# Cloud computing - Introduction

1. Fundamentals on cloud computing
2. Cloud characteristics
3. Cloud service models
4. Cloud implementation models
5. Cloud technology
6. Standardization
7. Cloud bigdata
8. Final remarks

# Fundamentals on cloud computing

According to NIST[1]:

NIST National Institute of Standards and Technology U.S. Department of Commerce

*"Cloud computing is a **model** for enabling **ubiquitous**, **convenient**, **on-demand** network access to a shared pool of **configurable computing resources** (e.g., networks, servers, storage, applications, and services) that can be rapidly **provisioned and released** with minimal management effort or service provider interaction.*

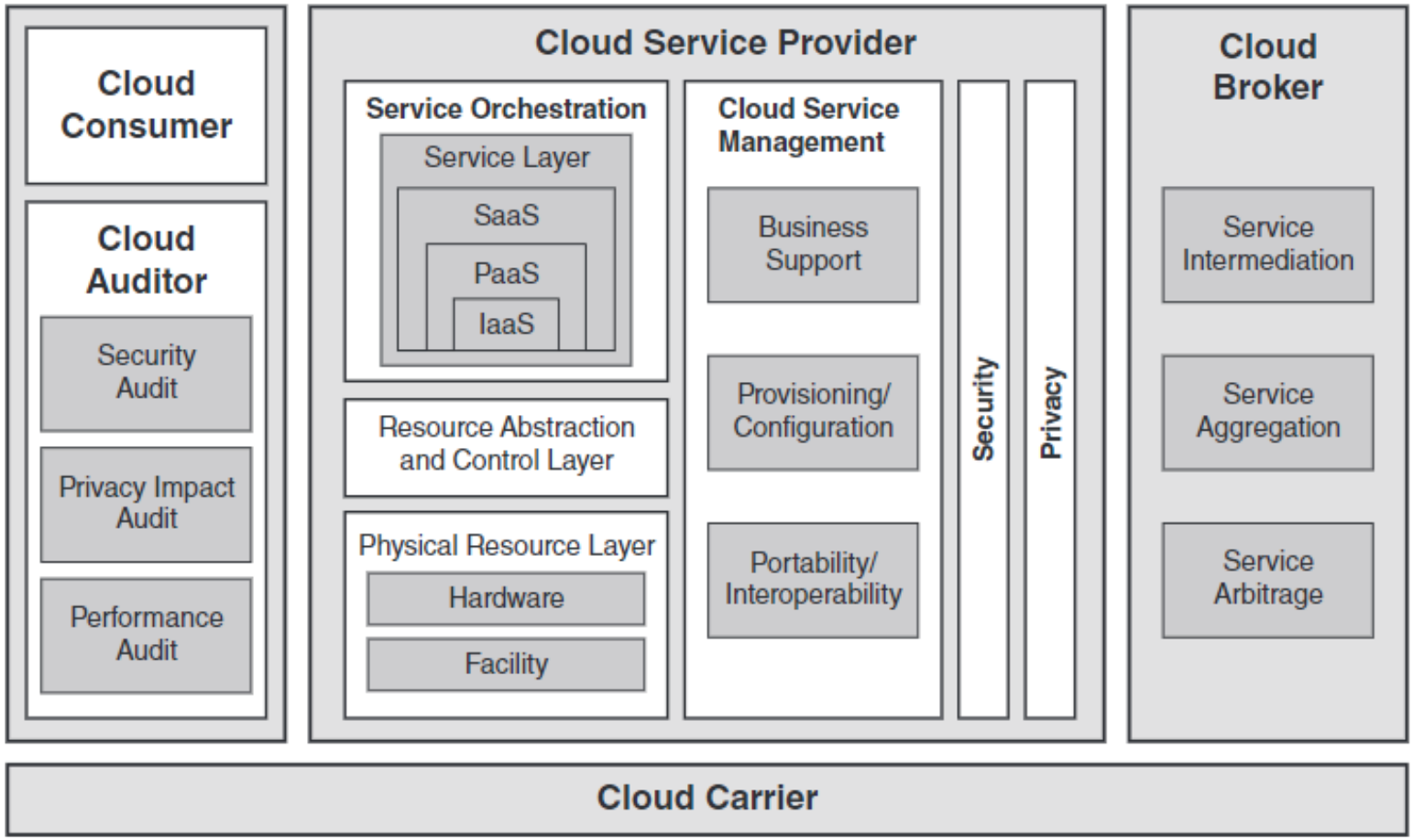
*This cloud model is composed of **five essential characteristics**, **three service models**, and **four deployment models**."*

[1] The NIST Definition of Cloud Computing; http://csrc.nist.gov/.



mario.antunes@ipleiria.pt

# Fundamentals on cloud computing

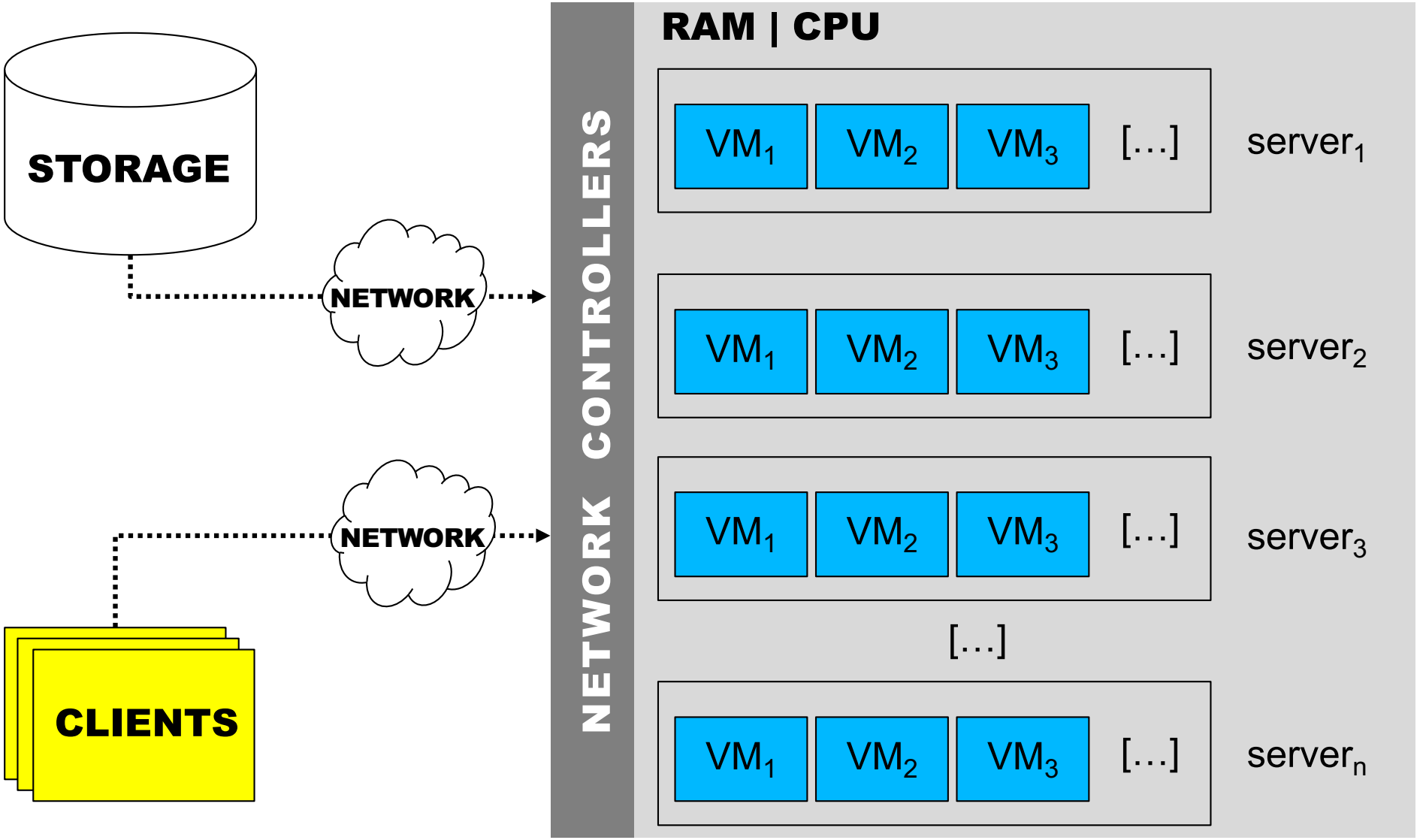



The Official (ISC)2® Guide to the CCSP℠ CBK ®, Second Edition
Adam Gordon; John Wiley & Sons, Inc, 2016



mario.antunes@ipleiria.pt

# Fundamentals on cloud computing






mario.antunes@ipleiria.pt

# Fundamentals on cloud computing - challenges

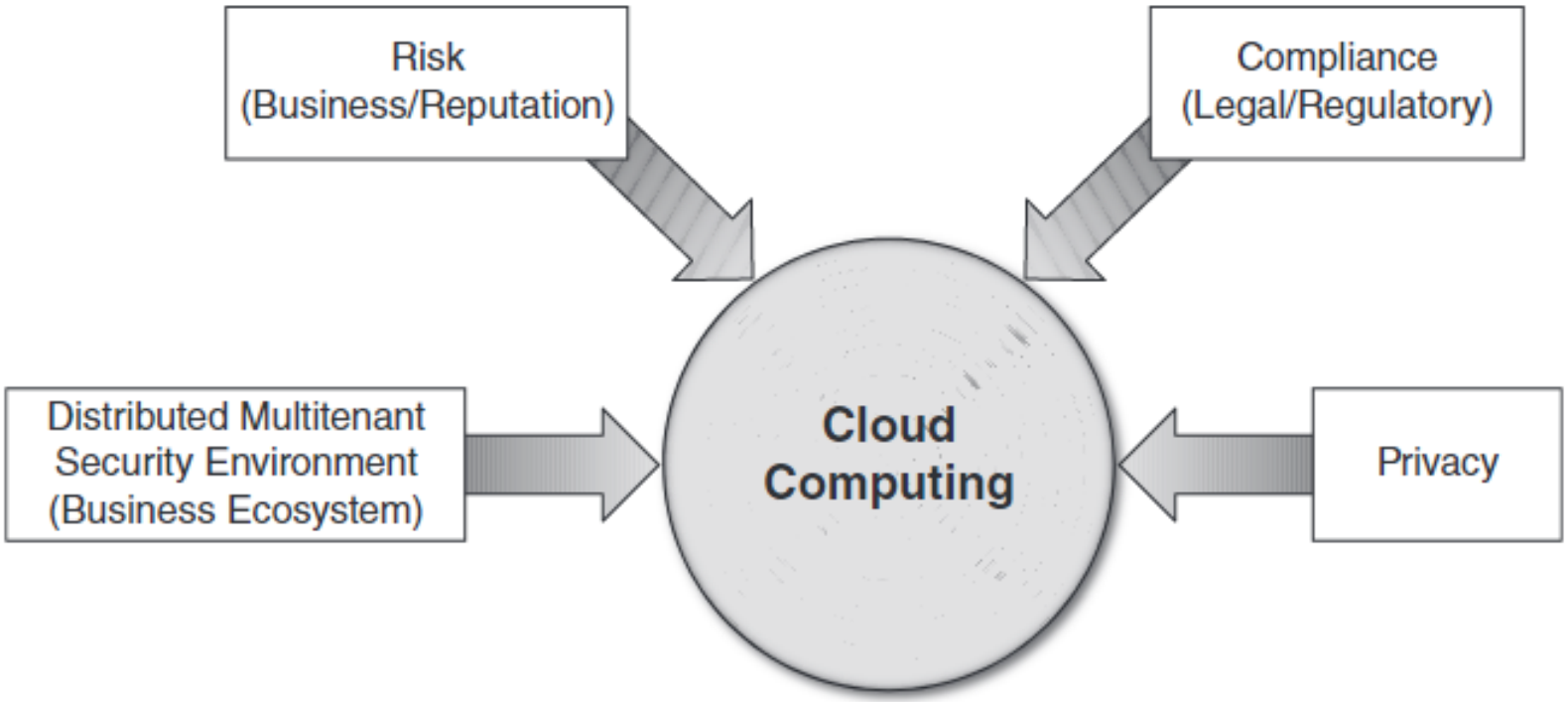
- **Investment on IT infrastructure** CAPEX versus OPEX
- **The desire to reduce IT complexity**
  - Risk reduction
  - Scalability
  - Elasticity
- **Consumption-based pricing**
  - Risk reduction
  - Elasticity
- **Business agility**
  - Mobility
  - Collaboration and innovation



mario.antunes@ipleiria.pt

# Fundamentals on cloud computing

## Security, risks and compliance




The Official (ISC)2® Guide to the CCSP℠ CBK ®, Second Edition
Adam Gordon; John Wiley & Sons, Inc, 2016


© Mário Antunes
mario.antunes@ipleiria.pt

# Fundamentals on cloud computing

Cloud ≠
- technology itself
- only virtualization

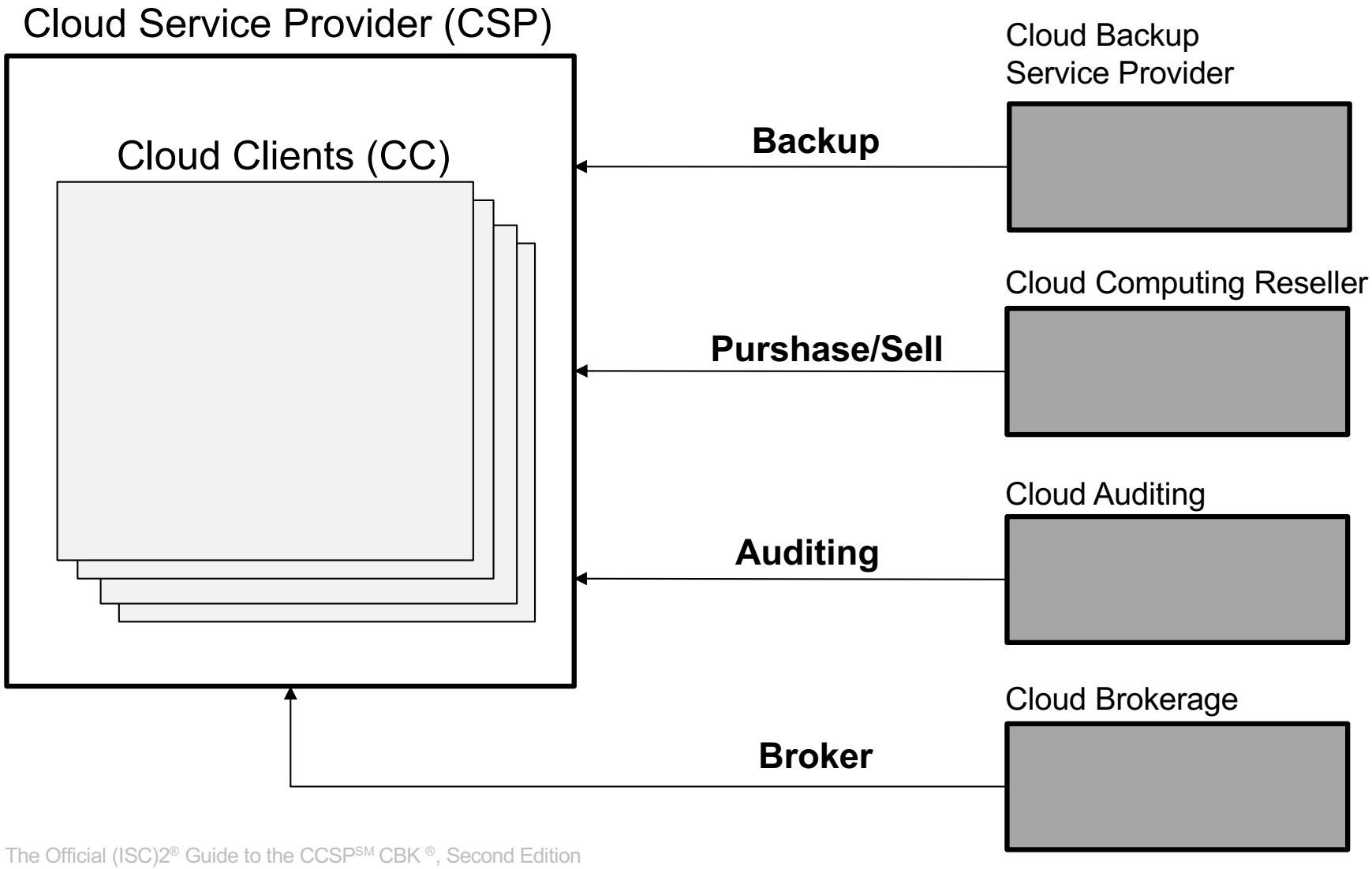
Cloud =
- is “real” and exists
- has a known geographic location

Cloud =
- Abstract concept and IT model
- IT technology independent ...
- ... but grounded on real IT resources



mario.antunes@ipleiria.pt

# Cloud roles

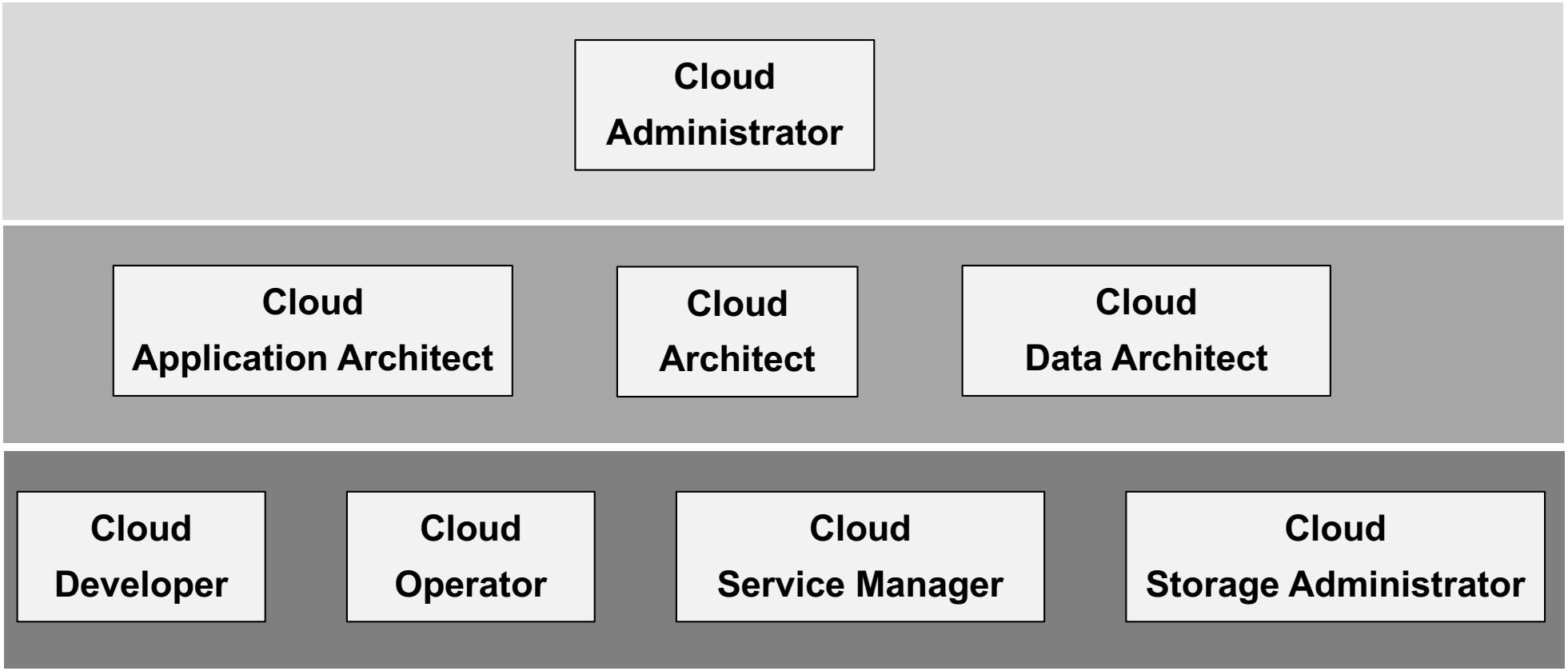



The Official (ISC)2® Guide to the CCSP℠ CBK ®, Second Edition
Adam Gordon; John Wiley & Sons, Inc, 2016 (pp.12)



mario.antunes@ipleiria.pt

# Cloud functions




The Official (ISC)2® Guide to the CCSP℠ CBK ®, Second Edition
Adam Gordon; John Wiley & Sons, Inc, 2016 (pp.16-17)



mario.antunes@ipleiria.pt

# Fundamentals on cloud computing

## Five characteristics

- *On-demand self service*
- *Broad network access*
- *Resource pooling*
- *Rapid elasticity*
- *Measured service*

The NIST Definition of Cloud Computing;
http://csrc.nist.gov/

## Three service models

- *Software as a Service (SaaS)*
- *Platform as a Service (PaaS)*
- *Infrastructure as a Service (IaaS)*
- **aaS*

## Four implementation models

- *Private cloud*
- *Public cloud*
- *Hybrid cloud*
- *Community cloud*

**5 x 3 x 4**

Characteristics Services Implementations



mario.antunes@ipleiria.pt

# Service models

**IaaS** - Infrastrucutre as a Service

**PaaS** – Platform as a Service

**SaaS** – Software as a Service

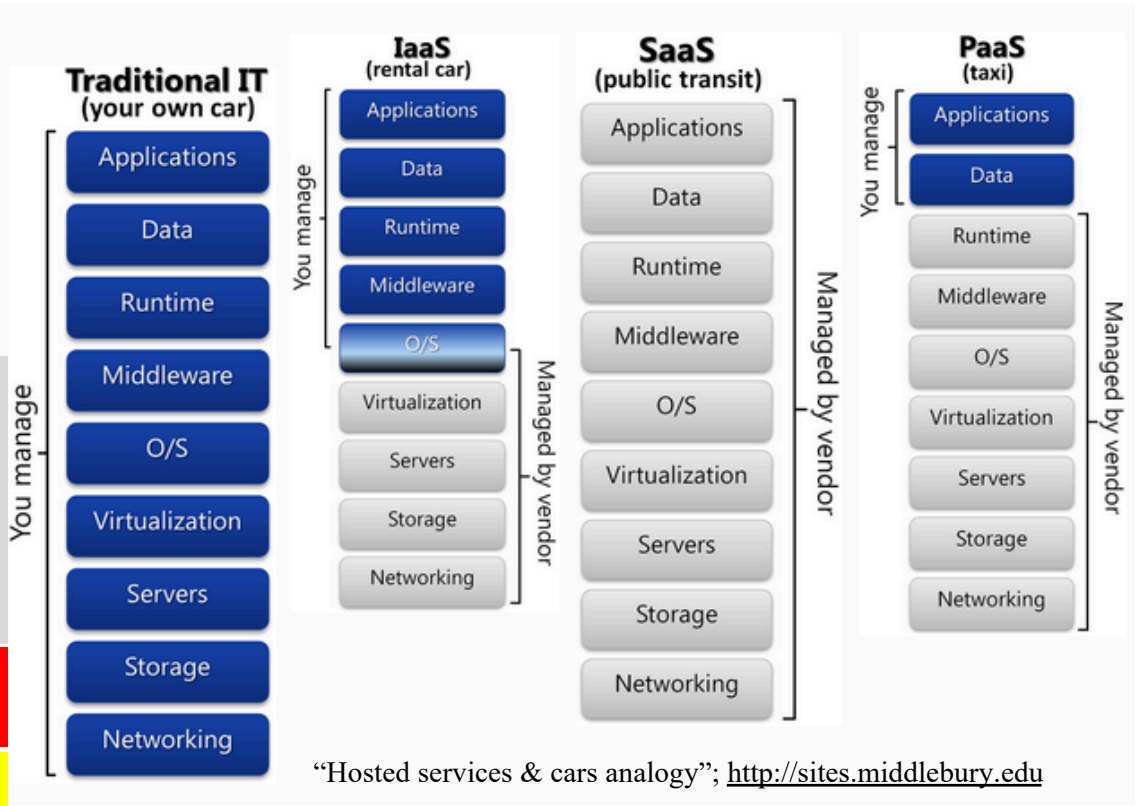
**DBaaS** – Database as a Service

**BaaS** – Billing as a Service

**NaaS** – Network as a Service

**MaaS** – Malware as a Service

***aaS** – "anything" as a Service




"Hosted services & cars analogy"; http://sites.middlebury.edu

How strong is your level of "independence" from the cloud provider?

What is being managed by you, *versus* by the cloud provider?



mario.antunes@ipleiria.pt

# Service models – IaaS

- **Resources made available by cloud provider:**
  - Almost everything!
  - Install and to manage computational fundamental resources: storage, memory, CPU and network
  - Install and to run programs: OS and applications
  - Control over OS and some IP networking configurations
- **User controls everything <u>but</u> the hardware used.**



mario.antunes@ipleiria.pt

# Service models – IaaS - providers

| | | | |
|---|---|---|---|
| Amazon Web Services<br>aws.amazon.com | 8 zonas (4 continentes) | EC2 (*compute*), S3 (*storage*) | 0,0500 € ou $ 0,0650 para 1.7 GM RAM, 1 CPU, 160 GB DISK |
| Rackspace Cloud<br>www.rackspacecloud.com | 3 zonas (3 continentes) | Cloud *Servers*, Cloud *Files* | 0,0170 € ou $ 0,0220 para 0.5 GB RAM, 1 CPU, 20 GB DISK |
| HP Cloud<br>www.hpcloud.com | 2 zonas (1 continente) | Cloud *Compute*, Cloud *Object Storage* | 0,0307 € ou $ 0,0400 para 1 GB RAM, 1 CPU, 30 GB DISK |
| GoGrid<br>www.gogrid.com | 3 zonas (2 continentes) | Cloud *Servers*, Cloud *Storage* | 0,0307 € ou $ 0,0400 para 0.5 GB RAM, 0.5 CPU, 25 GB DISK |
| Lunacloud<br>www.lunacloud.com | 2 zonas (1 continente) | Cloud *Servers*, Cloud *Storage* | 0,0155 € ou $ 0,0200 para 0.5 GB RAM, 1 CPU, 10 GB DISK |
| Joyent<br>www.joyent.com | 4 zonas (2 continentes) | *SmartMachine* | 0,0230 € ou $ 0,0300 para 0.5 GB RAM, 1 CPU, 15 GB DISK |
| ElasticHosts<br>www.elastichosts.com | 1 zona (1 continente) | Cloud *Hosting* | 0,0920 € ou $ 0,1200 para 1 GB RAM, 1 CPU, 10 GB DISK |
| Microsoft Azure<br>www.azure.microsoft.com | 17 zonas (4 continentes) | *Virtual Machines Storage* | 0,0144 € ou $ 0,0180 para 0.75 GB RAM, 1 CPU, 30 GB DISK |

**EC2** – Elastic Compute Cloud

Cloud regions and zones

António Miguel Ferreira; "Introdução ao Cloud Computing"; FCA; ISBN: 978-972-722-802-7; 2015 (Portuguese)



mario.antunes@ipleiria.pt

# Service models – IaaS - providers

Gartner's *Magic Quadrant* for IaaS cloud providers

Gartner

**2019**


Source: Gartner (July 2019)

**2020**

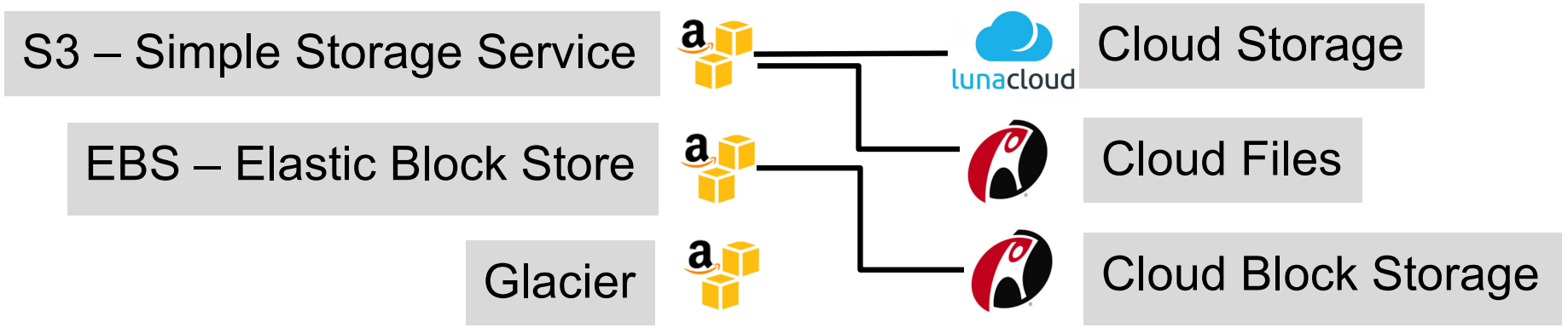

Quadrant for service models also available at http://www.gartner.com.


© Mário Antunes
mario.antunes@ipleiria.pt

# Service models – IaaS - nomenclature

- **Main characteristics of storage in the cloud:**
  - Speed
  - Resiliency
  - Accessibility
  - Measured in GB

- **About nomenclature:**






mario.antunes@ipleiria.pt

# Service models – IaaS - interoperability

- **Each provider has its own API for management and development**
- **Convencional method: web interface**

**Problems** – each provider has its own API

**Effect** – migration between cloud providers becames hard. Need to deal with different APIs.

**Solution** – To adopt ongoing standard APIs and access metods, like Openstack used with REST API. 

To use *cloud brokers* and *cloud aggregators* Gravitant



mario.antunes@ipleiria.pt

# Service models – PaaS

- **Resources made available by cloud provider:**
  - In house developed applications or purchased software packages
  - Programming languages compilers and libraries
  - Software versioning and revision control system
  - Aim: to use cloud as a software development platform
- **User has very litle control over cloud infrastructure.**



mario.antunes@ipleiria.pt

# Service models – PaaS - providers

| | | Services and Platforms | |
|---|---|---|---|
| Heroku<br>www.heroku.com | AWS USA<br>(1 continente) | Ruby, Node.js, Clojure, Java, Python, Scala, Postgres, Mongo, Hadoop, etc. | $ 0,05/hora para 1 processo +<br>+ $ 9/mês para 1 base de dados |
| Nodejitsu<br>www.nodejitsu.com | Joyent USA<br>(1 continente) | Node.js | $ 2,5/mês para 1 processo |
| Google App Engine<br>www.appengine.google.com | 13 zonas<br>(4 continentes) | Java, Python, Go | $ 0,05/hora para 1 app |
| CloudBees<br>www.cloudbees.com | AWS USA, Europa, HP<br>(3 continentes) | Java | $ 60/mês para 5 GB de código e 2 processos |
| Appfog<br>www.appfog.com | AWS USA, Europa, Ásia, Rackspace, HP, Azure<br>(3 continentes) | Java, Scala, Python, Node.js, PHP, Ruby, Erlang, MongoDB, MySQL, Postgres | $ 20/mês para 8 processos, até 2 GB RAM e 250 MB dados |
| dotCloud<br>www.dotcloud.com | AWS USA<br>(1 continente) | PHP, Node.js, Python, Ruby, Perl, Java, MySQL, MongoDB, Postgres | $ 8,64/mês |
| OpenShift<br>www.openshift.com | AWS USA<br>(1 continente) | PHP, Node.js, Python, Ruby, Java | $ 0,02/hora |

António Miguel Ferreira; "Introdução ao Cloud Computing"; FCA; ISBN: 978-972-722-802-7; 2015 (Portuguese)



mario.antunes@ipleiria.pt

# Service models – SaaS

- **Resources made available by cloud provider:**
  - Applications stored on the cloud.
  - Applications accessed  through HTTP, usually via web browser
  - Billing (examples): storage, number of accounts, duration and/or functionalities provided

- **User has no control over the cloud applications. Little control on some configuration features.**



mario.antunes@ipleiria.pt

# Service models – SaaS - providers

Google Apps 


Microsoft Office365 


iCloud 


Mailchimp 


SAP BusinessOne 

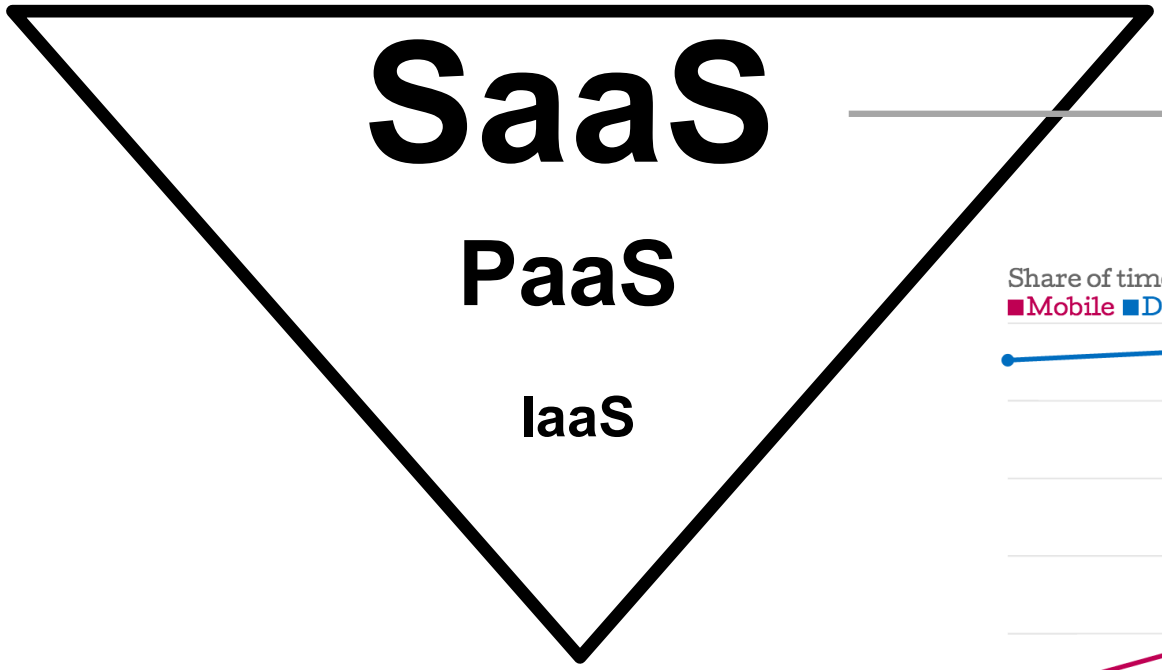

ServiceNow – Troubleticket servicenow

LogicMonitor – IT infrastructure monitoring LogicMonitor



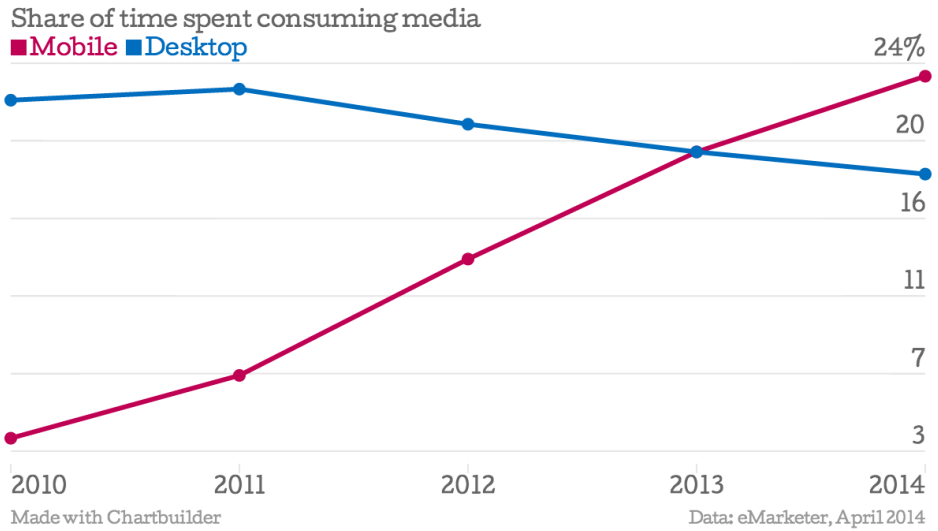
mario.antunes@ipleiria.pt

# Service models – a market perspective




Biggest growth potential

Biggest market value



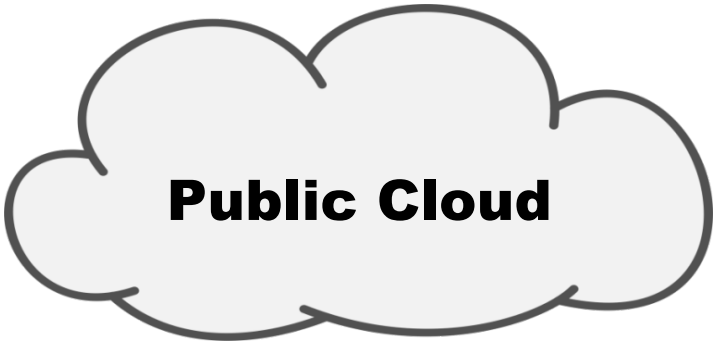

**Why?** Mainly due to growing development for mobile devices iOS e Android:

Examples: Google Apps, Evernote, Dropbox, Facebook, Shazam



mario.antunes@ipleiria.pt

# Implementation models



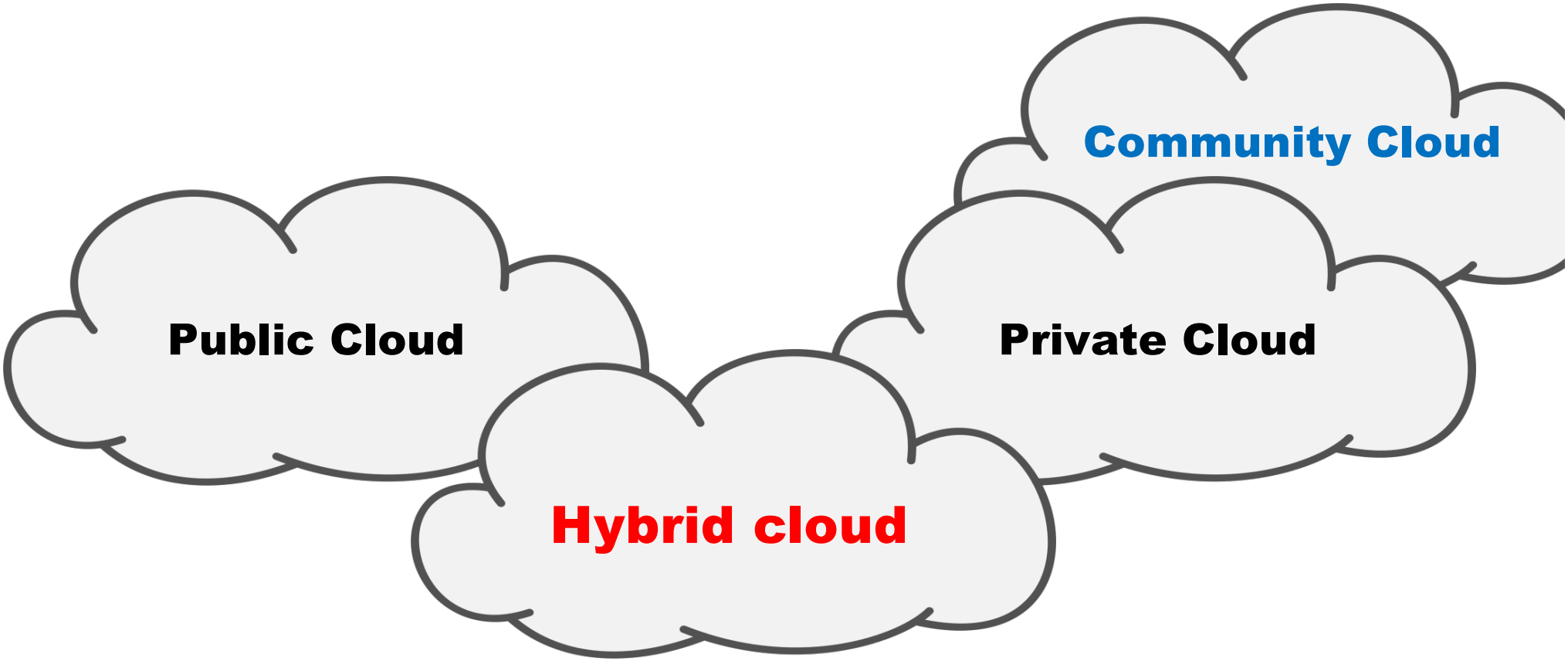

- Multiple clients
- Configured in a public Datacenter
- Shared infrastructure
- Access over web
- Low security
- Low cost in a *"pay per use"* basis
- "Do it yourself"


- Single-tenant solution
- Setup as a Virtual Private Datacenter
- Dedicated servers
- Access over secure private networks
- High security
- High TCO
- Custom solutions



mario.antunes@ipleiria.pt

# Implementation models

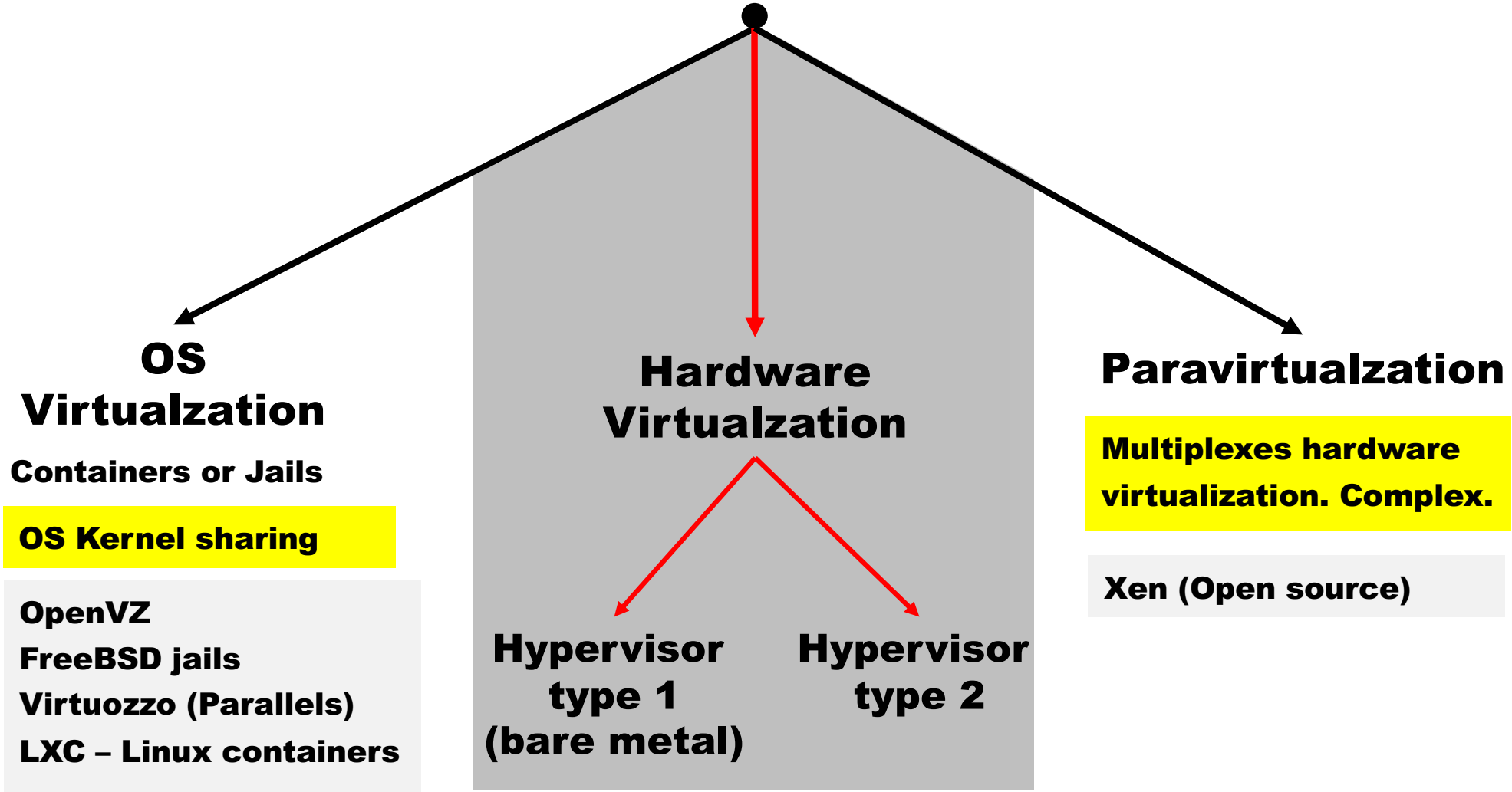



It combines features of public and private (and community) cloud models



mario.antunes@ipleiria.pt

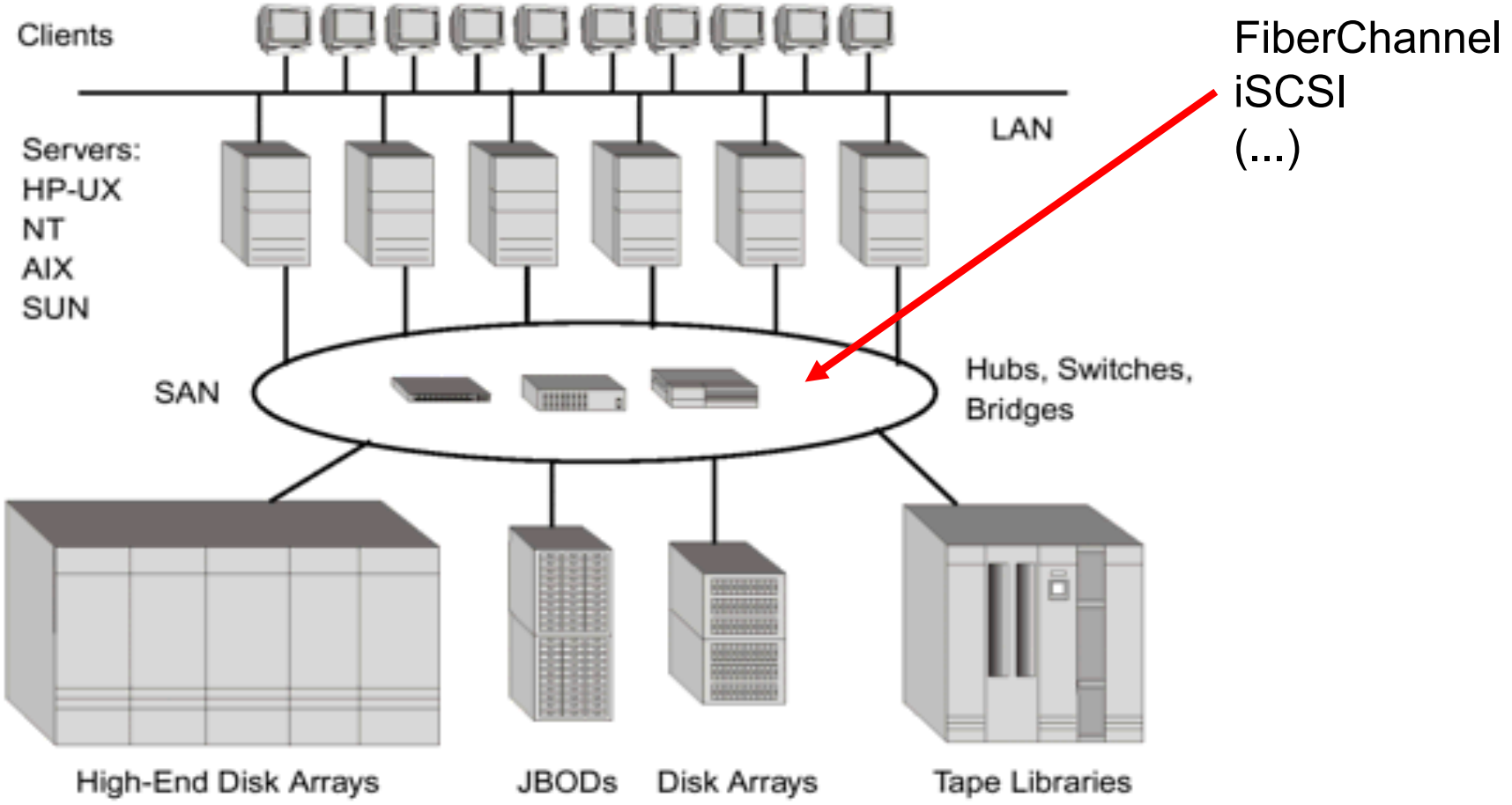
# Cloud technology - virtualization






mario.antunes@ipleiria.pt

# Cloud technology – virtualization - storage




Adapted from http://flylib.com



mario.antunes@ipleiria.pt

# Cloud technology – virtualization - storage

- Grouping physical devices in one “logical unit”
- Grouping is irrespective to physical disks location
- Used with other local strategies: e.g. RAID
- Shared, block-based and transparent access to end-users
- Smooth storage manager and data replication
- Essential in a fault-tolerant and HA perspective
- Implementation over IP: iSCSI and iFC



mario.antunes@ipleiria.pt

# Cloud technology – virtualization - Google

**Americas**

Berkeley County, South Carolina
Council Bluffs, Iowa
Douglas County, Georgia
Jackson County, Alabama
Lenoir, North Carolina
Mayes County, Oklahoma
Montgomery County, Tennessee
Quilicura, Chile
The Dalles, Oregon

**Asia**

Changhua County, Taiwan
Singapore

**Europe**

Dublin, Ireland
Eemshaven, Netherlands
Hamina, Finland
St Ghislain, Belgium

**15 datacenters world wide**

http://www.google.com/about/datacenters/inside/locations/
http://www.datacentermap.com



mario.antunes@ipleiria.pt

# Cloud technology – virtualization - security

**Critical component** = Hypervisor

**Security elements**

**Type 1** (hardware based)

Software that comprise the hypervisor package (virtualization function and OS functions)

**Type 2** (operating system based)

More attractive to attackers. More vulnerabilities. OS and applications expose breaches.

Limited access and strong control over embeeded OS increase robustness of Type 1 hypervisor.

Standardization is needed to effectively reduce the risk!



mario.antunes@ipleiria.pt

# Service models – security considerations - IaaS

**IaaS**

**Main Threats**

1. VM attacks
2. Virtual network
3. Hypervisor attacks
4. VM-based rootkits (VMBR)
5. Virtual switch attacks
6. DoS attacks
7. Colocation

**Highly dependent on the widespread use of virtualization and the associated hypervisor components.**

The Official (ISC)2® Guide to the CCSP℠ CBK ®, Second Edition
Adam Gordon; John Wiley & Sons, Inc, 2016 (pp.48-50)



mario.antunes@ipleiria.pt

# Service models – security considerations - IaaS

## New threats:

1. Provisioning tools and VM templates try to create new **unauthorized VM** or **patch the VM templates**

2. Infection propagates by new **VM clones**

3. These new threats are the result of a new, complex and dynamic nature of the cloud virtual infrastructure



mario.antunes@ipleiria.pt

# Service models – security considerations - IaaS

**Factors that determine the cloud dynamic notion:**

1. Multitenancy
2. Loss of control
3. Dynamic network topology
4. Logical network segmentation
5. No physical endpoints
6. Single Point of Access/Failure (SPoA/SPoF)



mario.antunes@ipleiria.pt

# Service models – security considerations - PaaS

**PaaS**

**Main Threats**

1. **System and Resource Isolation**
2. **User-level permissions**
3. **User Access Management**
   - Intelligence
   - Administration
   - Authentication
   - Authorization
4. **Protection against malware, backdoors and trojans**

The Official (ISC)2® Guide to the CCSP℠ CBK ®, Second Edition
Adam Gordon; John Wiley & Sons, Inc, 2016 (pp.50-52)



mario.antunes@ipleiria.pt

# Service models – security considerations - SaaS

**SaaS**

**Main Threats**

1. **Data segregation**
2. **Data access and policies**
3. **Web application security**

Cloud Security Alliance Controls Matrix (CCM)
https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview

The Official (ISC)2® Guide to the CCSP℠ CBK ®, Second Edition
Adam Gordon; John Wiley & Sons, Inc, 2016 (pp.52-54)



mario.antunes@ipleiria.pt

# Cloud technology – common threats


*"The notorious nine" – cloud computing top threats in 2013*

1. **Data breaches**
2. **Data loss**
3. **Account or service traffic hijacking**
4. **Insecure interfaces and API**
5. **Denial of Service**
6. **Malicious insiders**
7. **Abuse of cloud services**
8. **Insufficient due diligence**
9. **Shared technologies vulnerabilities**

The Official (ISC)2® Guide to the CCSP℠ CBK ®, Second Edition
Adam Gordon; John Wiley & Sons, Inc, 2016 (pp.43-47)



mario.antunes@ipleiria.pt

# Cloud technology – security risks


OWASP Top 10 Application Security Risks – 2017
[https://www.owasp.org]

| | |
|---|---|
| A1 - Injection | A6 - Sesitive Data Exposure |
| A2 – Broken Authentication and session management | A7 – Missing Function Level Access Control |
| A3 – Cross-Site Scripting (XSS) | A8 – Cross-Site Request Forgery (CSRF) |
| A4 – Insecure Direct Object References | A9 – Using Components with known vulnerabilities |
| A5 – Security Misconfiguration | A10 – Unvalidated Redirects and Forwards |

The Official (ISC)2® Guide to the CCSP℠ CBK ®, Second Edition
Adam Gordon; John Wiley & Sons, Inc, 2016 (pp.54-55)



mario.antunes@ipleiria.pt

# Cloud security – data and media sanitization

- Ability to safely remove all data from a system or media.
- Needed if you want to leave or migrate one CSP to another.

- Challenges:
  - Vendor lock-in
  - Cryptographic erasure
  - Data overwriting

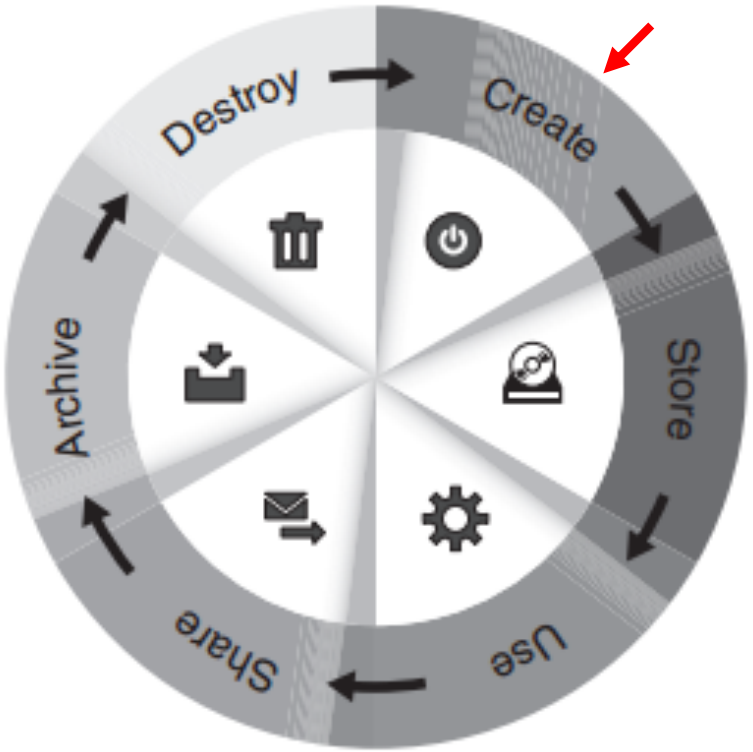


mario.antunes@ipleiria.pt

# Cloud secure data lifecycle

- Data is the single most valuable asset for most organizations.

- Auditing, compliance and other control requirements implies a good understanding of data lifecycle.




Be aware of logical and

Physical location of data.

The Official (ISC)2® Guide to the CCSP℠ CBK ®, Second Edition
Adam Gordon; John Wiley & Sons, Inc, 2016 (pp.55-56)

# Cloud cross-cutting aspects

**Cloud architecture - key principles**

- Define protections that enable trust in the cloud.
- Develop cross-platform capabilities and patterns for proprietary and open source providers.
- Facilitate trusted and efficient access, administration, and resiliency to the customer or consumer.
- Provide direction to secure information that is protected by regulations.
- Facilitate proper and efficient identification, authentication, authorization, administration, and auditability.
- Centralize security policy, maintenance operation, and oversight functions.
- Make access to information both secure and easy to obtain.
- Delegate or federate access control where appropriate.
- Ensure ease of adoption and consumption, supporting the design of security patterns.
- Make the architecture elastic, flexible, and resilient, supporting multitenant, multilandlord platforms.
- Ensure the architecture addresses and supports multiple levels of protection, including network, OS, and application security needs.

The Official (ISC)2® Guide to the CCSP℠ CBK ®, Second Edition
Adam Gordon; John Wiley & Sons, Inc, 2016 (pp.27)

# Cloud cross-cutting aspects

**NIST Cloud Technology roadmap**

1. **Interoperability**
2. **Portability**
3. **Availability**
4. **Security**
5. **Privacy**
6. **Resiliency**
7. **Performance**
8. **Governance**
9. **SLAs**
10. **Auditability**
11. **Regulatory compliance**

- Industry-recommended
- Guidance and recommendations
- Target: security architects, enterprise architects, and risk-management professionals
- Useful to review and understand which controls and techniques may be required

The Official (ISC)2® Guide to the CCSP℠ CBK ®, Second Edition
Adam Gordon; John Wiley & Sons, Inc, 2016 (pp.28-32)

# It is worth being on the cloud?

- **OP**erational **EX**penses *versus* **CAP**ital **EX**penses
- How big (€£$) is the TCO (OPEX + CAPEX)?
- How much (€£$) for the specialized human resources?
- How much (€£$) for the defined SLA?
- And what about to buy and to subscribe software?
- *"Pay only if you use and use only if you need"*
- Do you need support for entrepreneurship and inovation?



mario.antunes@ipleiria.pt

# Cost-benefits analysis

1. Resource pooling
2. Shift from CAPEX to OPEX
3. Factor in time and efficiencies
4. Have in mind depreciation of IT technologies
5. Reduction in maintenance and configuration time
6. Shift in focus regarding professionals' functions
7. Utilities cost (power, cooling, datacenter space, …)
8. Software and licensing costs
9. Pay per usage
10. Others – new tech, revised roles, legal costs, SLA revision, …



mario.antunes@ipleiria.pt

# It is worth being on the cloud?

**Initial costs (CAPEX)**

- hardware acquisition and instalation
- OS and software acquisition
- Building infrastrucutres

(...)

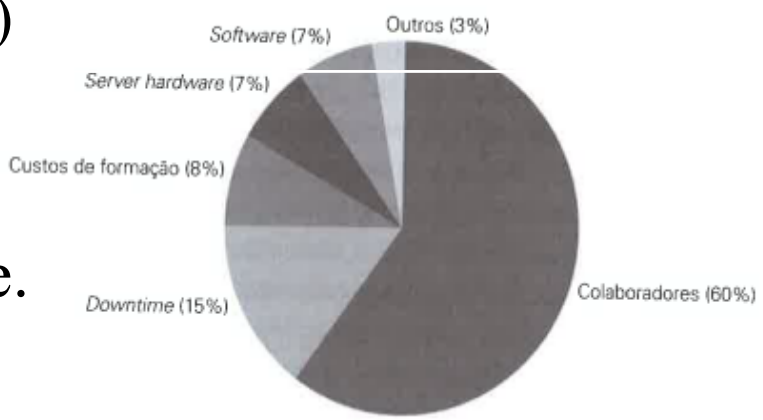
**Operational costs (OPEX)**

- Power consumption
- HAVC (rent)
- UPS (rent)
- Human resources
- (...)

**TCO = Total Cost of Ownership**

The value of the project through its lifetime.

TCO = CAPEX + OPEX




António Miguel Ferreira; "Introdução ao Cloud Computing"; FCA;
ISBN: 978-972-722-802-7; 2015
IDC Withepaper sobre TCO.



mario.antunes@ipleiria.pt

# Cloud technology – the future

- Ubiquity *de facto*
- Faster, wider , safer, bigger
- Interoperability – standards please!
- Fog Computing (*fogging*)
- Internet of Things (IoT)
- Bring Your Own Device (BYOD)
- Big Data



mario.antunes@ipleiria.pt

# Big data - overview

According to NIST[1]:

NIST National Institute of Standards and Technology U.S. Department of Commerce

***Big Data*** *consists of extensive datasets – primarily in the characteristics of* ***volume****,* ***variety****,* ***velocity****, and/or* ***variability*** *(and/or* ***value****) – that require a scalable architecture for efficient storage, manipulation, and analysis.*

[1] The NIST Definition of Cloud Computing; http://csrc.nist.gov/.

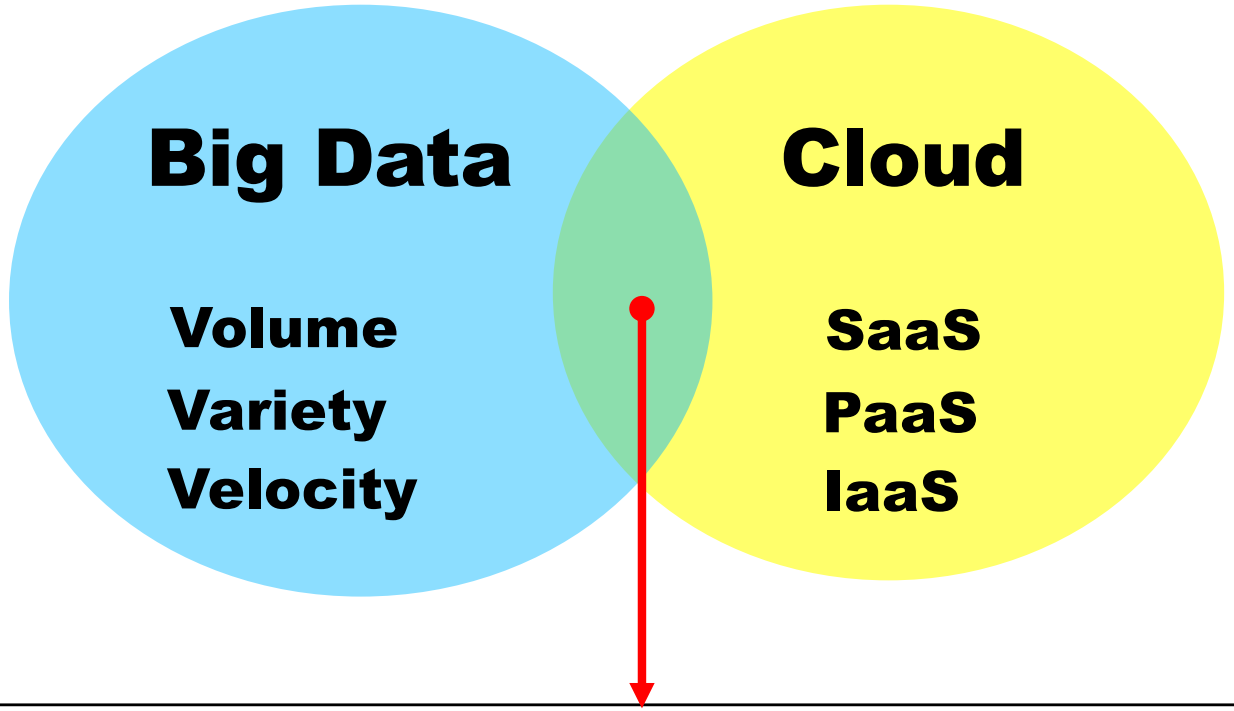
**3 V's definition**
- **Volume**
- **Velocity**
- **Variability**

**"new" V's**
- **Variety**
- **Value**
- **Veracity**



mario.antunes@ipleiria.pt

# Big data - overview




| | Volume | Variety | Velocity |
|---|---|---|---|
| **SaaS** | Client-side Personalization | Types of visualization | Real-time |
| **PaaS** | Distributed processing | Schemaless databases | Integration on the fly |
| **IaaS** | Scalable storage | Federated databased | On-demand resources |



mario.antunes@ipleiria.pt

# Certification

## Security standards applied to cloud environment:

- ISO/IEC 27001:2013
- ISO/IEC 27002:2013
- ISO/IEC 27017:2015
- SOC 1/SOC 2/SOC 3 → Audit Reports
- NIST SP 800-53
- PCI DSS

Cardholder data management for merchants.

Standards for Risk Management

1. Information Security Policies
2. Organization of Information Security
3. Human Resources Security
4. Asset Management
5. Access Control
6. Cryptographic
7. Physical and Environmental Security
8. Operations Security
9. Communications Security
10. System Acquisition, Development, and Maintenance
11. Supplier Relationship
12. Information Security Incident Management
13. Information Security Business Continuity Management
14. Compliance

The Official (ISC)2® Guide to the CCSP℠ CBK ®, Second Edition
Adam Gordon; John Wiley & Sons, Inc, 2016 (pp.62-72)

# Bibliography

- **Cloud Industry Forum** 

- **IEEE Cloud Computing** 

- **ISO/IEC 27017 cloud security** 

**17788, 17789 e 27017**
- **Asia Cloud Computing Association** 

- **EuroCloud Europe** 

**EuroCloud Portugal**
[www.eurocloud.pt]



mario.antunes@ipleiria.pt

# Bibliography


- "The NIST Definition of Cloud Computing"; Peter Mell, Timothy Grance; http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
- "NIST Cloud Computing Standards Roadmap"; http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf; 2013.
- *"Introdução ao cloud computing";* A.M. Ferreira; FCA; (pp. 11-78; pp. 89-106)
- "The Official ISC$^{2®}$ Guide to the CCSP$^{SM}$ CBK®, Second Edition"; Adam Gordon; John Wiley & Sons, Inc; 2016 (Chapter 1; pp.3-77)
- "Certified Cloud Security Professional (CCSP), Official Study Guide"; B. O'Hara, B. Malisow; John Wiley & Sons, Inc; 2017 (Chapter 1)
- "CCSP Official ISC$^{2®}$ Practice tests"; B. Malislow; Sybex; 2018; (Chapter 1; pp.1-30)





mario.antunes@ipleiria.pt