



MOBILE CLOUD COMPUTING

Baylee Jones


RESEARCH PROBLEM

**THE SECURITY CHALLENGES (AND
POTENTIAL SOLUTIONS) AFFECTING
CLOUD COMPUTING AND MOBILE CLOUD
COMPUTING**



OUTLINE

- ★ Cloud Computing
- ★ Architecture of Cloud Computing
- ★ Cloud Computing Security Issues
- ★ Proposed Solutions for Security Issues in Cloud Computing
- ★ Cloud Federation
- ★ Mobile Cloud Computing
- ★ Architecture of Mobile Cloud Computing
- ★ Mobile Cloud Computing Security Issues
- ★ Proposed Solutions for Security Issues in Mobile Cloud Computing
- ★ Future Work



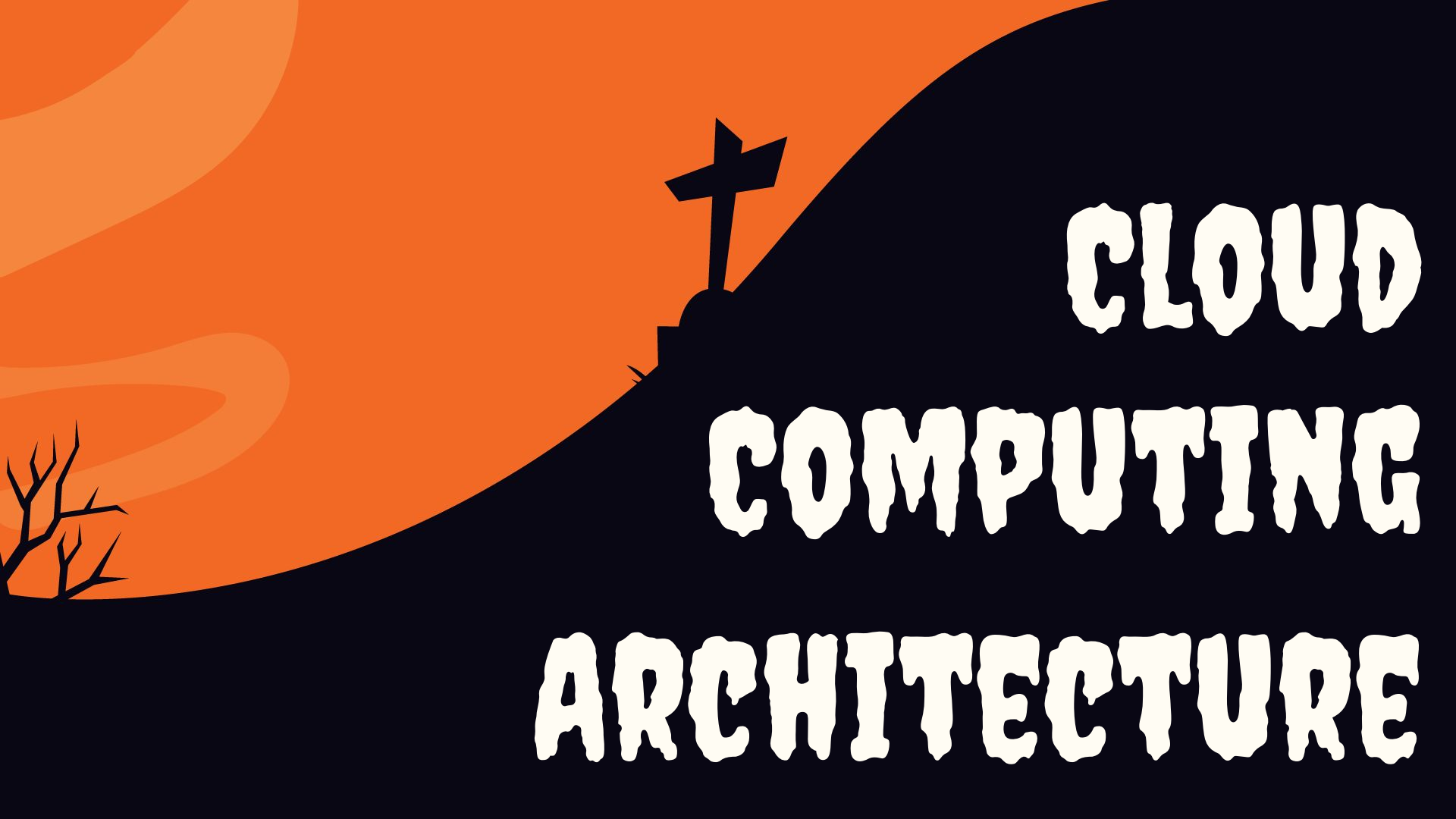
CLOUD COMPUTING

DEFINITION OF CLOUD COMPUTING [5]

- ★ Computing services that are accessed on-demand by customers and provided within a cloud infrastructure so that customers do not have to be worried about the details of service provisioning (Moura and Hutchison, 2016)
- ★ A parallel and distributed computing system made up of virtualized, interconnected computers that are dynamically provisioned and presented as a unified resource based on service-level agreements (SLAs) created amongst the service provider and consumers (Buyya et al., 2009)
- ★ A model that facilitates on-demand network access to shared, configurable computing resources (like networks, servers, and services) and can be quickly provisioned and released with minimal management or service provider engagement (NIST in Mell and Grance, 2011)

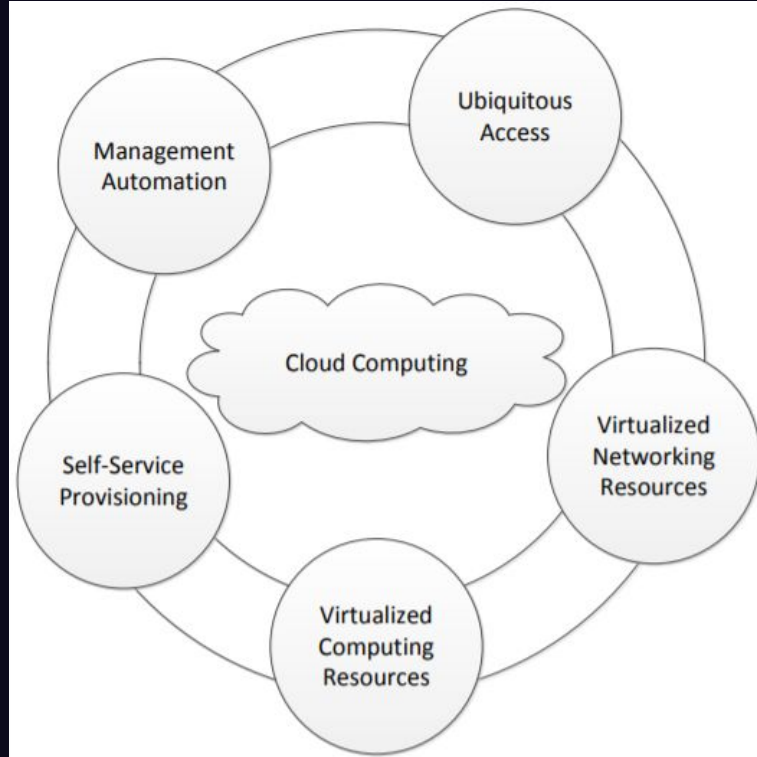
HYPERVERSOR / VIRTUAL MACHINE MONITOR (VMM) [5]

- ★ Hypervisor is a software that creates and runs VMs
- ★ It allows one computer to host multiple VMs by virtually sharing its resources
- ★ Three types of hypervisors based on where the entity is running:
 - Type 1: the hypervisor is running directly above the hardware of the host machine
 - Type 2: the hypervisor is running directly above the operating system of the host machine
 - Type 3: the hypervisor is running at the same layer as the host operating system



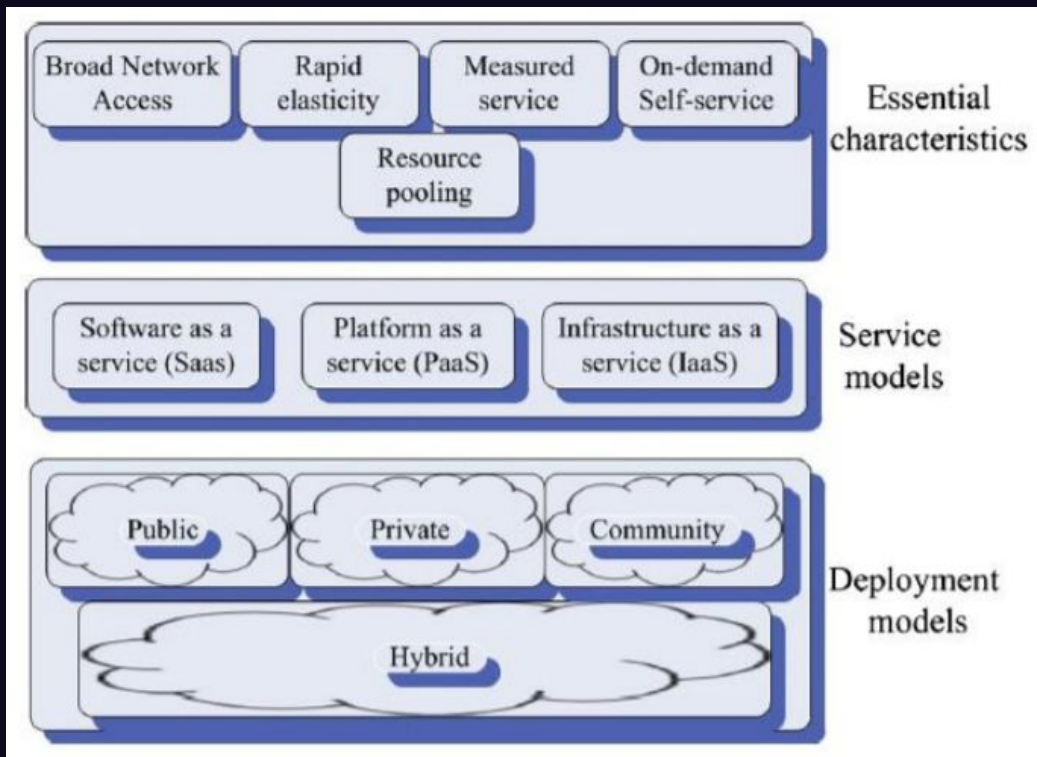
**CLOUD
COMPUTING
ARCHITECTURE**

ARCHITECTURAL FOUNDATION ELEMENTS OF CLOUD COMPUTING [5]



- ★ Virtualization offers advances in security, reliability, compatibility, utilization, maintenance, load-balancing, and problem recovery

NIST DEFINITION OF CLOUD COMPUTING [2]



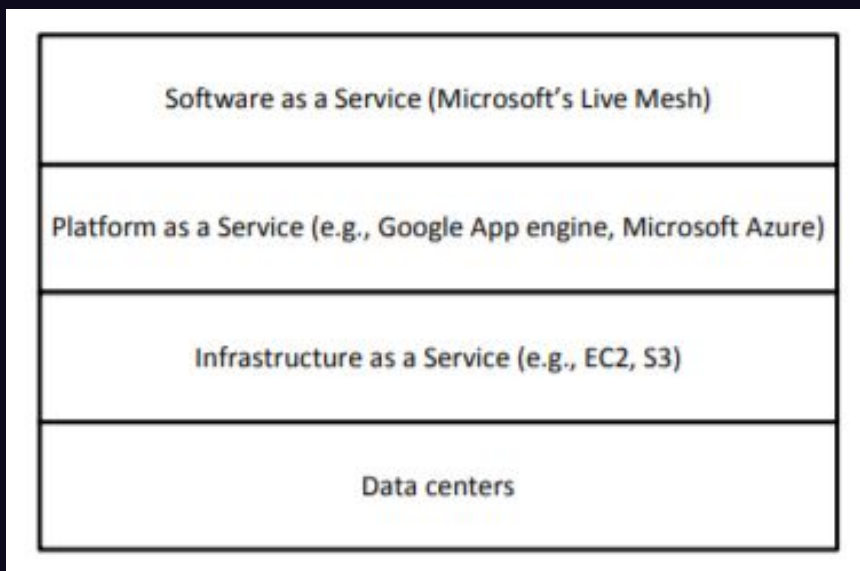
NIST DEFINITION OF CLOUD COMPUTING – ESSENTIAL CHARACTERISTICS [2]

- ★ Broad Network Access:
 - Services are accessible over the network to customers through standard mechanisms using thin or thick clients (smartphones, tablets, workstations)
 - Ubiquitous network access
- ★ Rapid Elasticity:
 - Resources can be easily and flexibly scaled and released based on customer's needs
 - To customers, resources seem infinite and can be used at any time
- ★ Measured Service:
 - Resources are optimized by using metering
 - Usage is reported to provider and customer to give transparency
 - Pay-per-use similar to utility services like water and electricity

NIST DEFINITION OF CLOUD COMPUTING – ESSENTIAL CHARACTERISTICS [2]

- ★ On-Demand Self-Service:
 - Customers can access services without needing human interaction
 - Resources are provisioned and de-provisioned automatically as needed
- ★ Resource Pooling:
 - Resources are shared amongst many customers using a multi-tenant model
 - Physical and virtual resources are assigned based on demand
 - Customers generally do not know the exact location of resources but can specify a more broad location if needed, such as country

DEFINITION OF CLOUD COMPUTING – SERVICE MODELS [3]



- ★ Each layer builds on top of the one below it
- ★ Data centers provide infrastructure for the cloud
- ★ The other three layers (IaaS, PaaS, and SaaS) will be discussed in the next slides

SOFTWARE-AS-A-SERVICE [2] [5]

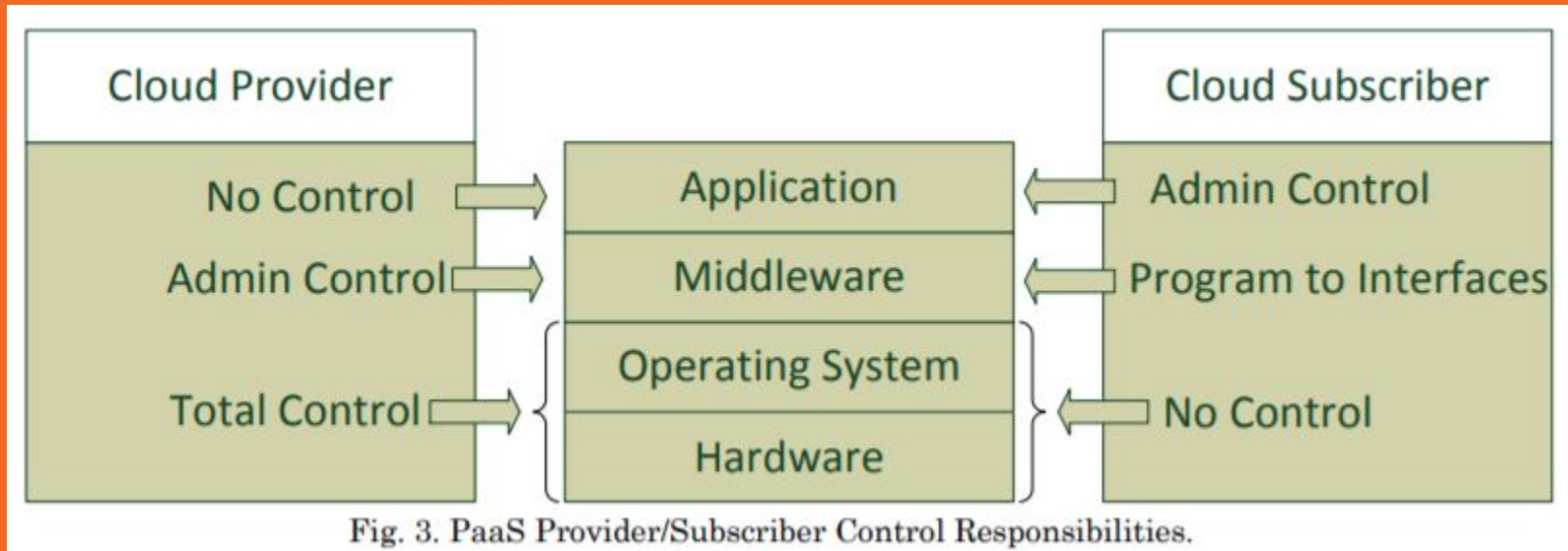
- ★ The capability provided to the customer is to use the provider's applications running on a cloud infrastructure
- ★ These applications are available from various client devices through either a thin client interface (e.g., web-based email using a web browser) or a program interface
- ★ The customer does not control the cloud infrastructure (including network, servers, operating systems, storage, or individual application capabilities)



Fig. 2. SaaS provider/subscriber control responsibilities.

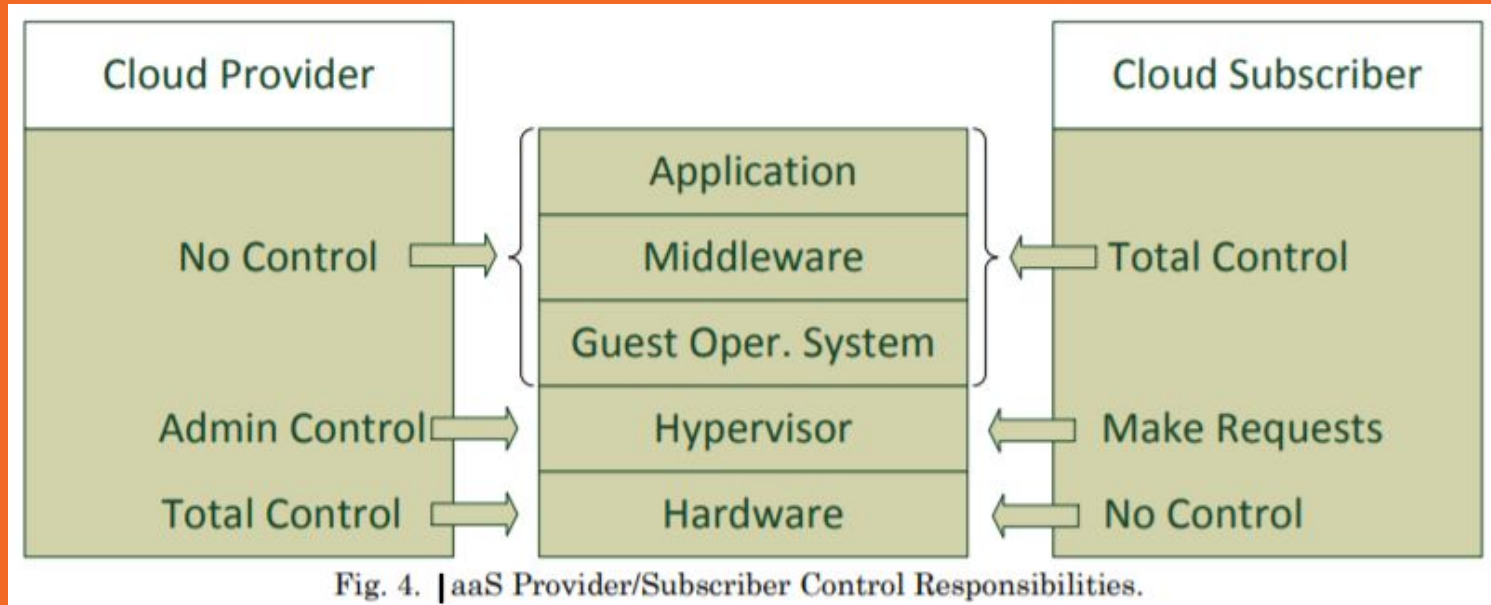
PLATFORM-AS-A-SERVICE [2] [5]

- ★ The capability provided to the customer is to deploy customer-created applications onto the cloud infrastructure using tools supported by the provider
- ★ The customer does not control the cloud infrastructure (including network, servers, operating systems, or storage) but does have control over the deployed applications



INFRASTRUCTURE-AS-A-SERVICE [2] [5]

- ★ The capability provided to the customer is to provision computing resources where the customer can deploy and run any software, including operating systems and applications
- ★ The customer does not control the cloud infrastructure but does have control over the operating system, storage, and deployed applications



NIST DEFINITION OF CLOUD COMPUTING – DEPLOYMENT MODELS [2]

- ★ Private Cloud:
 - Cloud infrastructure is exclusively used by a single organization
 - May be owned and managed by the organization or a third party
- ★ Community Cloud:
 - Cloud infrastructure is exclusively used by a specific community of customers that have shared concerns (e.g., mission, security, and policy)
 - May be owned and managed by one or more of the organizations in the community or a third party

NIST DEFINITION OF CLOUD COMPUTING – DEPLOYMENT MODELS [2]

★ Public Cloud:

- Cloud infrastructure is open for use by the general public
- May be owned and managed by a business, academic, or government organization

★ Hybrid Cloud:

- Cloud infrastructure is a combination of two or more of the above cloud infrastructures
- The clouds remain unique entities but come together by standardized technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds)



ADVANTAGES AND DISADVANTAGES OF CLOUD COMPUTING

ADVANTAGES OF CLOUD COMPUTING [1]

- ★ Unlimited storage capacity
- ★ Increased data safety
- ★ Improved performance
- ★ Easier group collaboration
- ★ Removes limits to specific devices

DISADVANTAGES OF CLOUD COMPUTING [1]

- ★ Requires a constant Internet connection
- ★ Does not work well with low-speed connections
- ★ Features might be limited
- ★ Stored data might not be secure
- ★ No solution if the cloud loses your data



**SECURITY
ISSUES WITH
CLOUD COMPUTING**

SECURITY ISSUES WITH CLOUD COMPUTING [2]

- ★ Communication Security
- ★ Architectural Security
- ★ Contractual and Legal Aspects

COMMUNICATION SECURITY CHALLENGES [2]

- ★ Two types of communication: external (between the customer and the cloud) and internal (between the cloud and its infrastructure)
- ★ External communication has the same security challenges as any communication over the internet:
 - Denial of Service, spoofing, eavesdropping, etc.
- ★ Therefore, it has the same solutions as well:
 - Packet filtering, authentication, encryption, etc.
- ★ Internal communication creates cloud-specific challenges:
 - Shared network infrastructure
 - Virtual network
 - Security misconfiguration

COMMUNICATION SECURITY CHALLENGES [2]

- ★ Shared Communication Infrastructure:
 - Resource pooling allows for sharing of network infrastructure to occur, which provides attackers the window for a cross-tenant attack
 - Other tenants on the same cloud access your data
 - Scanning is usually not allowed because it is hard to distinguish between attackers and customers accessing a component
- ★ Virtual Network:
 - Security mechanisms on a physical network cannot monitor the traffic over a virtual network
 - If a virtual network is shared on multiple VMs, attacks such as trafficking monitoring and sniffing can occur
 - Data being transferred by customers can be a potential target in breaches

COMMUNICATION SECURITY CHALLENGES [2]

- ★ Security Misconfigurations:
 - The smallest misconfiguration can hurt the security of a system
 - A system's configuration must be modified and updated when any changes are done to the system (e.g., when a system's traffic patterns change)
 - Any weaknesses in the configuration can be exploited in session hijacking, which can lead to attackers gaining sensitive data from users

ARCHITECTURAL SECURITY CHALLENGES [2]

- ★ Virtualization Issues
- ★ Data and Storage Issues
- ★ Web Application and API Security
- ★ Identity Management and Access Control

VIRTUALIZATION ISSUES [2]

- ★ VM Image Sharing:
 - Users can upload and download images from the repository
 - Attackers can upload images that contain malware
- ★ VM Isolation:
 - All VMs using the same hardware need to be isolated from each other
 - If not, since they would be using the same physical resources, data breaches and cross-VM attacks could occur
- ★ VM Escape:
 - Attackers escape from the control of the hypervisor, which can lead to them gaining access to other VMs
- ★ VM Rollback:
 - Rollbacks can restore previous vulnerabilities

VIRTUALIZATION ISSUES [2]

- ★ VM Migration:
 - Relocating a VM to another physical machine without shutting down
 - Data and code of the VM become vulnerable during this transition
 - Reasons for migration can include maintenance and load balancing
- ★ Hypervisor Issues:
 - The hypervisor is responsible for VM management and isolation, so if compromised, a large-scale attack can occur
- ★ VM Sprawl:
 - When the number of VMs on a host machine is continuously increasing, and the new VMs are in an idle state
 - Causes resources of the host machine to be wasted

DATA AND STORAGE ISSUES [2]

- ★ Cloud computing does not give customers full control over their data
- ★ Data Privacy and Integrity:
 - The security strength of the cloud equals the security strength of the weakest entity
 - A successful attack on one entity can give unauthorized access to data of all the customers
 - Cryptographic key generation and management is not standardized for cloud computing

DATA AND STORAGE ISSUES [2]

- ★ Data Recovery Vulnerability:
 - An attacker can use data recovery techniques to get the data of the previous customer
- ★ Improper Media Sanitization:
 - If a device is not sanitized properly by the provider, data can be exposed to risks
- ★ Data Backup:
 - Regular backups by the provider are needed
 - The backups also need to be protected from attacks

WEB APPLICATION AND API SECURITY [2]

- ★ Top Ten Risks in Web Applications:
 1. Injection (e.g., SQL)
 2. Broken authentication and session management
 3. Cross-site scripting (XSS)
 4. Insecure direct object references
 5. Security misconfiguration
 6. Sensitive data exposure
 7. Missing function level access control
 8. Cross-site request forgery (CSRF)
 9. Using known vulnerable components
 10. Invalidated redirects and forwards

WEB APPLICATION AND API SECURITY [2]

- ★ Traditional security measures cannot be used in the cloud environment because the risks of web applications in the cloud are much greater
- ★ The provider can publish their APIs to show off the features of their cloud
 - It helps potential customers to know the functions of the cloud
 - However, it exposes the architecture to potential attackers

IDENTITY MANAGEMENT AND ACCESS CONTROL [2]

- ★ A cloud needs dynamic, fine-grained, and strict access controls to manage unauthorized operations happening in the cloud
- ★ A cloud also needs a management system so that it can quickly update access control policies
- ★ Examples of weak identity management include insufficient authorization checks and a weak credential reset process

CONTRACTUAL AND LEGAL CHALLENGES [2]

- ★ When an organization joins the cloud, all of its data and applications move to the administrative control of the provider
- ★ Service-Level Agreements (SLAs):
 - Document that specifies the terms and conditions between the customer and provider
 - Indicates the minimum performance level expected of the provider and consequences in case the agreement is breached
- ★ Legal Issues:
 - Data may be present in multiple locations with different laws about digital security
 - Hardware of the provider may be seized because of one customer, but then data of all customers are at risk of a privacy breach



**SOLUTIONS TO
CLOUD COMPUTING
SECURITY CHALLENGES**

SOLUTIONS TO COMMUNICATION CHALLENGES [2]

- ★ A combination of virtual LANs, intrusion detection and prevention systems, and firewalls are recommended to protect data in transit
- ★ Advanced Cloud Protection System (ACPS):
 - Aims to provide greater security for cloud resources
 - It is divided into multiple modules, all located at the host platform
 - The interceptor module detects any suspicious activity at the host
 - The warning recorder module logs the detected suspicious activity and stores it in the warning pool
- ★ CyberGuarder:
 - Provides virtual network security by deploying virtual network devices
 - Implements isolation through VPNs

SOLUTIONS TO COMMUNICATION CHALLENGES [2]

- ★ DCPortalsNg:
 - Technique to isolate virtual networks for various VMs
 - Prevents cross-VM DoS attacks
- ★ SnortFlow:
 - Utilizes features of Snort and OpenFlow for intrusion prevention within the cloud environment

SOLUTIONS TO ARCHITECTURAL CHALLENGES [2]

- ★ Encrypted Virtual Disk Images in Cloud (EVDIC):
 - Uses advanced encryption standard (AES) with a key size of 256 bits to secure the VM images on the disk
- ★ CloudSec:
 - Monitors a VM's physical memory by using VM inspection techniques
 - After a VM launches, it identifies the memory layout of the hardware by inspecting the control registers of the CPU and requests the Kernel Structure Definition (KSD) from the hypervisor
 - Then, it maps the physical memory to the KSD, which generates the OS view of the VM
- ★ HyperCheck:
 - Ensures a secure execution of the hypervisor
 - Utilizes registers to detect and monitor

SOLUTIONS TO ARCHITECTURAL CHALLENGES [2]

- ★ SecCloud:
 - Secures user data and computations performed in the cloud
 - Uses bilinear Diffie-Hellman for key management
- ★ Security-as-a-Service (SECaaS)
- ★ Simple Privacy-Preserving Identity-Management for Cloud Environment (SPICE):
 - Exploits the concept of group signature and randomization
 - Provides anonymous authentication, unlinkability, and accountability

SOLUTIONS TO CONTRACTUAL AND LEGAL CHALLENGES [2]

- ★ SecAgreement:
 - Lays out the security parameters and services for provision in the SLA
- ★ SPECS:
 - SLA-based approach for Security-as-a-Service
 - Divides the SLA lifecycle into three stages: negotiation, enforcement, and monitoring



**CLOUD
FEDERATION**

CLOUD FEDERATION [5]

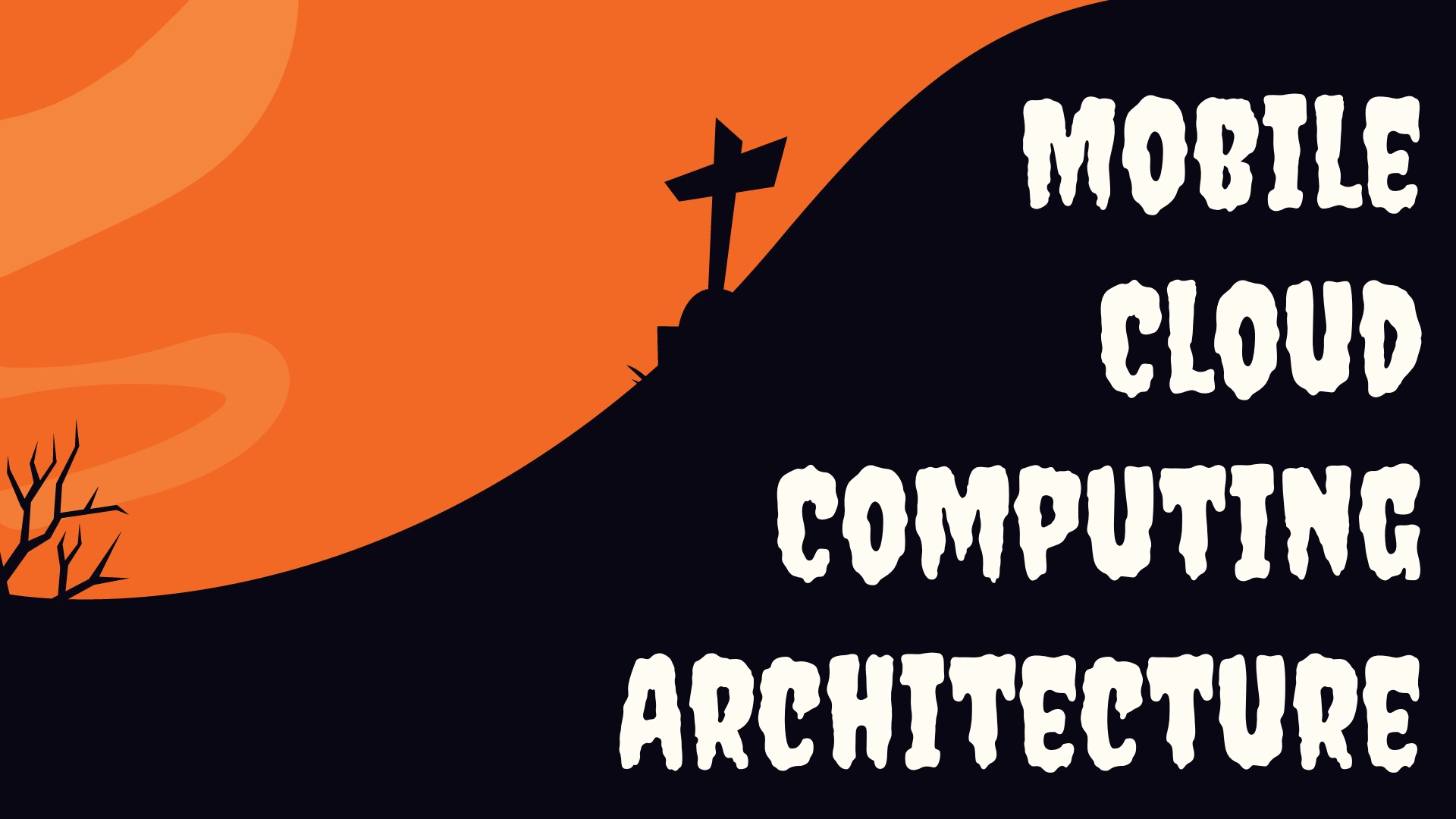
- ★ Manages access controls and consistency when two or more independent clouds share resources (Sridhar, 2009)
- ★ Since customers could need services from multiple providers, it is better for them, as a business, to cooperate and create compatible APIs



**MOBILE
CLOUD
COMPUTING**

MOBILE CLOUD COMPUTING

- ★ Technology that allows users to access cloud services through mobile devices [1]
 - Generalized so that all architectures and points-of-view can be included
- ★ The integration of cloud computing into a mobile environment [3]
- ★ An infrastructure where data storage and processing occur outside the mobile device. Mobile cloud applications put computing power and data storage in the cloud rather than in mobile phones. (Mobile Cloud Computing Forum)

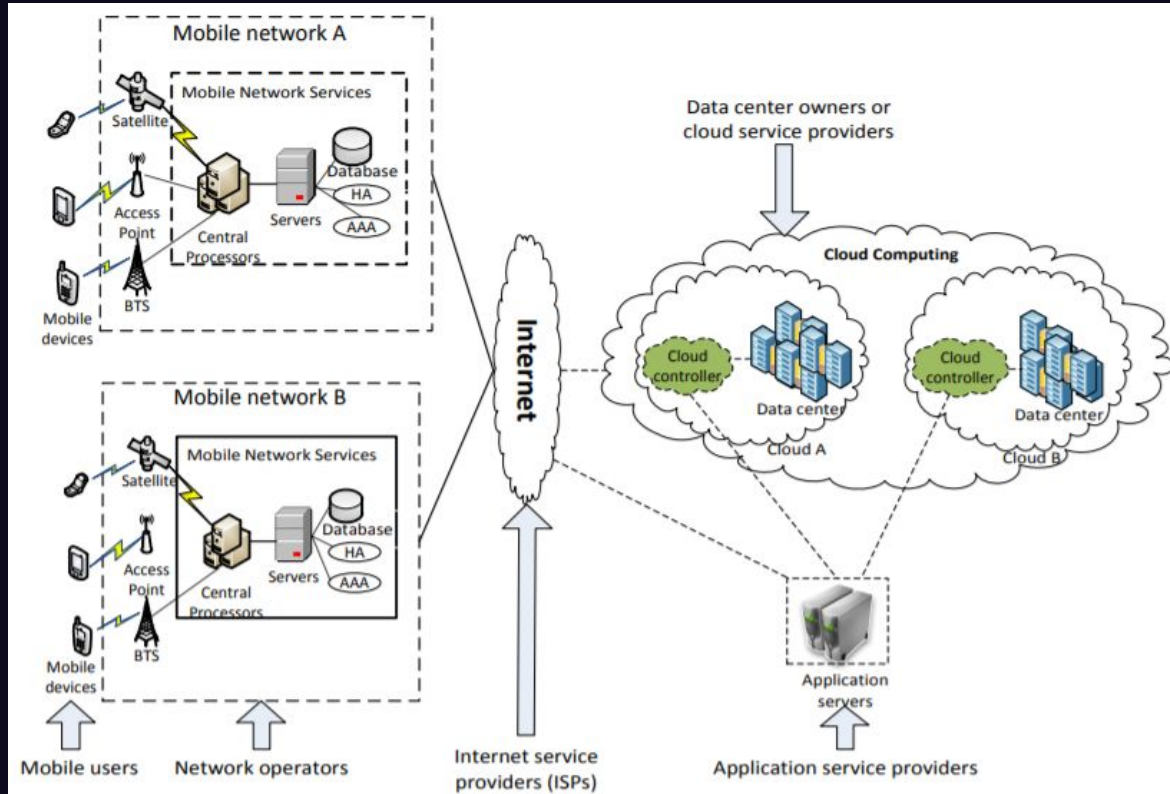


**MOBILE
CLOUD
COMPUTING
ARCHITECTURE**

MOBILE CLOUD COMPUTING ARCHITECTURE

- ★ Mobile cloud is controversial because researchers expect one architecture to be adequate for all mobile applications. No architecture can meet this standard; therefore, there is no architectural framework that has been standardized. [1]
- ★ [3] presents a general architecture of mobile cloud computing

MOBILE CLOUD COMPUTING ARCHITECTURE [3]



MOBILE CLOUD COMPUTING ARCHITECTURE [3]

- ★ Mobile devices are connected to mobile networks through base stations (e.g., base transceiver station (BTS), access point, or satellite)
- ★ The base stations create and control the connections (air links) and functional interfaces between the networks and mobile devices
- ★ Mobile users' requests and information are transmitted to the central processors, which are connected to servers that provide mobile network services
- ★ The mobile network operators at the servers can provide services to the users as AAA (giving authentication, authorization, and accounting) based on the home agent (HA) and users' data stored in databases
- ★ The users' requests are taken to the cloud through the Internet
- ★ Once in the cloud, cloud controllers analyze the request to give the user the correct cloud services



**SECURITY
ISSUES WITH
MOBILE CLOUD
COMPUTING**

SECURITY ISSUES WITH MOBILE CLOUD COMPUTING [2]

- ★ Mobile cloud computing inherits the security issues that come with cloud computing
- ★ It also has restrictions dealing with resources such as less storage capacity
- ★ Mobile App Security:
 - Traditional security software, such as antivirus, cannot be run continuously on mobile devices
 - Can utilize computational offloading to run heavy security programs on mobile devices

SECURITY ISSUES WITH MOBILE CLOUD COMPUTING [2]

- ★ User Privacy:
 - Mobile devices can cause location leakage through location-based services
 - Location cloaking can be used to prevent this by hiding the exact geographical location
- ★ Authentication:
 - Dynamic credential generation is a secure way to authenticate users and can be offloaded to a third party
- ★ Data Security:
 - Computationally intensive encryption algorithms with large keys are not feasible for mobile devices
 - Encryption and decryption can be done by a third party to secure user's data

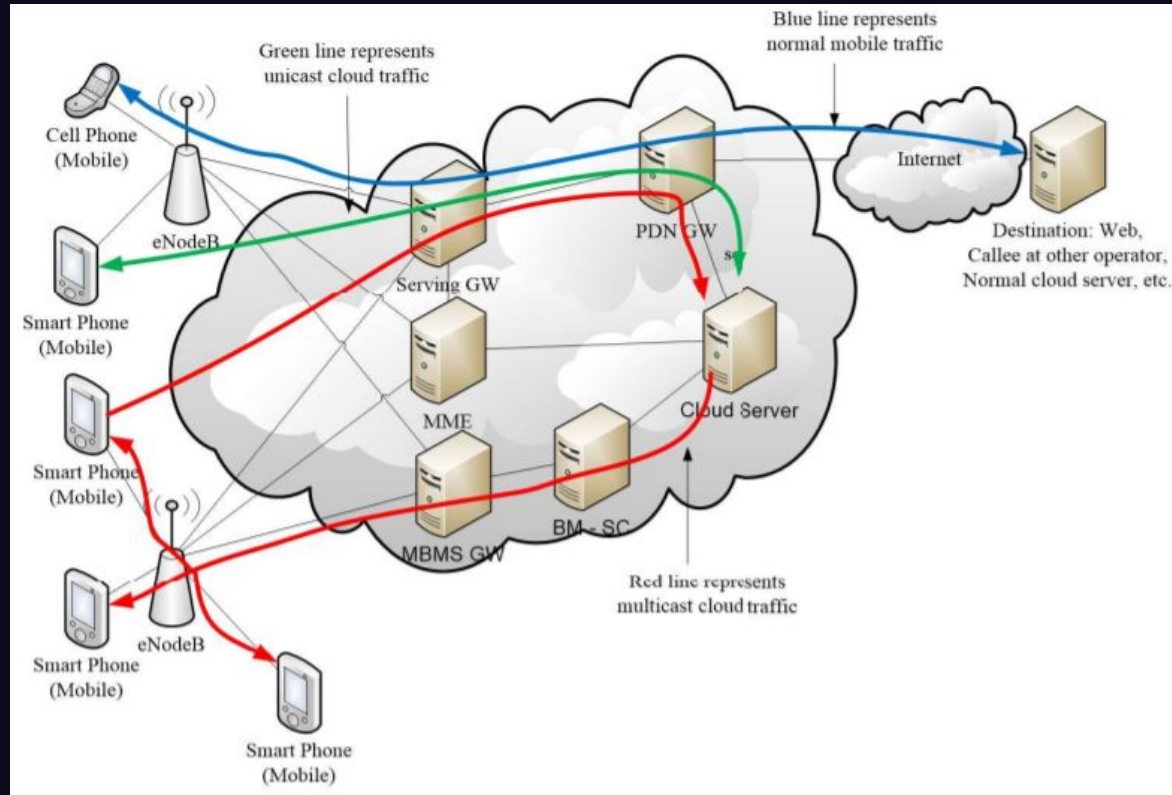


**SOLUTIONS
TO MOBILE
CLOUD COMPUTING
SECURITY CHALLENGES**

SOLUTIONS TO MOBILE CLOUD COMPUTING SECURITY CHALLENGES

- ★ Two architectures have been proposed for secure mobile cloud computing:
 - Operator Centric Mobile Cloud Architecture (OCMCA) [1]
 - CDN-as-a-Service [4]

OCMCA [1]



OCMCA [1]

- ★ Connects a customer and provider from opposite sides of the architecture and hosts a cloud within its network
- ★ Uses powerful cloud servers that are near mobile devices
 - Decrease delay
- ★ Offloads complex jobs onto the powerful servers
 - Decreases the power consumed by mobile devices while waiting for a reply
- ★ Uses multicast traffic when possible
 - Decreases users' costs and increases operator's revenues
- ★ Positions cloud servers in trusted environments
 - Increases privacy
- ★ Uses the mobile network to connect between cloud servers and users
 - Increases mobility
- ★ Uses cloud servers accessible by any user connected to the mobile operator's network with high bandwidth and low latency to provide scalability
 - Can increase scalability through cloud federation

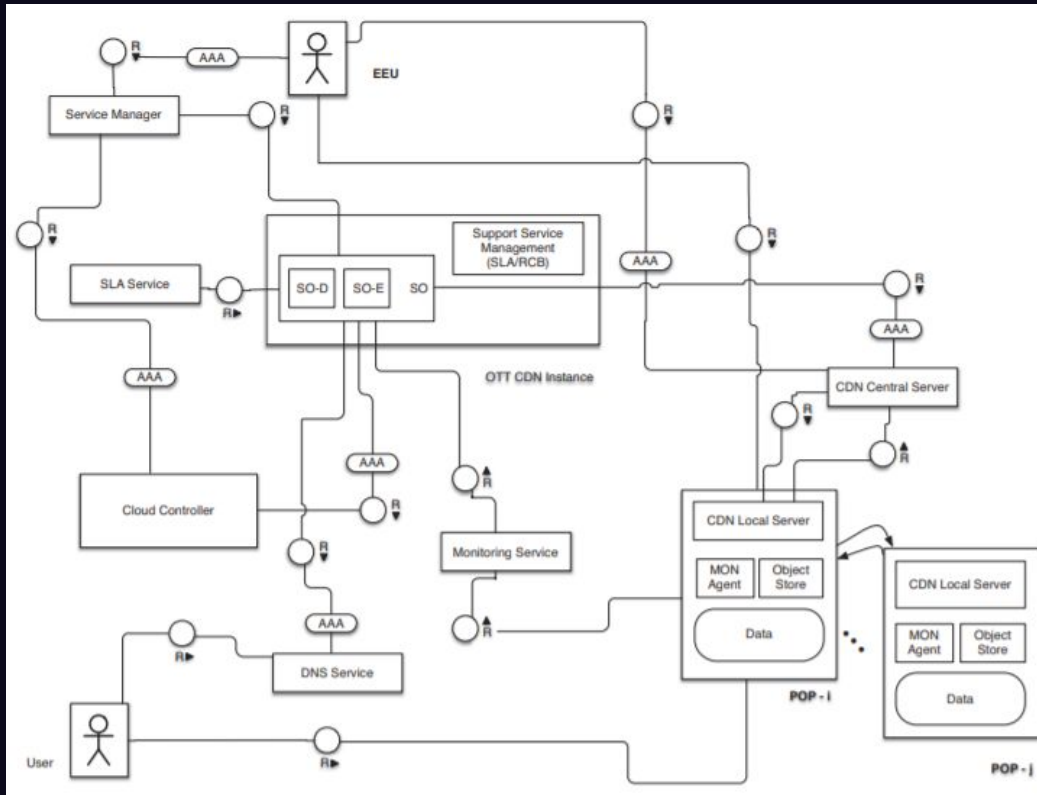
CDN-AS-A-SERVICE [4]

- ★ Mobile Cloud Networking (MCN) is a project that relies on three components to implement its lifecycle:
 - Service Manager (SM): provides an external interface to the user and manages the creation and deletion of service instances
 - Service Orchestrator (SO): describes how the service is implemented and is managed by the SM
 - Cloud Controller (CC): supports the deployment, provisioning, and disposal of SOs

CDN-AS-A-SERVICE [4]

- ★ The lifecycle model used in MCN has a technical and business phase. The technical phase includes:
 1. Design: the service's technical design is completed
 2. Implement: the service is implemented through the initialization of a SO through the CC
 3. Deploy: the SO deploys the needed resources to create the service and satisfy the SM's requirements
 4. Provision: the SO configures the deployed services
 5. Runtime and Operation: the SO monitors and manages the service until the end
 6. Disposal: the service is deleted

CDN-AS-A-SERVICE [4]



CDN-AS-A-SERVICE [4]

- ★ The SM is the initial point-of-entry for a customer, or end-user (EU), to create their new CDN service through a new SO
- ★ The SO manages the service's lifecycle
- ★ The Central Server (CS) is the central registry of the service
- ★ The MCN Rating, Charging, and Billing (RCB) engine charges the customer based on real-time bandwidth and disk usage data it gets from the monitoring service that is connected to each CDNaaS
- ★ The Local Server (LS) is the HTTP server on top of each Point of Presence (PoP) that acts as the main local entry point
- ★ DNSaaS provides DNS capabilities on-demand for each customer
- ★ MCN's Authentication and Authorization (AAA) is used to avoid multiplying methods



**FUTURE
WORKS**

FUTURE WORKS

- ★ Develop a comprehensive and integrated security solution that addresses a majority of challenges in the cloud environment without decreasing performance [2]
- ★ Address bandwidth limitations based on the increasing number of mobile and cloud users
 - Femtocell is a small, cellular base station that aims to solve this issue, but it still needs more research into its performance impact on mobile cloud computing [3]
- ★ Currently, Quality of Service is reduced for mobile users due to delays when communicating with the cloud caused by congestion
 - CloneCloud (clones data from smartphone onto the cloud and executes operations on the clones) and Cloudlets (cluster of computers that are well-connected to the Internet) are two research ideas that may be able to reduce network delay [3]

REFERENCES

- [1] Abdo, J. B. (2021). Efficient and Secure Mobile Cloud Networking. *arXiv preprint arXiv:2102.09051*.
- [2] Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in Cloud Computing: Opportunities and Challenges. *Information Sciences*, 305, 357-383.
- [3] Dinh, H. T., Lee, C., Niyato, D., & Wang, P. (2013). A survey of mobile cloud computing: architecture, applications, and approaches. *Wireless communications and mobile computing*, 13(18), 1587-1611.
- [4] Dudouet, F., Harsh, P., Ruiz, S., Gomes, A., & Bohnert, T. M. (2014, September). A Case for CDN-as-a-Service in the Cloud: A Mobile Cloud Networking Argument. In *2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 651-657). IEEE.
- [5] Moura, J., & Hutchison, D. (2016). Review and Analysis of Networking Challenges in Cloud Computing. *Journal of Network and Computer Applications*, 60, 113-129.



THANKS!
QUESTIONS?

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**.

Please keep this slide for attribution.