

A rock climber is shown in profile, ascending a vertical rock face. The climber is wearing a bright red jacket, a white helmet, and a backpack. They are secured by ropes and climbing gear. The background is a clear blue sky. The text 'SOME SECURITY CHALLENGES IN CLOUD COMPUTING' is overlaid in large white letters across the center of the image.

# SOME SECURITY CHALLENGES IN CLOUD COMPUTING

Hoang N.V.

A silver laptop computer is shown from a low angle, appearing to float above a vast, dense layer of white, fluffy clouds. The sky above is a clear, bright blue. The laptop's screen is open and displays a blurred image of the same cloud scene. The overall composition is clean and modern, symbolizing cloud computing.

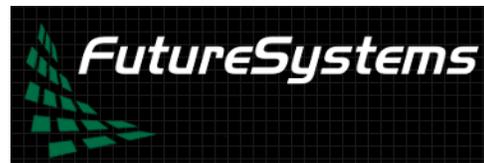
**What is cloud computing?**

# Cloud computing: **Advantages**

"**pay-per-use** model for enabling available, convenient and **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." by NIST

# Today

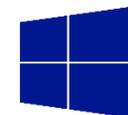
Google™ Apps  Cloud Services



amazon  
webservices™

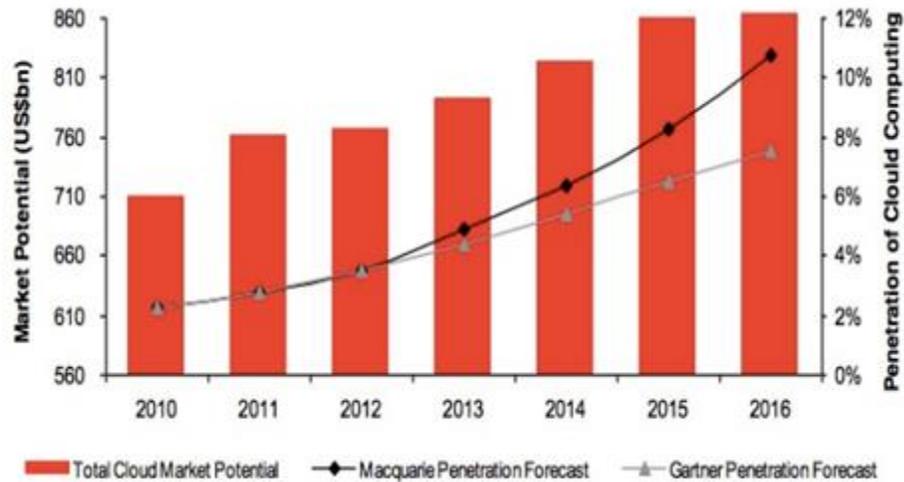


IBM SmartCloud



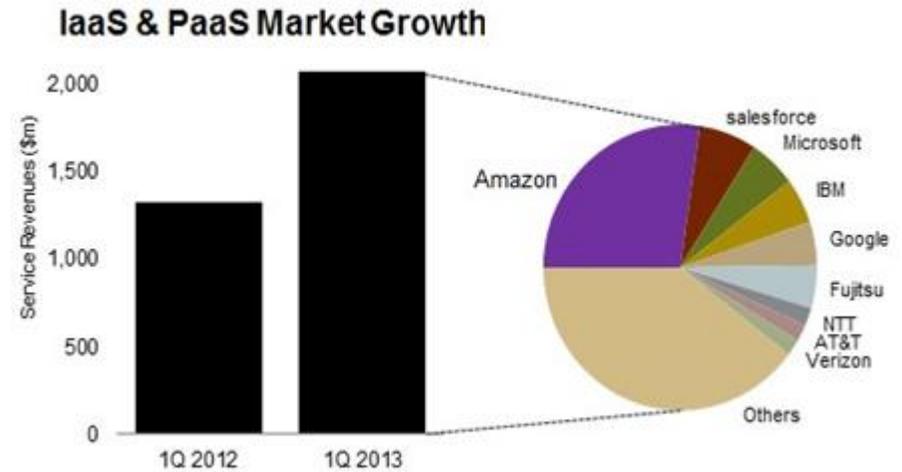
Windows Azure

# Future



**The overall cloud market will hit \$71 billion in 2015**

Source: Gartner Company data, Macquarie Capital (USA), Jan. 2013



Cloud providers bring in \$2B in first quarter -- source: Synergy Research Group, May, 2013

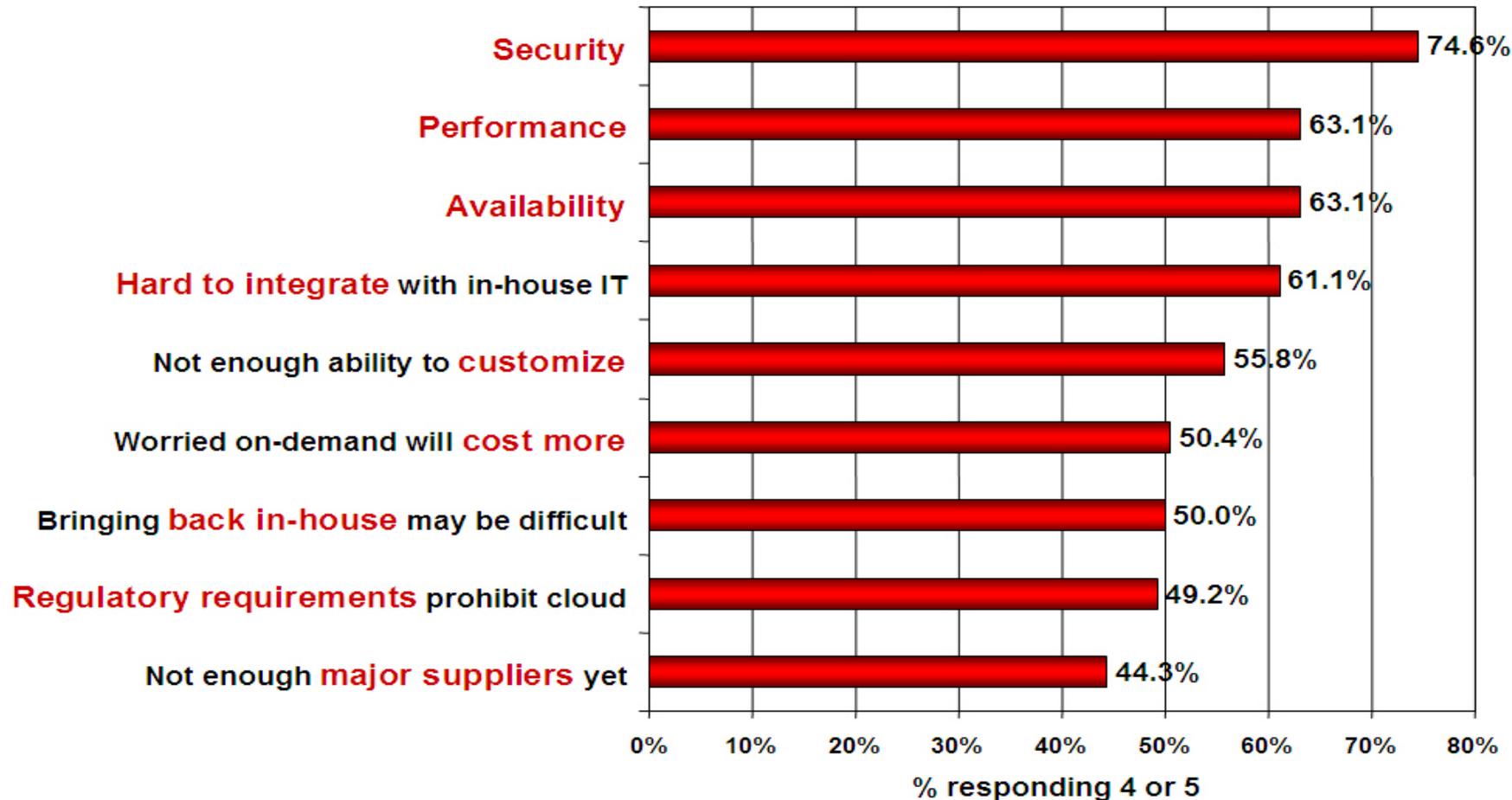
IT'S BEEN ANNOUNCED  
OUR COMPANY IS MOVING  
TO THE CLOUD. HOW'S  
YOUR FEAR OF HEIGHTS?

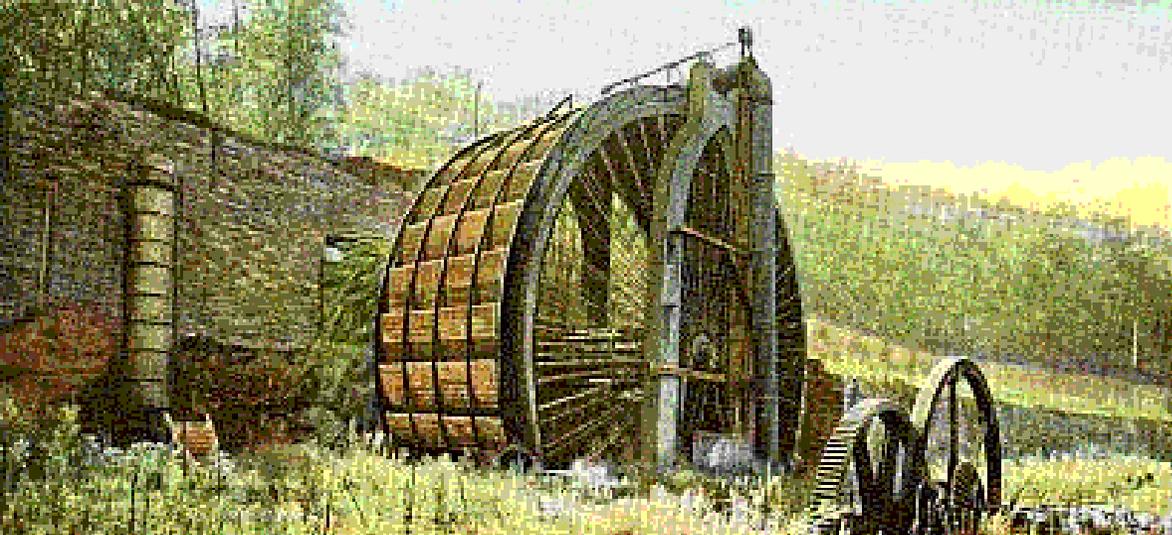


**Cloud computing is the next big thing**

# Challenges for Cloud Computing

Q: Rate the **challenges/issues** ascribed to the 'cloud'/on-demand model  
(1=not significant, 5=very significant)





# Trust





Trust me, please!



Oh, no



# **Broad** Attacking Surface



We have everything in the cloud. 😊

Everything is virtual. **Loss physical control** 😞

# Broad Attacking Surface

» Traditional adversaries: Hackers, Malwares, ...

» As well as:

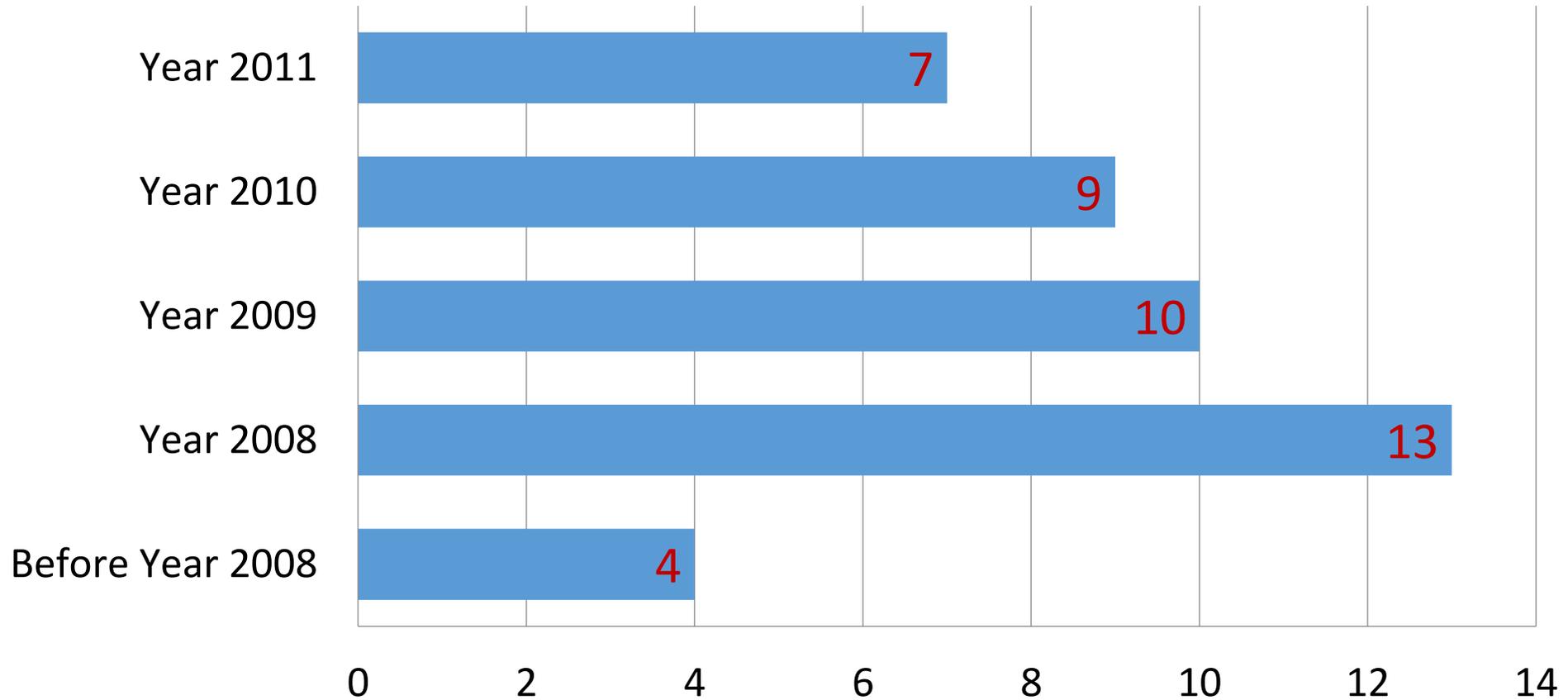
› Data breach

› Malicious Insider

› Insecure Interface or APIs

# Broad Attacking Surface

## No. of Incidents with Unknown Causes by Year



CSA report 2012 (Revised March 13, 2013)

» Many others yet to be identified ...

# Storage outsourcing



# Security challenges with storage outsourcing



**Data Integrity**

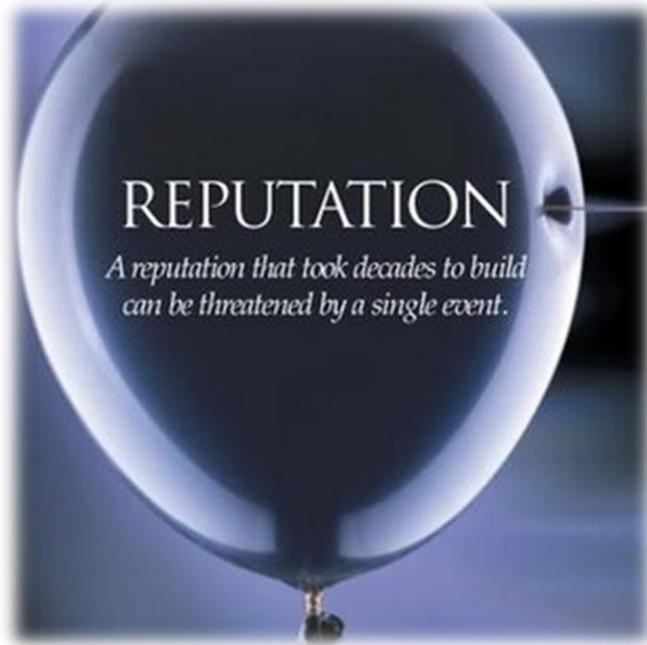
# Security challenges with storage outsourcing

## (Data Integrity)

- » Data integrity is hard problem
- » Broad range of threats
  - › Internal: Byzantine failure, management errors, software bugs, ...
  - › External: malware, economically motivated attacks, ...

# Security challenges with storage outsourcing (Data Integrity)

» Cloud providers might behave unfaithfully



# Data Integrity

## Gmail Disaster: Reports Of Mass Email Deletions

Posted Dec 28, 2006 by [Michael Arrington \(@arrington\)](#)

Just a week after I wrote "[Uh Oh, Gmail Just Got Perfect](#)" a number of users started [complaining](#) that all of their Gmail emails and contacts were auto deleted.

## Google blames software update for lost Gmail data

Internet giant says a bug introduced during a storage software update caused some users to lose access to their e-mail account, but the company says it is working to restore the data.

by [Steven Musil](#) [@stevenmusil](#) / February 28, 2011 8:33 PM PST

Wednesday, January 29, 2014, 06:03 am PT (09:03 am ET)

## Gmail for iOS bug may have caused users to accidentally remove messages

By [Shane Cole](#)

Google on Wednesday began notifying some users of Gmail's first-party iOS app that they may have inadvertently removed messages they intended to keep thanks to a now-rectified software error.

# Data Integrity

## Major Outage for Amazon S3 and EC2

BY RICH MILLER ON FEBRUARY 15, 2008

[ADD YOUR COMMENTS](#)

Many users of Amazon's utility computing platform report that their [services are inaccessible](#) this morning. The outage is having a ripple effect on many sites using Amazon to store images (such as [Twitter](#)) or widgets. Users are reporting issues with errors on both the S3 and EC2 services, and at least one user is reporting [file loss](#). Amazon hasn't provided any explanation yet on what has happened, but is trying to centralize discussion on a [thread in its developer forum](#).

## More outages hit Amazon's S3 storage service

Cloud storage service down for eight hours over the weekend

By Jon Brodtkin

NetworkWorld | Jul 22, 2008 1:00 AM PT

Amazon.com Inc.'s S3 [cloud storage service](#) suffered eight hours of downtime and elevated error rates in the U.S. and Europe Sunday.

The outage lasted several hours longer than a similar problem that hit the service [in February](#), disrupting Web sites that rely on the online Simple Storage Service. The social networking site [Twitter](#) was disrupted during both outages.

[Y](#) **Hacker News** [new](#) | [comments](#) | [show](#) | [ask](#) | [jobs](#) | [submit](#)

▲ Ask HN: Is it necessary to backup S3?

26 points by dawie 1872 days ago | [comments](#)

I have a consumer SaaS Web Application that uses S3 to store user's documents. Do you think it's necessary to backup the S3 data to Rackspace Cloud?

# Data Integrity

## Hotmail Cloud Problems Cause Temporary Loss of Data

By Tsvetanka Stoyanova | Jan 4, 2011

The New Year started abruptly for over 17,000 Hotmail users, who temporarily lost their email messages. Now the drama is over — or at least this is what Microsoft says — but the bitterness remains. Blame it on the cloud?

Macs & Mac OS X | 13 Jun 2011 | Listen  | Print  | Comment (33)

### MobileMe-to-iCloud Transition Messaging Provokes Confusion

by Glenn Fleishman  

 Email  1  Tweet  3  Like  7

Plans for MobileMe never seem to go right. Its launch in mid-2008, as a transition from the previous .Mac service, was riddled with failures, data loss, and confusion (see [“MobileMe Fails to Launch Well, But Finally Launches,”](#) 12 July 2008). Steve Jobs, according to [a recent Fortune report](#), berated the MobileMe team and then replaced the group’s head during a meeting at that time.

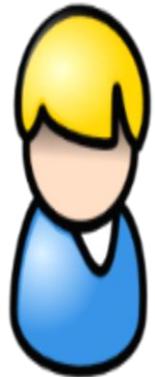
# Security challenges with storage outsourcing (Data Integrity)

Should we trust the cloud 100 percent for the storage integrity?

*Cloud currently offers no guarantee*

Data owners need a means to ensure continuous correctness of outsourced cloud data.

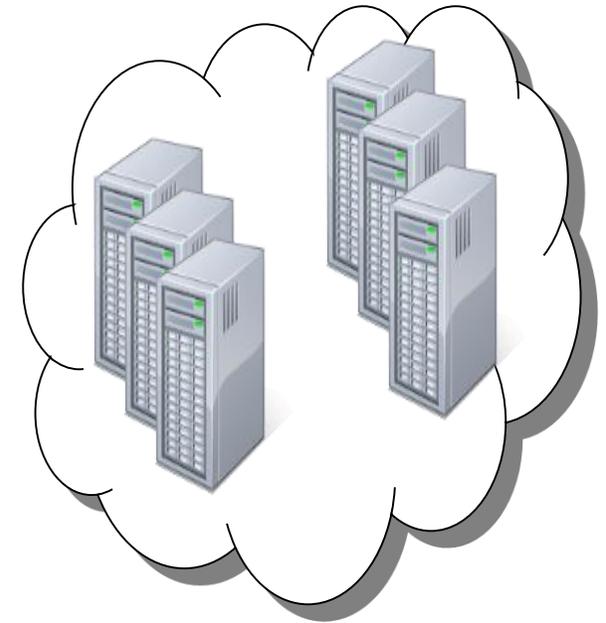
# Security challenges with storage outsourcing (Data Integrity)



*Is my data correctly stored?*



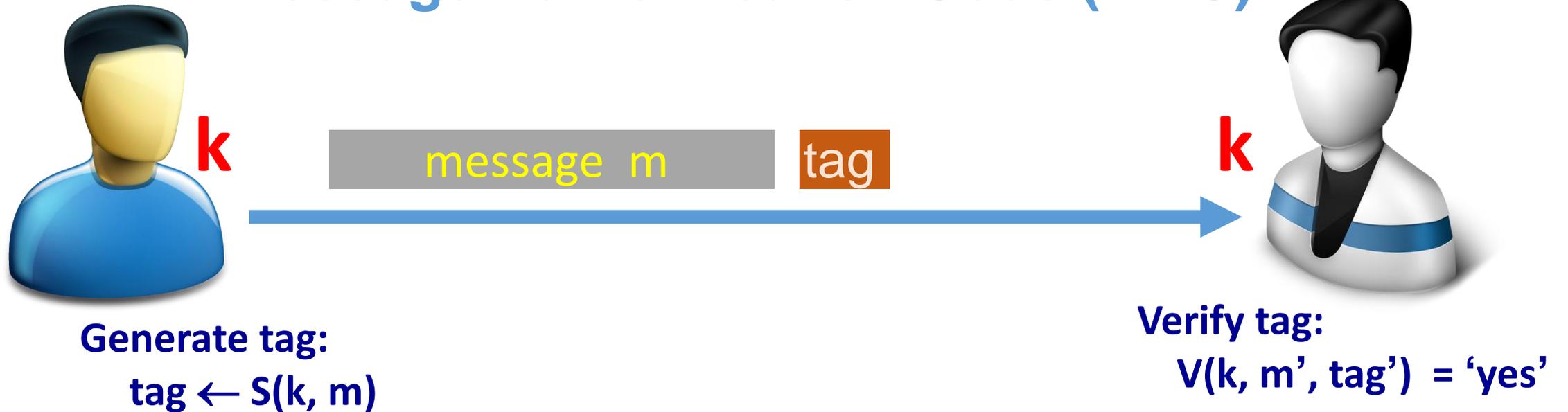
*Storage correctness proofs*



## Secure Cloud Storage Auditing

# Traditional method for data integrity

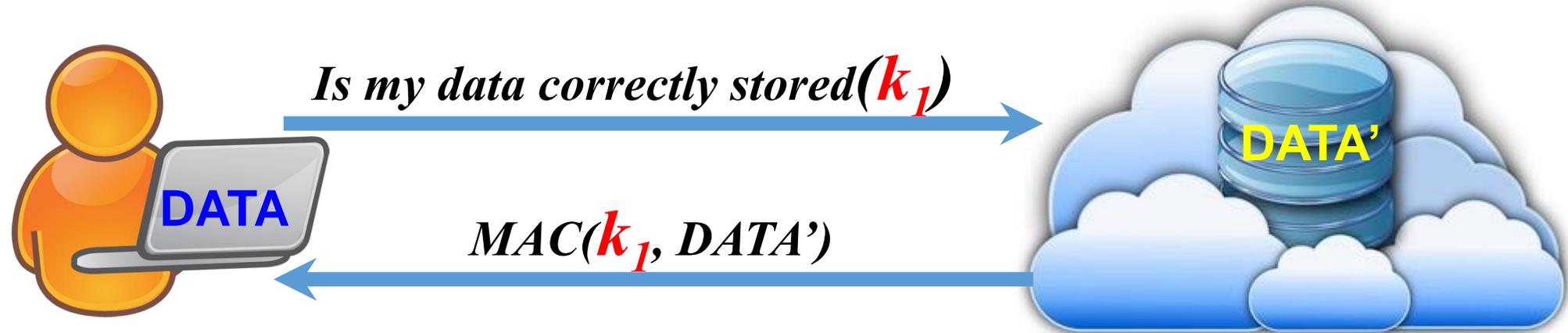
## Message Authentication Code (MAC)



Def: **MAC**  $I = (S, V)$  defined over  $(K, M, T)$  is a pair of algs:

- $S(k, m)$  outputs  $t$  in  $T$
- $V(k, m, t)$  outputs yes or no

# Secure Cloud Storage Auditing



Before putting data in the cloud, must calculate and store

$MAC(k_1, DATA)$

$MAC(k_2, DATA)$



$MAC(k_n, DATA)$

# Secure Cloud Storage Auditing Challenges

Have to explore tradeoffs to maintain low communication and computation overhead on both owner and server side.



Overhead

Convenience

Security

# Secure Cloud Storage Auditing Challenges



**Cope with frequent cloud data  
changing while ensuring continuous  
data auditing**



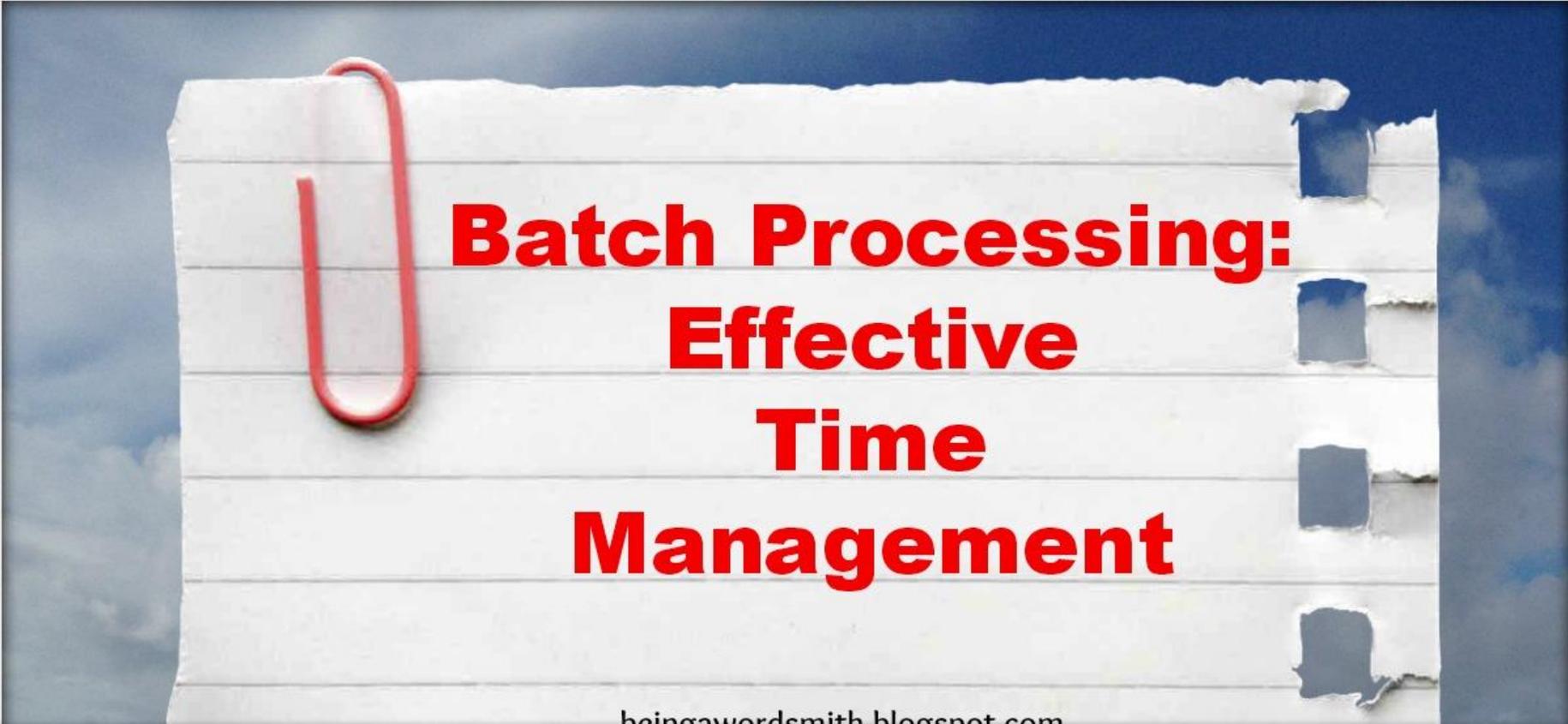
**Public**



**Private**

**Privacy-preserving public auditing**





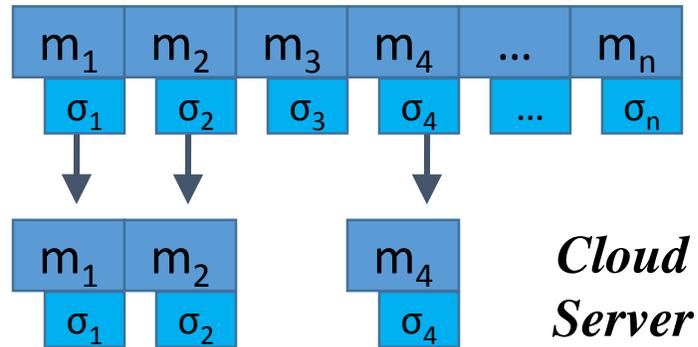
**Batch Processing:  
Effective  
Time  
Management**

[beingawordsmith.blogspot.com](http://beingawordsmith.blogspot.com)

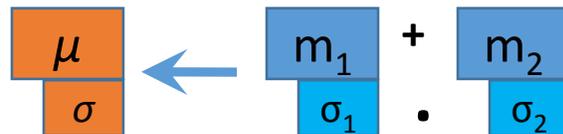
**Batch auditing improves efficiency and saves computation and communication overhead.**

# Secure Cloud Storage Auditing Solutions

» The random-sampling approach



» Construct Homomorphic Authenticator



## Data Durability and Reliability

Amazon S3 provides a highly durable storage infrastructure designed for mission-critical and primary data storage. Amazon S3 redundantly stores data in multiple facilities and on multiple devices within each facility. To increase durability, Amazon S3 synchronously

**Redundantly stores data in multiple facilities and on multiple devices with each facility.**

stores your data across multiple facilities before confirming that the data has been successfully stored. In addition, Amazon S3 calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data. Unlike traditional systems, which can require laborious data verification and manual repair, Amazon S3 performs regular, systematic data integrity checks and is built to be automatically self-healing.

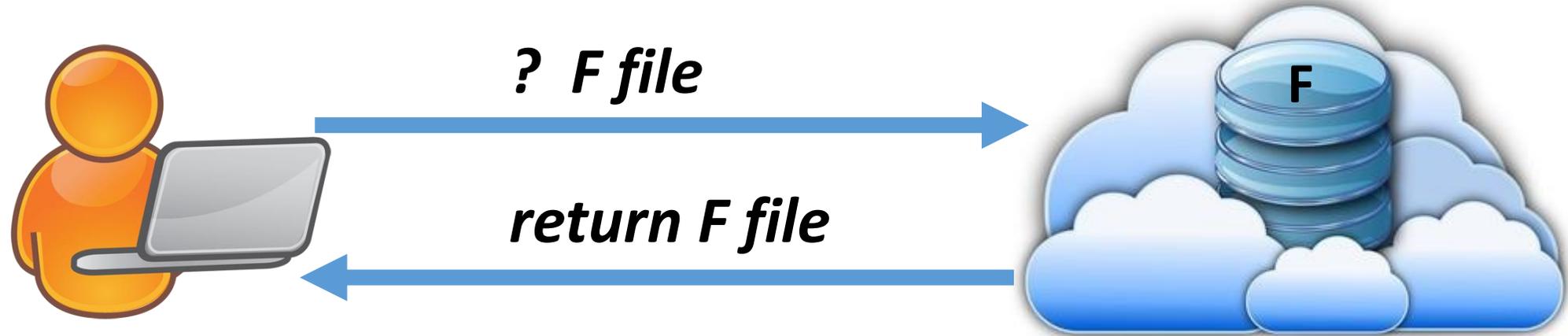
Amazon S3's standard storage class.

# Can we trust?

- Backed with the [Amazon S3 Service Level Agreement](#) for availability.
- Designed for 99.999999999% durability and 99.99% availability of objects over a given year.
- Designed to sustain the concurrent loss of data in two facilities.

**Designed to sustain the concurrent loss of data two facilities.**

# Security challenges with storage outsourcing (Data Integrity)



Cloud storage provider claims to store **three distinct copies** of my file for resillience.

Can we trust? No, if they can't **prove it (Redundancy)?**

# Security challenges with storage outsourcing



**Virtualization is a complication.  
We need proofs of data redundancy on the  
physical layer.**

**A single disk failure can destroy files**

# Proof of redundancy Solutions

## The Pizza Oven Protocol (Juels A. 2011)

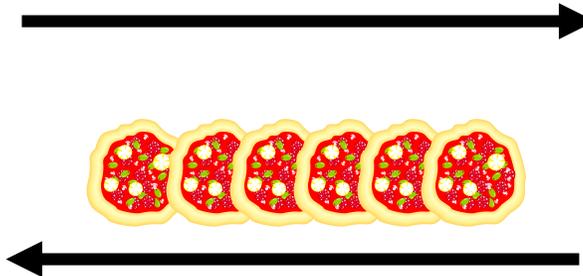
Network latency

Drive read time



**Eeta Pizza Pi**

“Six pizzas!”



**Cheapskate Pizza**

# Protecting Your Data

Data stored in Amazon S3 is secure by default; only bucket and object owners have access to the Amazon S3 resources they create. Amazon S3 supports multiple access control mechanisms, as well as encryption for both secure transit and secure storage at rest. With Amazon S3's data protection features, you can protect your data from both logical and physical failures, guarding against data loss from unintended user actions, application errors, and infrastructure failures. For customers who must comply with regulatory standards such as PCI and HIPAA, Amazon S3's data protection features can be used as part of an overall strategy to achieve compliance. The various data security and reliability features offered by Amazon S3 are described in detail below.

**as well as encryption for both secure transit and secure storage at rest.**

# Jennifer Lawrence, other celebrities have nude photos leaked on Internet after massive hacking scandal

Dozens of photos of the 'Hunger Games' star in various stages of undress first appeared Sunday on the online message board 4chan, along with those of 100 other possible A-list victims such as Rihanna, Lea Michele and Kate Upton.

BY [BILL HUTCHINSON](#) / NEW YORK DAILY NEWS / Published: Sunday, August 31, 2014, 8:08 PM

/ Updated: Monday, September 1, 2014, 5:59 PM

A A A

768

41

16



SHARE THIS URL

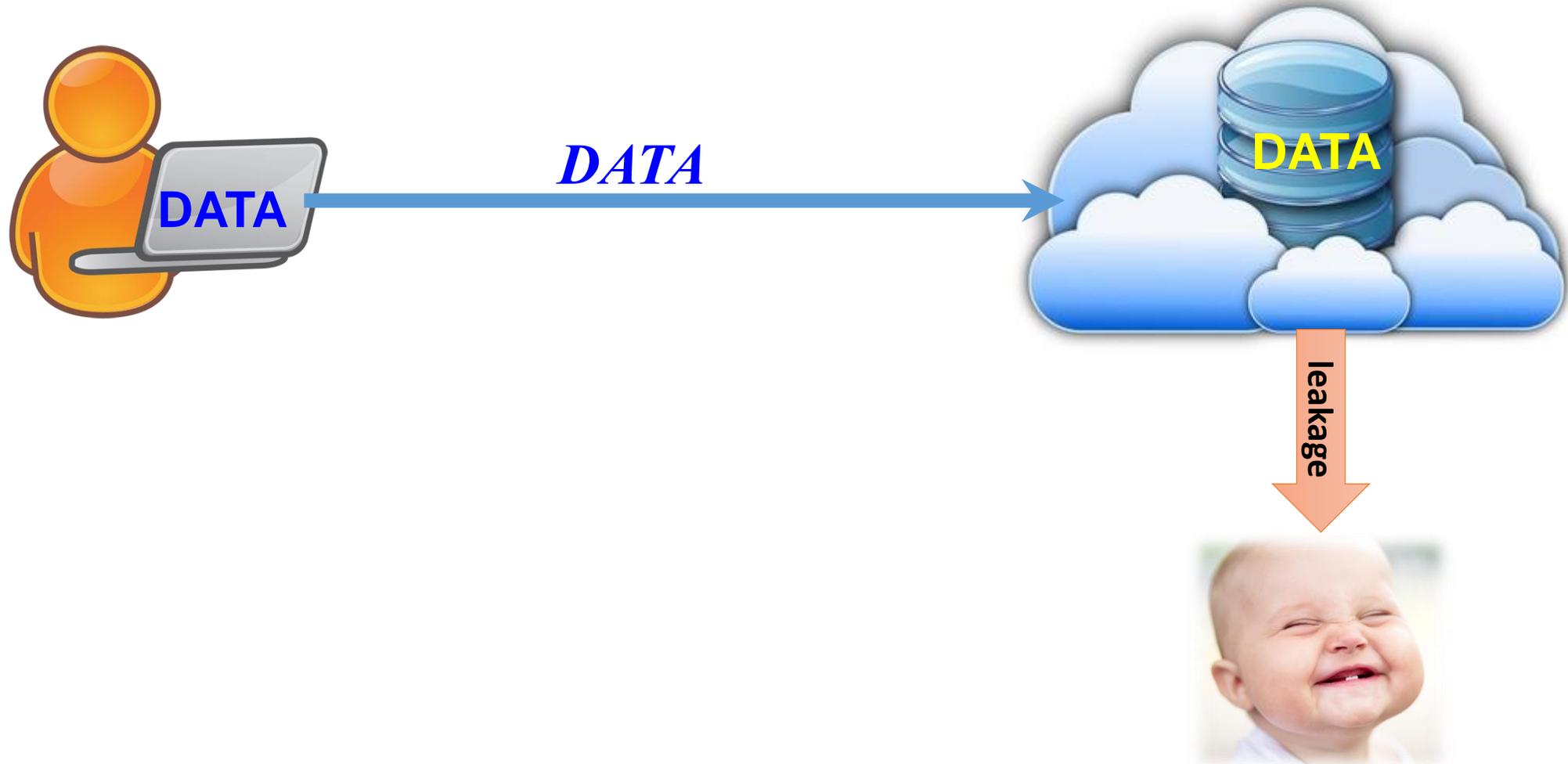
[nydn.us/1nhEpN1](http://nydn.us/1nhEpN1)

COPY





# Security challenges with storage outsourcing (Data leakage)



# Security challenges with storage outsourcing (Data leakage)



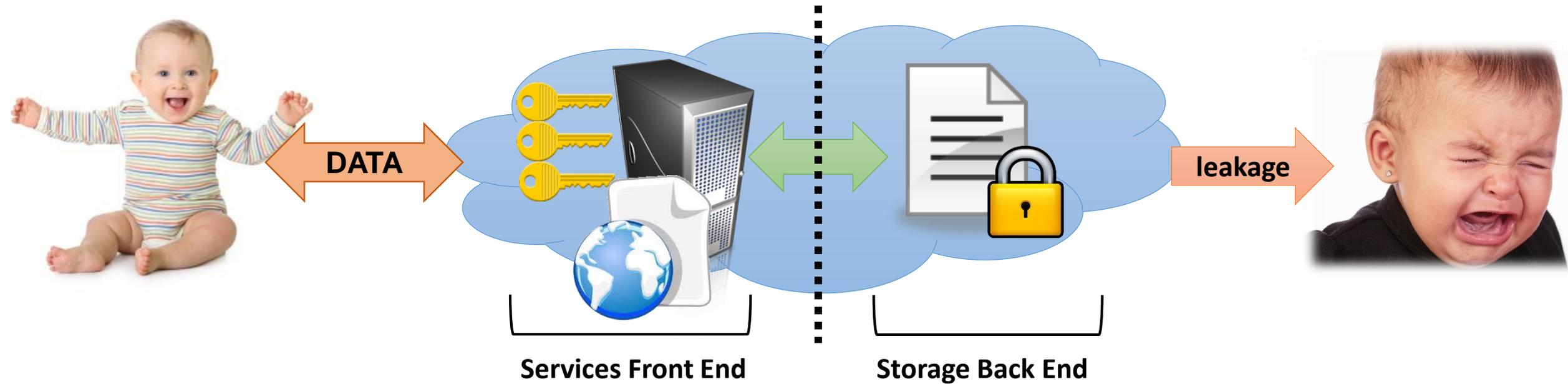
$E(\text{key}, \text{DATA})$



leakage



# Security challenges with storage outsourcing (Data leakage)



**Challenge: Proofs of encrypting data at rest**

12/2013

Are YOUR details at risk? Facebook, Gmail and 7

Edward Snowden đốt nóng mùa giải Nobel Hòa bình

10/2014

[Update] Hundreds

05/2013

Edward Snowden bắt đầu hôm nay, với những dự đoán rằng giải Hòa bình có thể được trao cho Edward Snowden, cựu nhân viên an ninh từng tiết lộ những bí mật của Mỹ khiến cả thế giới chấn động.

09/2010

Google fired engineer

Snowden được đề cử Nobel Hòa bình / Putin được đề cử giải Nobel Hòa bình / Tổ chức Cấm Vũ khí hóa học giành giải Nobel Hòa bình

9/2014

Google fired

privacy bre

David Barksdale, a Google engineer, accessed the accounts of several children, by Tom Krazit / September 14, 2010 5:27 PM



Cựu nhân viên CIA Edward Snowden là một trong số những người được đề cử giải Nobel Hòa Bình. Ảnh: Reuters

Sensitive data must be encrypted before putting on the cloud server



Kashmir Hill Contributor

FOLLOW

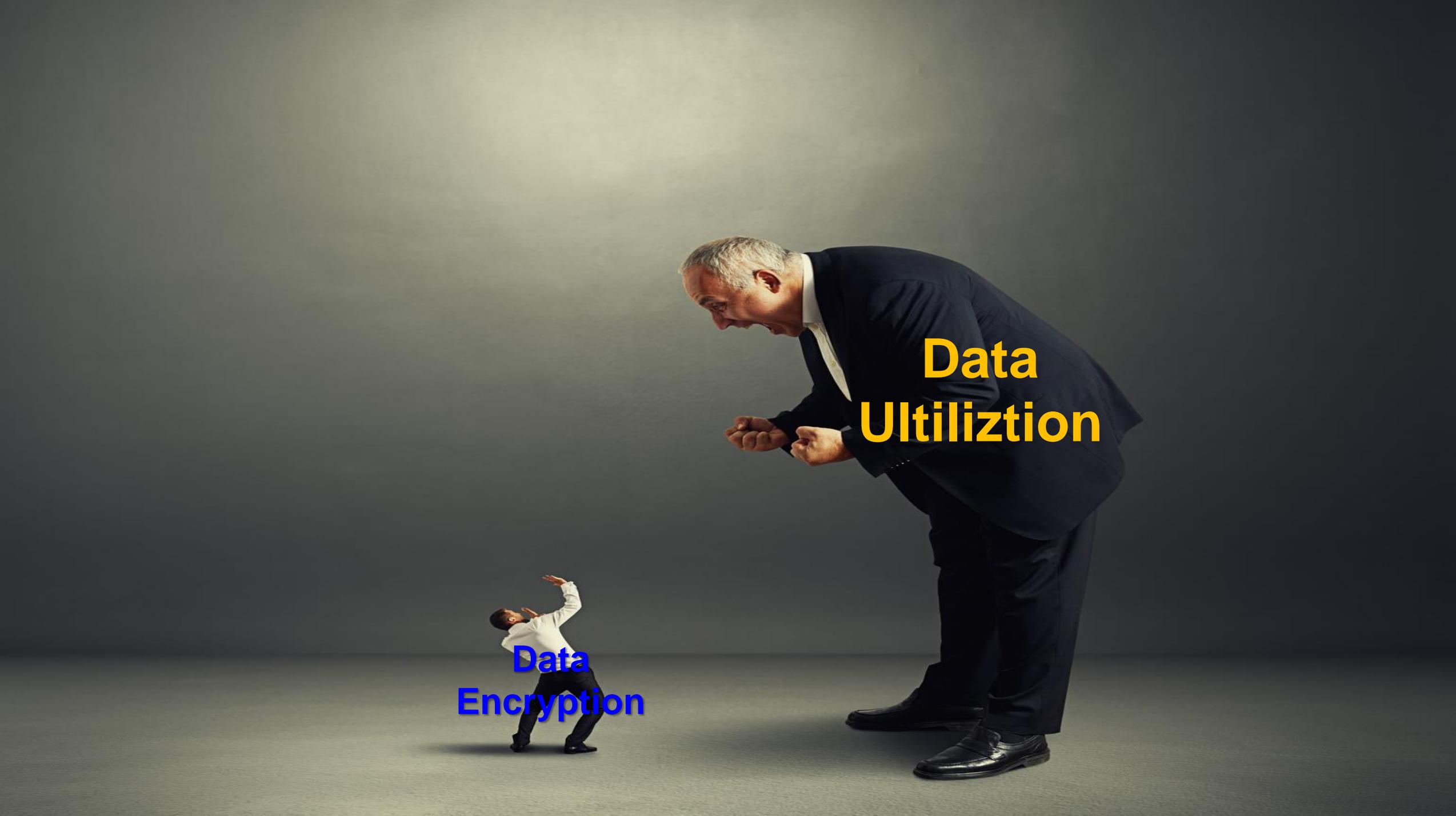
Welcome to The Not-So Private Parts where technology & privacy collide full bio ->

Opinions expressed by Forbes Contributors are their own.



itself; Earlier in the day, Gawker reported that Google's Seattle offices, used his position to break into the Gmail and Google Voice accounts of several children. After parents of the children complained to



A large man in a dark suit is leaning forward, looking down at a tiny man in a white shirt. The large man is on the right side of the frame, and the tiny man is on the left side. The background is a plain, light-colored wall with a dark floor. The text 'Data Utilization' is written in yellow on the large man's suit, and 'Data Encryption' is written in blue on the tiny man's shirt.

**Data  
Utilization**

**Data  
Encryption**



---

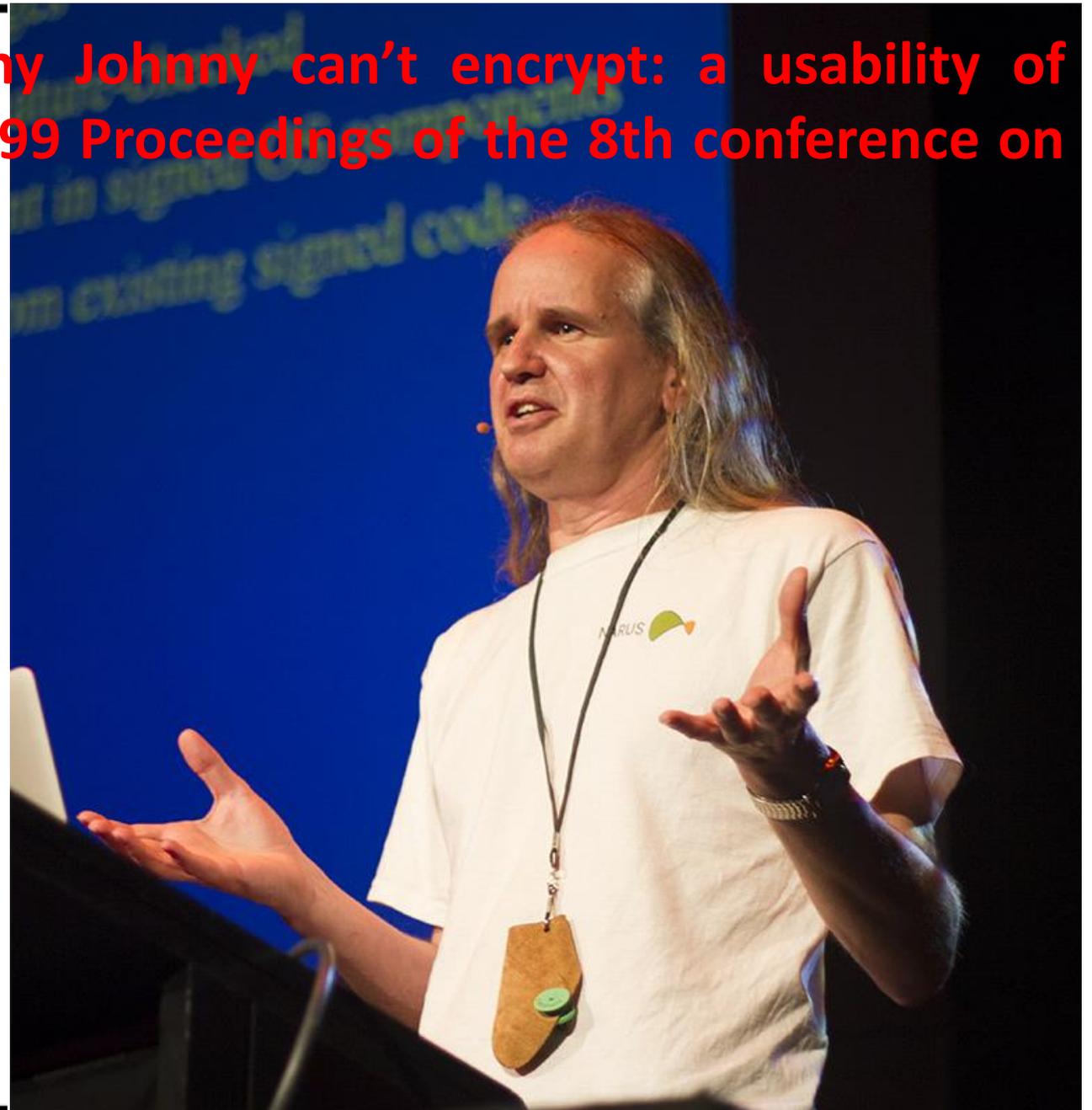
Whitten A., Tygar J. D., Why Johnny can't encrypt: a usability of  
evaluation of PGP 5.0, SSYM'99 Proceedings of the 8th conference on  
USENIX Security Symposium

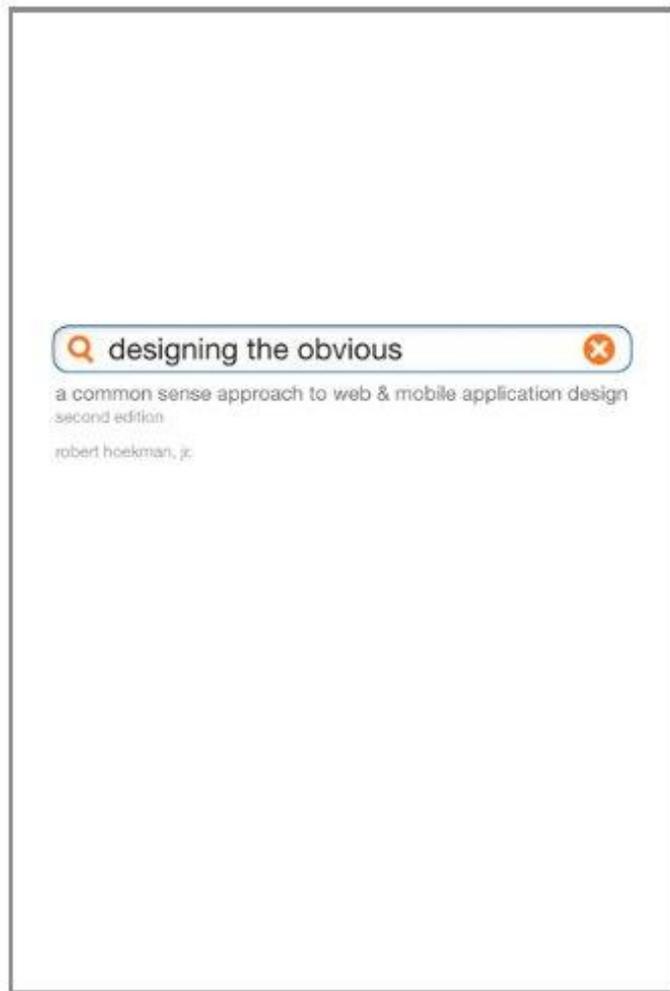
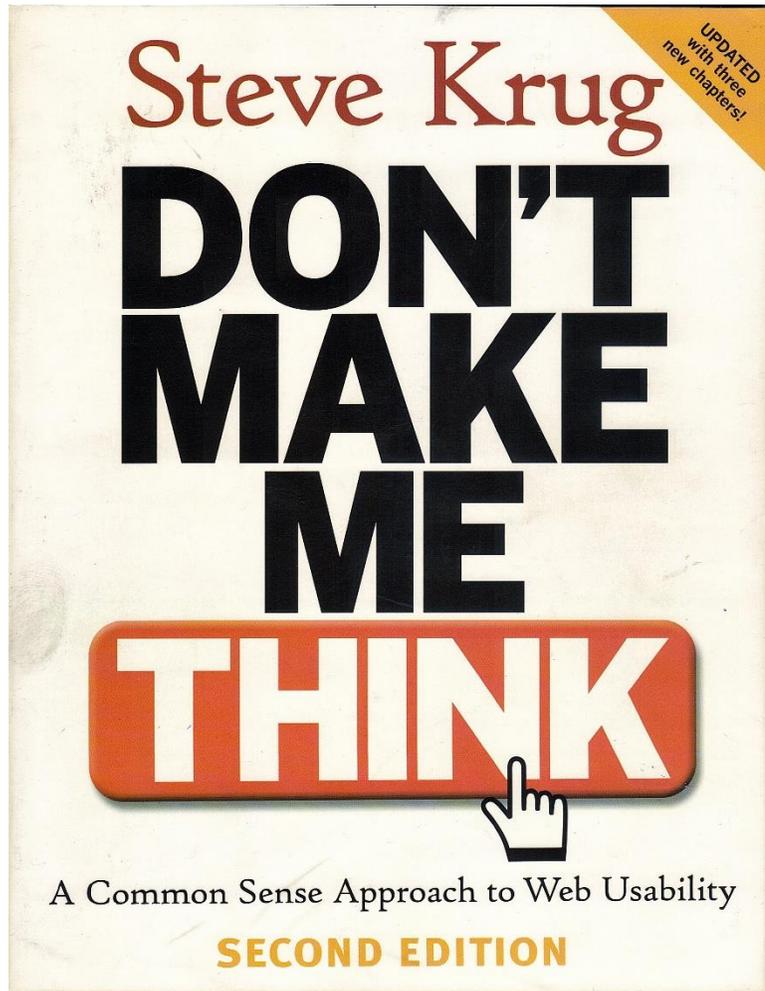
# *Engineering Security*

Book Draft

Copyright Peter Gutmann 2014

April 2014





Jakob Nielsen

# Data Encryption vs Data Utilization

## Solutions

### » Oblivious RAM types Protocol

› [Goldreich-Ostrovsky92]

### » Searchable symmetric encryption

› [Song-Wagner-Perrig-S&P00][Goh-ePrint-03, Chang-Mitzenmacher-ACNS05]  
[Curtmola-Garay-Kamara-Ostrovsky-ccs06]

### » Public Key Encryption with Keyword Search

› [Boneh et al. EUROCRYPT'04]

» etc

But, encryption is not always enough.



**Challenge: How to hide access patterns**

***Access patterns***  
can leak sensitive information.

# Access Pattern Problems

## » Private Information Retrieval (PIR)

- › The client is able to read a document  $m_i$  from the remote database without revealing his/her choice  $i$  to the server.

## » Oblivious Transfer (OT)

- › The same as PIR; in addition, it is required that the client can **only** learn  $m_i$  after protocol execution.

## » Oblivious RAM (ORAM)

- › The client is able to read and write the remote database without revealing his/her access pattern to the server.

Nội dung	Từ khóa	Xu hướng
Bài hát Việt	Không cảm xúc	Không cảm xúc
	Anh nhớ em	Nếu là anh
	Người ấy	Người ấy
	Nếu là anh	Người tôi yêu
	Con nhà nghèo	Anh nhớ em
Công nghệ	iPhone 5	iPhone 5s
	Nokia Lumia 520	Nokia Lumia 520
	iPhone 4s	Samsung Galaxy S4
	Samsung	iPhone 5c
	iPhone 5s	iOS 7
Hiện tượng mạng xã hội	Gangnam Style	Gangnam Style
	Bà Tung	Bà Tung
	Kính vạn bông	Happy Polla
	Forever Alone	Hoang mang style
	Jvevermind	Forever Alone
Thương hiệu	Honda	Nokia
	Nokia	Samsung
	Yamaha	HTC
	Samsung	Exciter
	Co.opmart	LG
Trò chơi trực tuyến	Gunny	Fast Fifa
	Pikachu	Đào rồng
	Game đua xe	Gunny Azo
	Patch Fifa 2.0	Nhật nhi ba
	Đào vàng	Mộng tam quốc
Tìm kiếm phổ biến nhất	Giá vàng	Gangnam Style
	Gangnam Style	Wanbi Tuấn Anh
	Doraemon	Phuong Mỹ Chi
	Không cảm xúc	Người thừa kế
	Phuong Mỹ Chi	Nick Vujicic

Từ khoá được

13 là từ đại gia.

àn Shinoda



WIRED

Yesterday at 10:48am · 🌐

Why are the nation's two largest carriers doing something that's so unfriendly to consumers?



# Computation Outsourcing vs Security

Verizon and AT&T Are the Only Wireless Carriers Using Perma-Cookies  
It's called the "perma-cookie" and Verizon has embraced this privacy-bus  
WRD.CM | BY ROBERT  
Like · Comment · Share

- Bookmark This Link
- Save Link As...
- Copy Link Location
- Search Google for "http://wrd.cm/1..."
- Inspect Element (Q)

### RELATED ARTICLES



**Verizon's 'Perma-Cookie' Is a Privacy-Killing Machine | WIRED**

Verizon Wireless has been subtly altering the web traffic of its wireless customers for the past two  
WIRED · 8,447 SHARES · OCT 27, 2014



**Somebody's Already Using Verizon's ID to Track Users**

Twitter is using a newly discovered hidden code that the telecom carriers are adding to every page you  
PROPUBLICA · 1,410 SHARES · OCT 30, 2014

Lén lút ghê vậ @@

- [TOP 1] - Longchaucusy Ho: lén lút vào 970 lần.
- [TOP 2] - Viet Nga: lén lút vào 880 lần.
- [TOP 3] - Manh Le: lén lút vào 797 lần.
- [TOP 4] - Hien Nguyen: lén lút vào 635 lần.
- [TOP 5] - Hà Thanh Chương: lén lút vào 553 lần.
- [TOP 6] - Nguyen Dang Ben: lén lút vào 469 lần.
- [TOP 7] - Nguyen Dinh Hung: lén lút vào 337 lần.
- [TOP 8] - Bồ Bảo Là: lén lút vào 205 lần.



**10 người hay lén lút vào tường bạn**  
sieuthiquanao.info

Ứng dụng vui facebook. Click để xem top 10 người hay lén lút vào tường bạn

# Computation Outsourcing

The image features a central collage of logos and branding for cloud computing services. At the top center is the "Powered by Windows Azure" logo. Below it are icons for "Microsoft Office 365" (a cloud with Office icons) and "Google Apps" (a circular arrangement of Google service icons). To the left is the "FutureSystems" logo, a vertical black bar with white text and a green grid pattern at the bottom. To the right is the "VIRTUAL COMPUTING LAB" logo, a vertical grey bar with red text and a red arrow pointing right, with "powered by Apache VCL" written below it. In the center-bottom is the "amazon web services™ EC2" logo. At the bottom is a highlighted box containing the "amazon web services™" logo and the text "Amazon Elastic Map Reduce (EMR)".

Powered by Windows Azure™

Microsoft Office 365

Google Apps

FutureSystems

VIRTUAL COMPUTING LAB  
powered by Apache VCL

amazon web services™ EC2

amazon web services™ Amazon Elastic Map Reduce (EMR)

# Computation Outsourcing



## » Challenges

- › How to protect data
- › How to protect result ( $f(\text{DATA})$ )
- › How to make sure the result is correct

# Computation Outsourcing

## Solutions

### » Bottom-up approach

- › Gentry C., Fully Homomorphic Encryption Using Ideal Lattices, STOC 2009
- › Lauter K., Naehrig M., Vaikuntanathan V., Can Homomorphic Encryption be Practical? IACR Cryptology ePrint Archive 2011/405, 2011
- › Brakerski Z., Vaikuntanathan V., Efficient Fully Homomorphic Encryption from (Standard) LWE. In Proc. of FOCS, 2011, pp. 97-106
- › Brakerski Z., Gentry C., Vaikuntanathan V., (Leveled) fully homomorphic encryption without bootstrapping. In Proc. of ITCS, 2012, pp. 309-325
- › Brakerski Z., Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP. IACR Cryptology ePrint Archive 2012/78, 2012
- › Seny Kamara and Lei Wei, Garbled Circuits via Structured Encryption, in *Workshop on Applied Homomorphic Encryption (WAHC '13)*, April 2013
- › Seny Kamara and Mariana Raykova, [Parallel Homomorphic Encryption](#), in *Workshop on Applied Homomorphic Encryption (WAHC '13)*, April 2013

# Computation Outsourcing Solutions

## » Top-down approach

- › Privacy preserving Datamining/Machine learning
- › Verykios V. S. et.al, State-of-the-art in privacy preserving data mining, ACM SIGMOD Record Volume 33 Issue 1, March 2004 Pages 50 – 57.
- › Wang C. et.al, "Secure and Practical Outsourcing of Linear Programming in Cloud Computing," in Proc. of IEEE INFOCOM, 2011.
- › Wang C. et.al, OIRS: Outsourced Image Recovery Service from Compressive Sensing with Privacy Assurance, in NDSS Short Talk, 2013.

# “Trusting trust”

» Whom do you trust?

- › Probability No
- › Sometimes Yes



**Thank for attention!**