Privacy-aware Storing and Searching in the Cloud

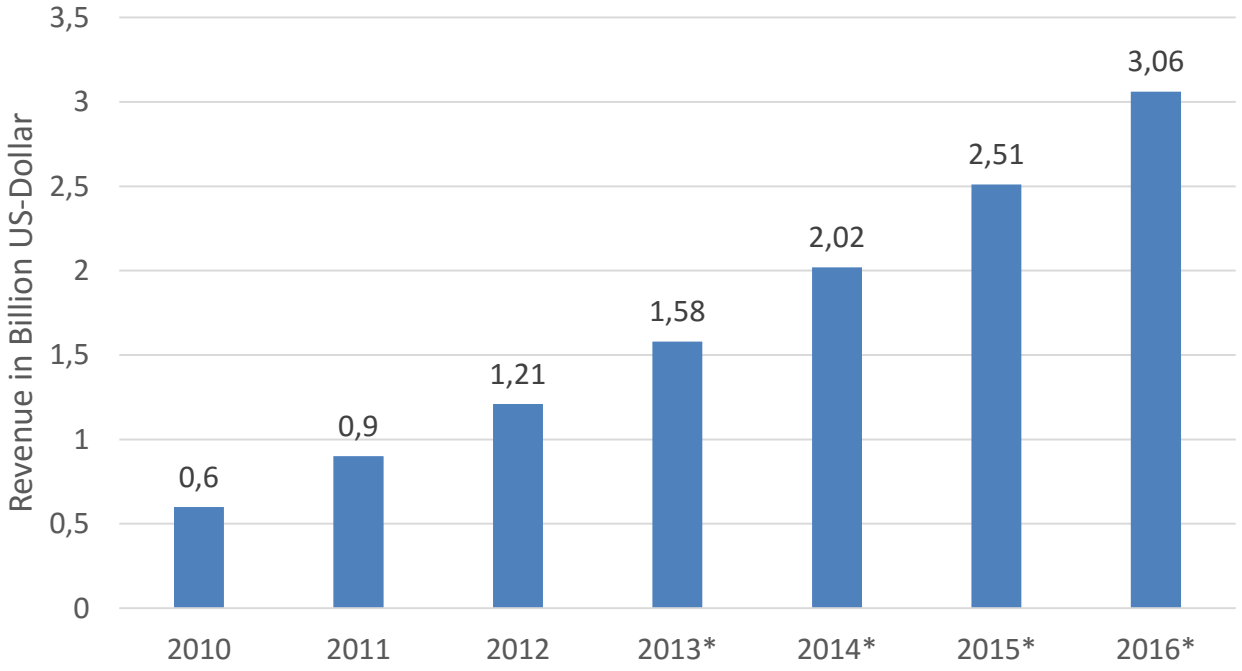
Fabian Wiedemann

VSR.*Informatik*.TU-Chemnitz.*de*

1

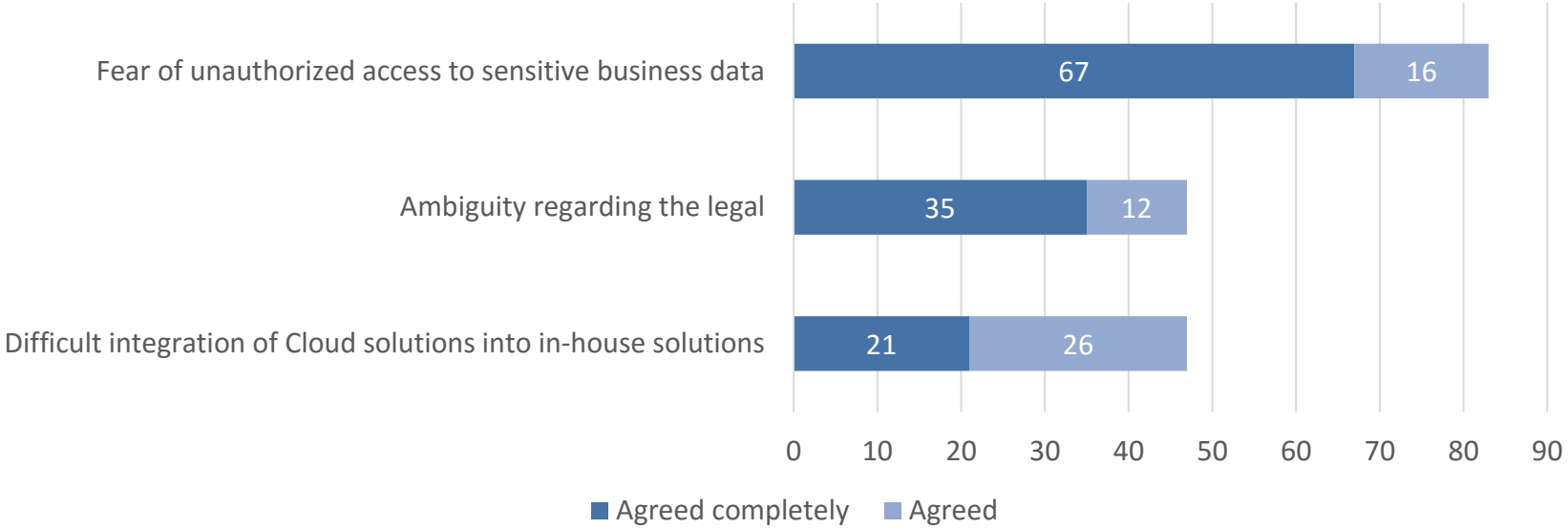
Why do we need Cloud Storage?

Worldwide Platform-as-a-Service (PaaS) Revenue from 2010 to 2016 (in Billion US-Dollar)



Quelle: http://de.statista.com/statistik/daten/studie/307023/umfrage/umsatz-mit-platform-as-a-service-weltweit-seit-2010/

Why Companies do not use Cloud Services (TOP3)



Quelle: http://www.kpmg.com/DE/de/Documents/cloudmonitor-2014-kpmg.pdf

Would you like to save sensitive Data in the Cloud?

„Security as Challenge – and Opportunity“

Quelle: http://www.kpmg.com/DE/de/Documents/cloudmonitor-2014-kpmg.pdf

2 State of the Art

2.1 Industry

NO Encryption

Encryption on Server-Side

(Google Cloud Storage [1], Amazon S3 [2])

[1] http://googlecloudplatform.blogspot.de/2013/08/google-cloud-storage-now-provides.html
[2] http://aws.amazon.com/de/s3/faqs/#What_options_do_I_have_for_encrypting_data_stored_on_Amazon_S3

2.2 Challenges

Challenges

Client-side encryption and decryption

Encryption of Data, Keywords, etc.

Efficient keyword-based search

Support of Multi-User Collaboration

Approaches

Approaches in General

1. Encrypting documents
2. Building Encrypted Database (EDB)
3. Search on EDB

Approaches - Overview

Property-Preserving-Encryption

Identity-based Encryption

Full-Homomorphic Encryption

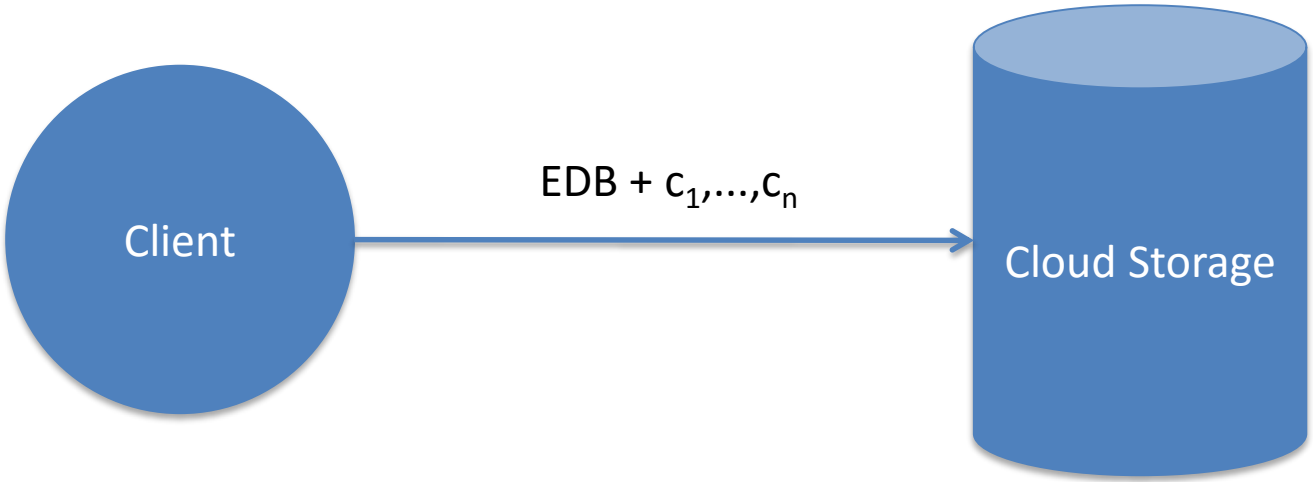
Oblivious RAMs

Property-Preserving Encryption (PPE)

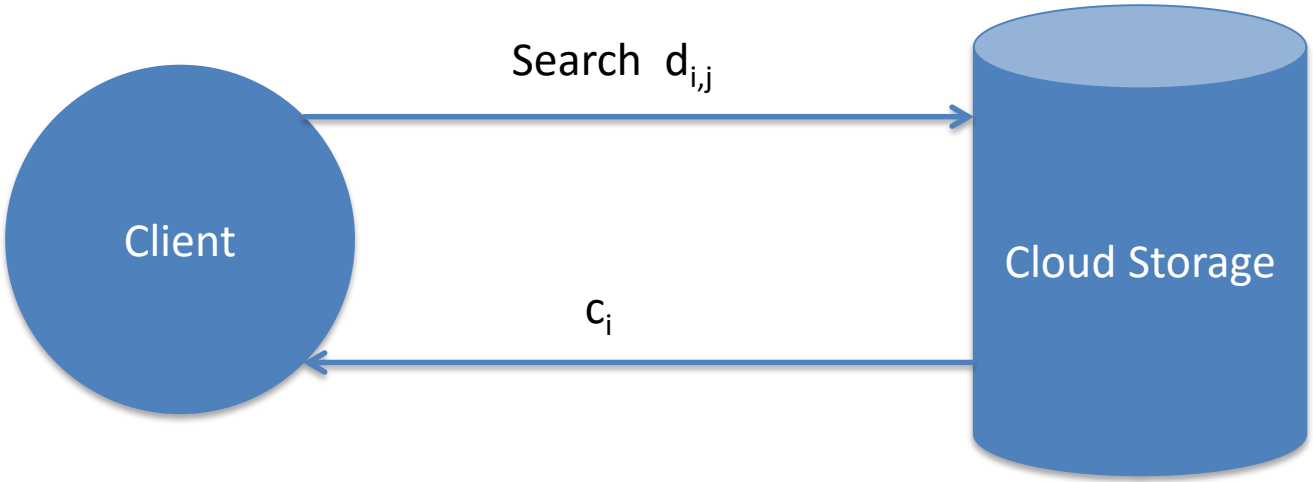
D_i	Documents
$w_{i,1} \ldots w_{i,m}$	Keywords
$c_i = E^R(D_i)$	Ciphertext
$d_{i,j} = E^D(w_{i,j})$	Encrypted keywords
$r_i = (d_{i,1}, \ldots, d_{i,m}, ptr(c_i))$	Tuple with pointer to ciphertext
$EDB = (r_1, \ldots, r_n)$	Encrypted database

Bellare, Mihir, Alexandra Boldyreva, and Adam O'Neill. "Deterministic and efficiently searchable encryption." In Advances in Cryptology-CRYPTO 2007, pp. 535-552. Springer Berlin Heidelberg, 2007.

PPE - Setup



PPE - Search



Objective

General Approach for multiple Storage Solutions

Document Storage

SQL-Databases

NoSQL-Databases

…

VSR

Thank You!

fabian.wiedemann@informatik.tu-chemnitz.de

VSR.*Informatik*.TU-Chemnitz.*de*

@tr3ddy @myVSR /myVSR