Article 2: Cloud Computing Architecture and Security Best Practices

Cloud computing refers to delivering computing services over the internet, including storage, processing, and networking. It enables scalable resources on-demand without owning physical infrastructure.

Cloud Service Models

- **Infrastructure as a Service (IaaS):** Provides virtualized hardware resources.
- **Platform as a Service (PaaS):** Offers platforms to develop and deploy applications.
- **Software as a Service (SaaS):** Delivers software applications over the web.

Cloud Deployment Models

- **Public Cloud:** Services offered over the public internet by providers like AWS and Azure.
- **Private Cloud:** Exclusive infrastructure for one organization.
- **Hybrid Cloud:** Combination of public and private clouds.

Security Considerations

Security in the cloud involves protecting data, applications, and infrastructure from threats. Best practices include:

- **Data Encryption:** Both at rest and in transit.
- **Identity and Access Management (IAM):** Controlling user permissions.
- **Regular Audits:** To monitor compliance and vulnerabilities.
- **Incident Response Planning:** For quick mitigation of breaches.

Emerging Trends

Serverless computing and edge computing are reshaping how cloud resources are utilized, emphasizing efficiency and low latency.