Emerging Issues in Computer Science

Week 6 Cloud Computing and Edge Computing

Lecturer: Ikwap Flavia Agatha

Learning out come

- By the end of this lesson, you will be able to:
- Understand the difference between On premise and cloud computing
- Comprehend the different cloud players
- Understand the deployment of services and service provisioned in the cloud
- Understand applicability of cloud computing
- Understand edge computing and how it works
- Understand Benefits and limitations of edge computing

On premise And Cloud Computing

- **On-premise computing** refers to the practice of hosting and managing computing infrastructure, software, and data within an organization's physical location (such as a data center or server room) rather than relying on external services like cloud computing. In on-premise computing, all the hardware, software, and data storage are owned, maintained, and operated by the organization itself. The load of managing the Data center is solely the responsibility of the organization.
- **Cloud Computing**
- In cloud computing another company takes the responsibility of hosting your applications.
- This means that they handle the costs of servers, they manage the data backup, software updates and other services at an affordable rate.

Comparison of On premise computing and Cloud computing

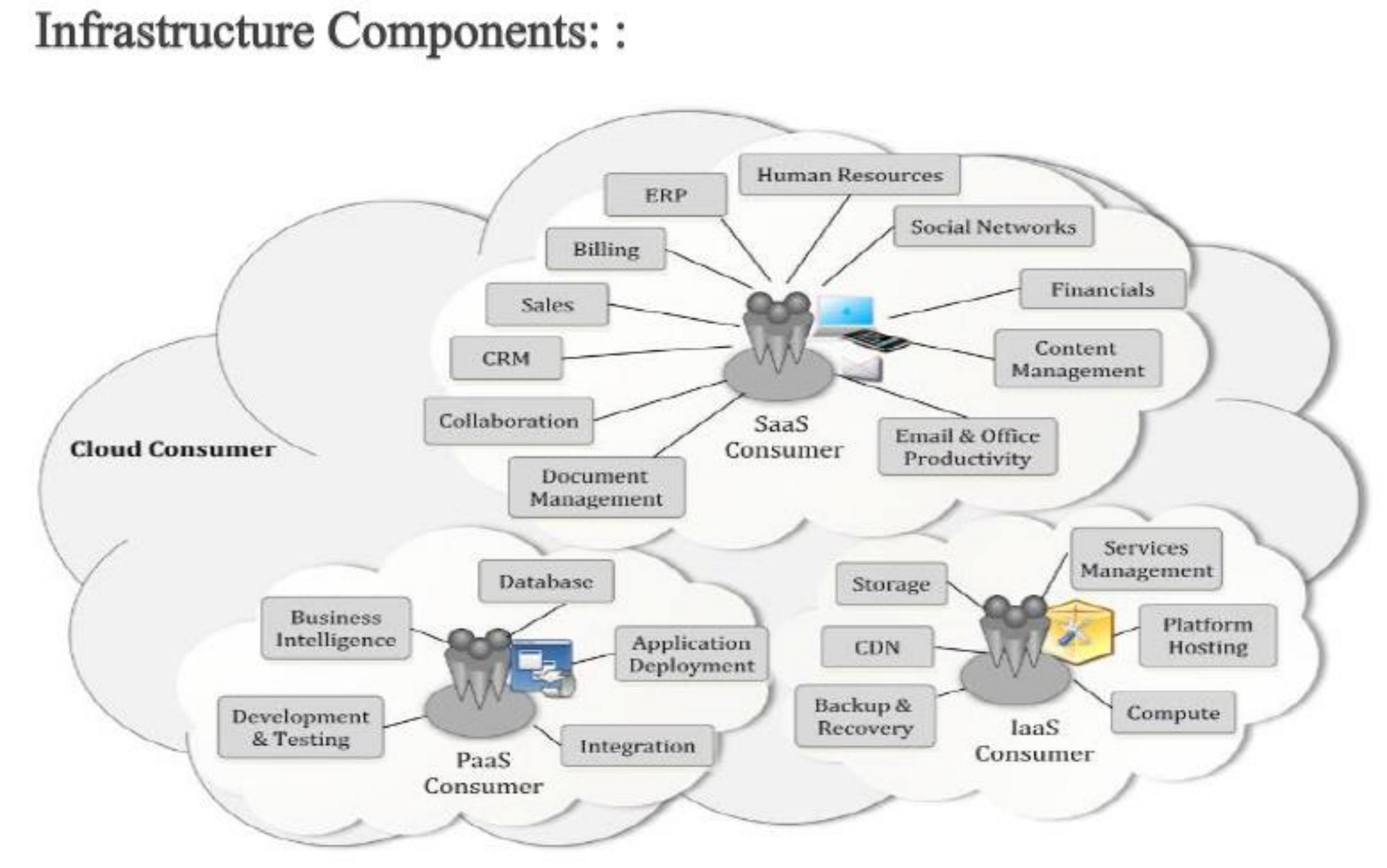
Aspect	Cloud Solutions	On-Premise Solutions
Upfront costs	Lower upfront costs	Higher Upfront costs
Maintenance	Managed by Cloud Provider	Self-managed by organization
Scalability	Easily scalable based on demand	Limited scalability, may require hardware upgrades
Flexibility	Offers flexibility to adjust resources as needed	Requires additional investments for flexibility
Total Cost of Ownership	Predictable subscription fees, Potential cost savings	Higher total costs of ownership due to maintenance costs
Security	Data security management by the Cloud Provider	Organization has control over data security measures
Accessibility	Remote access from anywhere with internet connectivity	Access limited to on-premise network
Customization	Limited customization options	Full control for customization and tailored options

- https://blog.invgate.com/cloud-vs-on-premise-which-is-better

Cloud Players in Cloud Computing

- NIST cloud computing reference architecture defines five major actors: cloud consumer, cloud provider, cloud carrier, cloud auditor and cloud broker. Cloud Consumer
- **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



- (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.
- 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.
- ***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.

Cloud Broker

- ***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.
- ***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

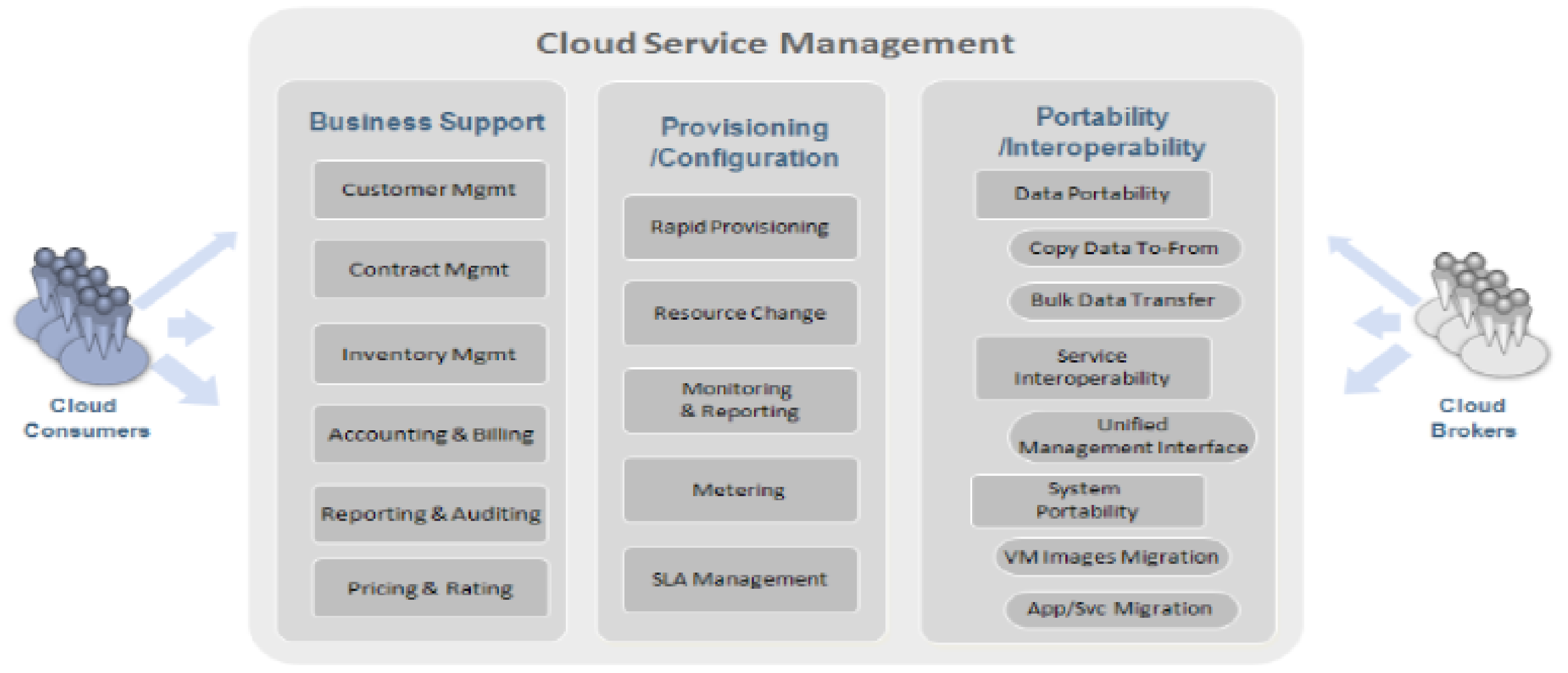


Figure 16: Cloud Provider - Cloud Service Management

- (Liu, 2011)

Cloud Services

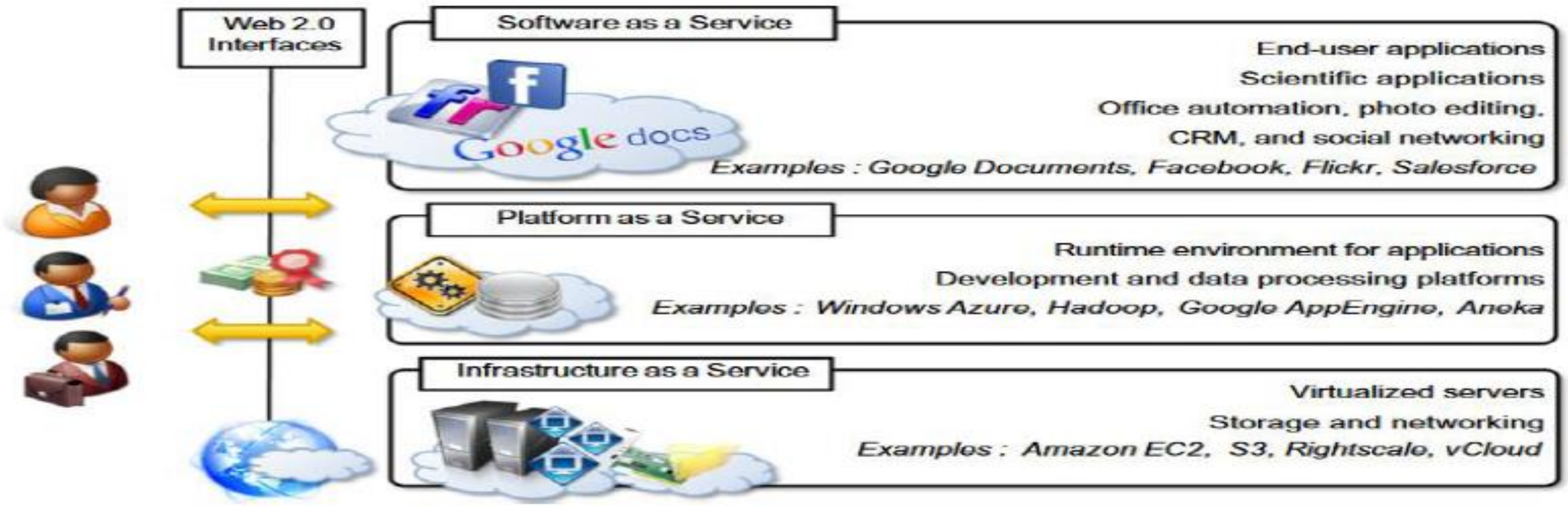
- National Institute of Standards and Technology (NIST) outlines three service layers to extend cloud computing capabilities: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS)
- **Software-as-a-service (SaaS):** Provides approved applications for customers to use. Licenses are granted on a pay-as-you-go or on-request basis. SaaS applications include Big Commerce, Google Apps, Salesforce, Dropbox, Mail Chimp, Zen Desk, DocuSign, Slack, and Hub spot, to name a few.

Cloud Services

- **Infrastructure-as-a-service (IaaS):** Delivers network services, servers, storage facilities, frameworks as part of an on-demand service. IaaS providers include Digital Ocean, Linode, Rackspace, Amazon Web Services (AWS), Cisco Meta pod, Microsoft Azure, and Google Compute Engine (GCE).
- **Platform-as-a-service (PaaS):** it is a platform for creating programming that is delivered over the Internet. Platforms like Salesforce.com and Heroku are used in this model.

Cloud Services

Cloud Computing Services



- Source: Buyya, R. (2013). Mastering Cloud Computing

Deployment Models for cloud services

- **Public Cloud**
- In the Public Cloud, services are broad casted to everyone, from anywhere, and at any time through the Internet. The public cloud is distributed system with one or more datacenters connected together, on top of which the specific services offered by the cloud are implemented.
- In the public cloud customer that are renting infrastructure or subscribing to application services, can easily upsize or downsize their IT according to the demands of their business. Currently, public clouds are used both to completely replace the IT infrastructure of enterprises and to extend it when it is required

Private cloud

- In private cloud resources are accessed within the boundaries of an organization
- Private clouds are virtual distributed systems that rely on a private infrastructure and provide internal users with dynamic provisioning of computing resources. Instead of a pay-as-you-go model, private cloud use different mechanisms like billing the different departments or sections of an enterprise.

Hybrid cloud

- Combination of both Public and Private Clouds
- Allow enterprises to exploit existing IT infrastructures, maintain sensitive information within the premises, and naturally grow and shrink by provisioning external resources and releasing them when they’re no longer needed.
- Hybrid clouds address scalability issues by leveraging external resources for exceeding capacity demand

Community clouds

- Community clouds are distributed systems created by integrating the services of different clouds to address the specific needs of an industry, a community, or a business sector.
- The infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
- Different organizations such as government bodies, private enterprises, research organizations, and even public virtual infrastructure providers contribute with their resources to build the cloud infrastructure.

Application of cloud computing

In R. Buyya, *Mastering Cloud Computing* (p. 1–469).

Application of cloud computing

- Cloud computing has changed the way organizations operate by offering scalable, cost-effective, and flexible solutions to organizations across industries. Cloud computing adoption in various sectors:
- **Healthcare:**
- **Electronic Health Records (EHR)**: Cloud computing allows healthcare providers to store, access, and share electronic health records securely, improving patient care and reducing paperwork. Cloud-based EHR systems also support real-time access to patient data for doctors, nurses, and other healthcare professionals.
- **Telemedicine**: Patients are able to consult doctors remotely.
- **Data Analytics**: Healthcare providers use cloud-based tools to analyze large datasets for research, improving diagnostics, treatment outcomes, and personalized care. Cloud also enables machine learning models to assist in predicting diseases based on patterns in patient data.

Finance and Banking:

- **Data Storage and Backup**: Cloud computing provides a secure, scalable solution for storing vast amounts of financial data. This helps financial institutions meet compliance requirements and ensures that critical data is backed up and accessible.
- **Mobile Banking**: Cloud infrastructure powers mobile banking apps, enabling customers to conduct banking transactions, check balances, transfer money, and access financial services from anywhere.

Education:

- **Learning Management Systems (LMS)**: Cloud computing supports online education platforms and Learning Management Systems (LMS), enabling educators to share course materials, conduct online exams, and track student progress.
- **Collaborative Tools**: Cloud-based tools like Google Drive, Microsoft Office 365, and Zoom facilitate collaboration between students and teachers, allowing them to work together in real time, regardless of location.

Retail

- **E-commerce Platforms**: Cloud computing supports the infrastructure for e-commerce websites, enabling online retailers to scale quickly, handle large volumes of customer traffic, and offer personalized shopping experiences.
- **Customer Data Analytics**: Retailers use cloud computing to analyze customer behavior, preferences, and purchase history, enabling targeted marketing campaigns, product recommendations, and enhanced customer service.
- **Point-of-Sale (POS) Systems**: Cloud-based POS systems allow retailers to track sales, manage transactions, and sync data across multiple store locations in real-time.

Manufacturing

- **IoT and Smart Manufacturing**: Cloud computing powers IoT devices and sensors used in smart factories, enabling manufacturers to monitor equipment performance, track production lines, and analyze operational data for efficiency improvements.
- **Predictive Maintenance**: Cloud-based systems use data analytics to predict when equipment will need maintenance, reducing downtime and preventing costly repairs by detecting potential issues before they become critical.

Government and Public Sector:

- **E-Government Services**: Governments use cloud computing to offer digital services to citizens, such as tax filing, license renewals, and public records access, which enhances convenience and reduces administrative overhead.
- **Disaster Recovery and Business Continuity**: Cloud-based backup systems ensure that government agencies can quickly recover from disasters, maintaining critical services with minimal downtime.

Entertainment and Media:

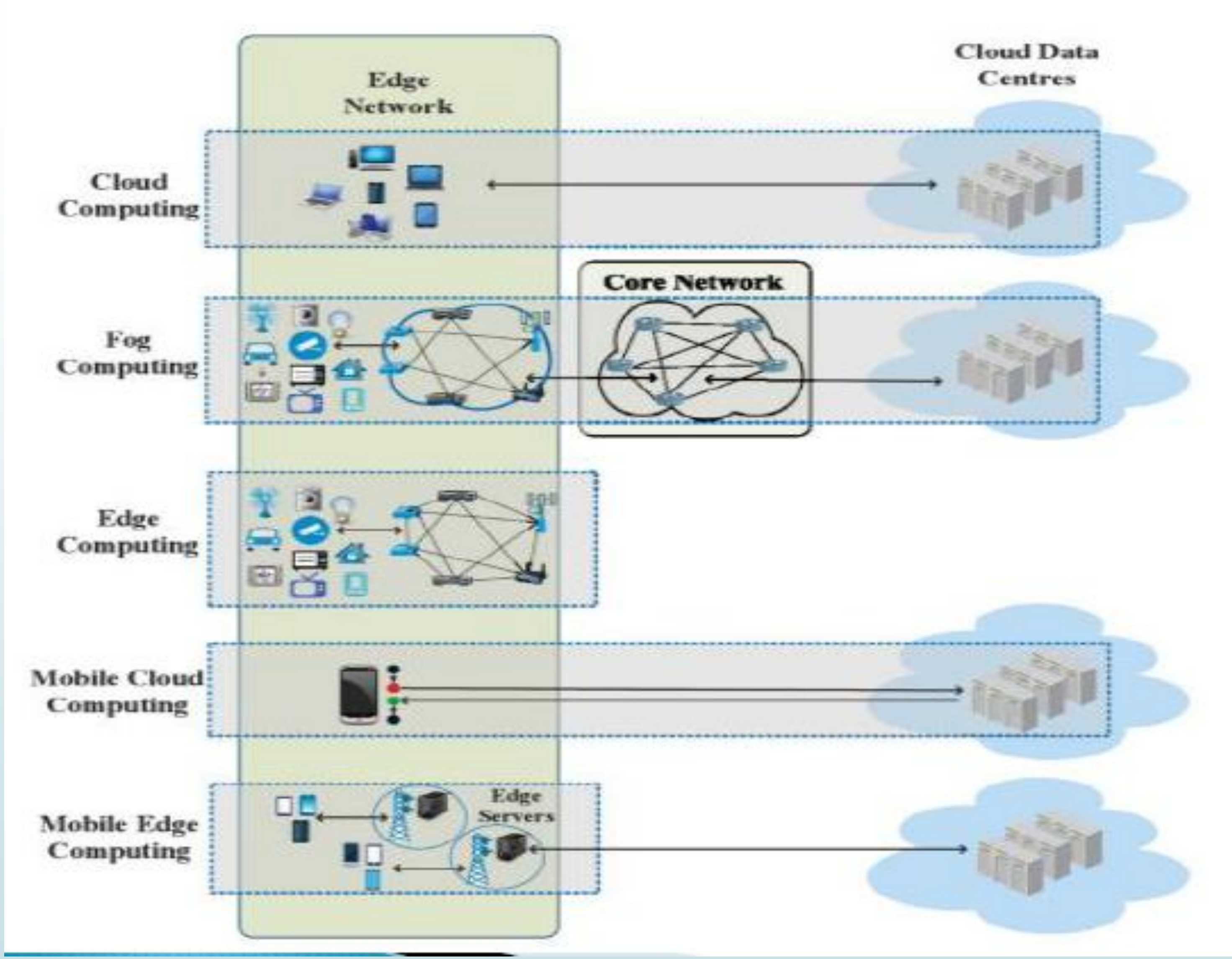
- **Streaming Services**: Cloud computing supports streaming platforms like Netflix, YouTube, and Spotify, providing scalable storage and processing power to deliver content to millions of users simultaneously.
- **Content Creation and Distribution**: Cloud-based tools allow creators to collaborate on video editing, graphic design, and animation in real time. It also enables media companies to distribute content worldwide.
- **Energy and Utilities:**
- **Smart Grids**: Cloud computing supports the development and management of smart grids, which use real-time data to optimize the distribution and consumption of electricity.

Transportation and Logistics:

- **Fleet Management**: Cloud computing helps logistics companies track vehicle locations, monitor fuel consumption, and optimize routes for deliveries in real time.
- **Route Optimization**: Cloud-based systems analyze traffic patterns and weather conditions to suggest the best delivery routes, helping companies reduce fuel costs and improve efficiency.
- **Telecommunications:**
- **Network Management**: Cloud-based solutions help telecom companies manage large-scale networks, monitor performance, and quickly resolve issues without needing extensive on-site infrastructure.

Edge-Computing

- Edge Computing refers to the enabling technologies allowing computation to be performed at the edge of the network, on downstream data on behalf of cloud services and upstream data on behalf of Internet of things services
- Edge Computing refers to applications, services, and processing performed outside of a central data center and closer to end users.



Edge Network
Cloud Data Centres
Cloud Computing
Core Network
Fog Computing
Edge Computing
Mobile Cloud Computing
Mobile Edge Computing
Edge Servers

- (Das, 2023)

Edge computing and IOT

- IOT devices can be used as edge nodes to provide services. As the number of IOT devices continues to grow, IOT and edge computing are likely to become inseparable.
- How does Edge computing work
- **Edge computing** is a distributed computing model that brings computation and data storage closer to the location where it is needed, rather than relying on a central data center that may be far away. This approach helps reduce latency, increase speed, and improve efficiency by processing data locally, right at the "edge" of the network, near the devices that generate it.

How edge computing works

- **Data Collection at the Edge:**
- Devices like sensors, cameras, or IoT (Internet of Things) devices collect data from their environment. This data could be from a factory floor, a smart home, or a fleet of delivery vehicles, for example.
- These devices are often called "edge devices."
- **Local Processing**
- Rather than sending all the raw data to a far-away cloud server, the edge devices or local servers (which can be small, low-power computing devices like gateways or micro data centers) perform some level of data processing right at the edge.

- This local processing allows quick decisions to be made in real-time, without the delay that would occur if the data had to be sent to a central server for processing.

Filtering and Analysis:

- The edge device can filter and preprocess the data to remove unnecessary information. For example, a camera in a factory might only send images to the central server if it detects something unusual.
- This reduces the amount of data that needs to be transmitted, saving bandwidth and lowering network congestion.

Sending Relevant Data:

- After processing and analysis at the edge, only the most important or relevant data may be sent to the cloud or centralized data center for further processing, storage, or more complex analytics.
- For instance, edge devices may detect a problem and then send an alert or a small amount of data (such as sensor readings or images) to a central system for more analysis.

Real-Time Action:

- Edge computing can enable real-time or near-real-time responses. For example, an autonomous vehicle can make immediate decisions about how to avoid obstacles or navigate traffic based on data processed at the edge, without waiting for cloud servers to respond.
- In industrial settings, edge computing might trigger a local action like shutting down equipment to prevent damage based on immediate sensor data.

Key Benefits of Edge Computing

- **Reduced Latency**: Since data is processed locally, the response time is much quicker than if it had to be sent to a distant cloud server.
- **Bandwidth Efficiency**: By processing data locally and only sending relevant or summarized data to the cloud, edge computing reduces the amount of data transferred, saving bandwidth and reducing network congestion.
- **Reliability**: Edge computing can operate even if the network connection to the cloud is slow or temporarily unavailable, since local processing can continue independently.
- **Improved Privacy and Security**: Sensitive data can be kept on local devices rather than transmitted to central servers, reducing potential privacy risks.

Examples of Edge Computing

- **Smart Cities**: Traffic lights and cameras in smart cities can process data locally to adjust traffic patterns or detect accidents in real-time, sending only relevant data to central systems.
- **Healthcare**: Wearable health devices, like fitness trackers or heart rate monitors, process data at the edge to track health in real-time and alert users or medical staff when needed.
- **Industrial IoT**: In factories, machines and sensors can analyze operational data locally, sending alerts if maintenance is needed, which reduces downtime and prevents costly repairs.
- **Autonomous Vehicles**: Self-driving cars rely on edge computing to process data from sensors and cameras in real-time to make driving decisions quickly.

Security and Privacy Concerns:

- **Distributed Security**: Since edge computing involves many distributed devices, each with its own local processing capabilities, securing each device can be complex. If one edge device is compromised, it could provide attackers with access to the entire network.
- **Data Privacy**: Sensitive data might be processed at the edge, and depending on the application, there may be concerns about how that data is stored, accessed, or transmitted. Ensuring compliance with privacy regulations (like GDPR) can be more difficult in decentralized environments.
- **Authentication and Authorization**: Managing authentication across a large number of edge devices can be complex. Ensuring that only authorized devices have access to the system is crucial to prevent unauthorized access and breaches.

Device and Network Heterogeneity

- **Variety of Devices**: Edge computing involves many different types of devices with varying processing power, storage capacity, and operating systems. This makes it difficult to ensure compatibility and standardized management across the network.
- **Scalability:**
- **Managing Large Numbers of Devices**: As edge networks expand, managing a large number of devices becomes increasingly complex. Ensuring consistent performance and security across thousands (or even millions) of edge devices is a significant challenge.
- **Data Synchronization**: Synchronizing data between edge devices and the central cloud (if necessary) can be difficult, especially when there are large amounts of data being generated. Ensuring that data is up-to-date and accurate across distributed devices is crucial for maintaining reliable operations.

Resource Constraints:

- **Limited Processing Power**: Edge devices, especially in remote or resource-constrained environments, often have limited computing power, memory, and storage. This can limit the complexity of algorithms that can be run locally and necessitate offloading tasks to the cloud, which may undermine some of the advantages of edge computing.
- **Complexity in Deployment and Management:**
- **Deployment Challenges**: Deploying edge computing infrastructure requires physical devices to be set up in many locations, which can be costly and time-consuming. Additionally, setting up the right network configuration for efficient data flow between devices and the cloud can be challenging.

Latency and Real-Time Processing

- **Latency vs. Centralized Systems**: While edge computing is designed to reduce latency, there may still be cases where the edge device itself cannot meet the strict real-time processing requirements due to limited resources. Some tasks may still need to be offloaded to the cloud, reducing the advantage of edge computing.
- **Interoperability:**
- **Communication Between Different Edge Devices**: Edge computing environments may involve a variety of different manufacturers, devices, and communication protocols. Ensuring seamless communication and interoperability across all edge devices and systems can be a significant challenge.
- **Data Formats and Standards**: Different edge devices may use different data formats, leading to the need for complex data transformation processes to integrate data from multiple sources. Standardizing data formats and communication protocols across diverse devices is often difficult.

Data Management and Storage

- **Local Data Storage**: Edge devices may need to store data locally due to limited or intermittent connectivity to the cloud. However, managing and ensuring the integrity of data stored across many devices can be challenging.
- **Data Offloading**: In some cases, edge devices may need to offload large volumes of data to the cloud for further processing or long-term storage. This can place significant stress on the network infrastructure, especially if there is limited bandwidth.
- **Cost:**
- **Infrastructure and Hardware Costs**: Setting up a reliable edge computing infrastructure can be expensive, as it involves deploying many distributed devices with local storage, processing power, and networking capabilities.
- **Operational Costs**: Maintaining and monitoring edge computing systems can also incur additional operational costs, including support for hardware upgrades, security management, and ongoing software maintenance.

Regulatory and Compliance Issues

- **Compliance with Regulations**: Since edge computing often processes data in various locations, it can be difficult to comply with data residency and privacy laws. For example, certain regulations may require that data be stored within a specific geographic region, which adds complexity to the management of edge devices.
- **Cross-border Data Flow**: Data generated by edge devices may cross national borders before being processed or stored. This can create legal challenges regarding data sovereignty and the enforcement of local laws.

References

- Buyya, R. (2013). Mastering Cloud Computing. Elsevier Inc.
- Bajaj, D. (2020). Paas Providers And Their Offerings. INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 9, ISSUE 02, 1-8.
- Bhardwaj, S. (2010). CLOUD COMPUTING: A STUDY OF INFRASTRUCTURE AS A SERVICE (IAAS). I nternational Journal of Engineering and I nform at ion Technology, 1-4.
- CHANDRASEKARAN, K. (2015). Essentials of Cloud computing. U.S: taylor anf francisgroup.
- https://www.hufocw.org/Course/1110

Next Lecture

The Internet of Things (IoT) and Smart Systems