**Cloud Computing**

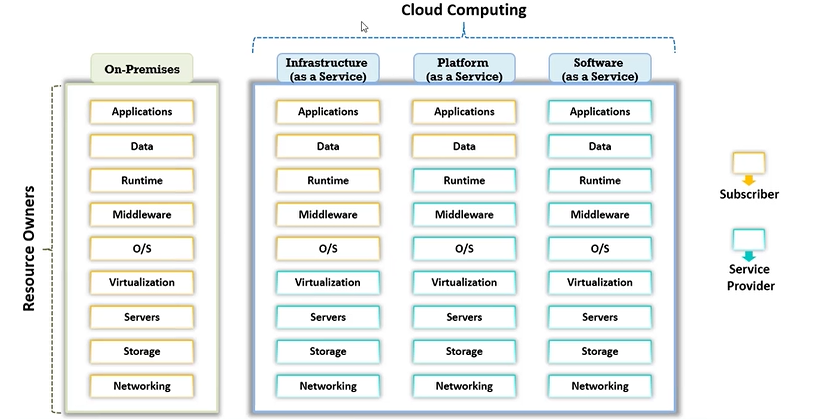
**Introduction to Cloud Computing:**

It is an on-demand delivery of IT capabilities where IT infrastructure and applications are provided to subscribers as a metered service over a network.

Characteristics of Cloud Computing:

* On-demand self-service
* Broad network access
* Distributed storage
* Resource pooling
* Rapid elasticity
* Measured service
* Automated management
* Virtualization technology

**Separation of Responsibilities in Cloud:**



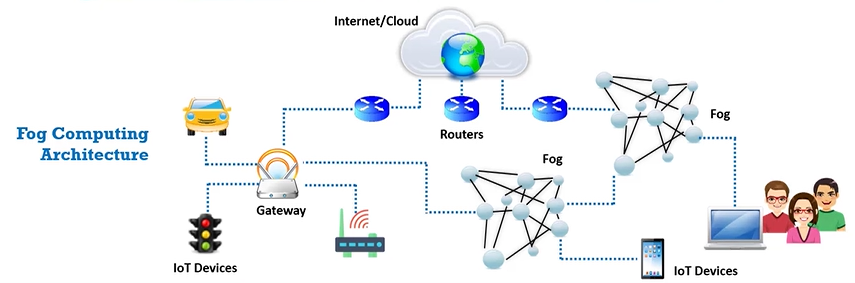
**Cloud Deployment Models:**

* Public Cloud: Services are rendered over a network that is open for public use
* Private Cloud: Cloud infrastructure is operated for a single organization only
* Community Cloud: Shared infrastructure between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.)
* Hybrid Cloud: Combination of two or more clouds (private, community, or public) that remain unique entities but are bound together, thereby offering the benefits of multiple deployment models
* Multi Cloud: Dynamic heterogeneous environment that combines workloads across multiple cloud vendors, managed via one proprietary interface to achieve long term business goals

**Fog Computing:**

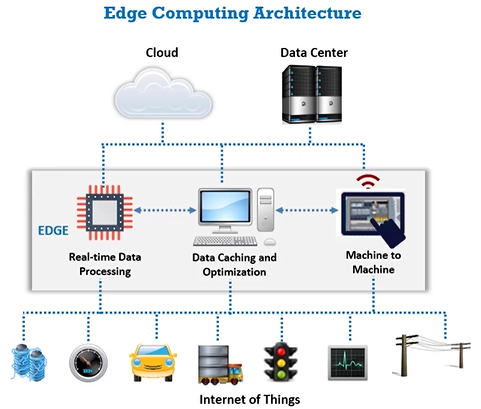
Fog computing extends cloud computing by bringing data processing and storage closer to the devices generating data, often at the edge of the network. It reduces latency, supports real-time analytics, and enhances efficiency in IoT systems by enabling localized computing resources instead of relying solely on centralized cloud infrastructure.

Fog computing operates near data sources, processing data locally or at the network edge, reducing latency and bandwidth usage. Cloud computing centralizes processing and storage in remote data centers, suitable for large-scale analysis but less efficient for time-sensitive or location-specific tasks, making fog ideal for IoT and real-time applications.

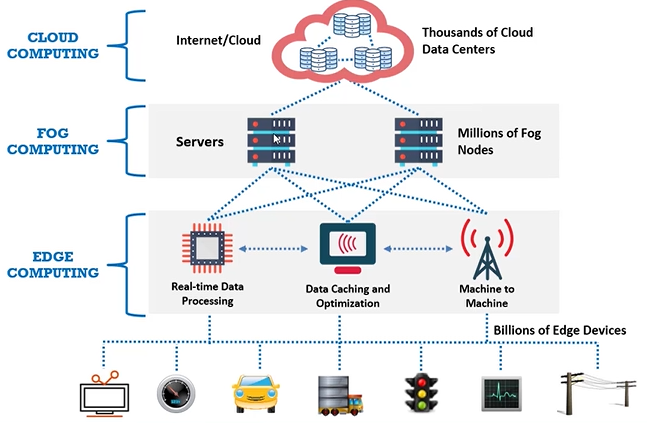


**Edge Computing:**

Edge computing processes data at or near its source, such as IoT devices or local edge servers, rather than relying on distant cloud data centers. This minimizes latency, conserves bandwidth, and enables real-time decision-making, making it ideal for time-sensitive applications like autonomous vehicles, smart cities, and industrial automation.



**Cloud vs. Fog vs. Edge Computing:**



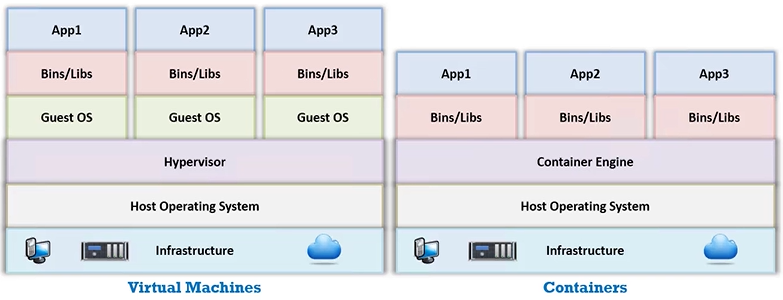
| **Aspect** | **Cloud Computing** | **Fog Computing** | **Edge Computing** |
| --- | --- | --- | --- |
| **Location of Processing** | Centralized in remote data centers | Distributed, near network edge (intermediate) | Directly at the data source (devices) |
| **Latency** | High latency due to distance | Moderate latency | Low latency |
| **Data Storage** | Centralized, large-scale storage | Distributed, partial storage | Localized, minimal storage |
| **Use Case** | Large-scale analytics, non-time-critical tasks | IoT, real-time analytics, hybrid processing | Real-time tasks like autonomous systems |

**What is a Container?**

In cloud computing, a container is a lightweight, portable unit that packages an application and its dependencies, ensuring consistency across different environments. Containers are isolated from one another, run on a shared OS kernel, and enable efficient scaling, deployment, and management of applications in cloud environments like Kubernetes.

**Container vs Virtual Machine:**

| **Aspect** | **Container** | **Virtual Machine** |
| --- | --- | --- |
| **Architecture** | Shares host OS kernel; lightweight isolation | Full OS stack per VM; includes guest OS and kernel |
| **Resource Efficiency** | More efficient, minimal overhead | Heavier, more resource-intensive due to full OS |
| **Startup Time** | Faster (seconds) due to shared OS resources | Slower (minutes) due to full OS boot process |



**What is Docker?**

Docker is an open-source platform that automates the deployment, scaling, and management of applications using containers. It packages applications and their dependencies into containers, ensuring consistency across environments. Docker simplifies application deployment, reduces conflicts, and enhances portability between development, testing, and production environments.

**What is Kubernets?**

Kubernetes is an open-source container orchestration platform for automating the deployment, scaling, and management of containerized applications. It helps manage clusters of containers, ensuring high availability, load balancing, and self-healing. Kubernetes supports complex workloads, enabling efficient scaling and coordination of distributed applications across a variety of cloud environments.

**What is Serverless Computing?**

**Serverless Computing** is a cloud computing model where developers focus solely on writing code without managing server infrastructure. The cloud provider automatically handles the provisioning, scaling, and maintenance of servers. With serverless, you pay only for the exact compute resources used during execution, making it cost-efficient and scalable for event-driven applications.

**Cloud Attacks: Service Hijacking using Social Engineering**

Service hijacking using social engineering involves tricking individuals into revealing their cloud service login credentials. Attackers send phishing links to users, redirecting them to fake login pages. Once users input their credentials, attackers steal them and gain unauthorized access to cloud services, potentially exposing sensitive data like personal o r business information.

**Cloud Attacks: Service Hijacking using Network Sniffing**

**Service Hijacking using Network Sniffing** involves intercepting and monitoring network traffic between cloud nodes. Attackers use packet sniffers to capture sensitive data, such as passwords and session cookies, or security configurations like UDDI, SOAP, and WSDL files. These stolen credentials allow attackers to log into cloud services and gain unauthorized access.

**Cloud Attacks: Side-Channel Attacks or Cross-guest VM Breaches**

**Side-Channel Attacks or Cross-guest VM Breaches** involve an attacker running a malicious virtual machine (VM) on the same physical host as the victim's VM. By exploiting shared resources like the CPU cache, the attacker can steal sensitive data such as cryptographic keys. These attacks exploit vulnerabilities in multi-tenant cloud environments, allowing co-resident users to access the victim's data through techniques like timing attacks, power monitoring, or acoustic cryptanalysis.

**Cloud Attacks: Man-in-the-Cloud (MITC) Attack**

**Man-in-the-Cloud (MITC) Attack** is an advanced form of Man-in-the-Middle (MITM) attacks. The attacker exploits cloud file synchronization services (e.g., Google Drive, Dropbox) by tricking the victim into installing malicious software. This malware plants a synchronization token on the victim's device, which the attacker then steals. Using the stolen token, the attacker gains access to the victim's files for data compromise, exfiltration, or remote access. After completing the attack, the attacker restores the original token, leaving no trace of the compromise.

**Cloud Attacks: Cloud Hopper Attack**

**Cloud Hopper Attack** targets managed service providers (MSPs) and their clients. Attackers use spear-phishing emails with custom malware to compromise MSP staff accounts. Once infiltrated, the attacker gains remote access to MSP systems, extracts sensitive customer data, and stores it for further exploitation. By accessing MSP accounts and network interfaces, attackers can reach customer information, leading to data breaches and further attacks.

**Cloud Attacks: Cloud Cryptojacking**

**Cloud Cryptojacking** is the unauthorized use of a victim's computing resources to mine digital currencies without their consent. Attackers often exploit cloud misconfigurations, compromised websites, or vulnerabilities in client/server systems to embed cryptomining scripts. When a victim connects to the compromised cloud service, their resources are used to mine cryptocurrency, with the attacker receiving the mining rewards. This attack is highly profitable and can involve both external hackers and rogue insiders.

**What is Cloud Hacking?**

**Cloud Hacking** refers to exploiting vulnerabilities in cloud technologies to carry out attacks on cloud storage and services, often with the aim of compromising sensitive data. Attackers target cloud environments to steal, block, or misuse data and resources.

The main goals include gaining unauthorized access, stealing credentials, exfiltrating data, launching DoS attacks, and leveraging cloud resources for illicit activities like cryptocurrency mining.

**Enumerating S3 Buckets:**

**Enumerating S3 Buckets** involves techniques used by attackers to discover and exploit Amazon S3 (Simple Storage Service) buckets for unauthorized access. These buckets store files, folders, and objects, and attackers aim to find the bucket's location and vulnerabilities.

**Common Techniques for Enumerating S3 Buckets:**

1. **Inspecting HTML Source Code**:  
   Attackers analyze the HTML source code of web pages to find hidden URLs that may link to S3 buckets.
2. **Brute-forcing Bucket URLs**:  
   Using tools like **Burp Suite**, attackers perform brute-forcing on the bucket’s URL to guess the correct location.
3. **Finding Subdomains**:  
   Tools like **OWASP Amass** or **Robtex** are used to identify subdomains that may reveal S3 bucket locations.

**Tools:**

* **Amass**: A tool for asset discovery that helps in identifying possible bucket names, subdomains, and related assets. It can perform active scans to find vulnerable configurations.

**Attacker's Goal:**

* **Discovering vulnerable or misconfigured S3 buckets** to steal sensitive data, modify files, or perform other malicious activities.

**Enumerating AWS Account ID**

Enumerating an AWS Account ID involves discovering the unique identifier for an AWS account, which can be exploited to gain insights into the structure of the cloud environment. Attackers may target the Account ID to manipulate services, attempt unauthorized access, or perform targeted social engineering attacks.

**Enumerating IAMs (Identity and Access Management)**

IAM enumeration involves identifying users, roles, and permissions in AWS environments. Attackers perform IAM enumeration to discover privileged users, misconfigurations, or overly permissive roles. This can lead to unauthorized access, privilege escalation, and exploitation of misconfigured permissions, compromising the security of cloud resources.

**Cloud Network Security**

**Virtual Private Cloud (VPC)**

A VPC is a private, secure environment within a public cloud, allowing users to execute programs, store data, and host applications in isolation. Each VPC client has its own dedicated network, enhancing security by isolating workloads from other tenants in the public cloud.

**Public and Private Subnets**

In a VPC, subnets are divided into public and private types. Public subnets allow virtual machines to directly communicate with the internet via an Internet Gateway (IGW). Private subnets, however, use a NAT Gateway to access the internet, providing an additional layer of security by keeping internal instances isolated from direct external access.

**Cloud Access Security Broker (CASB):**

CASBs are security solutions, either on-premise or cloud-hosted, that enforce policies related to security, compliance, and governance for cloud applications. Positioned between cloud service consumers and providers, CASBs monitor and control data traffic, ensuring secure access to cloud resources, and protecting against unauthorized use, data leaks, and breaches. Services like Azure include CASB functionalities for enhanced security management.

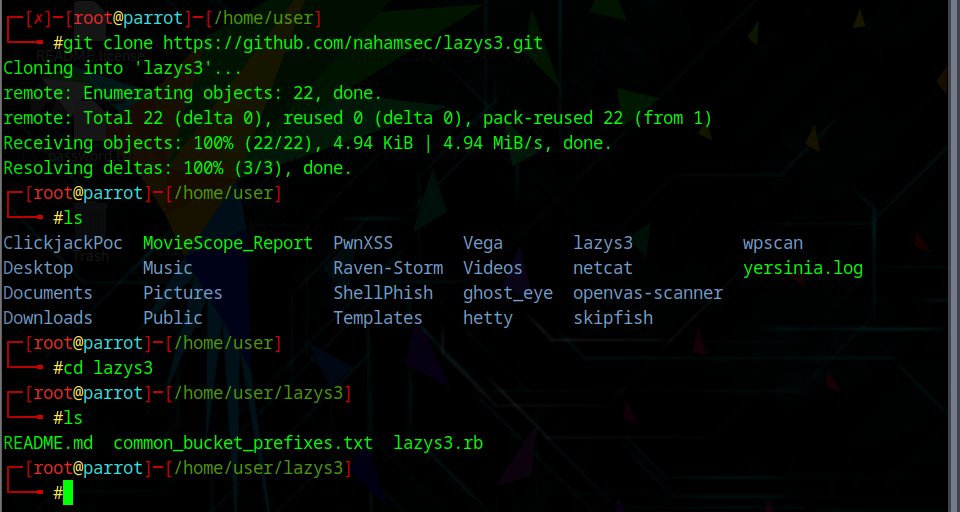
**Next-Generation Secure Web Gateway (NG SWG)**

NG SWG is a cloud-based security solution that protects organizations from cloud-based threats like malware, data theft, and other cyber risks. It ensures secure access to cloud services by inspecting and controlling web traffic in real-time, providing advanced threat protection, data loss prevention (DLP), and secure web access.

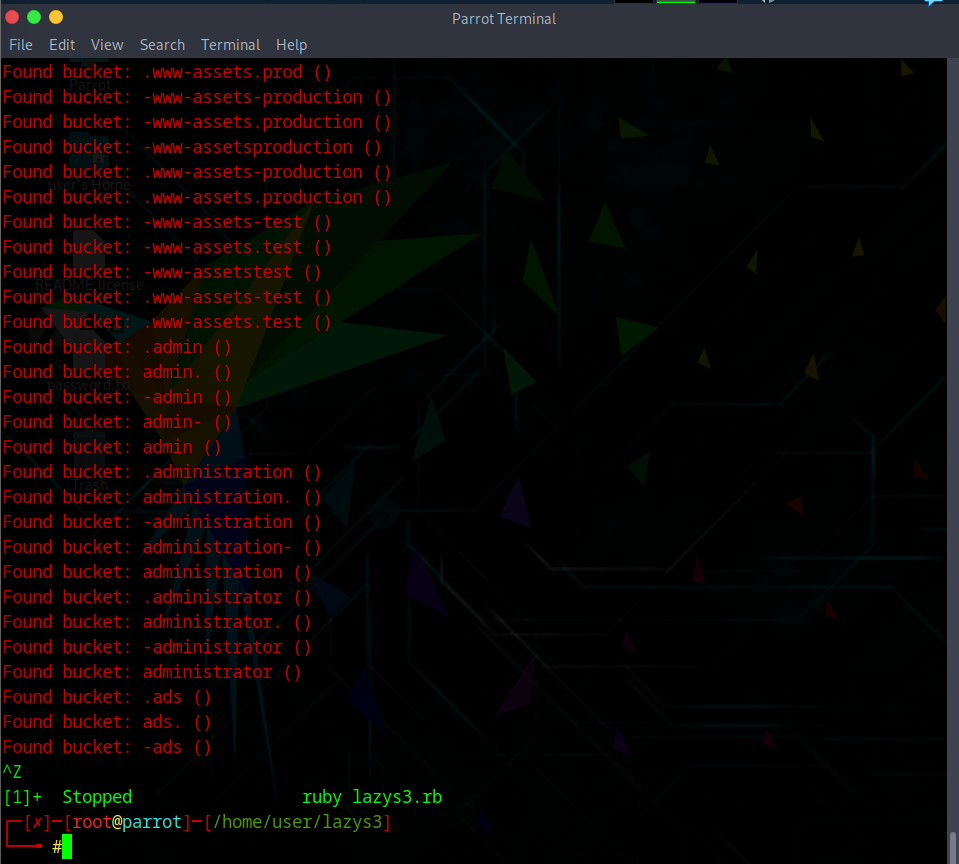
**Key NG SWG Solutions:**

* **Netskope Next-Gen SWG**: Offers advanced threat protection and data security for cloud environments.
* **Cloudflare Gateway**: Provides security, threat intelligence, and secure web access.
* **Checkpoint Quantum Next-Gen Firewall**: Integrates NG SWG features with firewall capabilities for comprehensive web security.

**Enumerate S3 buckets using S3:**

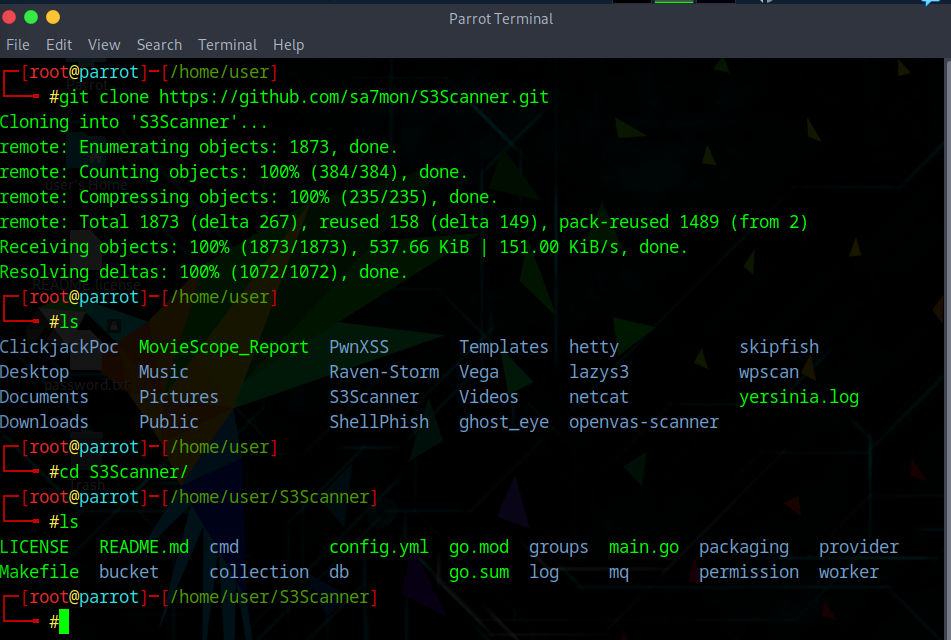




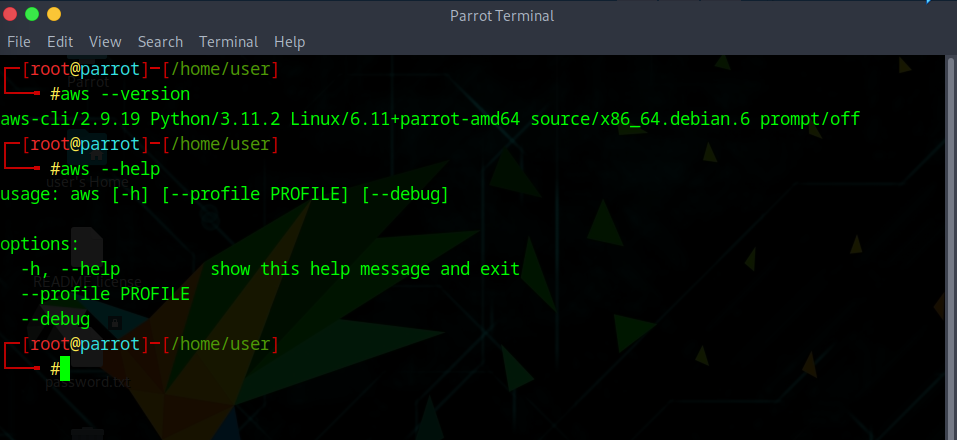


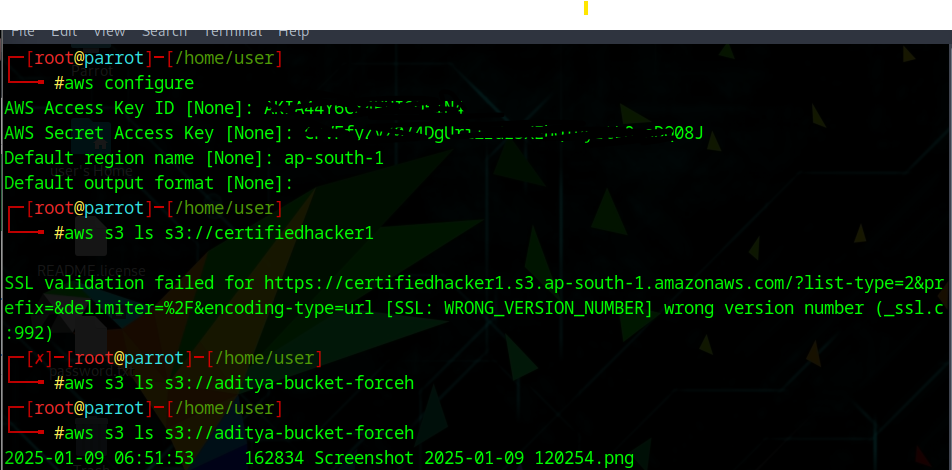


**Enumerate S3 Buckets using S3Scanner:**



**Exploit Open S3 Buckets Using Aws CLI**





**Escalate IAM User Priv. by Exploiting Misconfigured User Policy:**



