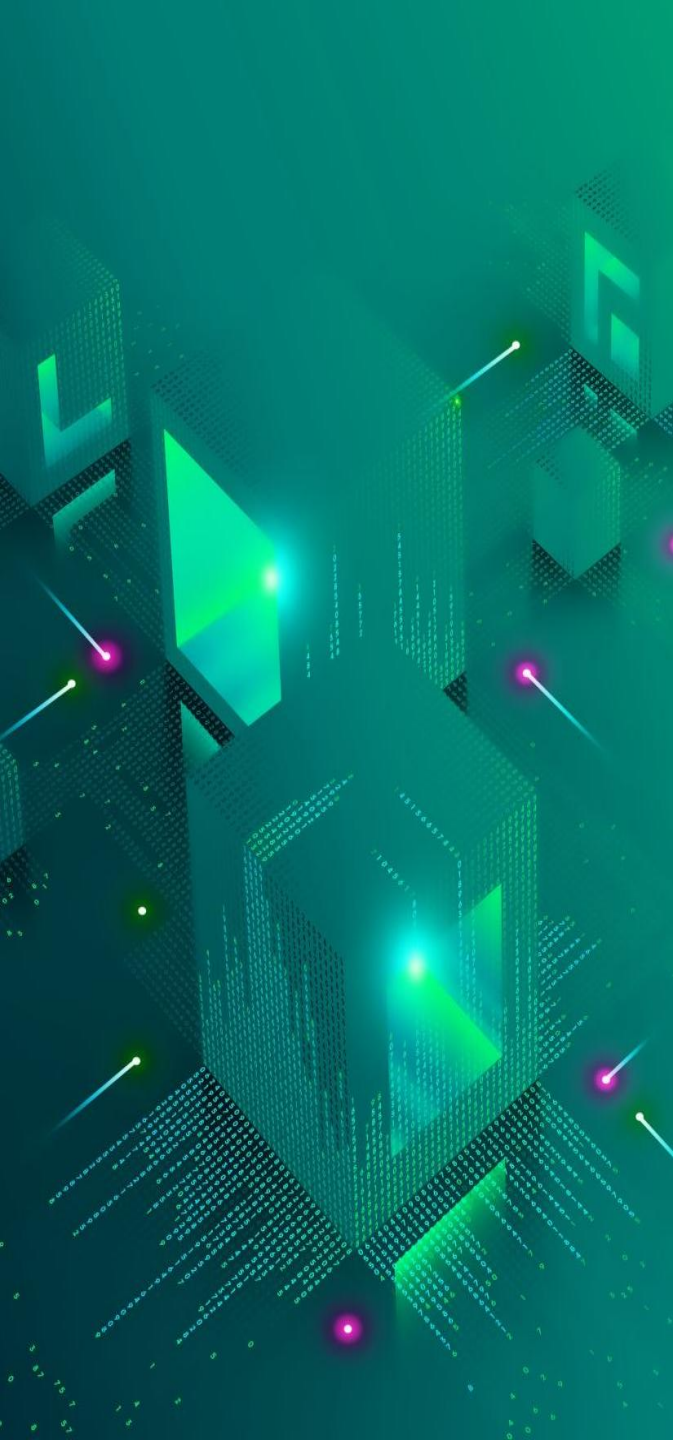
Key Components of Hadoop

Hadoop Distributed File System (HDFS) – A scalable storage system that splits large files into smaller blocks and distributes them across multiple nodes for fault tolerance and high availability.

MapReduce – A programming model that processes large datasets in parallel by breaking tasks into smaller chunks.

YARN (Yet Another Resource Negotiator) – Manages and allocates computing resources across Hadoop clusters.

Hadoop Common – A set of utilities and libraries that support the other Hadoop components.



VMware

- VMware is a leading virtualization software that enables users to run multiple operating systems on a single physical machine. It provides a virtualized hardware environment for guest operating systems, allowing efficient resource management and flexibility.
- **Features of VMware:**
- -Cross-Platform Compatibility – VMware's desktop software runs on Windows, Linux, and macOS.
- -Virtualized Hardware – Presents a fully virtualized set of hardware to guest operating systems, enabling seamless system simulation.
- -Hardware-Assisted Virtualization – Allows applications that require direct hardware access to run efficiently without binary translation.
- -Resource Management – Optimizes CPU, memory, and storage allocation across multiple virtual machines.
- -Snapshot & Cloning – Enables users to save system states and duplicate virtual machines for testing or backup purposes.
- -Security & Isolation – Provides strong security measures, ensuring virtual machines remain isolated from each other.

Eucalyptus Cloud Computing Framework

Eucalyptus is an open-source cloud computing platform designed for creating private and hybrid cloud environments. It provides a scalable and flexible infrastructure that mimics Amazon Web Services (AWS) functionality.

Key Components of Eucalyptus:

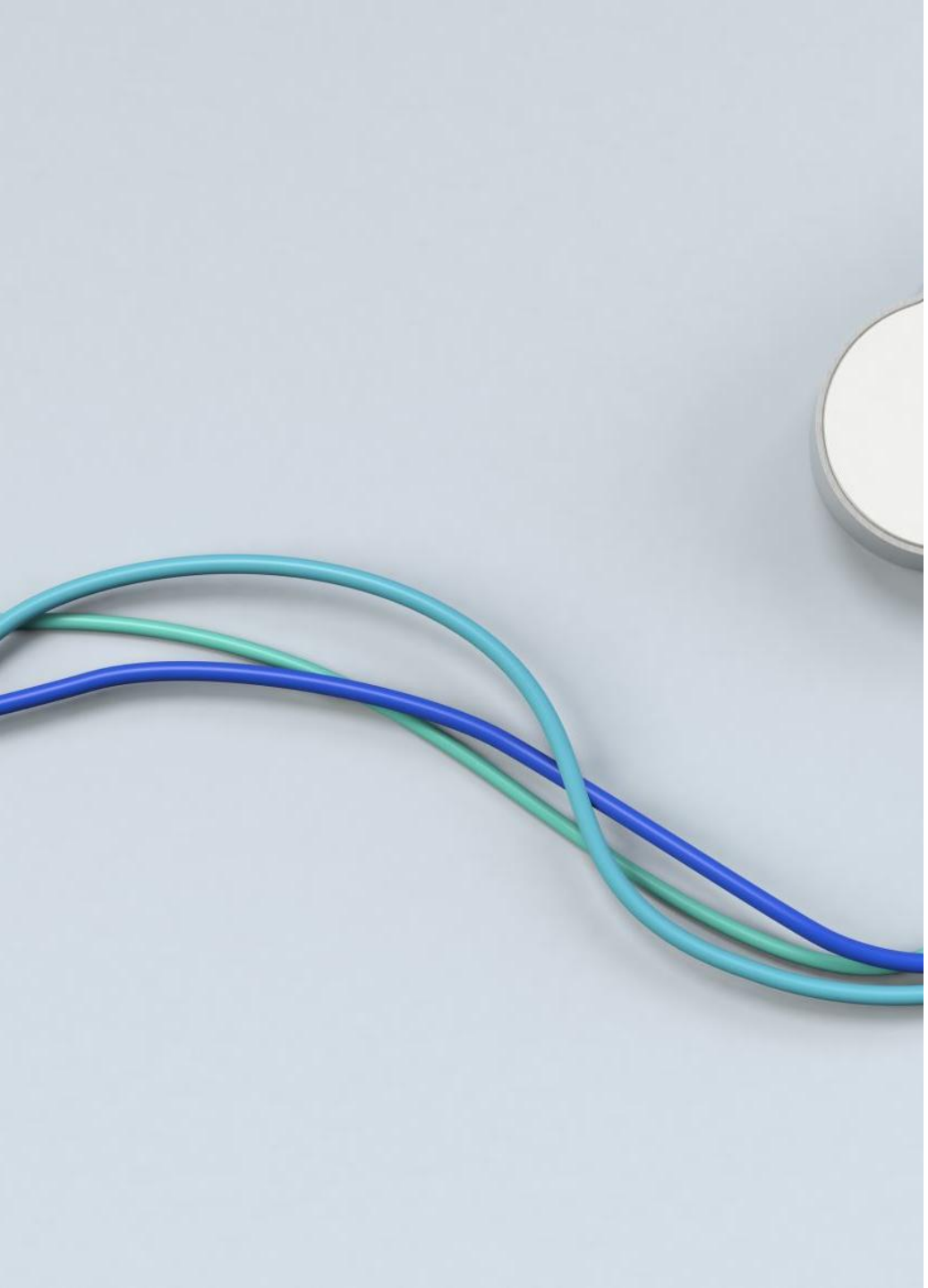
- Cloud Controller (CLC) – Manages the overall cloud infrastructure and user requests.
- Cluster Controller (CC) – Oversees multiple node controllers within a cluster, handling virtual machine execution.
- Node Controller (NC) – Manages individual compute nodes and virtual machine instances.
- Storage Controller (SC) – Handles cloud storage services, ensuring data availability.
- Walrus Storage Controller (WSC) – Provides storage services similar to AWS Simple Storage Service (S3).

CloudSim

CloudSim is a simulation framework designed for modeling, replicating, and experimenting with cloud computing environments. It provides a flexible and extensible structure that allows researchers and developers to evaluate cloud infrastructure and application services without deploying real cloud systems.

OpenNebula

OpenNebula is a powerful open-source cloud computing platform designed for Infrastructure-as-a-Service (IaaS) deployment. It enables organizations to build private, public, and hybrid cloud environments, offering flexibility and scalability. Known for its simplicity and efficiency, OpenNebula provides advanced virtualization and automation features, making it a preferred choice for cloud infrastructure management.

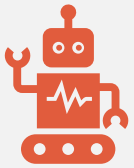


Nimbus

- Nimbus is an **open-source cloud computing toolkit** focused on delivering **Infrastructure-as-a-Service (IaaS)**. It provides researchers and the scientific community with **cloud-based computing capabilities**, allowing them to deploy and manage virtual machines for advanced computing tasks. Nimbus enables efficient resource allocation and scalability for specialized research applications.

Security Solutions & Best Practices

Firewalls & Intrusion Detection Systems (IDS) – Protecting cloud environments from cyber threats.



AI & Machine Learning in Security – How AI enhances threat detection and response.

Disaster Recovery & Backup Strategies – Ensuring business continuity in case of cyberattacks or system failures.