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

- Loss of Governance
- Lock in Hazard
- Incomplete Data Deletion
- TrustworthyClouds September 12-13, 2013, RHUL, UK
Accountability Approach
**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

Tracking activities in the cloud  Transparency  User privacy
Use case: 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

<table>
<thead>
<tr>
<th>Schemes</th>
<th>Data Privacy</th>
<th>Query Privacy</th>
<th>Delegation with revocation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Song ‘04</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Boneh ‘04</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Bellare ‘06</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Curtmola ‘06</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>PRISM (Blass ‘12)</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
Delegated Word Search: Building Blocks

- Privacy preserving word search (PRISM)
- One time keys
- Attribute-based Encryption
### Delegated Word Search - PRISM

**File Upload**

\[ F = \{w_1, w_2, \ldots, w_n\} \]

\[ L = \{\omega_1, \omega_2, \ldots, \omega_m\} \]

\[ C_l = \text{Enc}_K(w_l) = \text{Enc}_k(\omega, \text{ctr}) \]

\[ C = \{C_1, C_2, \ldots, C_n\} \]
Delegated Word Search - PRISM

- File Upload
- File processing at the cloud
  - Maps each ciphertext $C_i$ to position $(i, j)$ in $(t, t)$ matrix
    \[ H(C_i) = i || j \]
  - Fills $q$ binary matrices $M_p$
    \[ H'(C_i) = b_1 || \ldots || b_p || \ldots || b_q \]
    if $b_p = 1
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

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

\[ \text{PIRQuery } (i) = \bar{u} \]

Cloud

\[ \bar{u} = (u_1, u_2, \ldots, u_t) \]

\[ \bar{v}_p = \text{PIRResponse}(M_p, \bar{u}) = M_p^*\bar{u} \]

\[ \bar{v}_1, \bar{v}_2, \ldots, \bar{v}_q \]
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**
  - $H(Enc(w, 1)) = i || j$
  - $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_q \rightarrow \vec{v}_p = (v_{p,1}, v_{p,2}, \ldots, v_{p,j}, \ldots, v_{p,t})$
  - $h = b_1 || b_2 || \ldots || b_q \leftarrow \ldots \leftarrow b_p$

  - If $H'(Enc(w, 1)) \& h = H'(Enc(w, 1))$ output 1
Delegated Word Search - Solution

- **Upload File**

  \[ F = \{w_1, w_2, \ldots, w_n\} \]

  \[ L = \{\omega_1, \omega_2, \ldots, \omega_m\} \]

  \[ C_i = Enc_K(w_i) = Enc(\omega, \text{ctr}) \]

- **Delegate**

  \[ C = \{C_1, C_2, \ldots, C_n\}, \text{AP} \]

  \[ K \]

  \[ \text{Authorized user} \]
Delegated Word Search

- **Search**

  Authorized user

  \[ H(\text{Enc}_K(w, 1)) = i \parallel j \]

  \[(i', j') = \text{Perm}(K', i, j) \]

  \[ \bar{u} = \text{PIRQuery}(i') \]

  Cloud

  \[ C' = \text{Enc}_{\text{ABE}}(\text{AP}, K') \]

  \[ K' \leftarrow \mathbf{F}_I \]

  \[ C' = \text{Enc}_{\text{ABE}}(\text{AP}, K') \]

  \[ \bar{u} = (u_1, u_2, \ldots, u_t) \]

- **PRISM verification**

  \[ \bar{v}_p = M'_p * \bar{u} \]

  \[ \bar{v}_1, \bar{v}_2, \ldots, \bar{v}_q \]
Delegated Word Search - Solution

- Solution vulnerable to dictionary attacks
- Alternative

Authorized user

\[ H(\text{Enc}_K(w, 1)) = i \parallel j \]

\[ \tilde{u} = \text{PIRQuery}(i) \]

1. Decrypt \( C' \)
2. Decrypt relevant component of \( \tilde{v}_p \)
3. PRISM verification

Cloud

\[ \tilde{u} = (u_1, u_2, \ldots, u_t) \]

1. \( K' \leftarrow F_1 \)
2. \( \tilde{v}_p = \text{Enc}_{K'}(M_p \ast \tilde{u}) \)
3. \( C' = \text{Enc}_{\text{ABE}}(AP, K') \)
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