PRACTICAL NO: 07

Aim: Case Study: Amazon Web Services (AWS) SaaS

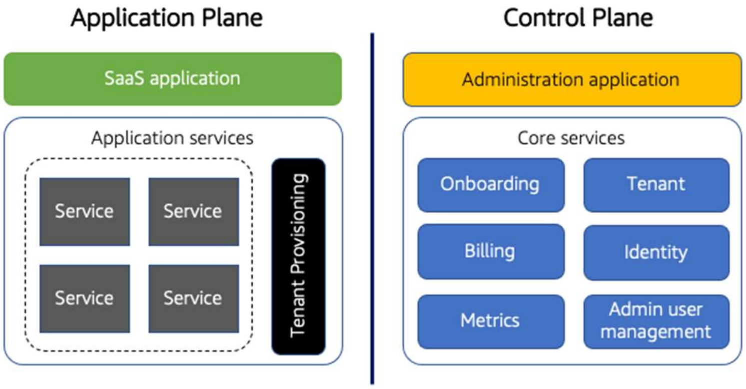
Introduction

Amazon Web Services (AWS) is a prominent example of Software as a Service (SaaS) cloud computing. It offers a wide range of services, from infrastructure to application development, making it a versatile platform for businesses of all sizes. This practical aims to delve into the architecture, working model, service offerings, and security aspects of Amazon AWS.

Basic Architecture of Amazon AWS

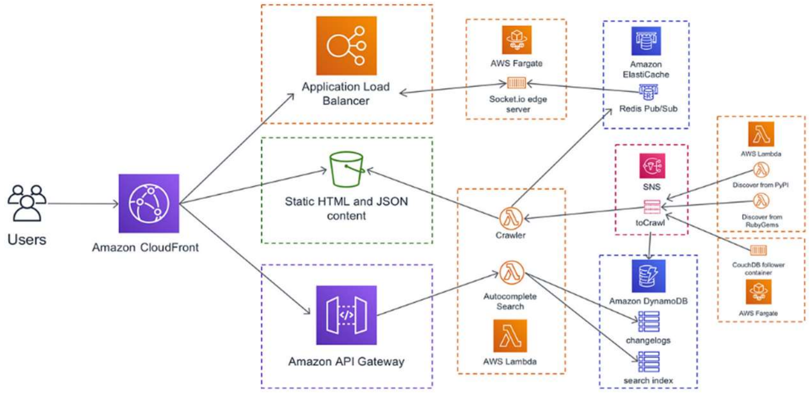
The basic architecture of Amazon AWS consists of the following key components:

1. **Control Plane:** This layer manages and controls the AWS resources, including account management, billing, security, and compliance.



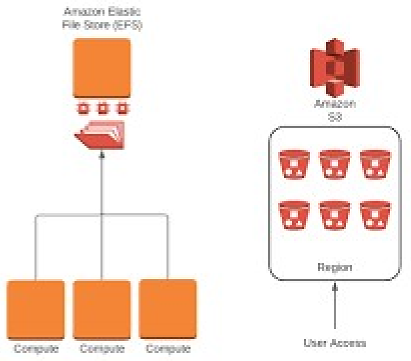
AWS Control Plane

2. **Compute Services:** These services provide the processing power and memory required for applications. Popular options include:
   - **EC2 (Elastic Compute Cloud):** Virtual machines for running various workloads.
   - **Lambda:** Serverless computing platform for executing code without managing servers.
   - **Fargate:** Serverless compute engine for running containers.



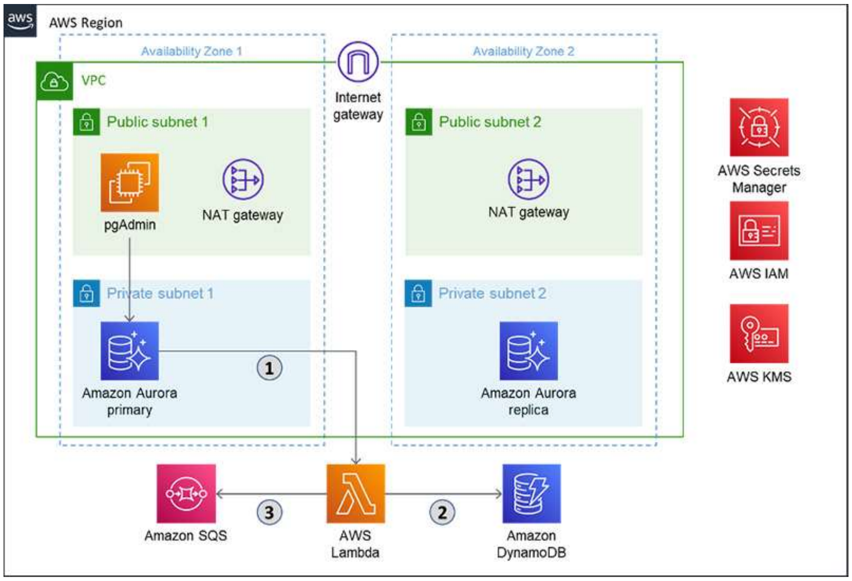
EC2, Lambda, and Fargate architecture

3. **Storage Services:** AWS offers a variety of storage options to suit different needs:
   - **S3 (Simple Storage Service):** Object storage for storing and retrieving data.
   - **EBS (Elastic Block Store):** Block storage for attached to EC2 instances.
   - **EFS (Elastic File System):** File system for shared access across multiple EC2 instances.



S3, EBS, and EFS architecture

4. **Database Services:** AWS provides managed database services, including:
   - **RDS (Relational Database Service):** For relational databases like MySQL, PostgreSQL, and SQL Server.
   - **DynamoDB:** For NoSQL databases.
   - **Aurora:** A high-performance, fully managed relational database.



RDS, DynamoDB, and Aurora architecture

5. **Networking Services:** AWS offers networking capabilities to connect resources and communicate securely:
   - **VPC (Virtual Private Cloud):** A private network within AWS.
   - **EC2 instances:** Can be configured with network interfaces and IP addresses.
   - **Route 53:** DNS service for routing traffic to AWS resources.

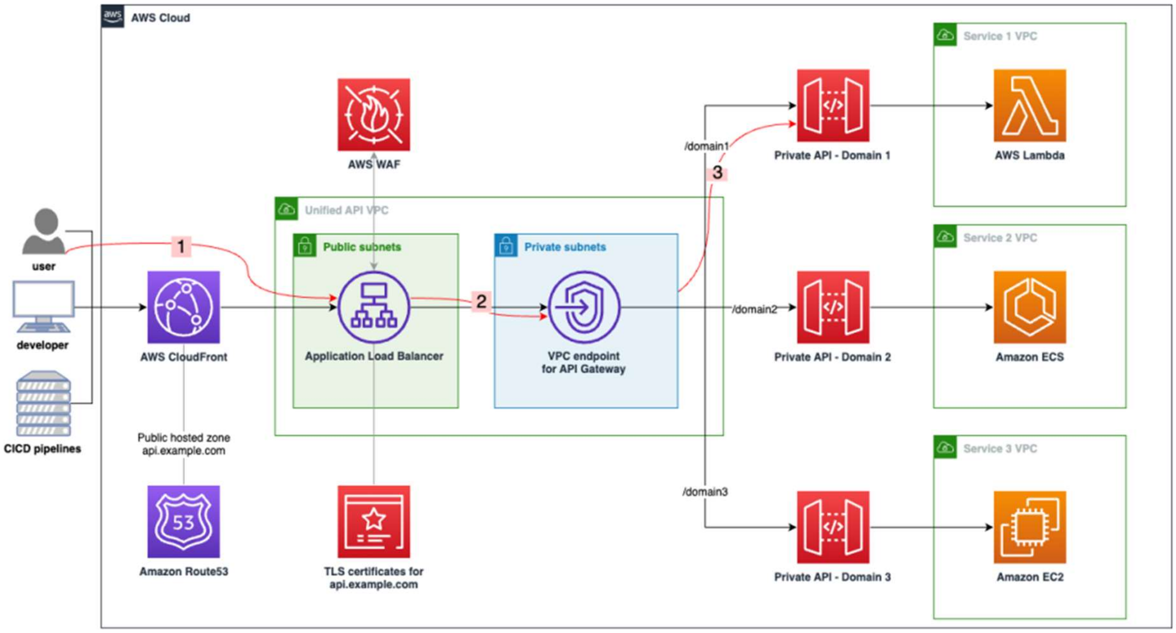
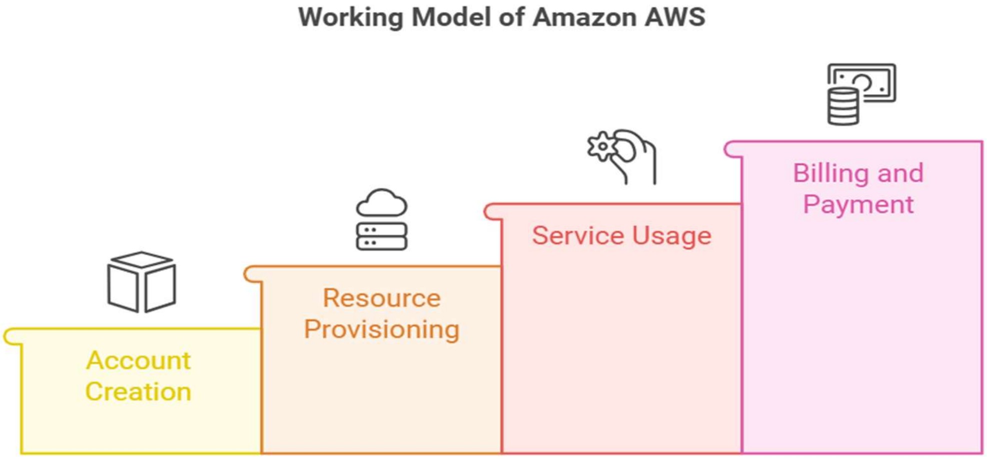


Figure 1. Unified API architecture

VPC, EC2, and Route 53 architecture

Working Model of Amazon AWS

1. **Account Creation:** Users create an AWS account, providing necessary information and payment details.
2. **Resource Provisioning:** Users can choose and provision the required services and resources through the AWS Management Console or API.
3. **Service Usage:** Users access and utilize the services according to their needs, paying only for the resources consumed.
4. **Billing and Payment:** AWS calculates usage and charges based on the pricing model of each service. Payment is typically processed monthly.



Service Offerings in Amazon AWS

Amazon AWS offers a vast array of services, categorized into several categories:

- **Compute:** EC2, Lambda, Fargate, Lightsail
- **Storage:** S3, EBS, EFS, Glacier
- **Databases:** RDS, DynamoDB, Aurora, Redshift
- **Networking:** VPC, Route 53, Elastic Load Balancing
- **Analytics:** Kinesis, Athena, EMR
- **Machine Learning:** SageMaker, Rekognition, Translate
- **Serverless:** Lambda, API Gateway, Step Functions

Freely Available Services:

Some AWS services have free tiers or usage limits, allowing users to experiment and learn without incurring significant costs. These include:

- **EC2:** Free tier for a limited number of hours.
- **S3:** Free tier for the first 5 GB of storage.
- **DynamoDB:** Free tier for a limited number of reads and writes.
- **Lambda:** Free tier for a certain number of requests and compute time.

Security Issues in Amazon AWS

While AWS provides robust security measures, it is essential to address potential security risks:

- **Data Privacy:** Ensuring compliance with data privacy regulations like GDPR and CCPA.
- **Access Control:** Implementing strong access controls to prevent unauthorized access.
- **Encryption:** Encrypting data at rest and in transit to protect against unauthorized access.
- **Patch Management:** Keeping systems up-to-date with security patches.
- **Malware Protection:** Using security tools to detect and prevent malware attacks.
- **DDoS Attacks:** Mitigating Distributed Denial of Service attacks.
- **Shared Responsibility Model:** Understanding the shared responsibility between AWS and the customer for security.

Additional Considerations

- **Cost Optimization:** Implementing strategies to optimize costs, such as using reserved instances, spot instances, and on-demand pricing.
- **Hybrid Cloud:** Integrating AWS with on-premises infrastructure to create a hybrid cloud environment.
- **Migration:** Planning and executing migration strategies to move workloads to AWS.
- **Automation:** Utilizing automation tools to streamline operations and reduce manual tasks.

Conclusion:

Amazon AWS is a powerful and versatile SaaS platform that offers a wide range of services to meet the diverse needs of businesses. By understanding its architecture, working model, service offerings, and security considerations, organizations can effectively leverage AWS to achieve their cloud computing goals.