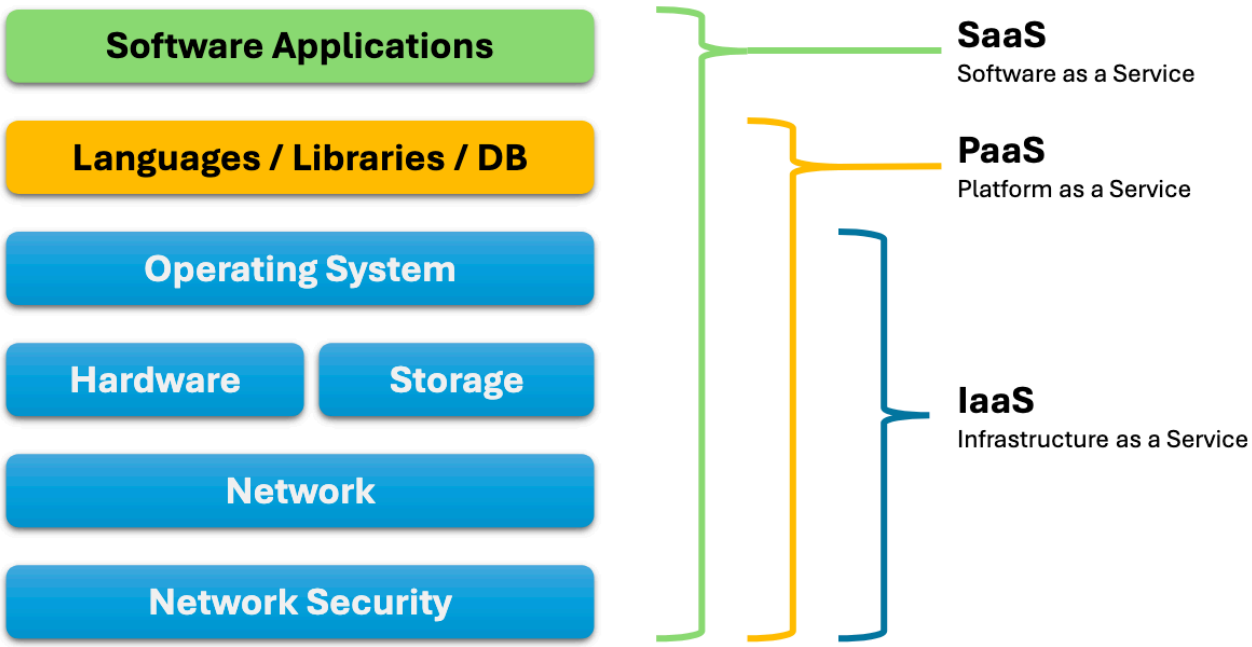
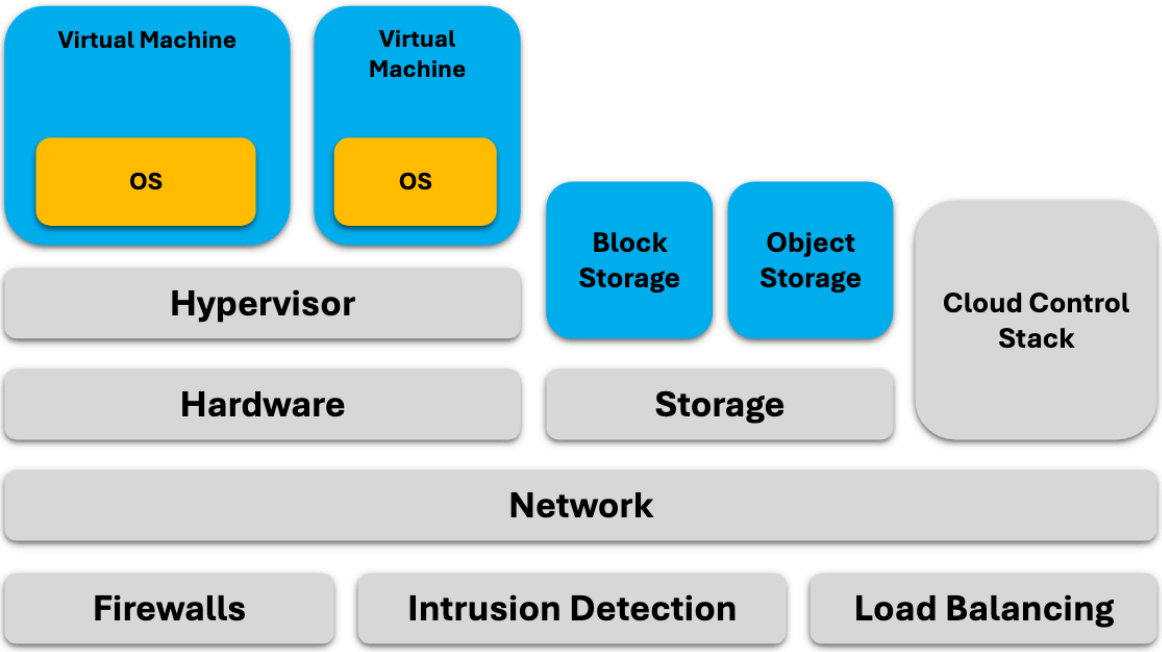


- PaaS - AWS
- IaaS - EC2



Trust in Cloud Env

- clients trust CSP to provide confidentiality, integrity and availability
- CSP trusts client to not behave maliciously

Confidentiality

- customer software and data
- usage statistics/patterns

- **threats**
  - observing access patterns of storage and VMs (even if encrypted)
  - side channel leakage

Integrity

- customer software and data
- **threats**
  - race conditions: exploits of weakness in data caching, data consistency
  - manipulation of block/object storage
  - integrity of the VM image

Availability

- uptime of hypervisor & VM; durability of client data
- **threats** attacks on hypervisor & storage layer

Hypervisors

- low level software component allowing commodity compute hardware to be virtualized & partitioned into VMs
- **trusted** to isolate VM, security & performance standpoint
- **compromised hypervisor?**
  - TPM (Trusted Platform Module)
  - a secure co-processor, on the motherboard of the host running the hypervisor
  - TPM signs a hash of the software running at boot (attestation), which it can make available to the client or CSP, to verify the integrity of the code that's running

Firewalls

- customer-controlled firewalls allow customers to restrict traffic to VMs
  - attacker who compromises a M doesn't gain ability to change firewall settings
  - physically separate, non-virtualized firewall

Cryptography

- protect customer data in transit
  - protected by SSL/TLS
  - public-facing CSP have certificates signed by CAs #TODO
- protect customer data at rest
  - Amazon - Object storage encrypted & signed
  - OpenStack - block storage can be encrypted & signed
  - Joyent - no encryption; customers responsible for own encryption

Networking

- customer VM's IP belongs to CSP (address to be banned/blacklisted)
- a customer who causes an IP to be banned could adversely affect the next customer who later uses the same IP
- **defenses**
  - monitoring for spoofed packets, blocking some outbound services

Information Leakage

- loss of confidentiality of data & computations?
- leakage channels include shared caches, storage channels & covert channels

Cache-Timing Exploits

- same CPU = shared cache
- Prime → fill shared cache with data, Probe → access again; long access time = victim accessed

Defenses

- allocate memory s.t. no overlap in cache lines used by different customers
- allocate memory s.t. cache lines that contain sensitive info cannot be evicted from the cache and thus do not affect the timing of the attacker's memory access

Covert Channels

- attacker who compromises a VM covertly exfiltrates info without victim knowing

Data Security

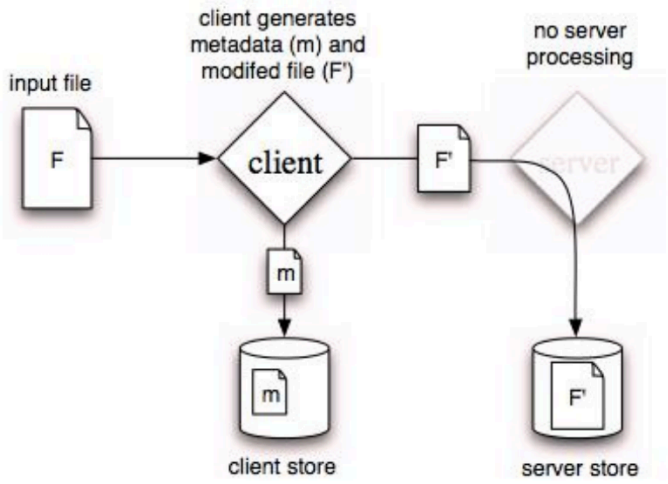
- GOAL: prove with high probability that a CSP has maintained the integrity, availability and durability of customer data
- Solution: probabilistic alg, customers make specially constructed queries on data
  - queries answered correctly by CSP, proves integrity, availability and duribility.

Proof of Retrieval (POR)

- customer encrypts the file and randomly embeds a set of randomly-valued check blocks called *sentinels*
  - encryption allows sentinels indistinguishable from other file blocks
- customer later challenges CSP by asking for random collection of the sentinel blocks
  - if the CSP has modified or deleted a substantial portion of the file, then with high probability it will also have suppressed a number of sentinels
- small changes made → detected by **checksums**

Provable Data Possession (PDP)

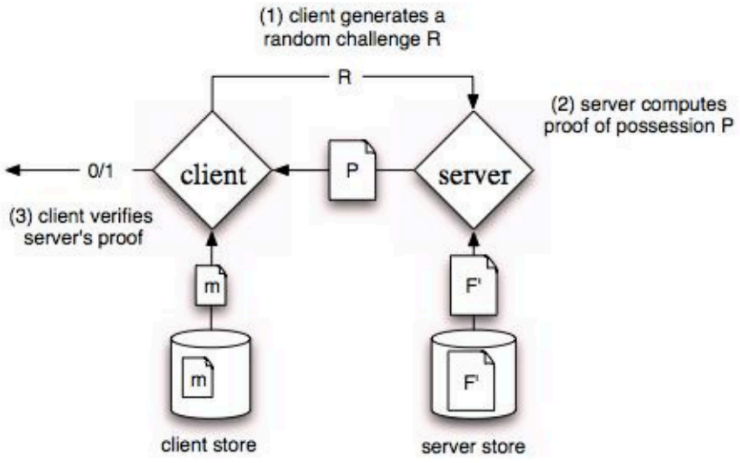
- The client pre-computes tags for each block of a file and then stores the file with a server
- Tags are computed using *homomorphic encryption*: this means that tags computed for multiple, arbitrary file blocks can be combined into a single value



Source: *Provable Data Possession at Untrusted Sources*, Ateniese et al.

Provable Data Possession (PDP)

- At a later time, the client can verify that the server possesses the file by generating a challenge against a randomly selected set of file blocks.
- The server calculates a result for the requested blocks, and sends it back as a proof of possession.
- The client is thus convinced of data possession, without actually having to retrieve the file blocks.



Source: *Provable Data Possession at Untrusted Sources*, Ateniese et al.