technology
from seed

Clouds-of-Clouds: Segurança e Confiança no Funcionamento nas Nuvens

Miguel P. Correia
Trabalho conjunto com A. Bessani, F. Rocha, B. Quaresma, F. André, P. Sousa (Universidade de Lisboa, Fac. Ciências)
UNICAMP, 3 de Maio de 2011

Cloud computing (public cloud)

technology
from seed

- Cloud provider vs cloud users
- Fundamental ideas
  - Computing as a utility
  - Pay-as-you-go
  - Resource pooling
  - Elasticity
- Large-scale datacenters

Cloud computing models

Service models:

- *Infrastructure as a Service* (IaaS): virtual machines, storage (e.g., Amazon EC2, Amazon S3)
- *Platform as a Service* (PaaS): programming and execution (e.g., Google AppEngine, Force.com, Windows Azure)
- *Software as a Service* (SaaS): mostly web applications (e.g., Yahoo! Mail, Google Docs, Facebook,…)

Security in the cloud (from the user viewpoint)

- Security is a key aspect of cloud computing
  - Reason in favor and against adoption
- Recall the three attributes – all important in the cloud
  - Confidentiality – no disclosure of data to unauthorized entities
  - Integrity – no unauthorized modifications of the system or data
  - Availability – readiness of the system to provide its service
- Challenges
  - The system is no longer in the organization premises
  - The system is shared with other users
  - The access is made through the internet

Outline

- Security threats in the cloud
- Stealing confidential data in the cloud
- DepSky: Dependable and Secure Storage in a Cloud-of-Clouds
- DepSky Evaluation
- Conclusions

Security threats in the cloud

Unavailability

- Problems in the Internet – relatively frequent
  - Congestion
  - Problems in the equipment of client or ISP (routers, etc.)
  - More global problems (Cisco bug + RIPE NCC test Aug. 2010)
- Problems at the cloud (e.g., Google AppEngine, Apr. 2011)
- Denial of service attacks (e.g., Amazon EC2 2009)

RIPE NCC and Duke University BGP Experiment

On 27 August 2010, the RIPE NCC's Routing I
was involved in an experiment using optional a
Gateway Protocol (BGP). As a result of this ex
significant percentage of global Internet traffi
of about 30 minutes. The following article provides som
on the experiment itself and its effect on the network.

DDoS attack rains down on Amazon cloud

Code haven tumbles from sky

By **Cade Metz in London** · **Get more from this author**

Posted in Enterprise Security, 5th October 2009 15:32 GMT

Sign up for The Reg enterprise storage newsletter

Updated Web-based code hosting service Bitbucket experienced more than 19 hours of downtime over the weekend after an apparent DDoS attack on the sky-high compute infrastructure it rents from Amazon.com.

Loss and corruption of data

Can happen in the cloud as anywhere else

- Danger Inc. / Sideckick lost contacts, notes, photos etc. of its clients; took days to recover them (Oct. 2009)
- Ma.gnolia lost all data from all clients, half TB (Feb.2009)

Ma.gnolia Suffers Major Data Loss, Site Taken Offline

By Michael Calore January 30, 2009 | 12:56 pm | Categories: Uncategorized

Cloud computing takes hit in Sidekick data loss

Share

The "cloud" turned stormy for Microsoft Corp. this weekend, after a technical glitch apparently wiped out personal data for users of the T-Mobile Sidekick smartphone.

A Microsoft unit aptly named Danger Inc. based its operation on the cloud model, which provides computing power and storage at big remote datacenters.

In theory, if the phones were lost or destroyed, the photos, contacts, to-do lists and calendars still would be available. That supposedly offered a big advance in safety, security and efficiency.

Attacks through management interface

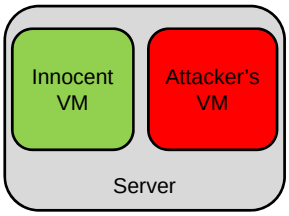
- In the cloud the *attack surface* is expanded with the *cloud management interface*
  - Control/monitoring of virtual machines, users, etc.
  - Web console, web services, REST
- Attacks through the interface
  - Vulnerabilities that allow personification of legitimate user: CSRF, SQL injection, etc.
  - Microsoft, “Secure Use of Cloud Storage”, July 2010
- Phishing / social engineering to obtain authentication credentials

Attacks against the billing scheme

- Billing is a function of the usage of
  - Virtual machines/hour, traffic received/sent, CPU time consumed
- Certain attacks can cost – directly – money:
- High number of accesses/requests/…
  - Some cloud services use automatically more resources if the usage increases (elasticity)
  - Related to DDoS attacks)
- Also through the management interface
  - Attacker requires allocation of, e.g.,1 million VMs

Attacks between VMs

- In IaaS, VMs of several users can share the same physical machine (co-residence)
  - Only recently Amazon started allowing a user to ask for no co-residence



Attack in two steps

- The attacker instantiates several VMs until co-residence with the victim is achieved
- The attacker's VM attacks the victim
  - e.g., using a vulnerability in the hypervisor
  - or using shared resources to obtain confidential information

Confidentiality/privacy violation

- Data is in the cloud provider's machines
  - The provider may be trusted; there are legal defenses; but
- There can be a malicious insider
  - Can capture passwords, private keys, software, etc.
  - Not specific in the cloud, but the cloud operators are unknown/…
- Data can't be encrypted (or it can't be processed)

CRIMINAL JUSTICE

Producer Sues ISP and its Fired Employee, Saying Hack Destroyed Season of Kids' TV Series

Posted Apr 1, 2011 4:13 PM CDT
By Intern

Email Print Reprints Shar

A new lawsuit alleges a fired employee hacked into his f
deliberately destroyed an entire season of a syndicated

JULY 18, 2008

Why San Francisco's network admin went rogue

An inside source reveals details of missteps and misunderstandings in the curious case of Terry Childs, network kidnapper

By Paul Venezia | InfoWorld

technology from seed

inesc id lisboa

Stealing confidential data in the cloud

Lucy in the Sky *without* Diamonds: Stealing Confidential Data in the Cloud,
F. Rocha, M. Correia, *DCDV 2011 (with DSN'11)*

Motivation

technology from seed

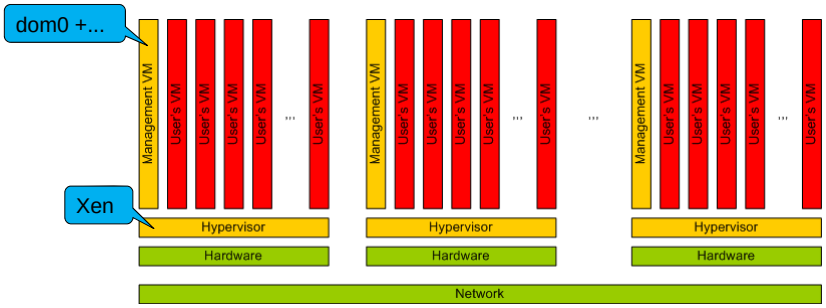
inesc id lisboa

- Many people don't understand/believe attacks can happen
- Same as years ago with critical infrastructure protection:
  - Researchers launched an experimental cyber attack that caused a generator to self-destruct – sponsored by the US DHS

Infrastructure as a Service and Virtualization

technology from seed

- Servers run an Hypervisor (or VMM) that supports the execution of several Virtual Machines (VMs)
  - VMs have the illusion of running on top of the hardware so they have their own OS



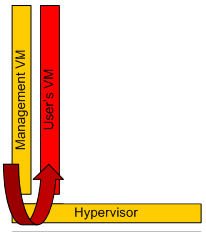
What can the administrators do in commercial IaaS?

technology from seed

- We have to guess from info available
  - Amazon EC2, open source implementations (Open Stack, Open Nebula, Eucalyptus…)
- Some administration operations:
  - Instantiate VM, delete VM
  - Login in the management VM of the servers
  - Migrate VMs to other servers
  - Take memory snapshots (needed for migration)
  - Mount file systems (needed for backups)
- *This is what can be available to a malicious insider!*

What we did

- We run several attacks to demonstrate that it is possible to access the cloud user's data
  - That was the initial objective; we've shown that it's easy!
- In the attacks, the cloud was a single machine
  - Xen, Dom 0 was Linux (Ubuntu)
  - Only 1 VM (victim) with Linux and the Apache web server
- Attack model
  - Malicious insider with access to the management VM (dom 0)
  - Attacker has no login in the victim VM



Attack 1: Cleartext passwords in memory snapshots

- Trivial: just take a snapshot *(dumpcore)* and look for passwords!

```
$ xm dump-core 2 -L lucidomu.dump
Dumping core of domain: 2 ...
$ cat lucidomu.dump | strings | grep loginpwd
loginpwd
loginpwd
$ cat lucidomu.dump | strings | grep apachersapwd
apachersapwd
apachersapwd
apachersapwd
```

Attack 2: Obtaining private keys using memory snapshots (1)

technology from seed

- Disclosing such keys has a high security impact
  - e.g., they're used the authenticate a Apache web server
- Private keys are numbers; looking for a number in memory should be like looking for a needle in a haystack
  - But keys are usually stored in a standard format, e.g., PKCS#1
  - In PKCS#1 a key is an ASN.1 object
  - Includes 0x30 and the sequence 02 01 00 02; can be found!
  - We used *rsakeyfind* that comes in package with the same name (available for several Linux distributions)
  - There can be false positives but we found none

Attack 2: Obtaining private keys using memory snapshots (2)

technology from seed

```
$ xm dump-core 2 -L lucidomu.dump
Dumping core of domain: 2 ...
$ rsakeyfind lucidomu.dump
found private key at 1b061de8
version = 00
modulus = 00 d0 66 f8 9d e2 be 4a 2b 6d be 9f de
46 db 5a
...
publicExponent = 01 00 01
privateExponent = ...
prime1 = ...
prime2 = ...
```

Attack 3: Extracting confidential data from the hard disk

- Assumes Logical Volume Manager (LVM) is used
  - Manages logical volumes on top of physical vols.
- Attack is similar to making a backup:

```
$ lvcreate -L 2G -s -n lv_st /dev/main_vol/domu
Logical volume 'lv_st' created
$ kpartx -av /dev/main_vol/lv_st
...
$ vgscan
Found volume group 'LucidDomU'
$ vgchange -ay LucidDomU
$ mount /dev/LucidDomU/root /mnt/
```

Create snapshot of the victim VM drive as a new volume

Adds partition map to the new vol.

Search for LVM volumes

Activate the snapshot volume

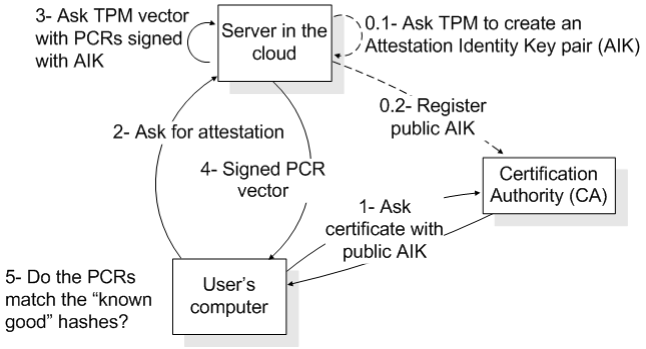
- Now, copy files, …

A futuristic IaaS cloud (1)

- Uses an trusted hypervisor and a Trusted Platform Module (TPM) in each server
  - TPM: a tamperproof chip now available in many PCs
  - Provides a set of simple security functions
- Assume a configuration "known good" by the cloud user
  - Configuration = {hypervisor, dom 0}
  - "Known good" because does not support mem/disk shapshots
- During the boot process, each component stores in the TPM a hash of the next one to be loaded
  - In some of the Platform Configuration Registers (PCR)
  - e.g., PCR-01 ← hash(hypervisor) and PCR-02 ← hash(dom 0)
  - TPM is tamperproof, PCRs can't be modified (only "extended")

A futuristic IaaS cloud (2)

- What's that good for? For remote attestation: the user can obtain a proof that the configuration is the "known good"
  - Get the PCRs signed by the TPM



Attack 4: Virtual machine migration in the futuristic cloud

- Attestation can show that the hypervisor/dom 0 have a set of dangerous functionality disabled; however, migration can't be disabled
- Attack:
  - 1- Attacker lets the victim VM be installed in a server with a trusted hypervisor
  - 2- Attacker waits until attestation finished, then migrates the VM into a server with an hypervisor that it controls
  - 3- Attacker runs any of the previous attacks

More attacks

- These attacks are against confidentiality
- Attacks against availability are even simpler, e.g., delete VM(s)
- Attacks against data and code integrity are also possible

Solutions from the cloud providers

- Taken from “Cloud Computing Roundtable”
  - IEEE Security & Privacy – Nov/Dec 2010
  - 5 directors/senior people from: Google, Microsoft, Cisco, Amazon, Cloud Security Alliance

- No physical access
  - But all attacks we saw can be done remotely
- Logging all accesses to the servers with users’ data
  - Takes place after the attack has happened
  - What if the attacker that was fired or left voluntarily?
- Zero tolerance policy for insiders that access data
  - Same as the previous

“there’re some things that will never go into Azure, for example, our SAP back end”

DepSky: Dependable and Secure Storage in a Cloud-of-Clouds

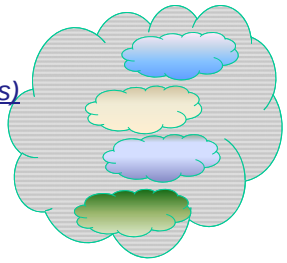
DEPSKY: Dependable and Secure Storage in a Cloud-of-Clouds,
A. Bessani, M. Correia, B. Quaresma, F. André, P. Sousa, *EuroSys 2011*

Securing the cloud

- Two options:

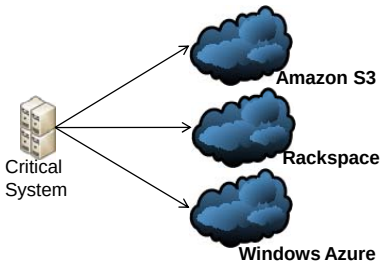
1) *Improve the cloud infrastructure*

2) *Use several cloud providers (cloud-of-clouds)*



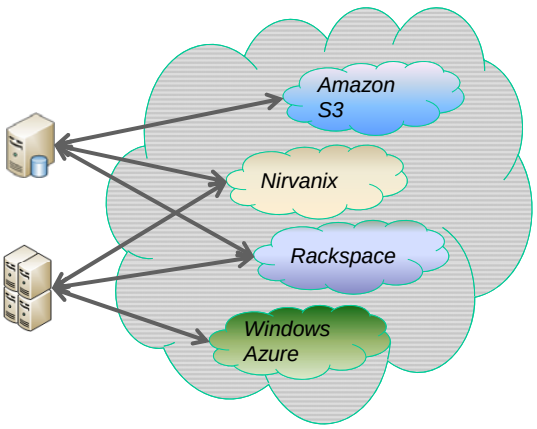
Benefits of replication in several clouds

- Datacenter and cloud outages
- Vendor lock-in
- Data corruption
  - Bugs
  - Malicious insiders
  - Attacks and intrusions
- Better read performance



Cloud-of-Clouds object storage

- Cloud-of-Clouds provides same service as single cloud



DepSky design principles

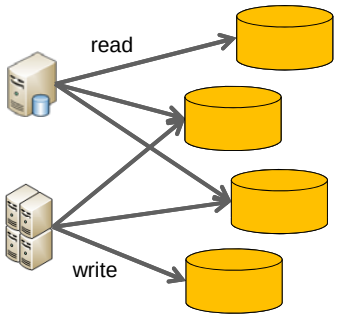
technology from seed

- 1. No trust on individual cloud providers
  - Distributed trust is built by using multiple clouds
- 2. Use storage clouds as they are
  - No server-side code on the replication protocols
- 3. Data is updatable
  - Quorum replication protocols for consistency

Key challenges

technology from seed

- How to implement an efficient replication protocol using only passive storage nodes?
- How to make it affordable?



DepSky interface

- **write(data_unit, data)**
- **read(data_unit)**

Object Storage

- *create(data_unit)*
- *destroy(data_unit)*
- *lock(data_unit, …)*
- *unlock(data_unit)*
- *garbageCollect(data_unit, …)*
- *reconfigure(data_unit,…)*

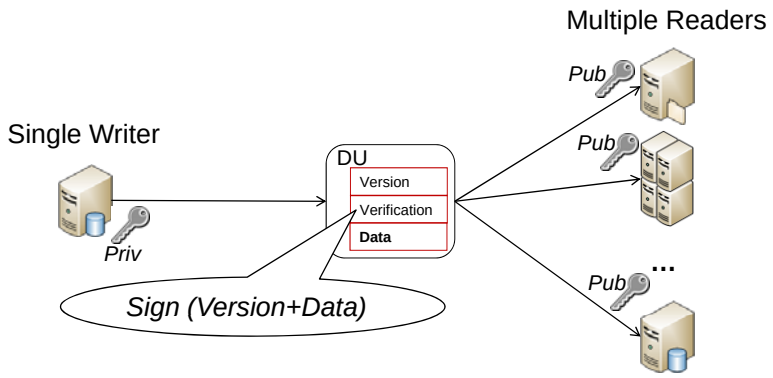
details in the paper

System model

- Asynchronous distributed system
- Faults
  - Clouds can be unavailable, corrupt or destroy data
  - Readers can do whatever they want

  } Byzantine faults
  - Writers can **crash and recover**
- *n = 3f +1* clouds to tolerate *f* faults
  - In practice: *f = 1*
- Symmetric and asymmetric cryptography

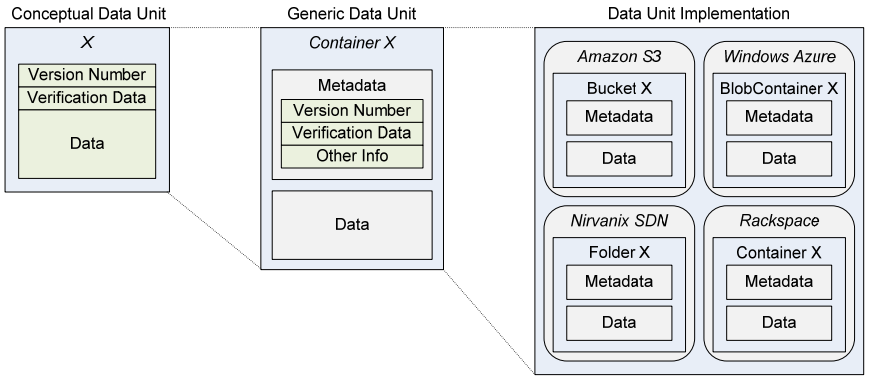
Data model



single-writer multi-reader regular register

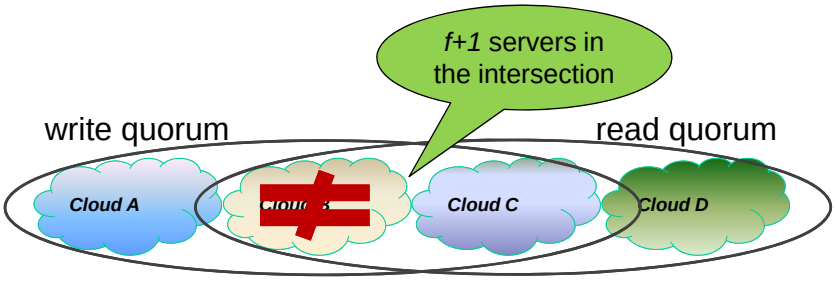
(but multiple writers are supported through a locking algorithm)

Data model implementation

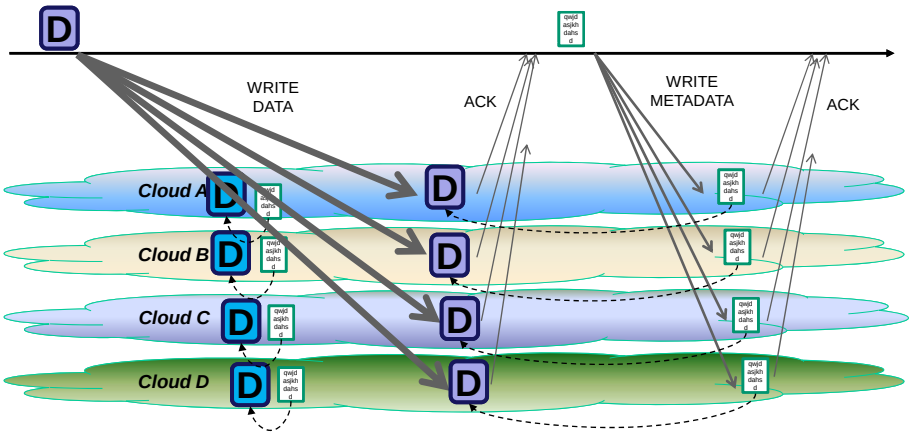


Read/Write protocols and quorums

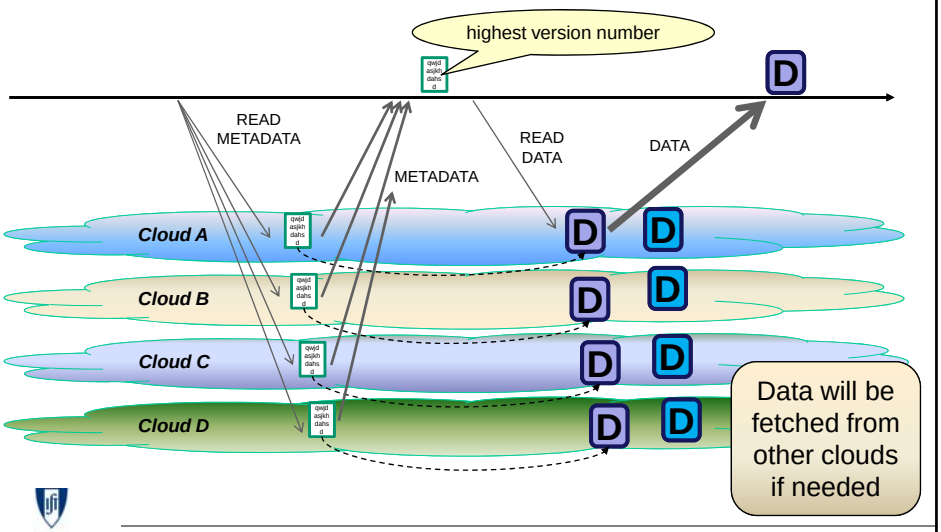
- *f*-dissemination Byzantine quorum systems [Malkhi & Reiter 1998]
  - quorums of *2f+1* servers out-of *3f+1* servers
  - data is self-verifiable (signed)



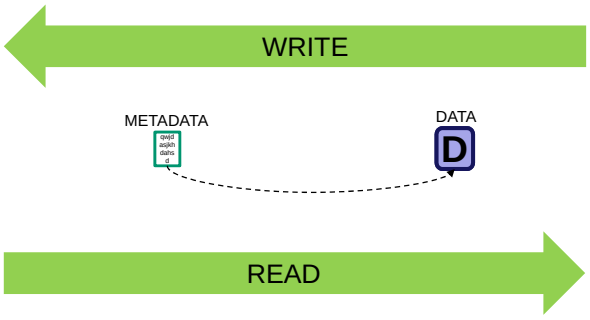
Write protocol



Read protocol

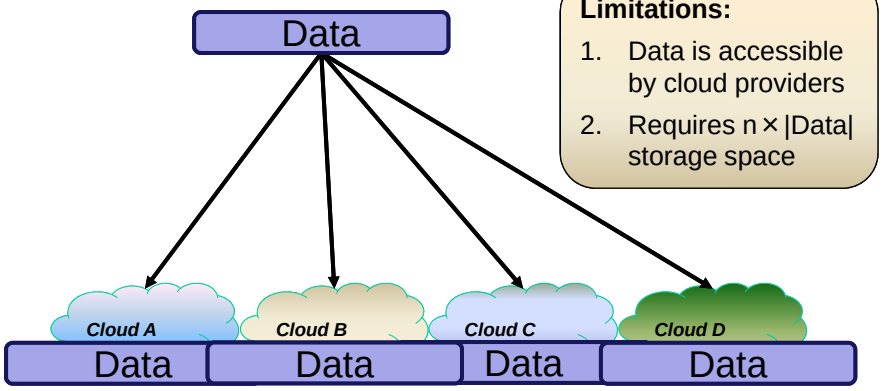


Why does it work?



Key property: if metadata pointing to D is read, D can be read

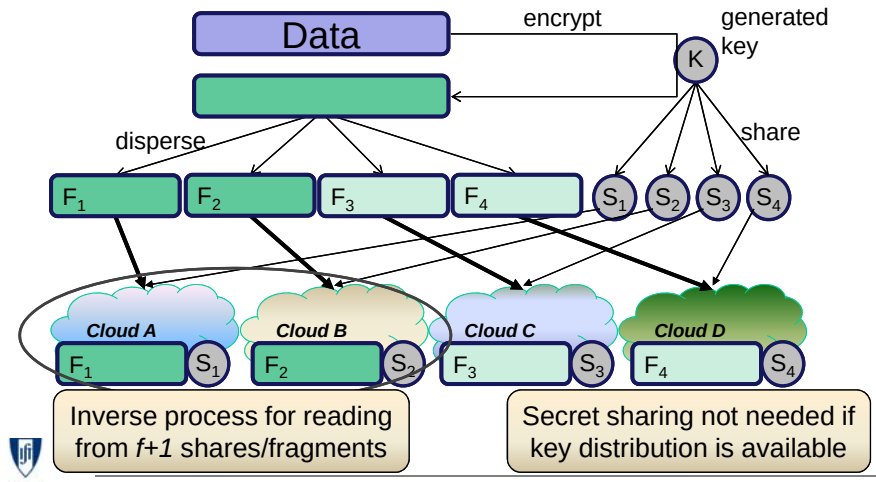
Problems of the solution so far



Limitations:

1. Data is accessible by cloud providers
2. Requires n × |Data| storage space

Combining erasure codes and secret sharing



Inverse process for reading from *f+1* shares/fragments

Secret sharing not needed if key distribution is available

Consistency proportionality

- The consistency provided by DepSky is the same as the base storage clouds
  - If the weakest consistency cloud provides eventual consistency, DepSky provides eventual consistency
  - If the weakest consistency cloud provides "read your writes", DepSky provides "read your writes"
  - If the weakest consistency cloud provides regular storage, DepSky provides regular storage
- This notion may be useful for other systems

DepSky Evaluation

DepSky performance

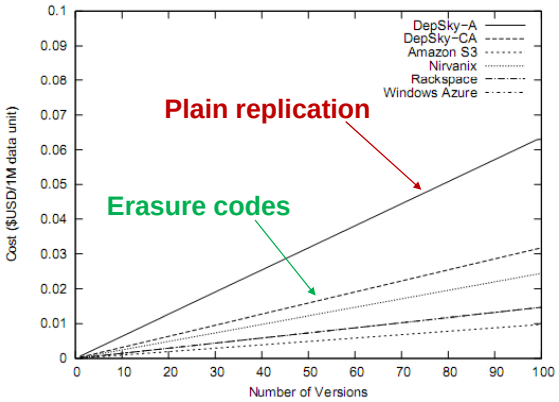
- Prototype: 3K locs (Java), REST/HTTPS
- Experimental Setup
  - Two DepSky versions: **A** (DepSky) and **CA** (DepSky with confidentiality)
  - Four commercial storage Clouds: **S3** (Amazon S3), **WA** (Windows Azure), **NX** (Nirvanix SDN) and **RS** (Rackspace)
  - Clients spread through 8 PlanetLab sites around the world
  - Three clients on each site, reading/writing data units of three sizes (100kb, 1Mb and 10Mb)
  - 437000+ reads/writes between Sep. 10th and Oct. 7th 2010
- Experiments cost: ~400€

DepSky operation costs ($)

Operation	DepSky-CA	Amazon S3	Rackspace	Win. Azure	Nirvanix
10K Reads	1.47	1.46	2.15	1.46	1.46
10K Writes	3.08	1.46	0.78	0.98	2.93

- Monetary costs (in USD) for 1Mb data unity and **four** clouds
  - Read cost is the same of reading from the less expensive cloud
  - Write cost is the cost of writing 50% of the DU size on each cloud
- These costs don't include data storage

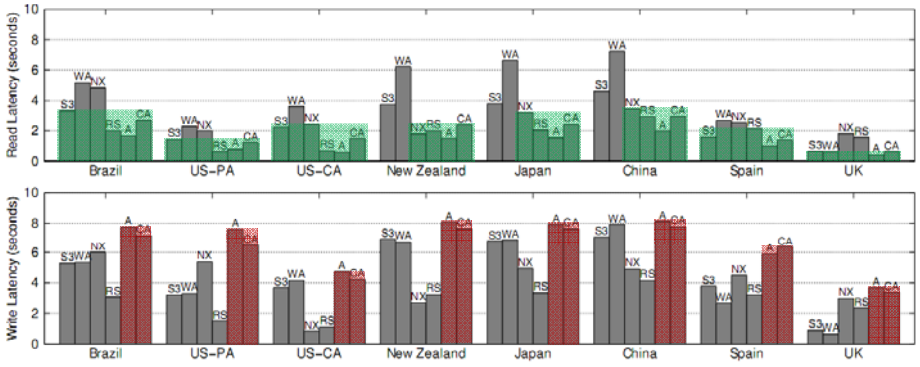
DepSky storage costs ($)



- *DepSky-CA* storage cost (1M data unit) =
  2 ×(Avg. individual cloud cost per GB/month)

DepSky latency (100kb DU)

DepSky **read** latency is close to the cloud with the **best** latency



DepSky **write** latency is close to the cloud with the **worst** latency

DepSky performance: other aspects

- Secret sharing latency overhead < 0.1%
- Effectiveness of read optimization
  - Fetch data first from the clouds that returned metadata faster
  - Effective in 83% (A) and 68% (CA) of reads
- Throughput **per client**:
  - 65-1480 kb/s (read) and 3-108 kb/s (write)
    - Orders of magnitude smaller than LAN BFT storage systems [Hendricks et al 2007]
  - Cloud aggregate throughput may be “infinite”

DepSky perceived availability

Location	Reads Tried	DepSky-A	DepSky-CA	Amazon S3	Rackspace	Azure	Nirvanix
Brazil	8428	1.0000	0.9998	1.0000	0.9997	0.9793	0.9986
US-PA	5113	1.0000	1.0000	0.9998	1.0000	1.0000	0.9880
US-CA	8084	1.0000	1.0000	0.9998	1.0000	1.0000	0.9996
New Zealand	8545	1.0000	1.0000	0.9998	1.0000	0.9542	0.9996
Japan	8392	1.0000	1.0000	0.9997	0.9998	0.9996	0.9997
China	8594	1.0000	1.0000	0.9997	1.0000	0.9994	1.0000
Spain	6550	1.0000	1.0000	1.0000	1.0000	0.9796	0.9995
UK	7069	1.0000	1.0000	0.9998	1.0000	1.0000	1.0000

- Apparently, some clouds don’t provide the promised 5 or 6 9’s of availability
- Internet availability plays an important role

Conclusions

Conclusions

- Cloud security is a problem, especially vis-à-vis a malicious insider
  - He/she can run several simple but harsh attacks
- DepSky: Cloud-of-clouds storage with untrusted clouds
  - Techniques: Byzantine quorum systems (integrity and availability), erasure codes (storage efficiency) and secret sharing (confidentiality)
  - Can be used on storage clouds as they are
  - Can be basis for more complex storage systems (e.g., file system)
  - A use case for Byzantine fault tolerance – diversity already there

Conclusions

- Costs × Benefits
  - Four clouds are needed to tolerate a single “faulty cloud”
  - Reads are faster than single cloud reads
  - Writes are slower than single cloud writes
  - Monetary costs roughly twice the average costs of individual clouds
  - It can be improved: data doesn’t need to be in all *3f+1* clouds

Publicidade: sanduíche/pós-doc no Instituto Superior Técnico

- IST – a principal escola de engenharia portuguesa – 100+ anos
- Na capital, Lisboa, perto de todas as capitais europeias
- Equipe de topo na Europa, participação em projectos europeus

“foi tão bom... que eu não queria sair mais de Lisboa :-) esse é o perigo de fazer doutorado aí... :-D ”


technology
from seed
inesc id
lisboa
10 anos