Cloud Security

Protecção de dados na cloud

Seminário

2019

Nuno Santos

TÉCNICO LISBOA

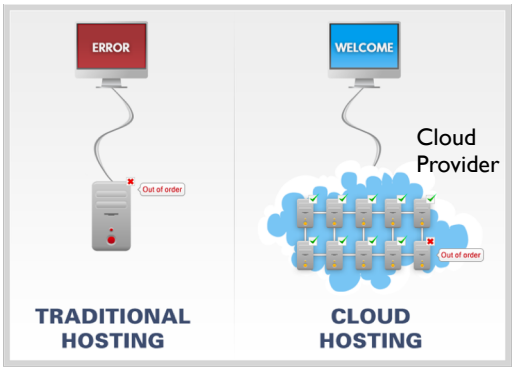
O que é a cloud?

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

NIST

Principais características de cloud computing

- Self-service on demand
- Acesso através de rede de banda larga
- Partilha de recursos (multi-tenant)
- Rápida elasticidade
- Monitorização do serviço
- Pay per use



Panorama de cloud computing

Applications	Docs, Sheets, Slides; ZOHO Work · Online; EVERNOTE
Storage	Your stuff, anywhere; box
Computing	amazon web services; rackspace the open cloud company
Development platform	Windows Azure; salesforce force.com

Quem utiliza cloud computing?

UPMC MyCloud

Carnegie Mellon University

TOYOTA

ally

zynga

BMW

NETFLIX

NASA NEBULA

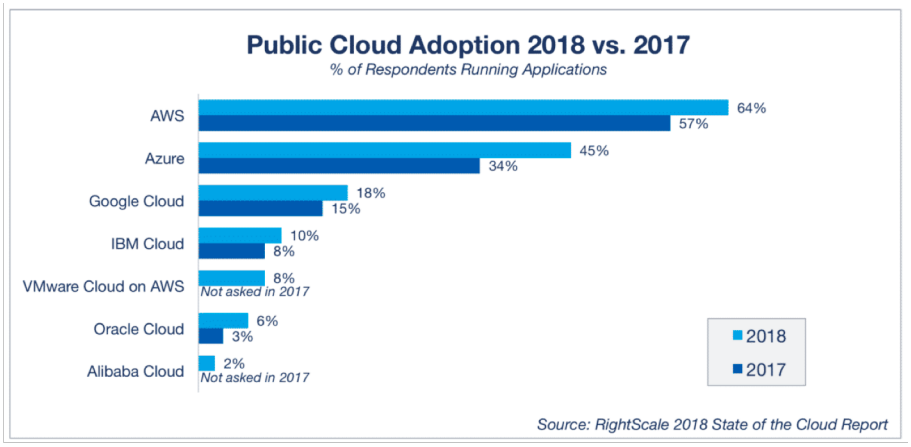
AVON
the company for women

Instagram

NSA CLOUD
Your backup service

DEPARTMENT OF ENERGY · UNITED STATES OF AMERICA

Tendências

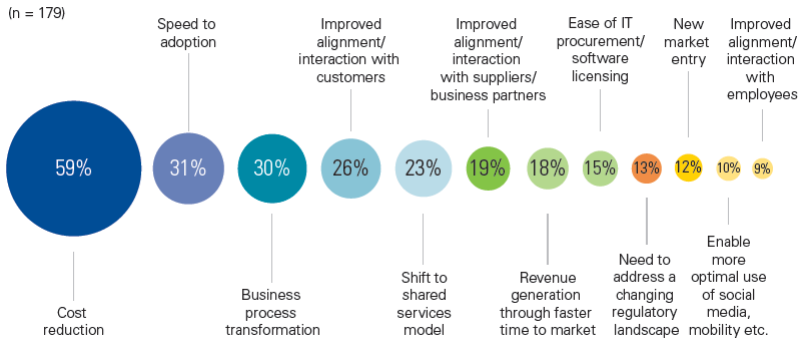


Amazon Web Services (AWS)

- Elastic Cloud Compute (EC2)
  "Virtual Servers in the Cloud"
- Simple Storage Service (S3)
  "Scalable Storage in the Cloud"
- DynamoDB
  "Fast, Predictable, Highly-scalable NoSQL data store"
- Outros serviços cloud…

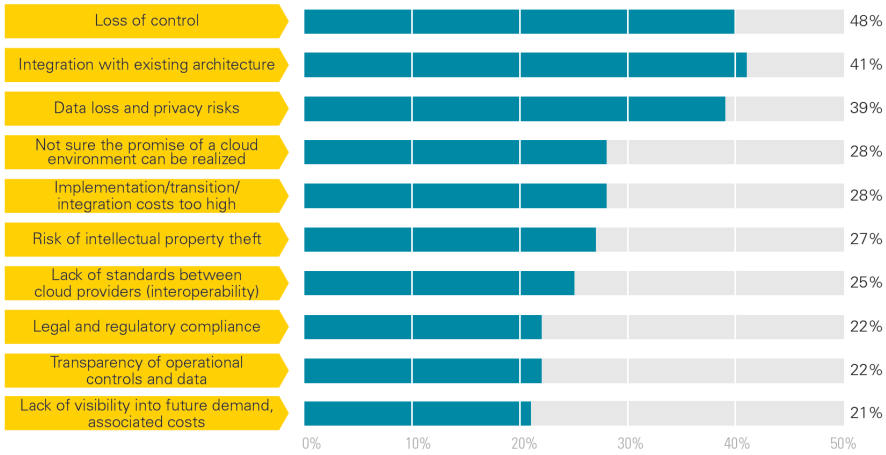
https://aws.amazon.com/

Porque é que os clientes usam a cloud?



KPMG International's 2012 Global Cloud Provider Survey (n=179)

Principais preocupações de potenciais clientes



KPMG International's 2012 Global Cloud Provider Survey (n=179)

Dados sensíveis na cloud: Exemplos

Aplicações hospedadas na cloud

Billing
- Aria Systems
- eVapt
- nDEBIT
- Redi2
- Zuora

CRM
- 37 Signals
- Capsule
- Dynamics
- Intouchcrm
- LiveOps
- Oracle CRM
- Parature
- Responsys
- RO|Enablement
- Salesforce.com
- Save My Table
- Solve 360

Dados de empresas

ERP
- Acumatica ERP
- Blue Link Elite
- Epicor Express
- NetSuite
- OrderHarmony
- Plex Online

Saúde
- CECity
- SNO

Dados Pessoais
- Google Docs
- Microsoft Office
- Mint.com

Dados pessoais

http://cloudtaxonomy.opencrowd.com/taxonomy/

Dados sensíveis na cloud: Exemplos

Aplicações hospedadas na cloud

Billing
- Aria Systems
- eVapt
- nDEBIT
- Redi2
- Zuora

CRM
- 37 Signals
- Capsule
- Dynamics
- Intouchcrm
- LiveOps
- Oracle CRM
- Parature
- Responsys
- RO|Enablement
- Salesforce.com
- Save My Table
- Solve 360

ERP
- Acumatica ERP
- Blue Link Elite
- Epicor Express
- NetSuite
- OrderHarmony
- Plex Online

Saúde
- CECity
- SNO

Dados Pessoais
- Google Docs
- Microsoft Office
- Mint.com

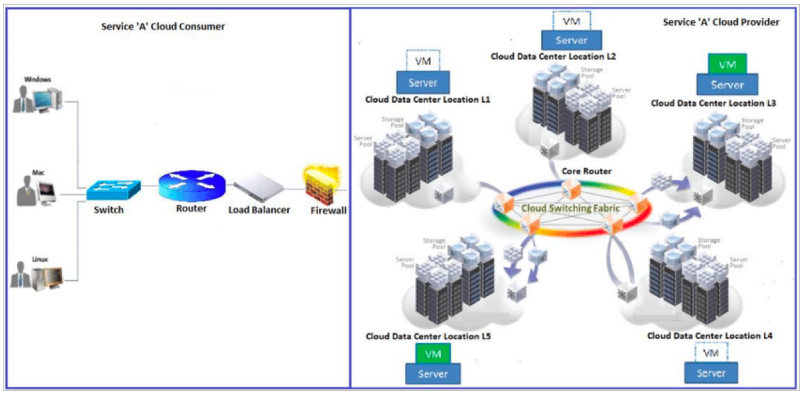
Dados pessoais

Como garantir a protecção de dados *outsourced* para a cloud?

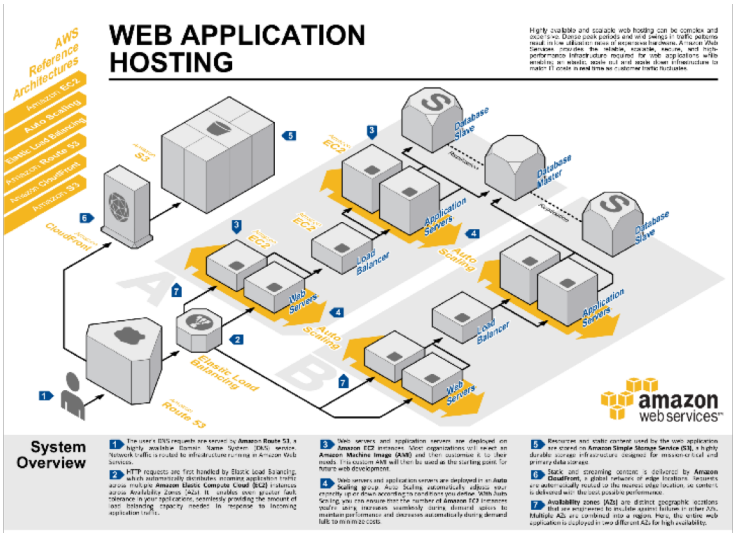
TÉCNICO LISBOA

Breve anatomia da cloud

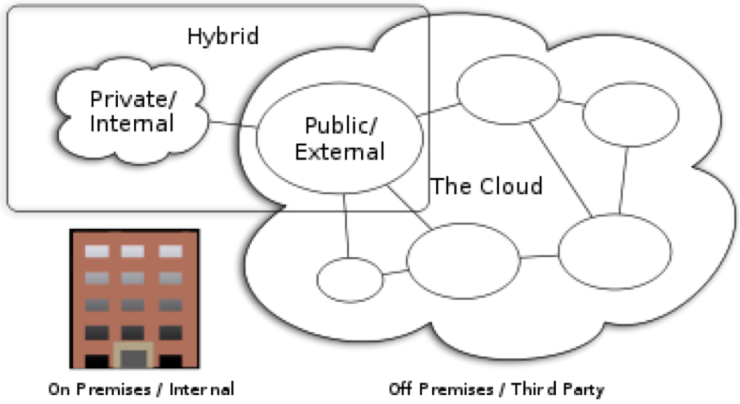
Arquitectura simplificada de uma cloud



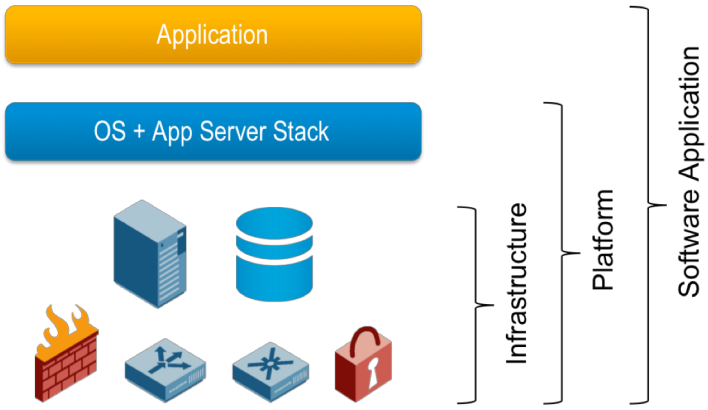
A coluna vertebral da cloud: Datacenters

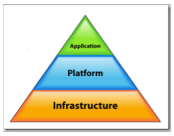


Modelos de cloud deployment



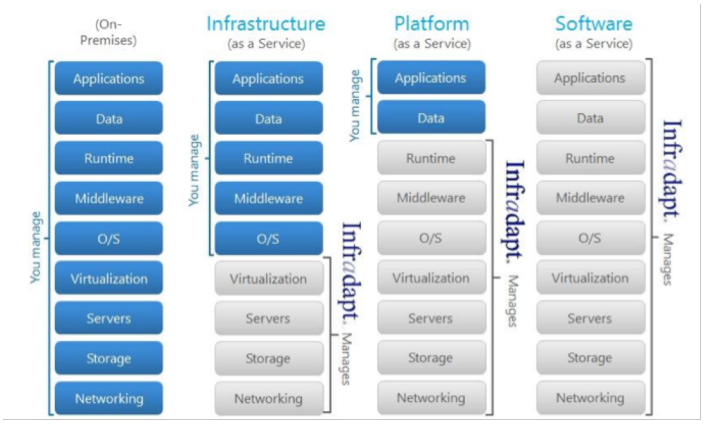
Modelos de cloud service delivery





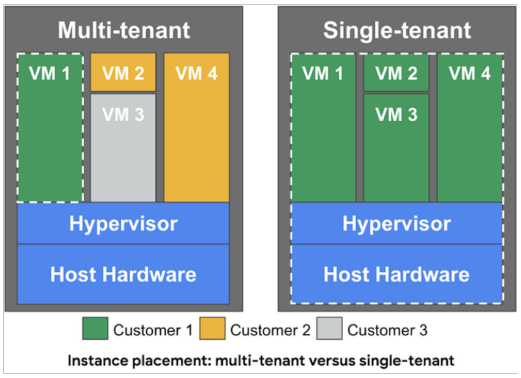
Modelos de cloud service delivery

- Três modelos principais: IaaS, PaaS, and SaaS
  - "You" – o cliente cloud; "Infradapt" – o provedor de serviço cloud



Virtualização muito usada na cloud

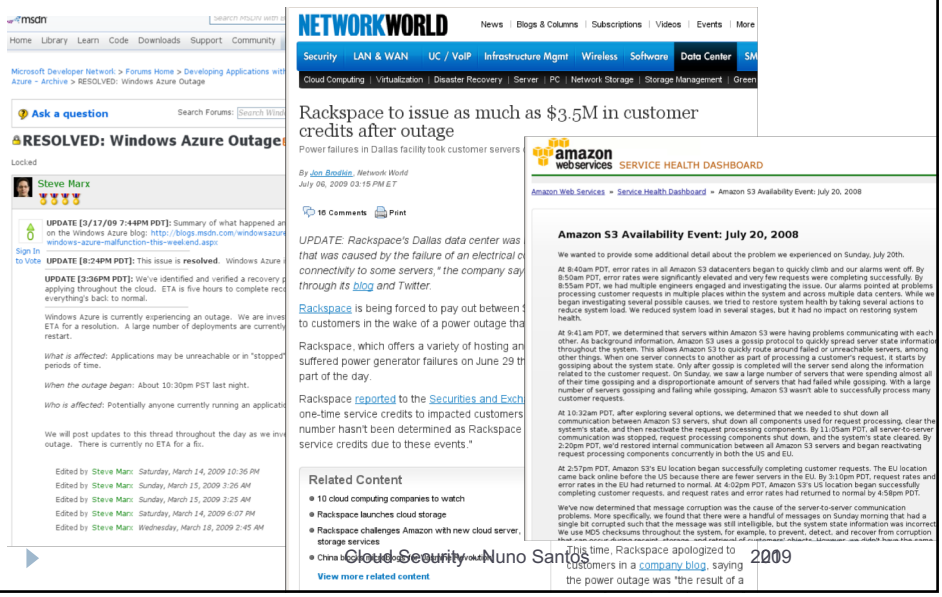
Permite particionar recursos entre utilizadores / aplicações; garante **isolamento**



TÉCNICO LISBOA

Principais riscos com a cloud

Downtimes



Perda de dados

"Regrettably, based on Microsoft/Danger's latest recovery assessment of their systems, we must now inform you that personal information stored on your device—such as contacts, calendar entries, to-do lists or photos—that is no longer on your Sidekick almost certainly has been lost as a result of a server failure at Microsoft/Danger."

Mais problemas de disponibilidade de dados

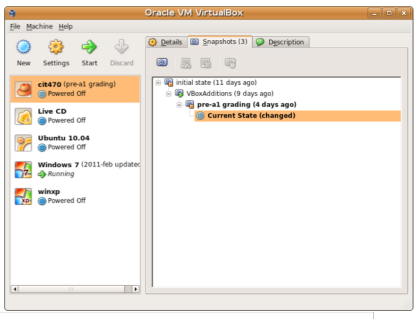
- O que acontece se a cloud for alvo de um ataque de DDoS?
- O que acontece aos meus dados se o cloud provider vai à falência?
- Será que a cloud consegue crescer a uma escala suficientemente grande?

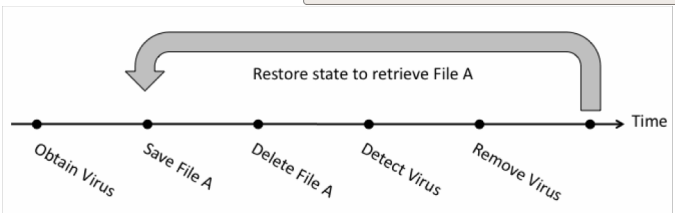
Confidencialidade e integridade dos dados

- **Confidencialidade**
  - Receio de perda de controlo sobre os dados:
    - Será que os dados irão permanecer confidenciais?
    - Será que ataques à cloud irão resultar em fugas de dados?
  - O cloud provider é honesto e não vai espreitar os dados?
- **Integridade**
  - Como é que eu sei que o cloud provider está a computar os dados correctamente?
  - Como garantir que o cloud provider guardou efectivamente os meus dados sem os corromper?

Tempo de vida dos dados

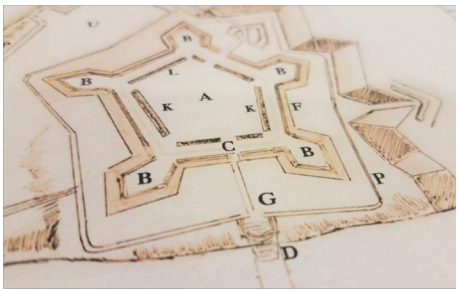
Ainda que os dados tenham sido correctamente tratados e / ou apagados, *snapshots* podem manter cópias antigas da memória e / ou disco da VM disk data.





Perímetro de segurança

- Pouco controlo sobre a localização física ou na rede de instâncias de VMs na cloud



Conformidade regulatória

Por exemplo: PCI DSS para cartões de crédito, e HIPAA para registos médicos

Certifications

Is AWS now PCI certified?

The AWS core infrastructure and services listed below are PCI DS
by an authorized independent Qualified Security Assessor.

PCI "certification" is a term reserved for those merchants who re
AWS, as a service provider, does not directly manage cardholder
not require certification). AWS provides a secure environment th
establish a secure cardholder environment and to achieve their o
underlying technology infrastructure is compliant. Achieving PCI D
helps our customers obtain their own PCI certification.

Service provider levels are defined as:

- Level 1: Any service provider that stores, processes and/
- Level 2: Any service provider that stores, processes and/
  annually

What Amazon Web Services product offerings
transmission of credit card data?

Services that support the processing, storage, and transmission
have been validated as being compliant with PCI standards. Thes

- Amazon Elastic Compute Cloud (EC2)
- Amazon Simple Storage Service (S3)
- Amazon Elastic Block Storage (EBS)
- and Amazon Virtual Private Cloud (VPC)

ISO 27001 Certification

The following information will help you understand in greater detail why ISO 27001 certification is important and how it helps to demonstrate our commitment to providing a secure infrastructure for your business-critical applications and data.

What is ISO 27001 certification?

ISO 27001 is a security management standard that specifies security management best practices and comprehensive security controls following the ISO 27002 best practice guidance. This is a widely-recognized international security standard in which our customers showed significant interest. Certification in the standard requires us to:

- Systematically evaluate our information security risks, taking into account the impact of company threats and vulnerabilities
- Design and implement a comprehensive suite of information security controls and other forms of risk management to address company and architecture security risks
- Adopt an overarching management process to ensure that the information security controls meet the our information security needs on an ongoing basis

The key to the ongoing certification under this standard is the effective management of a rigorous security program. The Information Security Management System (ISMS) required under this standard defines how we perpetually manage security in a holistic, comprehensive way. The ISO 27001 certification is specifically focused on the AWS ISMS and measures how our internal processes follow the ISO standard. Certification means a third party accredited independent auditor has performed an assessment of our processes and controls and confirms they are operating in alignment with the comprehensive ISO 27001 certification standard.

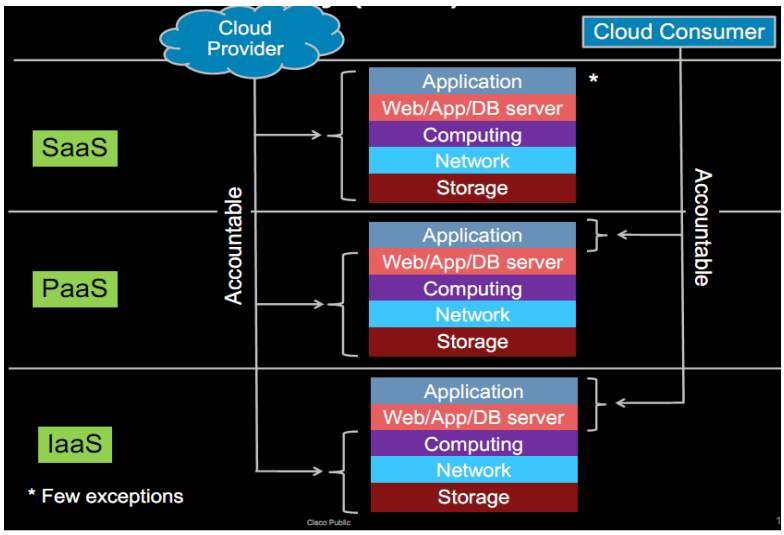
How does this certification impact AWS?

AWS welcomes the ISO 27001 standard and best practices into our organization. The certification confirms our longstanding commitment to the security of our services to our customers. Going through the certification process confirms that we are addressing each element of the ISO standard and that our management practices follow internationally-recognized best practices.

What does this mean to you as a customer?

Our ISO 27001 certification demonstrates our commitment to information security at every level. Compliance with this internationally-recognized standard, validated by an independent third-party audit, confirms that our security [illegible] leading practices. This certification provides more clarity and assurance for customers evaluating the breadth and strength of our security practices.

Accountability (apurar responsabilidades)

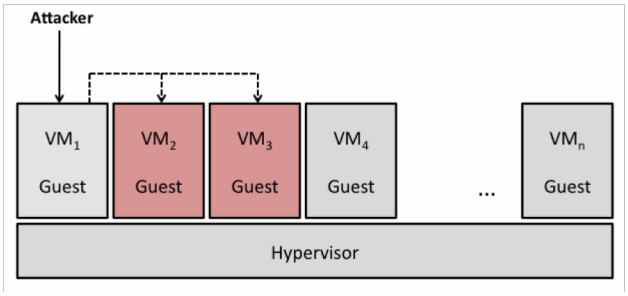


Fraca auditabilidade

- Só o cloud provider tem acesso a todo o tráfego de rede, logs do hypervisor, dados da máquina física
- É necessária **auditabilidade mútua:**
  - Possibilidade do cloud provider poder auditar VMs cliente potencialmente maliciosas ou infectadas
  - Possibilidade do cliente auditar o ambiente do cloud provider

Ataques inter-VM

- Ataque através de um clipboard partilhado
  - http://www.securiteam.com/securitynews/5GP021FKKO.html
- Pasta partilhada permitie alterar imagem do disco de VMs
  - CVE-2007-1744



Ataques side channel

- Os clientes não sabem com que VMs a máquina física está a ser partilhada
  - Atacantes podem colocar as suas VMs no mesmo host
- Recursos físicos partilhados incluem
  - CPU data cache
  - CPU branch prediction
  - CPU instruction cache
- Num ambiente OS sem ser partilhado, é possível extrair chaves criptográficas com estes ataques
  - Também é possível num ambiente virtualizado

Segurança hypervisor

Consequências de vulnerabilidades

- Execução de código guest com privilégios
- Fuga da VM (Host code execution)

Vendor	CVEs
KVM	32
QEMU	23
VirtualBox	9
VMware	126
Xen	86

Home > Support & Downloads > Support Resources > Security Advisories

VMware Security Advisories (VMSAs)

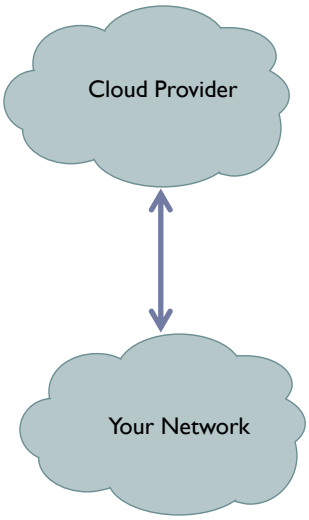
VMSA-2009-0006

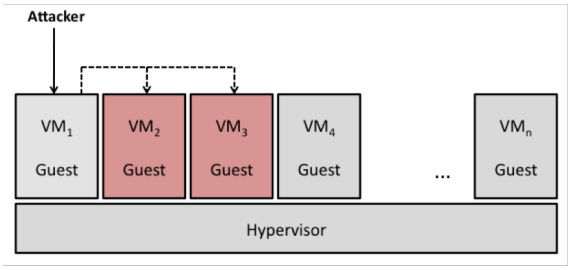
VMware Hosted products and patches for ESX and ESXi resolve a critical security vulnerability

```
-------------------------------------------------------------------------
                    VMware Security Advisory

Advisory ID:        VMSA-2009-0006
Synopsis:           VMware Hosted products and patches for ESX and ESXi
                    resolve a critical security vulnerability
Issue date:         2009-04-10
Updated on:         2009-04-10 (initial release of advisory)
CVE numbers:        CVE-2009-1244
-------------------------------------------------------------------------

1. Summary

   Updated VMware Hosted products and patches for ESX and ESXi resolve a
   critical security vulnerability.

2. Relevant releases

   VMware Workstation 6.5.1 and earlier,
   VMware Player 2.5.1 and earlier,
   VMware ACE 2.5.1 and earlier,
   VMware Server 2.0,
   VMware Server 1.0.8 and earlier,
   VMware Fusion 2.0.3 and earlier,

   VMware ESXi 3.5 without patch ESXe350-200904201-O-SG,

   VMware ESX 3.5 without patch ESX350-200904201-SG,

   VMware ESX 3.0.3 without patch ESX303-200904403-SG,

   VMware ESX 3.0.2 without patch ESX-1008421.

   NOTE: General Support for Workstation version 5.x ended on 2009-03-19.
         Users should plan to upgrade to the latest Workstation version
         6.x release.

         Extended support for ESX 3.0.2 Update 1 ends on 2009-08-08.
         Users should plan to upgrade to ESX 3.0.3 and preferably to the
         newest release available.

3. Problem Description

   a. Host code execution vulnerability from a guest operating system

      A critical vulnerability in the virtual machine display function
      might allow a guest operating system to run code on the host.

      This issue is different from the vulnerability in a guest virtual
      device driver reported in VMware security advisory VMSA-2009-0005
      on 2009-04-03. That vulnerability can cause a potential denial of
      service and is identified by CVE-2008-4916.

      The Common Vulnerabilities and Exposures project (cve.mitre.org)
      has assigned the name CVE-2009-1244 to this issue.
```

Xen CVE-2008-1943
VBox CVE-2010-3583

Superfície de ataque alargada





- Ligação entre o cloud provider e a rede do cliente pode ser comprometida
- Cloud provider pode ser atacado, ex., empregados podem ser phished

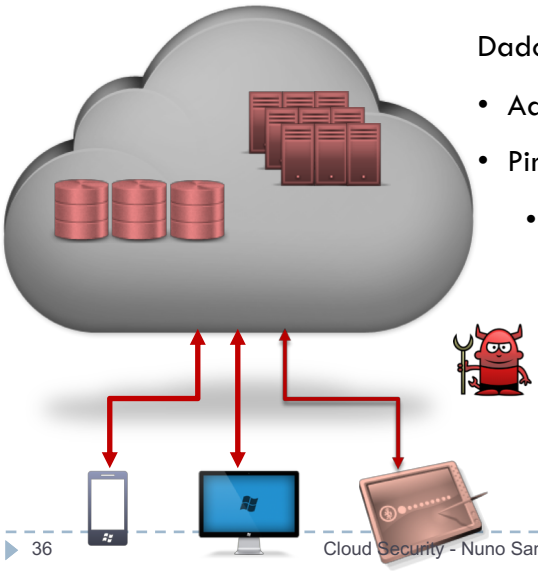
Causas dos problemas de segurança na cloud

- A maior parte dos problemas derivam de:
  - Perda de controlo
  - Perda de confiança
  - Partilha de recursos (multi-tenancy)
- Estes problemas existem sobretudos em modelos de gestão que envolvem uma 3º partido
  - Clouds "self-managed" ainda têm problemas de segurança, mas não relaciondas com as de cima

TÉCNICO LISBOA

Protecção de dados na cloud

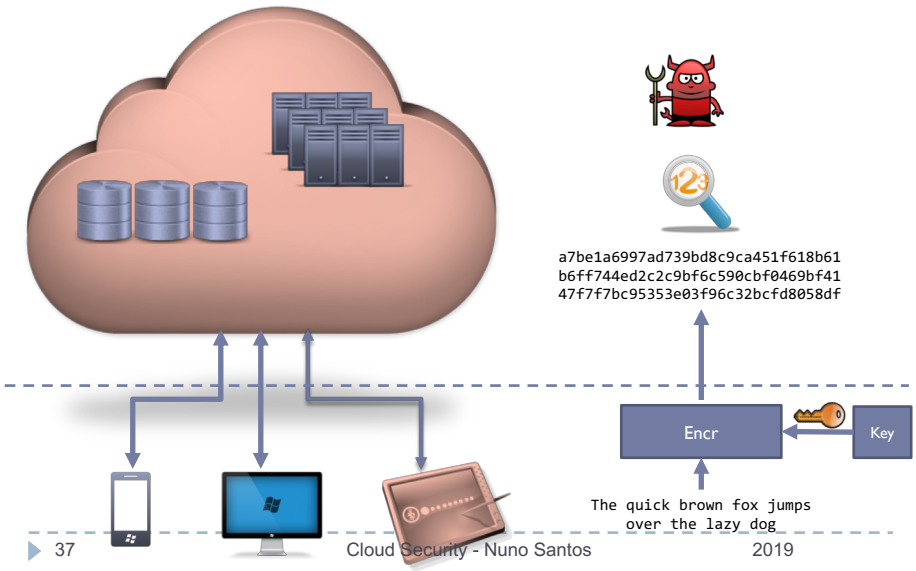
Um problema de segurança particularmente difícil



Dados na cloud vulneráveis a:

- Administradores curiosos
- Piratas com acesso ilegal
  - Servidores comprometidos

Abordagem natural: Encriptação de dados

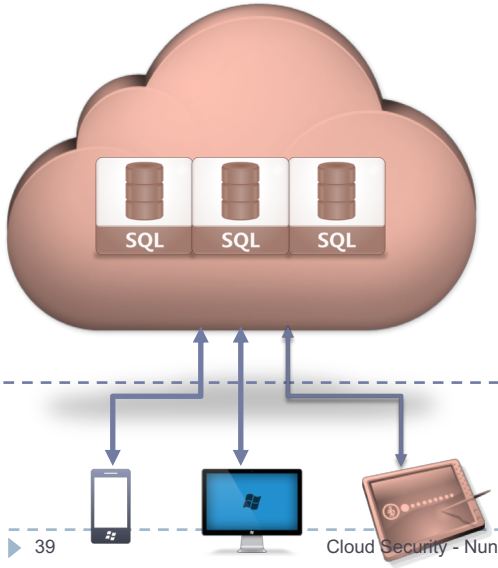


Recomendação de segurança da Amazon AWS

7.2. Security. We strive to keep Your Content secure, but cannot guarantee that we will be successful at doing so, given the nature of the Internet. Accordingly, without limitation to Section 4.3 above and Section 11.5 below, you acknowledge that you bear sole responsibility for adequate security, protection and backup of Your Content. We strongly encourage you, where available and appropriate, to use encryption technology to protect Your Content from unauthorized access and to routinely archive Your Content. We will have no liability to you for any unauthorized access or use, corruption, deletion, destruction or loss of any of Your Content.

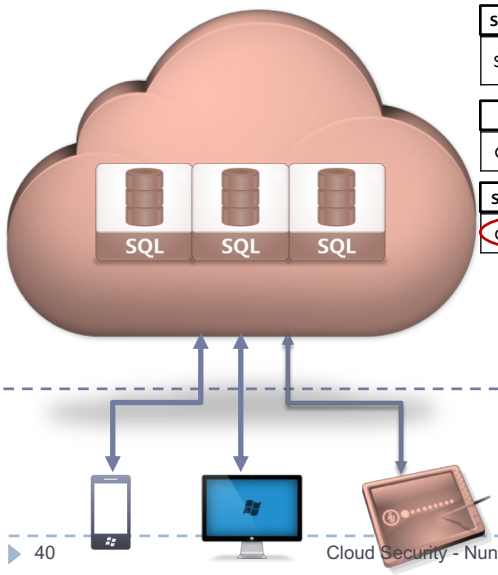
Source: http://aws-portal.amazon.com/gp/aws/developer/terms-and-conditions.html

E se os dados estiverem em bases de dados?



Que implicações tem a encriptação de dados em termos de funcionalidade?

Exemplo: Base de dados de curso online



Student

StudentId	Name	Addr	GPA	CreditCard	…

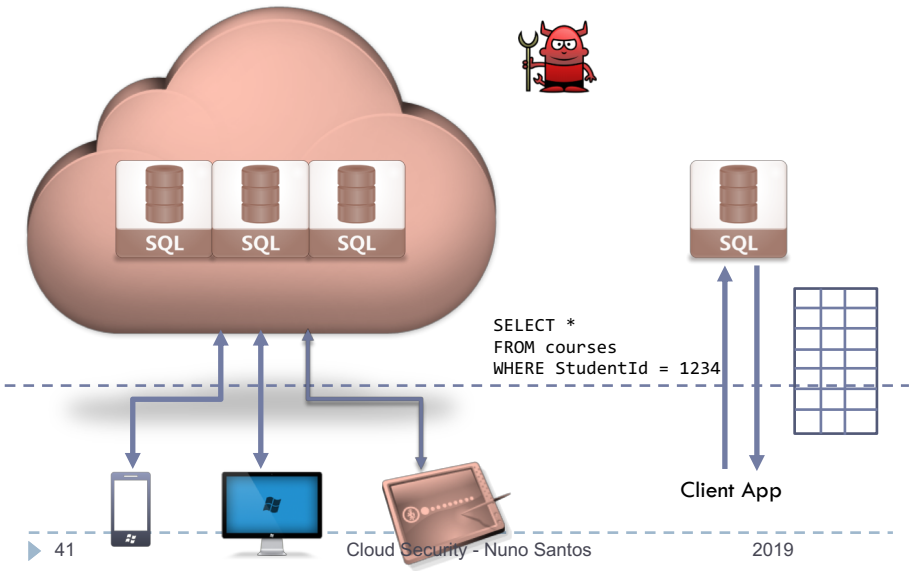
Course

CourseId	Name	InstrId	…

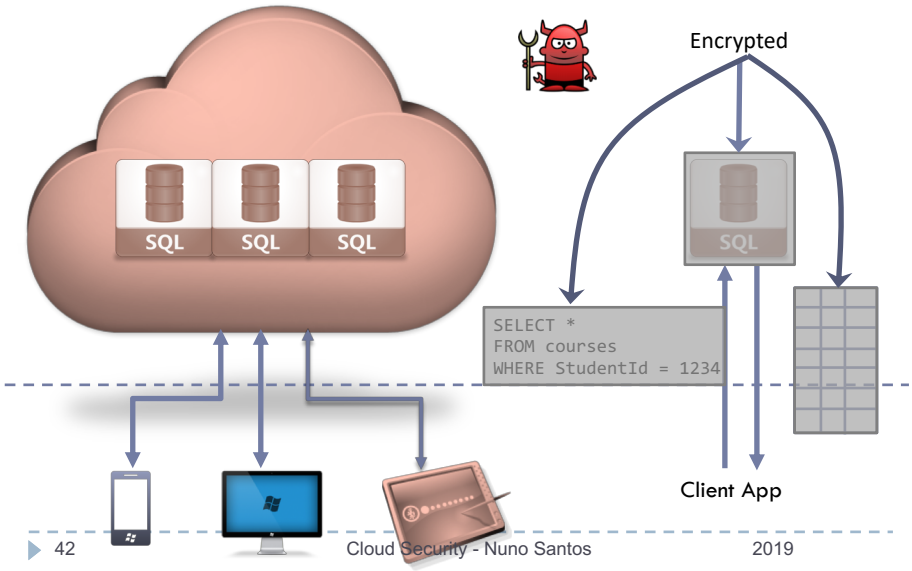
StudentCourse

CourseId	StudentId	Grade	…

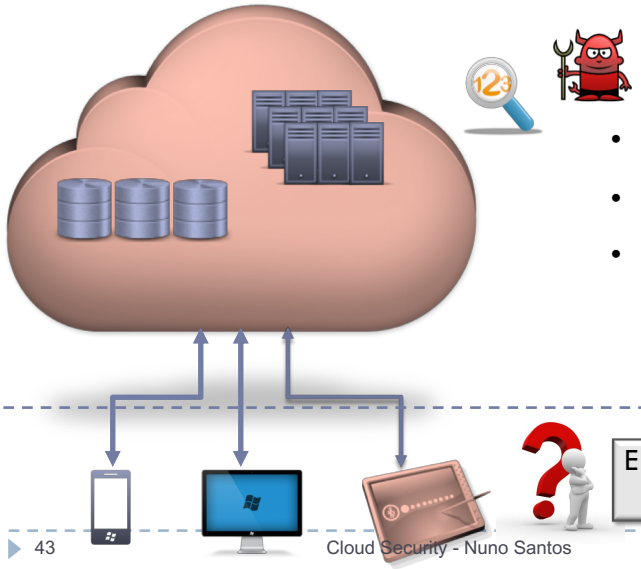
Encriptação e bases de dados: Funcionalidade



Encriptação e bases de dados: Funcionalidade



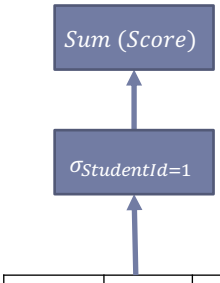
Adversário passivo



- Passivo
- Honesto mas curioso
- Não altera:
  - Base de dados
  - Resultados

E para adversários activos?

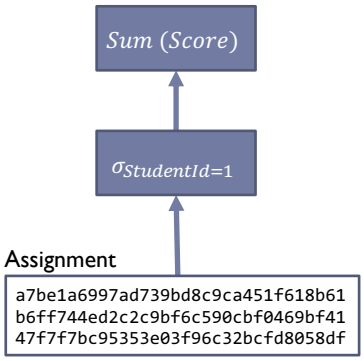
Encriptação: Um desafio de fundo



StudentId	AssignId	Score
1	1	68
1	2	71
3	4	99
...	...	...

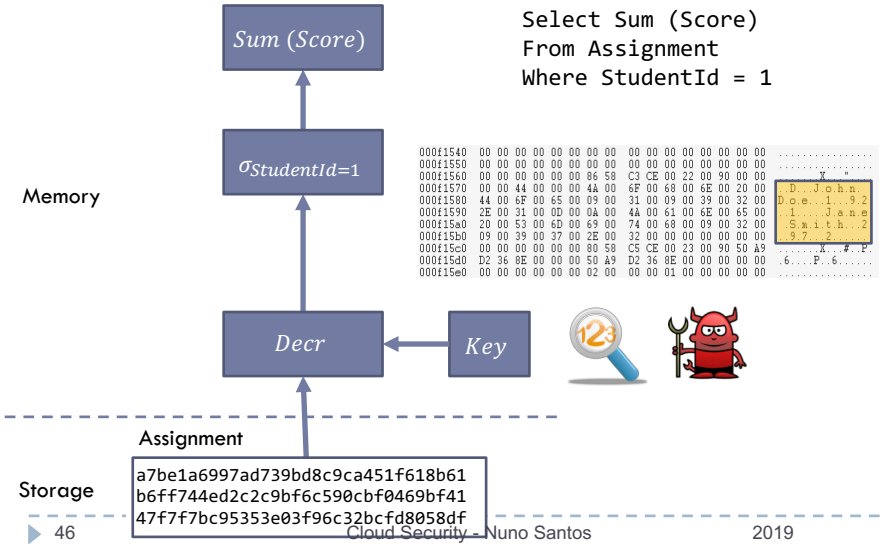
```
Select Sum (Score)
From Assignment
Where StudentId = 1
```

Encriptação: Um desafio de fundo




```
Select Sum (Score)
From Assignment
Where StudentId = 1
```


Encriptação: Um desafio de fundo

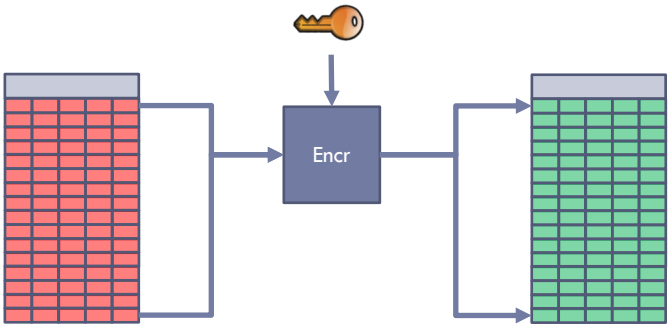



```
Select Sum (Score)
From Assignment
Where StudentId = 1
```

Espectro de soluções

- Duas abordagens fundamentais:
  - Computar directamente sobre dados cifrados
  - Computar os dados num ambiente seguro

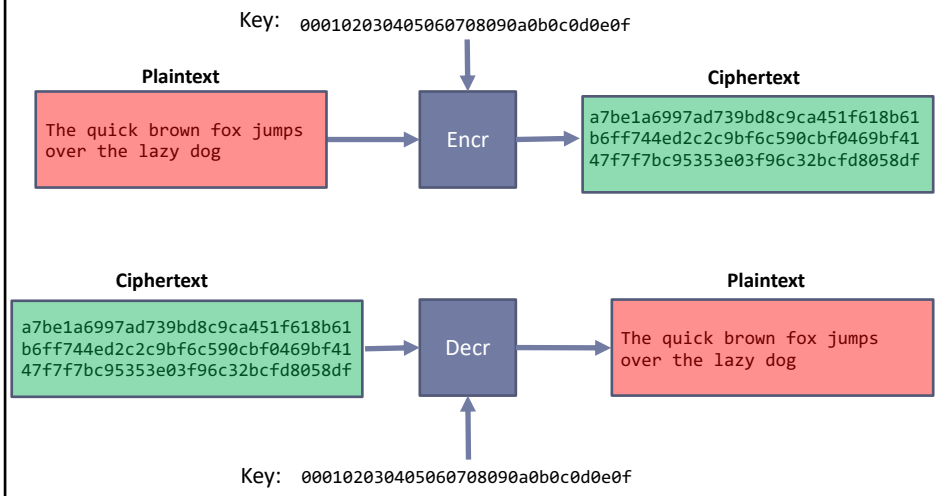
Como cifrar a base de dados?



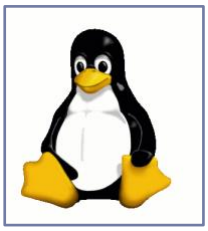
Cell granularity

E ainda assim, permitir a realização de operações sobre os dados sem ter que os decifrar?

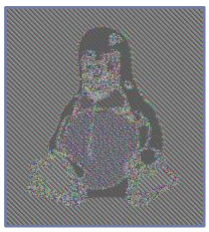
Esquema criptográfico (chave simétrica)



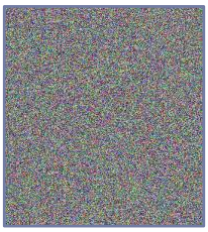
Segurança forte implica não determinismo



Original



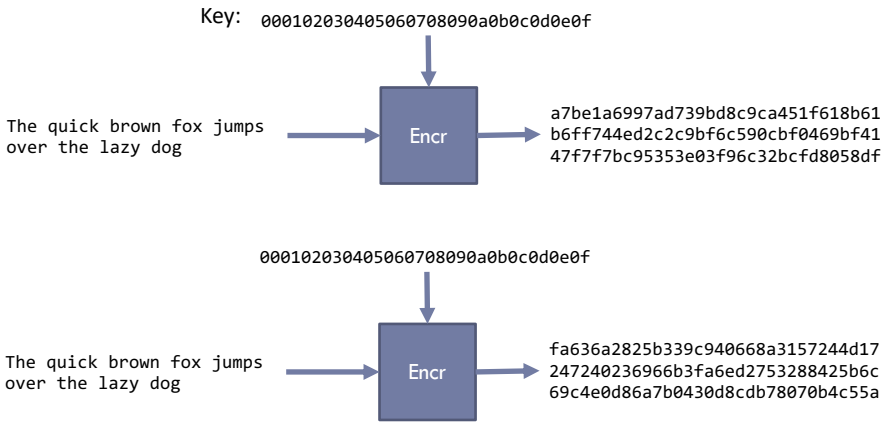
Deterministic



Non-Deterministic

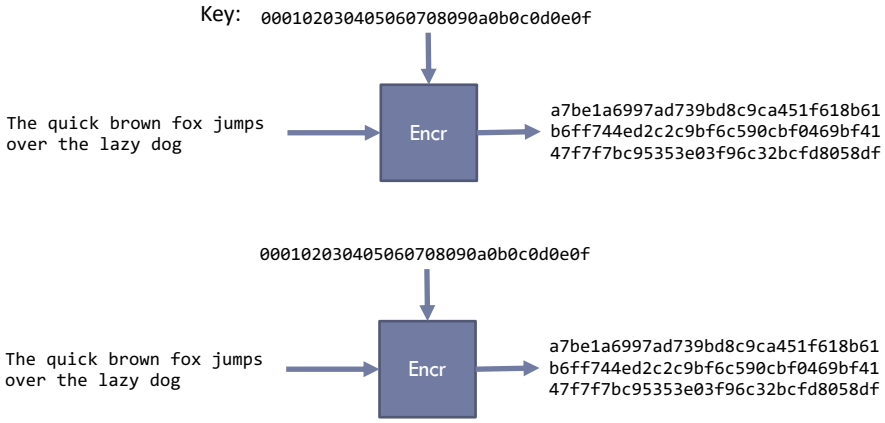
Source: http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

Esquema de encriptação não determinista



Example: AES + CBC + variable IV

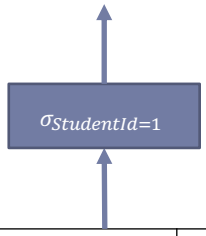
Esquema de encriptação determinista



Example: AES + ECB

Usando encriptação determinista

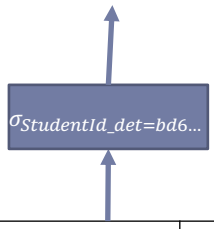
```
select *
from assignment
where studentid = 1
```



StudentId	AssignId	Score
1	1	68
1	2	71
3	4	99
...	...	...

Usando encriptação determinista

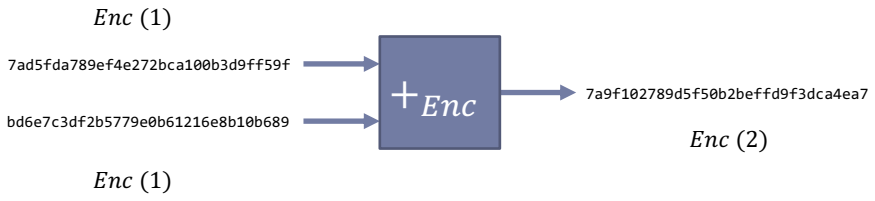
```
select *
from assignment
where studentid_det = bd6e7c3df2b5779e0b61216e8b10b689
```



StudentId_DET	AssignId	Score
bd6e7c3df2b5779e0b61216e8b10b689	1	68
bd6e7c3df2b5779e0b61216e8b10b689	2	71
7ad5fda789ef4e272bca100b3d9ff59f	4	99
...	...	...

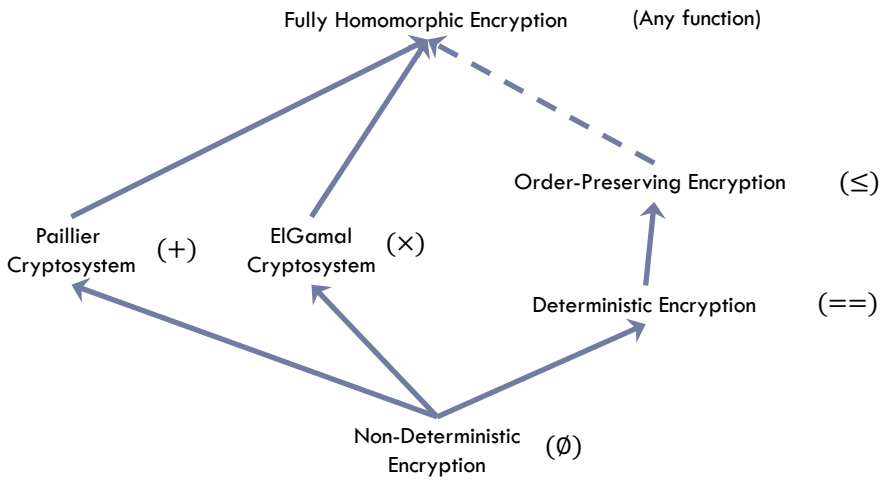
E se quiseremos somar as notas?

Encriptação homomórfica

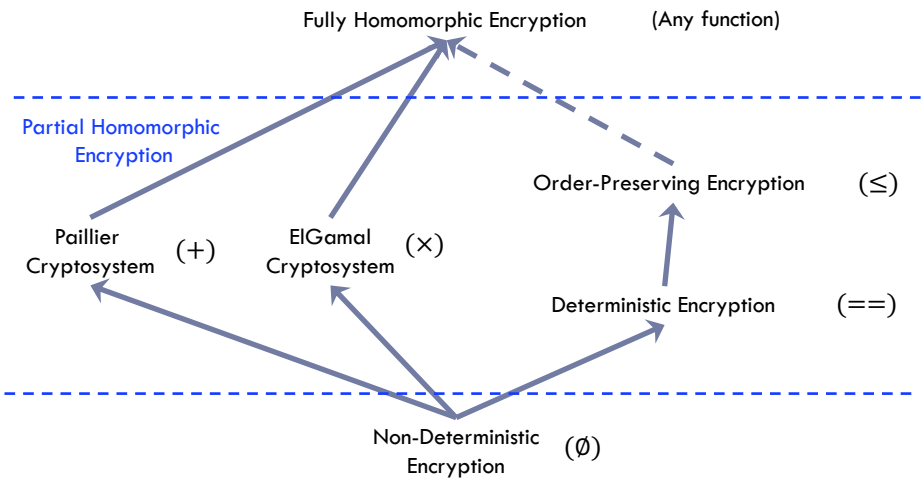


A chave de encriptação não é um input

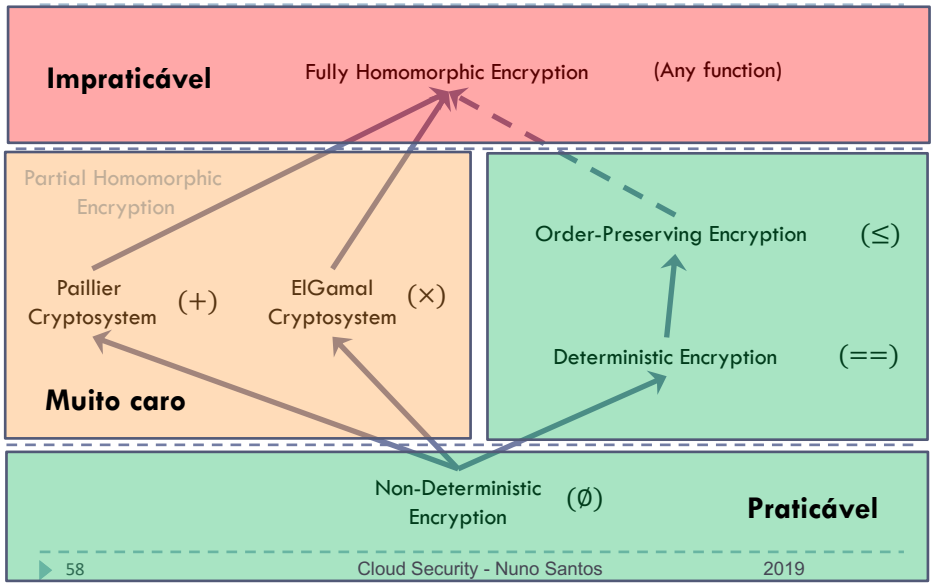
Esquemas de encriptação homomórfica



Esquemas de encriptação homomórfica



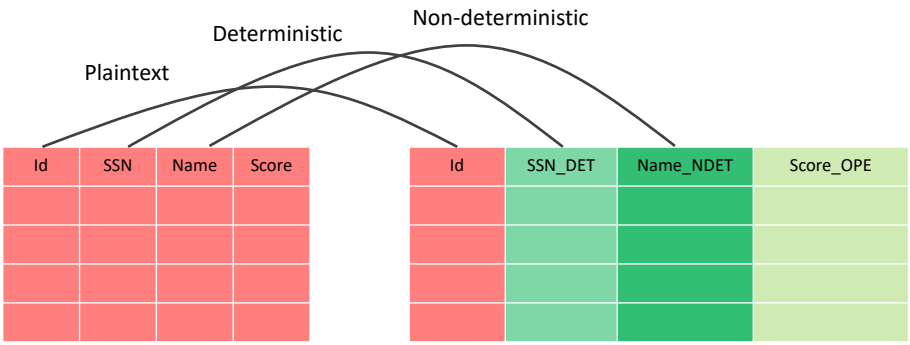
Esquemas de encriptação homomórfica



Esquemas de encriptação homomórfica: Performance

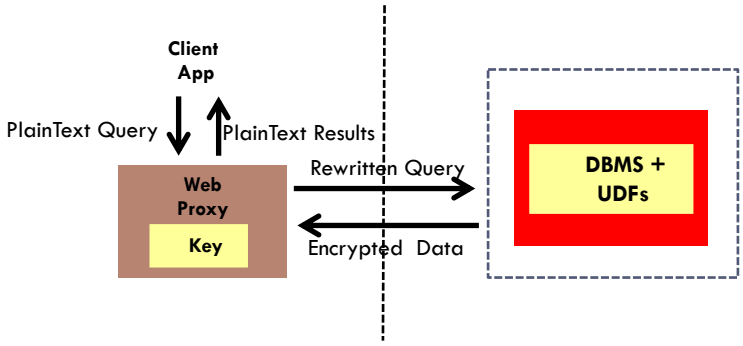
Scheme	Space for 1 integer (bits)	Time for 1 operation
Fully Homomorphic Encryption	2^{14}	Cosmic time scales
Paillier ElGamal	2048	≈ ms
Deterministic Order-preserving	128	≈ µs

Como cifrar a nossa base de dados?



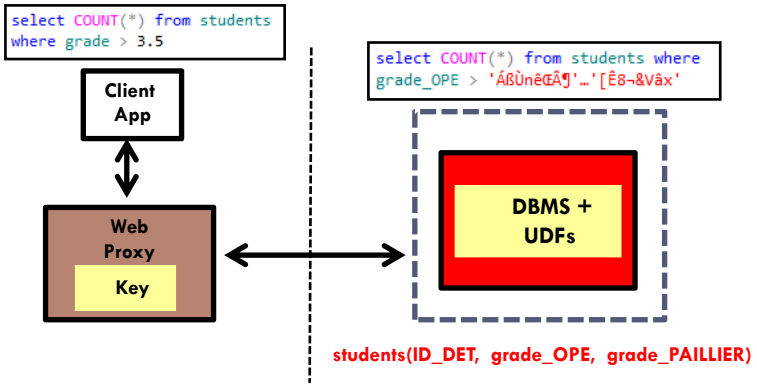
Esquema de encriptação Mix n Match

Um sistema representativo: CryptDB



- Web proxy reescreve as queries, e decifra o resultado
  - Utiliza técnicas de encriptação parcialmente homomórfica
  - https://css.csail.mit.edu/cryptdb/

Processamento das queries



Limitações encriptação parcialmente homomórfica

- PHE não é de "borla" – overheads de espaço
  - Para Paillier, um inteiro (32 bits) resulta em ciphertext de 2048 bits!
- PHE é por natureza limitado – não suporta todo SQL

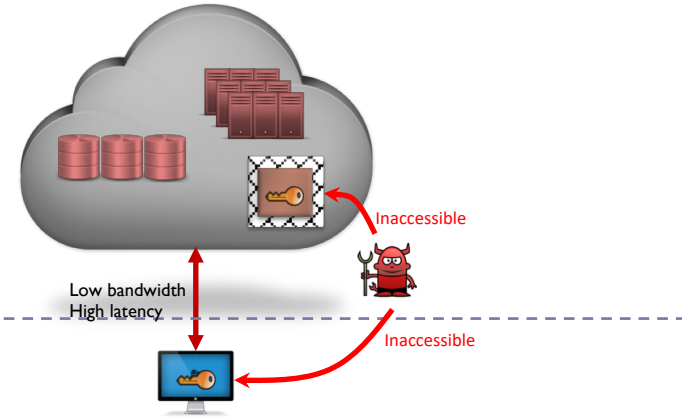
```
select STDEV(grade) from students
```

- Tradeoffs funcionalidade e segurança
- Overheads em termos de desempenho

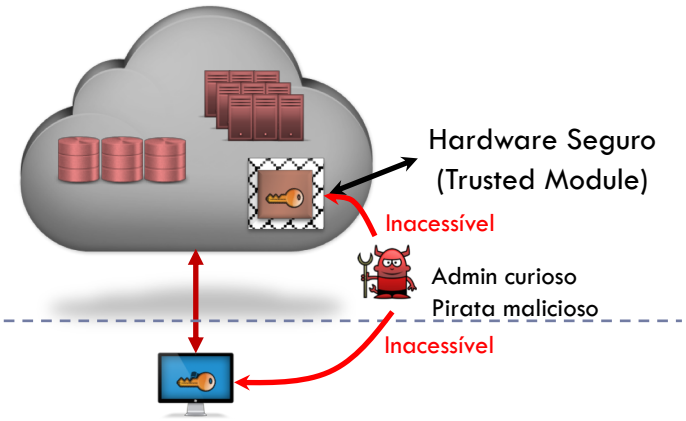
Espectro de soluções

- Duas abordagens fundamentais:
  - Computar directamente sobre dados cifrados
  - **Computar os dados num ambiente seguro**

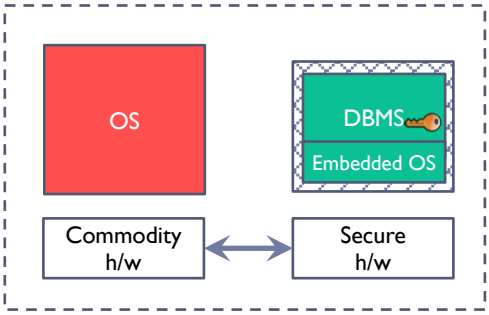
Processamento seguro na cloud



Processamento seguro na cloud c/ hw seguro



Ideia chave: Isolamento



Algumas tecnologias de hardware seguro

- Co-processador seguro
  - ATMs, smart cards
- Hardware Security Modules
  - Cripto-aceleração tamper-proof
- FPGAs
  - Para uso militar
- Chips TPM
  - Laptops, etc.

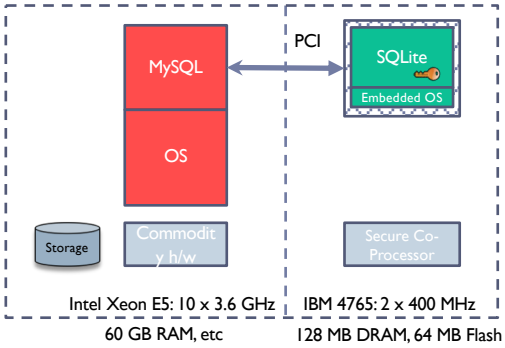
IBM 4764 PCI-X Cryptographic Coprocessor

Secure FPGA

TrustedDB: Baseado em co-processadores

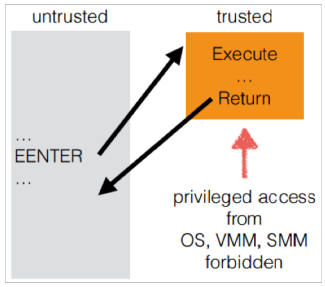
Sensitive columns

```
SELECT SUM(l_extendedprice * l_discount) as revenue
FROM  lineitem
WHERE l_shipdate >= '1993-01-01'       AND
      l_shipdate < '1994-01-01'        AND
      l_discount between 0.05 and 0.07 AND
      l_quantity < 24
```

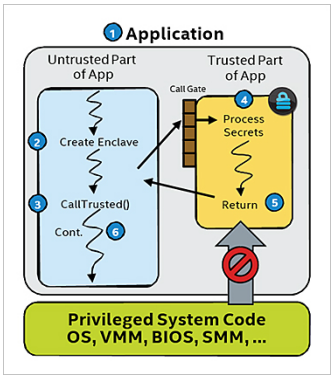


Tecnologia mais recente: Intel SGX

- Novo modo do processador: enclave
- Aplicação pode criar um ambiente de execução protegido assegurado por HW, inacessível ao OS
- Aplicação apenas precisa confiar na Intel e na implementação SGX

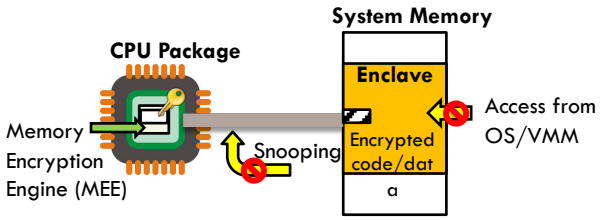


Intel SGX: Exemplo em runtime



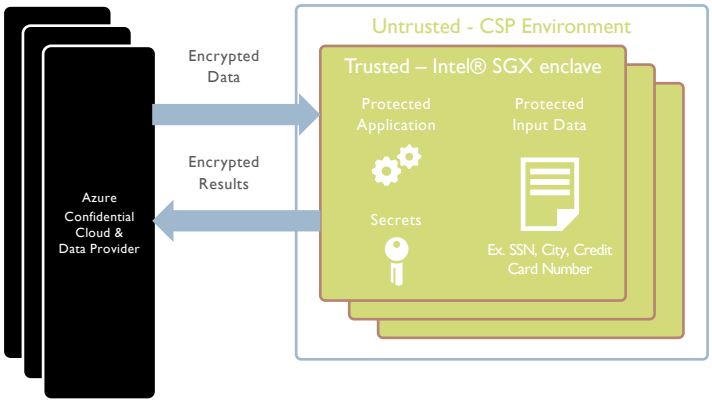
1. App tem componentes trusted e untrusted
2. App cria enclave, enclave é área de memória protegida por CPU, e OS não pode aceder
3. App chama a parte trusted, e executa-se em ambiente protegido
4. Dados no enclave em plaintext, não podem ser acedidos de fora e vão ser cifrados logo que saiam do enclave
5. App termina a tarefa do enclave e retorna
6. App continua em ambiente comum

Intel SGX, isolated execution



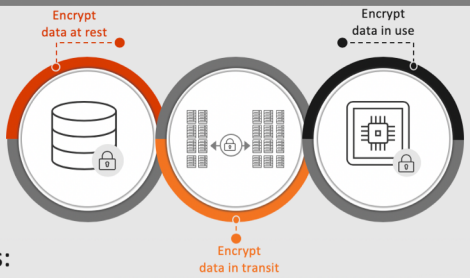
- Aplication mantém os dados e código dentro do enclave
  - Menor superfície de ataque possível (aplicação + processor)

Já suportado pelos serviços da MS Azure



MS Azure e TEEs baseados em SGX

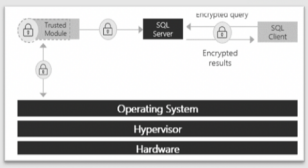
Azure Confidential Cloud Trusted Execution Environments (TEE's)



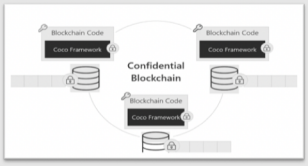
All use cases are currently 128MB EPC enabled

Current Use Cases:

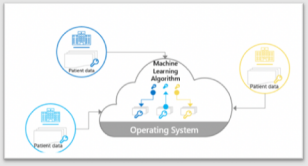
Confidential SQL



Blockchain



Confidential Multiparty Machine Learning



Conclusões

- Cloud computing constitui um modelo muito atractivo para tratamento de dados, mas que também acarreta problemas e segurança
- Existem novos desafios na protecção de dados migrados para a cloud que resultam do modelo de partilha de controlo de dados entre o dono e o cloud provider
- Duas aborgens actualmente em estudo para garantir a segurança dos dados na cloud consistem na utilização de encriptação parcialmente homomórfica e hardware seguro