Microsoft® Research
FacultySummit

Cryptographic Cloud Storage and Services

Kristin Lauter
Principal Researcher
Manager, Cryptography Group
Microsoft Research

2031
FUTURE/WORLD
2011

Microsoft® Research
FacultySummit

Joint work with Seny Kamara:
Cryptographic Cloud Storage

Joint work with Michael Naehrig and Vinod Vaikuntanathan:
Can Homomorphic Encryption Be Practical?

FUTURE/WORLD 2011 2031

Business Problem 1: Pharmaceutical

- Pharma has large databases of lab results and drug reagents
- Much of this information is sensitive and proprietary, and should not be shared with the competition
- Pharma needs to securely store this database and selectively give access to parts of it to employees with different roles: researchers, managers, auditors…
- They have partner companies with whom they need to selectively share parts of their data
- Similar problem throughout the pharmaceutical industry and in other industries such as financial, healthcare,…

Business Problem 2:
Electronic Medical Records

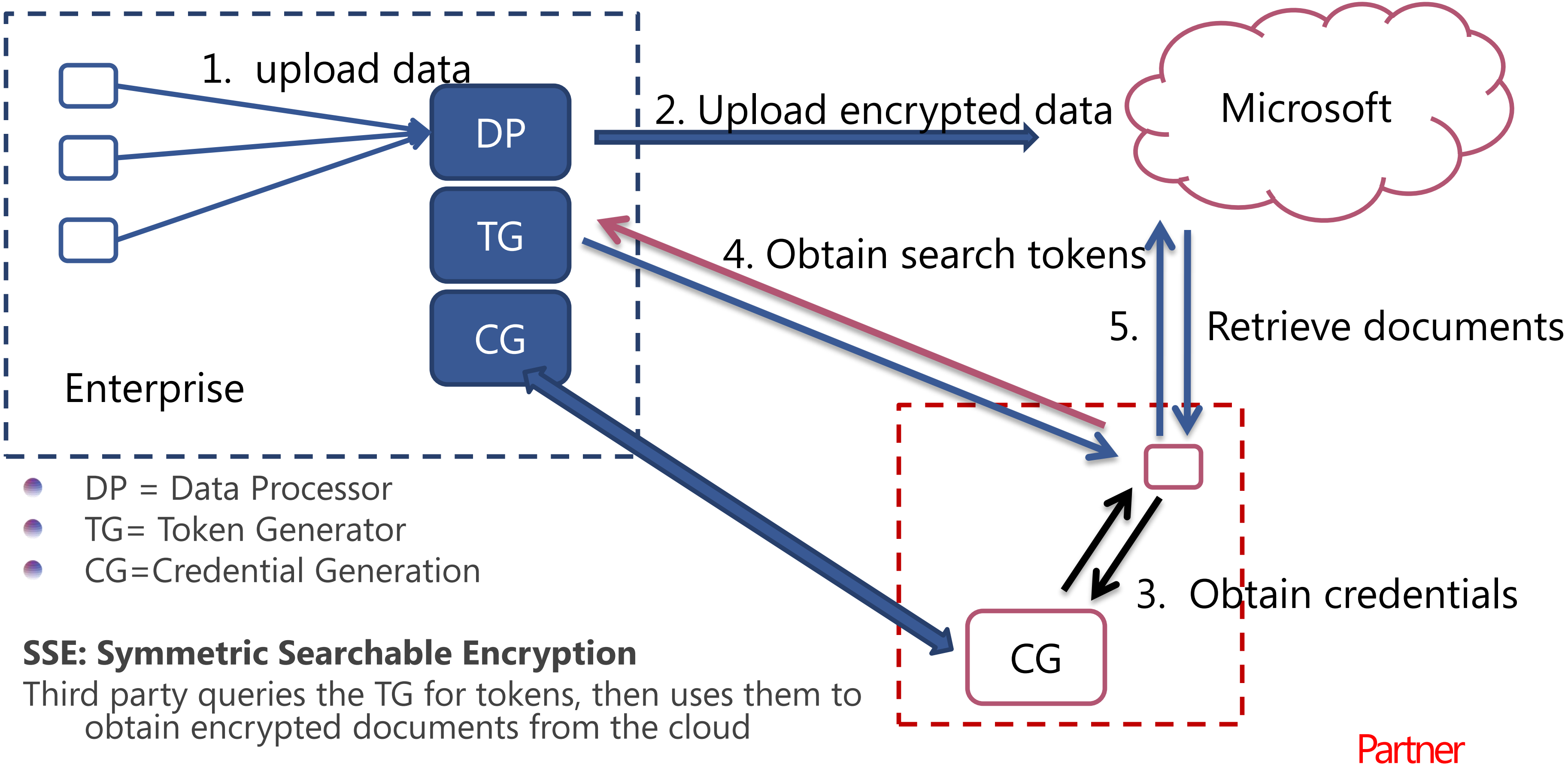
- Hospitals, doctors, patients, insurance companies, pharmacies want to store patient medical records electronically
- $19 billion from U.S. gov’t to move to EMR within 5 years
- Patients want to retain privacy of their medical record, share portions selectively

Solution: Cryptographic Cloud Storage

- Cloud storage provides
  - *availability*
  - *reliability*
  - *efficient retrieval*
  - *data sharing*
- Pillars of cryptographic cloud storage
  - *Confidentiality*: the cloud storage provider does not learn any information about customer data.
  - *Integrity*: any unauthorized modification of customer data by the cloud storage provider can be detected by the customer.
  - *Search:* queries answered and encrypted results returned without leaking the terms in the query

Searchable Encryption

- Encryption scheme
  - Hides information about documents
  - Given a *search token* for a *search term*, returns which documents contain the *search term*
  - Without leaking the term!
- SSE: Symmetric Searchable Encryption
  - [CGKO06] Symmetric searchable encryption: improved definitions and efficient construction, R. Curtmola, J. Garay, **S. Kamara**, R. Ostrovsky. CCS '06
  - [AKK08] Proofs of data possession from homomorphic sigma-protocols, G. Ateniese, **S. Kamara**, J. Katz, AsiaCrypt'09
  - [KL] Cryptographic Cloud Storage, Kamara, Lauter, Proceedings of Financial Cryptography 2010: Workshop on Real-Life Cryptographic Protocols and Standardization.
  - [BCHL] Patient Controlled Encryption: patient privacy in electronic medical records, Benaloh, Chase, Horvitz, Lauter, CCSW'09 ACM Cloud Computing Security Workshop.
  - [KPR] CS2: A Semantic Cryptographic Cloud Storage System, Kamara, Papamanthou, Roeder, May 2011



- DP = Data Processor
- TG= Token Generator
- CG=Credential Generation

SSE: Symmetric Searchable Encryption

Third party queries the TG for tokens, then uses them to obtain encrypted documents from the cloud

Private personal health record

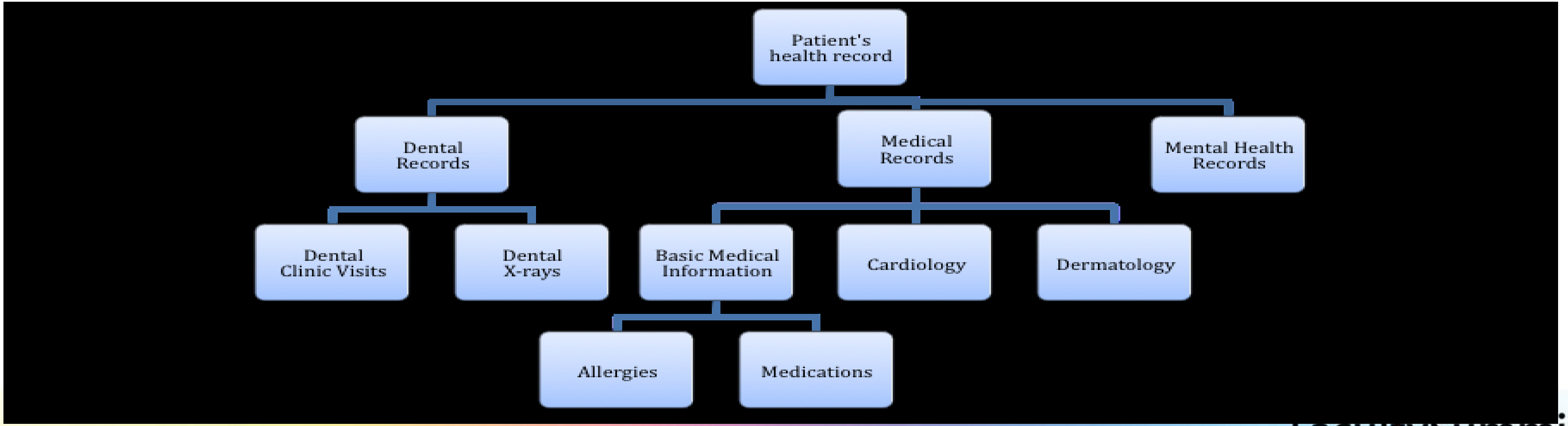
Doctor

Lab results

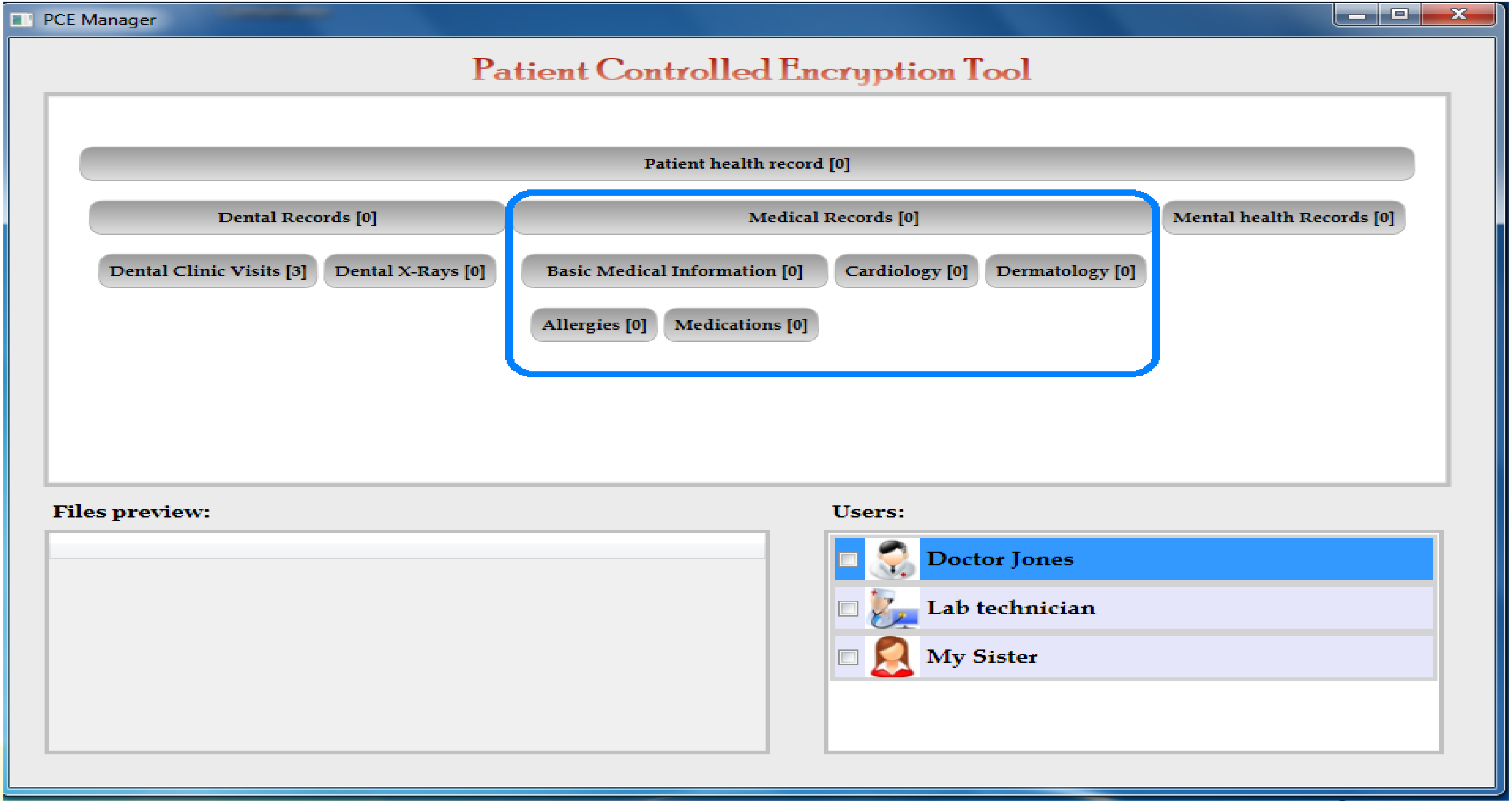
- All data uploaded to the server encrypted under Alice’s public or private key
- Alice decides the access policy and who keys or search permissions to share with

Electronic Medical Records

- Patient-Controlled Encryption
  - SSE based, with hierarchichal structure
  - Policy-based encryption



Showing access policy



PCE Manager

Patient Controlled Encryption Tool

Patient health record [0]

Dental Records [0]

Medical Records [0]

Mental health Records [0]

Dental Clinic Visits [3]

Dental X-Rays [0]

Basic Medical Information [0]

Cardiology [0]

Dermatology [0]

Allergies [0]

Medications [0]

Files preview:

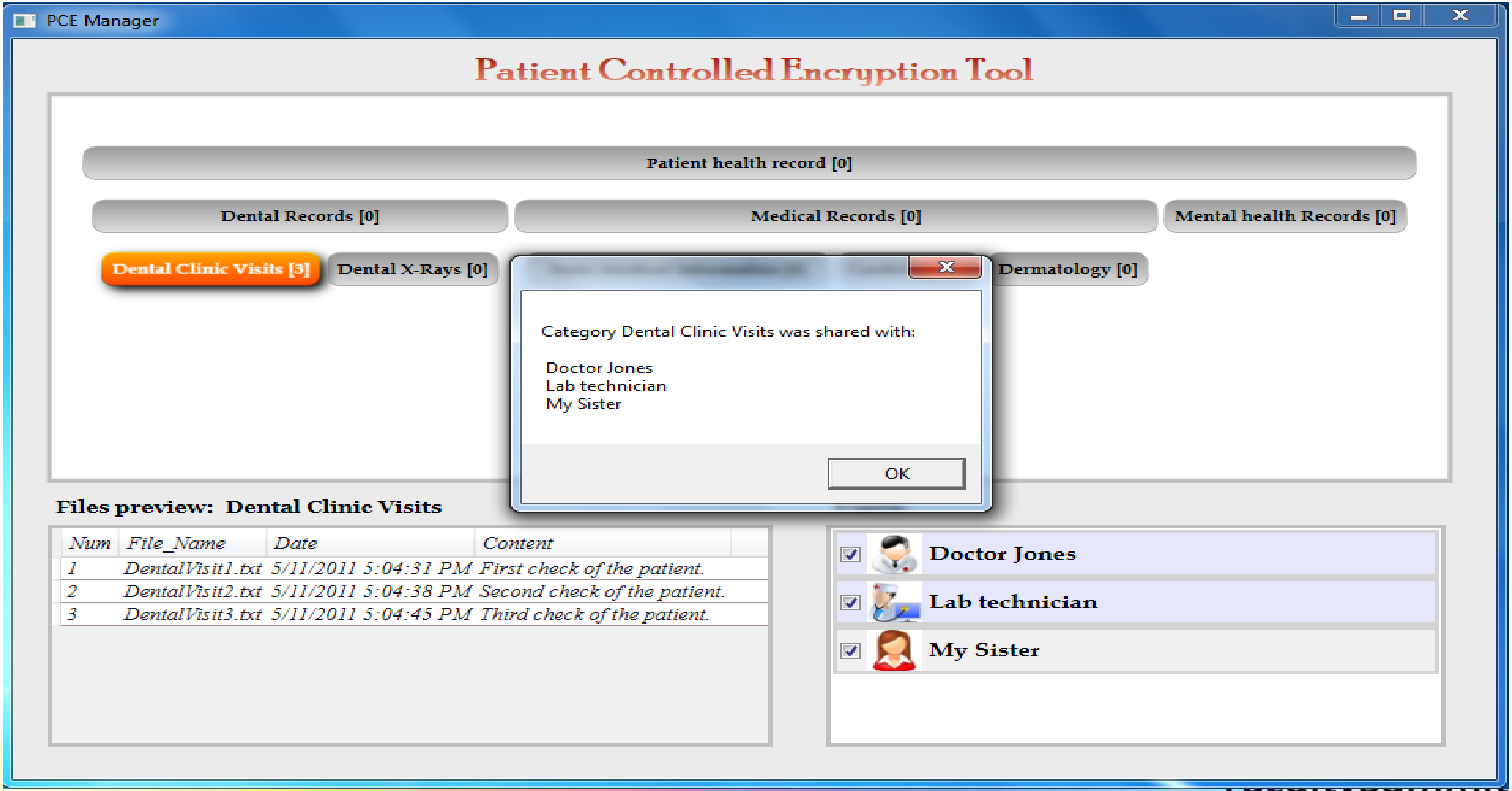
Users:

□ Doctor Jones

□ Lab technician

□ My Sister

Sharing a category:



Category Dental Clinic Visits was shared with:

Doctor Jones
Lab technician
My Sister

Files preview: Dental Clinic Visits

Num	File_Name	Date	Content
1	DentalVisit1.txt	5/11/2011 5:04:31 PM	First check of the patient.
2	DentalVisit2.txt	5/11/2011 5:04:38 PM	Second check of the patient.
3	DentalVisit3.txt	5/11/2011 5:04:45 PM	Third check of the patient.

☑ Doctor Jones
☑ Lab technician
☑ My Sister

Related work and collaborations

- SHARPS grant, Carl Gunter et al. ONC funded
- JHU group, implementations (Matt Green’s talk)
- ABE (Attribute Based Encryption) Brent Waters et al.
- U Calgary group, (access policy via ABE) Rei Safavi-Naini

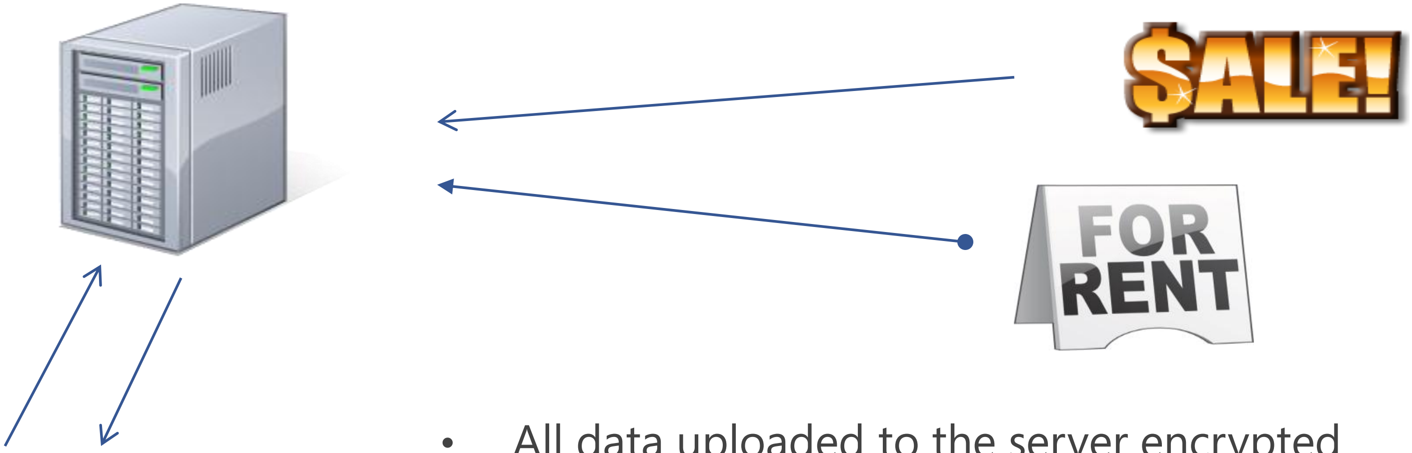
Cloud services

which process encrypted data and give useful results:

- Streaming data from medical devices to a server which processes and gives recommendations
- Streaming financial data processed via proprietary functions to give predictions or recommendations
- Contextual and location data streamed to a server to deliver targeted advertising and pricing/coupons.

Functions we can compute on encrypted data: average, deviation, regression analysis…

Private targeted advertising



- All data uploaded to the server encrypted under Alice’s public key
- Server computes on encrypted data
- Server returns contextual ads or info to the consumer’s phone

Homomorphic Encryption

- Parameters with security > 128 bits for somewhat homomorphic public key scheme

#mult	n	size(q)	PK size	SK size	CT size
1	2048	58 bits	30 KB	2 KB	≥ 30 KB
10	8192	354 bits	720 KB	8 KB	≥ 720 KB
32	65536	1298 bits	20 MB	66 KB	≥ 20 MB

Homomorphic Encryption

- Reference implementation of somewhat homomorphic PK scheme in computer algebra system Magma
- Experimentation phase, still search for better parameters, more optimizations
- Timing for n = 2048, q has 58 bits, 1 mult

Operation	x86-64 Intel Core 2 @ 2.1 GHz
SH_Keygen	250 ms
SH_Enc	24 ms
SH_Add	1 ms
SH_Mul	41 ms
SH_Dec (2-element ciphertext)	15 ms
SH_Dec (3-element ciphertext)	26 ms

MSR Cryptographic pairings library

Curve	Security level	ARM Cortex A9 @ 1 GHz	x86 Intel Core 2 @ 2.4 GHz	x86-64 Intel Core 2 @ 2.4 GHz
bn254	128 bits	51 ms	11 ms	6 ms
bn638	192 bits	650 ms	113 ms	57 ms

Homomorphic Encryption

- "Fully Homomorphic Encryption from Ring LWE and Key-Dependent Message Security"
  Brakerski, Vaikuntanathan, ***CRYPTO 2011.***
- "*Efficient* Fully Homomorphic Encryption from Standard LWE"
  Brakerski, Vaikuntanathan, ***IEEE FOCS 2011.***
- "Can Homomorphic Encryption be Practical?"
  Lauter, Naehrig, Vaikuntanathan, MSR Technical Report MSR-TR-2011-61
- "Affine Pairings on ARM" *Acar, Lauter, Naehrig, Shumow, eprint archive:* no. 2011/43
- "An Analysis of Affine Coordinates for Pairing Computation",
  Lauter, Montgomery, Naehrig, in ***Pairing 2010,*** Springer Verlag, 2010

Microsoft® Research
FacultySummit

2031

FUTURE WORLD

2011