

# Secure Storage in the Cloud

14. ISSS Berner Tagung für Informationssicherheit  
"Cloud Computing: Chancen und Risiken"

24. November 2011, Bern

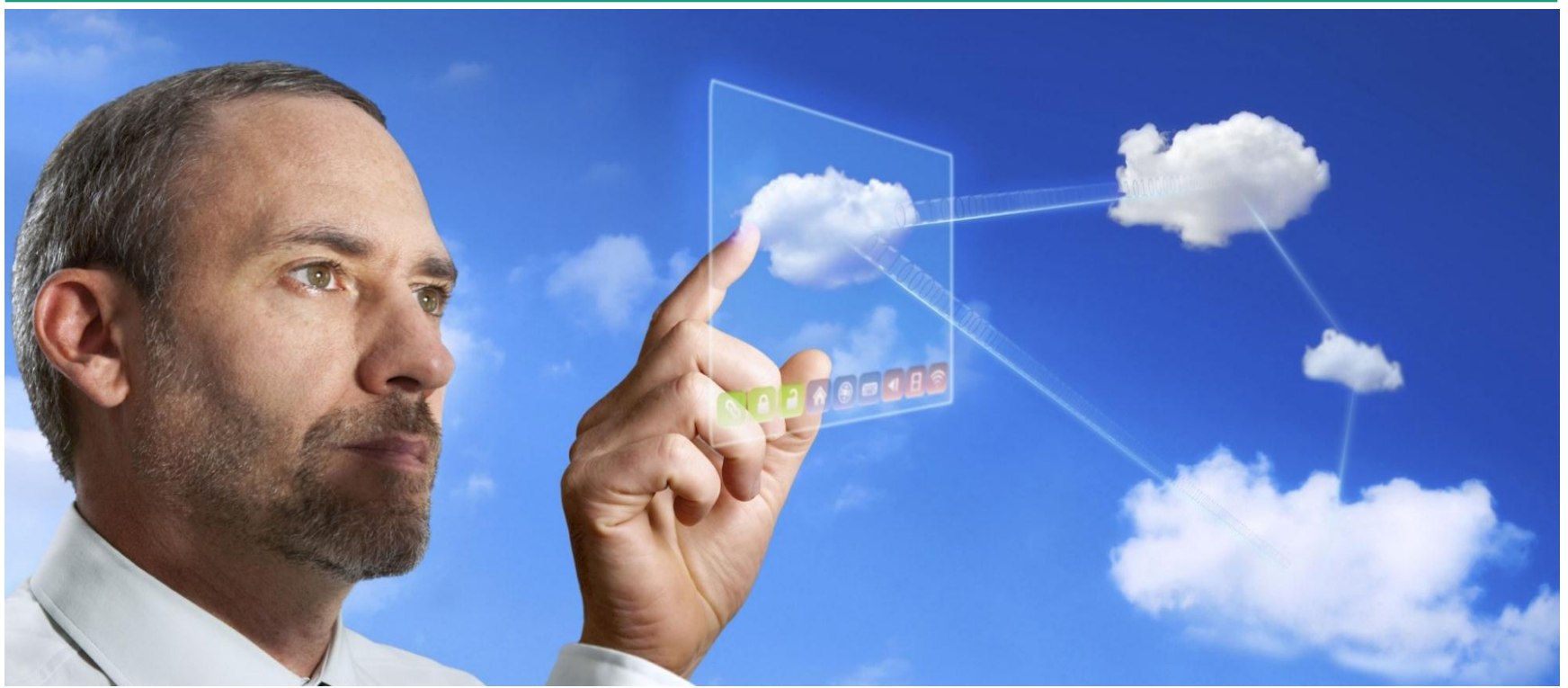
**Prof. Dr. Michael Waidner**  
**Fraunhofer SIT, Direktor**  
**Technische Universität Darmstadt, Chair SIT Research Group**

# Secure Storage in the Cloud

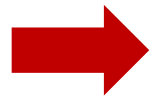
**Prof. Dr. Michael Waidner**

Fraunhofer SIT and

SIT Research Group and Chair, Technische Universität Darmstadt



# Outline

- 
- 1. Security and Cloud Storage**
  - 2. Fraunhofer OmniCloud:  
Secure Usage of Any Cloud**
  - 3. Summary**

# Cloud Storage is ...



- Data storage
- Version backup
- Synchronization
- Sharing with some
- Publication to all
- *... in the Cloud*

## Cloud Storage offers ...

# Opportunities and ...

- **Costs** No hardware, no licenses, no management
- **Convenience** Accessible from anywhere, by anybody
- **Scale** “Infinite” storage capacity, paid per use

# ... Risks

- **Liability** Lack of clear regulations
- **Data Protection** Where is the data? What law applies?
  
- **Loss of Control** Access by other clients, by cloud provider?
- **Service level** Acceptable level of reliability and security?
- **Vendor Lock-in** One-way street due to proprietary APIs?

# Types of Cloud Storage

Our focus is on value-added storage for productivity



## ■ Raw Storage for Enterprises Apps

- Amazon S3, Rackspace, Nirvanix, ...
- Access through provider API

## ■ Value-added Storage for Productivity

- Dropbox, Mozy, TeamDrive, ...
- Access through provider application
- Often based on raw service of another cloud

# Bottleneck “Upload”



- Keep data within cloud
  - Do everything in the cloud
  - **Nothing** is sent
  
- Differential data transfer
  - Mostly isolated, small changes
  - Only **deltas** are sent
  - Remember “rsync”?
  
- Deduplication
  - 90% is already in the cloud!
  - Only **hashes** are sent
  - **Within** one client’s space
  - **Across** all clients’ spaces

# Why is Cross-client Deduplication Risky?

## Brute-force attack on data confidentiality



... total amount is CHF **10'000.00** ...



... total amount is CHF **11'000.00** ...



... total amount is CHF **12'000.00** ...



... total amount is CHF **13'000.00** ...



Danny Harnik, Benny Pinkas, Alexandra Shulman-Peleg: Side Channels in Cloud Services; IEEE Security and Privacy Magazine 8/2 (2010)

# Why is Cross-client Deduplication Risky?

## Some countermeasures

- **No cross-client deduplication**

- Clients may encrypt their files

- **Server-side deduplication**

- Clients always send files, no hashes

- **Something in between**

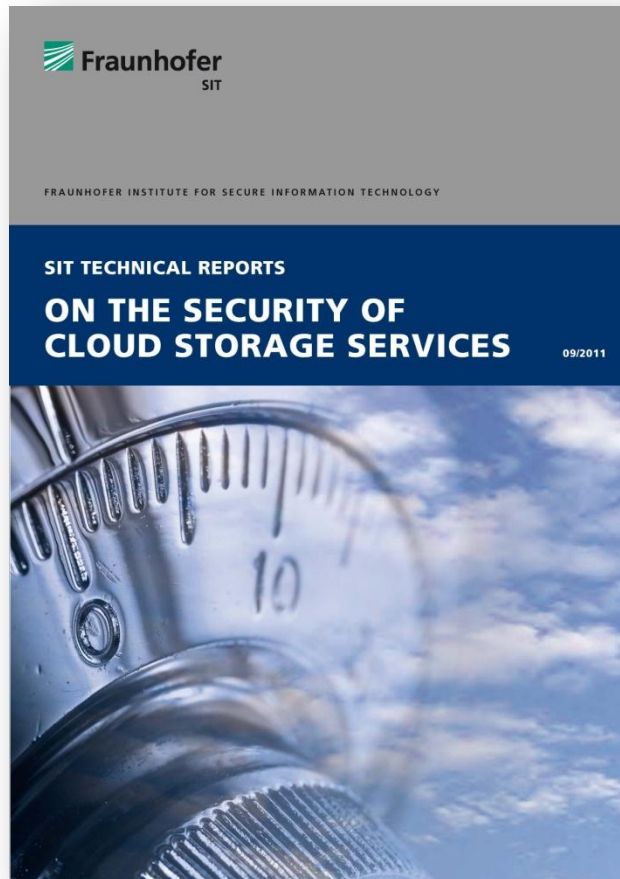
- Server flips a coin and may ask for file even if it already exists



Danny Harnik, Benny Pinkas, Alexandra Shulman-Peleg: Side Channels in Cloud Services; IEEE Security and Privacy Magazine 8/2 (2010)

# Fraunhofer Study

## “On the Security of Cloud Storage Services”



Release date: December 2011

- CloudMe
- CrashPlan
- Dropbox
- Mozy
- TeamDrive
- Ubuntu One

Remember: Our focus is on value-added storage for productivity.

# Criteria



## 1. Encryption of Data in Transit

- Transport Layer Security (TLS)
  - Server authentication
  - Secure cryptographic algorithms
  - Suitable key lengths

## 2. Encryption of Data at Rest

- Client side encryption\*
- Secure algorithms and suitable key lengths
- *Secure key escrow*

\*: Prevents delta updates and server-side deduplication

# Criteria



## 3. Secure Registration and Login

- Transport Layer Security (TLS)
- Data collection minimization (privacy)
- Account activation
- Strong passwords
- Protection against user/email enumeration
- *Multi-factor authentication*

## 4. Data Location

- Information on geographic data location
- *Choice of geographical data locations*

# Criteria



## 5. File Sharing / File Publication

- Sharing: configurable access rights
- Publication: obfuscated link, no indexing by external search engines
- *List of currently shared / published files*

## 6. Access from Different Machines

- List of registered devices
- Manual device activation / de-activation

## 7. Deduplication

- Threshold
- Secure hash algorithm

# Summary of Findings

Security is taken seriously ... but lots of room for improvements

	CloudMe	Dropbox	Ubuntu One	Mozy
No encryption at all	X		X	
Insecure communication (HTTP)	X			
Only server-side encryption		X		
No filename obfuscation for public files		X	X	
Allows weak passwords	X	X		X
Provider does not verify email	X	X		X
Shared files can be search indexed	X	X	X	

# Outline

## 1. Security and Cloud Storage

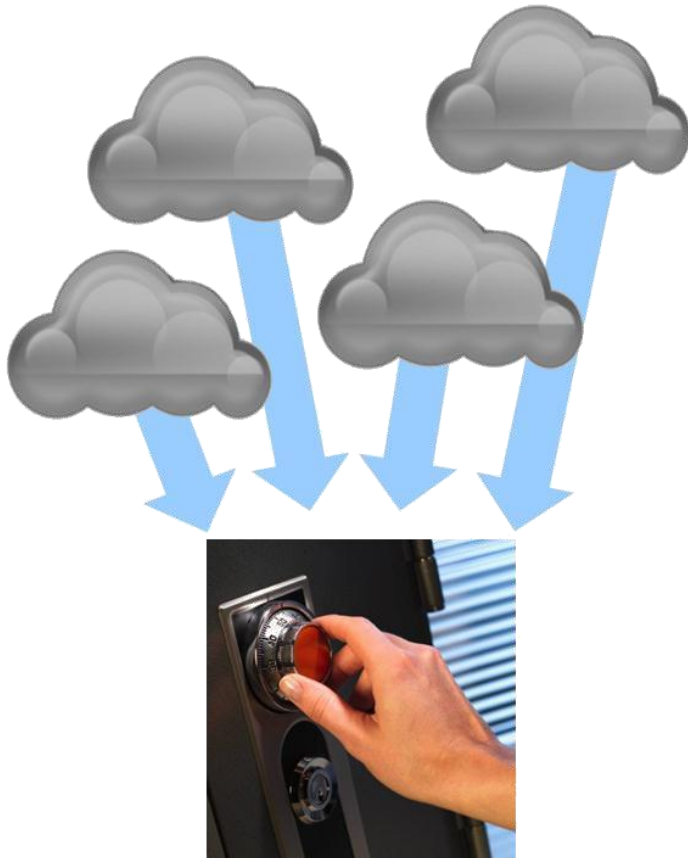


## 2. Fraunhofer OmniCloud: Secure Usage of Any Cloud

## 3. Summary

# Fraunhofer OmniCloud

## Secure Usage of Any\* Cloud



OmniCloud

- **Client-driven data security**
  - Security does not depend on provider
  - Client-side encryption and file name / directory structure obfuscation
  - Client-side key management
- **Client-side deduplication and incremental updates**
- **Client-specific or gateway**
- **No vendor lock-in**
  - Single unified framework
  - Mapping between APIs and file transfer protocols

# Fraunhofer OmniCloud

## Obfuscated filenames and folders



Now Introducing Teams!  
1000GB of space to start.

Search your Dropbox

Files Events Sharing Help

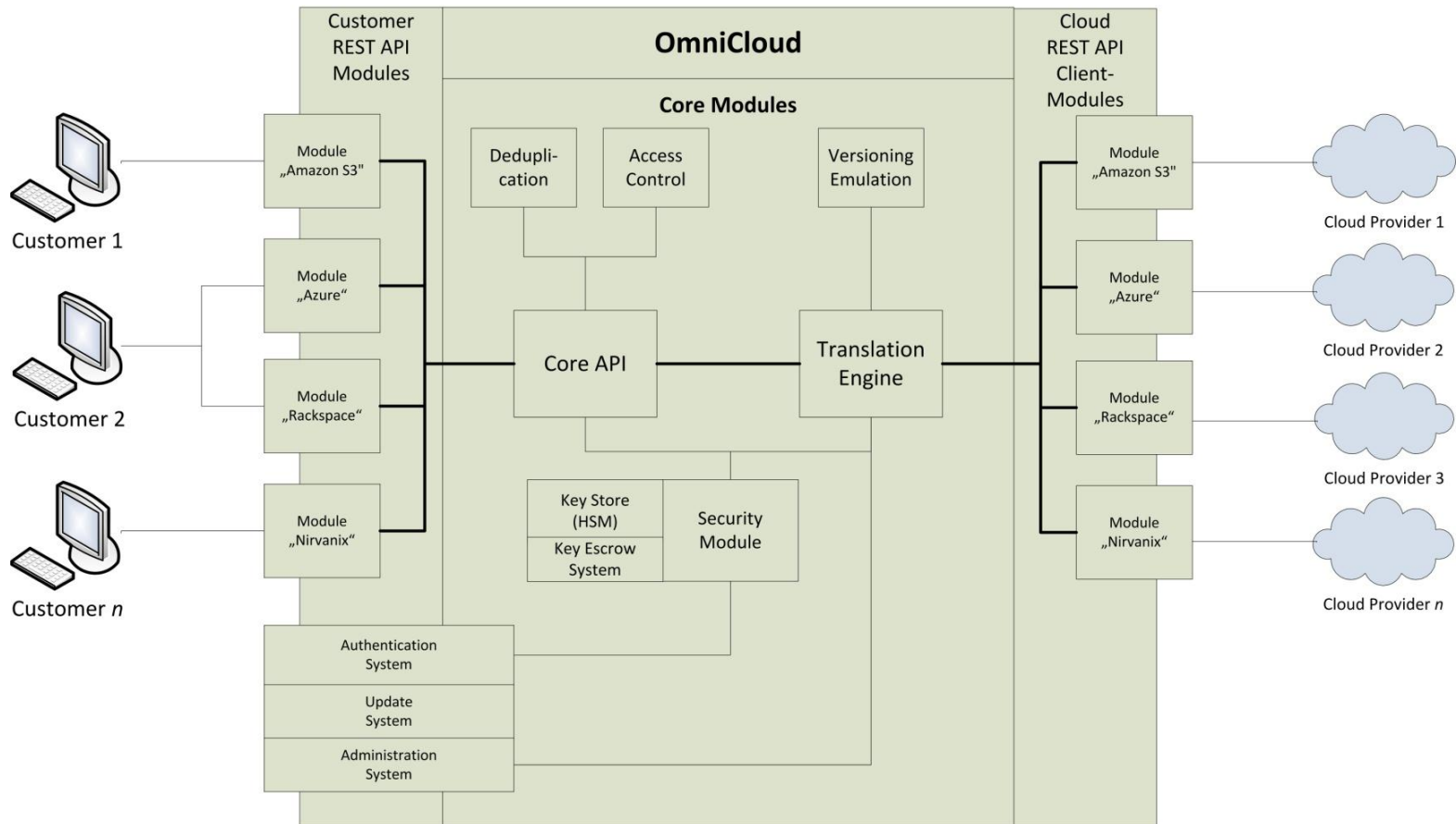
Dropbox » 4dd41ddc51f811772b15d9e5e08...a02d50f037

Upload New folder Invite to folder Show deleted files More

<input type="checkbox"/> File Name	Size	Modified
Parent folder		
<input type="checkbox"/> 04b8be5c41ab7e45e482123d1...0fc6e2286		
<input type="checkbox"/> 4d4ba6190790d0f8733760a301...294f3f6ac9		
<input type="checkbox"/> 27d25f06f54e0b10140c954762...00a1a32a9		
<input type="checkbox"/> bce3f03c15ec5adffae71a4a1b...5883b8a7	218.5KB	15 mins ago
<input type="checkbox"/> eca5b6a3923cad8986c3d9bb6...6a793cb2d	7.7KB	15 mins ago

# Fraunhofer OmniCloud

## Prototype architecture



# Outline

**1. Security and Cloud Storage**

**2. Fraunhofer OmniCloud:  
Secure Usage of Any Cloud**

 **3. Summary**

## Fraunhofer's experience so far

- **Cloud storage reduces costs, improves productivity**

- **Slow adoption by enterprises**

- Privacy and data protection laws
- Confidentiality and data security technologies

- **Fraunhofer OmniCloud**

- Client-driven security and efficiency
- No undue reliance on cloud provider
- No vendor lock-in through APIs and protocols

# Acknowledgements

This presentation reports on work done by members of the Department “Cloud Security, Identity and Privacy” at the Fraunhofer SIT:

- Moritz Borgmann
- Tobias Hahn
- Michael Herfert
- Thomas Kunz
- Marcel Richter
- Sven Vowé

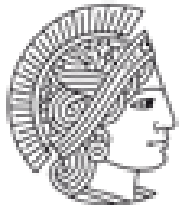


**Prof. Dr. Michael Waidner**  
[michael.waidner@sit.fraunhofer.de](mailto:michael.waidner@sit.fraunhofer.de)

**Fraunhofer-Institut für  
Sichere Informationstechnologie**

Rheinstraße 75  
64295 Darmstadt

[www.fraunhofer.de](http://www.fraunhofer.de)  
[www.sit.fraunhofer.de](http://www.sit.fraunhofer.de)



**TECHNISCHE  
UNIVERSITÄT  
DARMSTADT**

**Technische Universität Darmstadt**

Lehrstuhl für Sicherheit in der IT  
Mornewegstraße 30  
64289 Darmstadt

[www.cased.de](http://www.cased.de)  
[www.sit.tu-darmstadt.de](http://www.sit.tu-darmstadt.de)