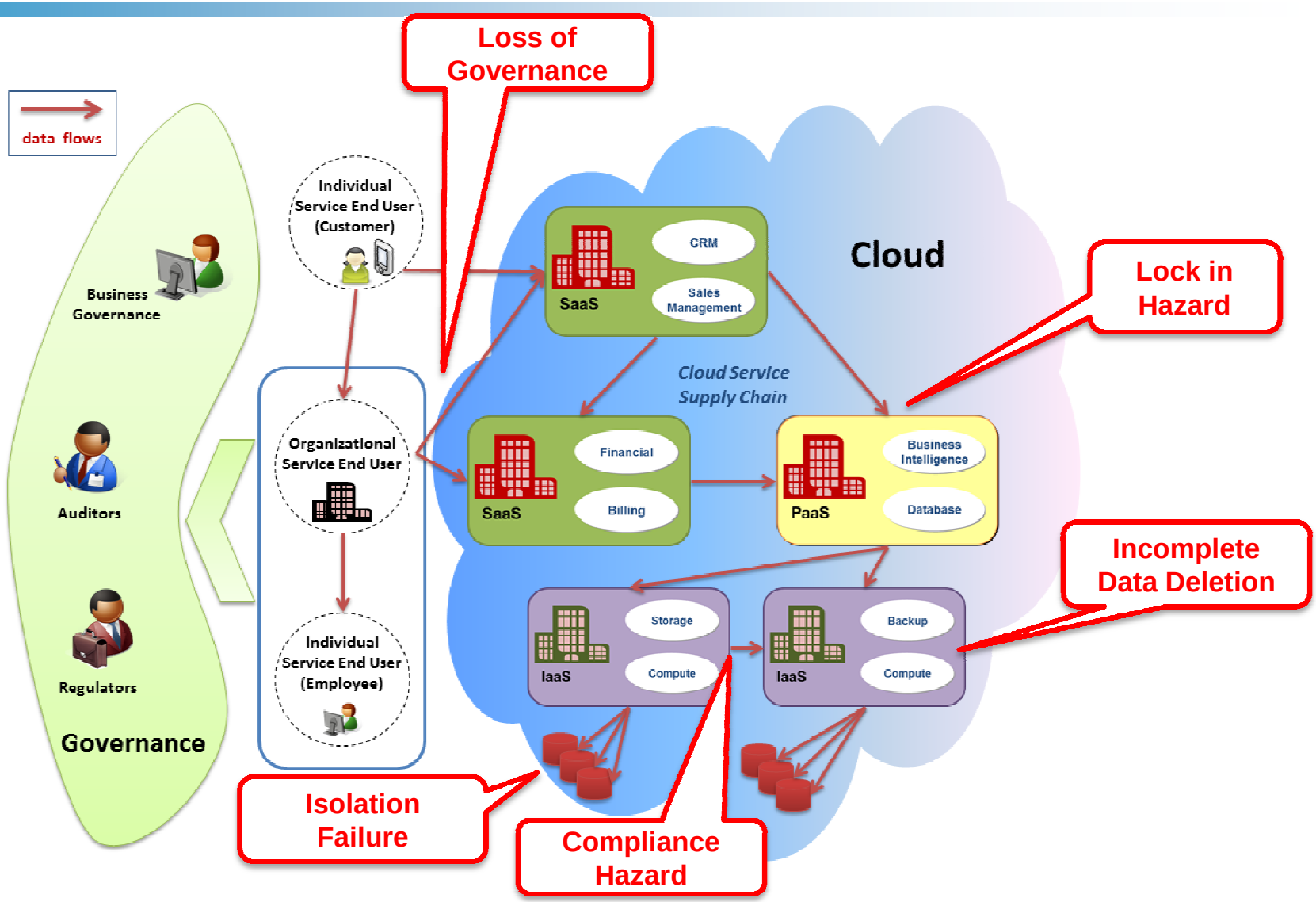
Privacy Preserving Delegated Word Search

Kaoutar Elkhiyaoui, Melek Önen, Refik Molva

A4Cloud – Accountability for Cloud

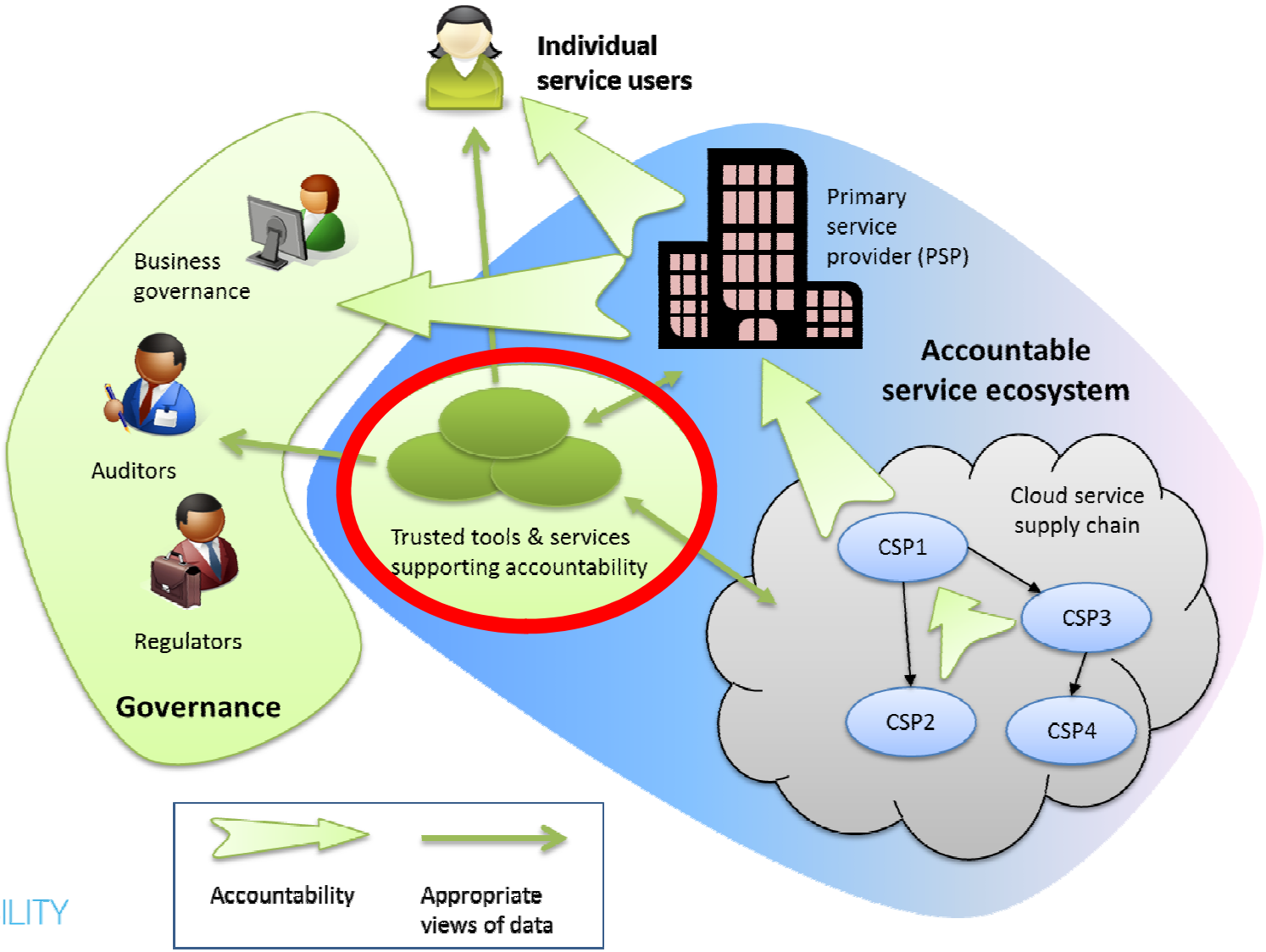
- **Accountability for Cloud and Future Internet Services**
- **Partners**
- **October 2012**

Emerging Issues



CLOUD ACCOUNTABILITY PROJECT

Accountability Approach



CLOUD ACCOUNTABILITY PROJECT

A4Cloud - Objectives

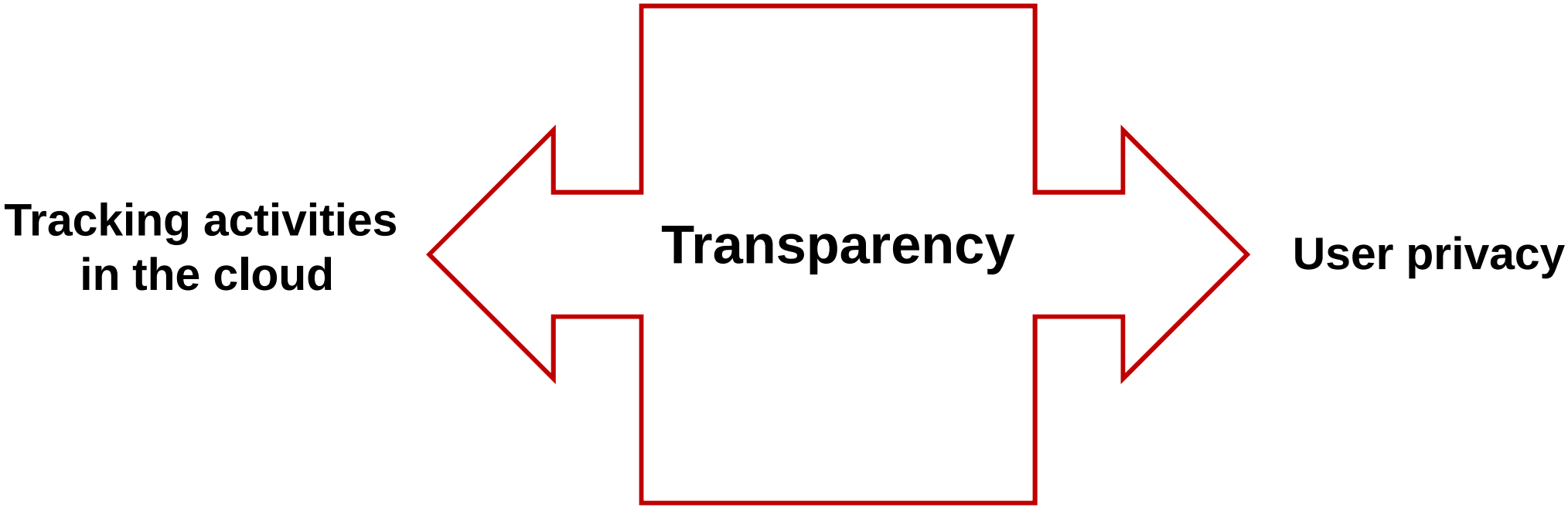
Objective 1: Develop tools that enable cloud service providers to give their users appropriate control and transparency over how their data is used, confidence that their data is handled according to their expectations and is protected in the cloud, delivering increased levels of accountability to their customers.

Objective 2: Create tools that enable cloud end users to make choices about how cloud service providers may use and will protect data in the cloud, and be better informed about the risks, consequences, and implementation of those choices.

Objective 3: develop tools to monitor and check compliance with users' expectations, business policies and regulations.

Objective 4: Develop recommendations and guidelines for how to achieve accountability for the use of data by cloud services, addressing commercial, legal, regulatory and end user concerns and ensuring that technical mechanisms work to support them.

A4Cloud: User privacy + Transparency



Goal: Design privacy preserving solutions that assure transparency

Usecase: Logging & User Privacy

- **Transparency via action logging tools**
- **User privacy** ⇒ **Encrypted logs**
- **Logs can be outsourced**
- **Audit: Third party search on encrypted logs**

Privacy Preserving Delegated Word Search

- **Prying Clouds (Honest but Curious)**

Cloud should not be able to infer any information about the logs

- **Third party audit**
  - *Revocation*
- **Privacy requirements**
  - Data privacy
  - Query privacy
  - Authorized access with revocation

Word Search vs Delegated Word Search

Schemes	Data Privacy	Query Privacy	Delegation with revocation
Song ‘04	Yes	No	No
Boneh ‘04	Yes	No	No
Bellare ‘06	Yes	No	No
Curtmola ‘06	Yes	No	Yes
PRISM (Blass ‘12)	Yes	Yes	No

Delegated Word Search: Building Blocks

- **Privacy preserving word search (PRISM)**
- **One time keys**
- **Attribute-based Encryption**

Delegated Word Search - PRISM

- **File Upload**

Client | Cloud

$F = \{w_1, w_2, \ldots, w_n\}$

$L = \{\omega_1, \omega_2 \ldots, \omega_m\}$

$C_l = Enc_K(w_l) = Enc_k(\omega, ctr)$

$C = \{C_1, C_2, \ldots, C_n\}$ →

Delegated Word Search - PRISM

- **File Upload**
- **File processing at the cloud**
  - Maps each ciphertext C_l to position (i, j) in (t, t) matrix

$$H(C_l) = i \,||\, j$$

  - Fills q binary matrices M_p

$$H'(C_l) = b_1 \,||\, \ldots \,||\, b_p \,||\, \ldots \,||\, b_q \quad \text{if } b_p = 1$$

$$\begin{array}{cc} & \begin{array}{ccccc} & & j & & \end{array} \\ i & \begin{pmatrix} 0 & 0 & \ldots & & 0 \\ 0 & 0 & \ldots & & 0 \\ . & & & & \\ . & & & & \\ . & & 1 & & \\ 0 & 0 & \ldots & & 0 \end{pmatrix} \end{array}$$

Delegated Word Search - PRISM

- **PIR-based word search**
  - Trostle Parrish '10
  - retrieve a row in (t, t) matrix
- **Prepare query for some word w**

Client | Cloud

$H(Enc_k(w, 1)) = i \,||\, j$

$PIRQuery\ (i) = \vec{u}$

$\vec{u} = (u_1, u_2, \ldots, u_t)$ →

$\vec{v}_p = PIRResponse(M_p, \vec{u}) = M_p * \vec{u}$

← $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_q$

Delegated Word Search - PRISM

- **PIR-based word search**
  - Trostle Parrish '10
  - retrieve a row in (t, t) matrix
- **Prepare query for some word w**
- **Verify response**
  - H(Enc(w, 1)) = i || j

$$\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_q \longrightarrow \vec{v}_p = (v_{p,1}, v_{p,2}, \ldots v_{p,j}, \ldots v_{p,t})$$

$$\downarrow$$

$$h = b_1 \| b_2 \| \ldots \| b_q \longleftarrow b_p$$

  - If H'(Enc(w, 1)) & h = H'(Enc(w, 1)) output 1

Delegated Word Search - Solution

- **Upload File**

Client

Cloud

$F = \{w_1, w_2, \ldots, w_n\}$

$L = \{\omega_1, \omega_2 \ldots, \omega_m\}$

$C = \{C_1, C_2, \ldots, C_n\}$, AP $\longrightarrow$

$C_l = Enc_K(w_l) = Enc(\omega, ctr)$

- **Delegate**

Client $\xrightarrow{K}$ Authorized user

Delegated Word Search

- **Search**

Authorized user

I want to make search query →

Cloud

$K' \leftarrow \mathbf{F}_l$

$C' = Enc_{ABE}(AP, K')$

← $C' = Enc_{ABE}(AP, K')$

$H(Enc_K(w, 1)) = i \| j$

$(i', j') = Perm(K', i, j)$

$\vec{u} = PIRQuery(i')$

$\vec{u} = (u_1, u_2, \ldots, u_t)$ →

Permute M_p using K'

$\vec{v}_p = M'_p * \vec{u}$

← $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_q$

- **PRISM verification**

Delegated Word Search - Solution

- **Solution vulnerable to dictionary attacks**
- **Alternative**

Authorized user

Cloud

$H(Enc_K(w, 1)) = i \,||\, j$

$\vec{u} = PIRQuery(i)$

$\vec{u} = (u_1, u_2, \ldots, u_t)$ →

1. $K' \leftarrow \mathbf{F}_l$
2. $\vec{v}_p = Enc_{K'}(M_p * \vec{u})$
3. $C' = Enc_{ABE}(AP, K')$

← $C', \vec{v}_1, \vec{v}_2, \ldots, \vec{v}_q$

1. Decrypt C'
2. Decrypt relevant component of $\vec{v}_p$
3. PRISM verification

Conclusion and Future Work

- **PRISM benefits from Map Reduce**
  - An average computational overhead of 11%

- **Privacy preserving delegated word search against authorized third parties**
  - The third party only learns 1 bit of information (i.e., the result of the search)

References

- *PRISM: Privacy-Preserving Search in MapReduce.* Erik-Oliver Blass, Roberto Di Pietro, Refik Molva, Melek Önen. PETS 2012, 12th Privacy Enhancing Technologies Symposium, July 11-13, 2012, Vigo, Spain / Also published in LNCS, Volume 7384/2012, Springer