An Integrated Privacy Preserving Attribute Based Access Control Framework

Runhua Xu & James Joshi

University of Pittsburgh

runhua.xu@pitt.edu
Cloud Storage

Top Cloud Storage Providers
- Google Cloud
- Amazon Web Service
- Microsoft Azure…

Take MS Azure as an Example
- 2012, 4 Trillion Objects
- 2015 Jan, 10 Trillion Objects

Cloud Storage

Recent advances have enabled applications that generate/collect huge amounts of personal data.

Cloud Storage Providers

Honest-but-Curious

-- run the programs and algorithms correctly
but gather information related to the stored data and access records.

Security & Privacy Concerns: Personal Data / Sensitive Data
Initial Solution

Initial Requirement

- Data confidentiality
- Fine-grained access control for data

Ciphertext Policy Attribute Based Encryption

- Combination of encryption and access control
- Friendly for access scenario in cloud storage

Data: self-protection

Scenario

A patient-centric health application
-- that allows a patient/user to store and manage all his Electronic Health Records (EHRs) by storing them in Cloud Storage

Similar scenarios:
User-centric applications
Organization-centric applications
Hospital-centric applications

How to protect user-sensitive data in the public cloud?
Challenges

• Challenges of applying CP-ABE to the Scenarios
  • Support both revocation and privacy-preserving policy
  • Limitation of all CP-ABE schemes
    • Only support read access
    • But don’t support write access & policy update
• Access patterns leak
  • Data is protected by encryption, it doesn’t matter?
    • E.g., encrypted data in the cloud, which is often accessed from hospitals, may be identified as EHRs, then link to a specific patient.
The key contributions

- A privacy-preserving revocable CP-ABE scheme (PR-CP-ABE)
  - *Privacy-preserving Access Structure*
    - Linear Secret Sharing Scheme (LSSS)
  - *Supports immediate attribute revocation*

[ID: abc@xyz.com OR SSN: 123-45-6789) OR (Affiliation: University Hospital AND Vocation: Physician)

(ID: * OR SSN: *) OR (Affiliation: * AND Vocation: *)
The key contributions

• An extended path oblivious RAM (ePath-ORAM) protocol
  • Prevents privacy disclosure of access patterns
  • Supports data/policy update

• Security proof of the PR-CP-ABE scheme
Preliminaries: What’s CP-ABE

Slide from ESORICS
CP-ABE in detail

PK

PK_{CS}, PK_{EE}, ...
PK_{PhD}, PK_{ALU}, ...
PK_{M}, PK_{F}, ...
PK_{1980}, PK_{1981}, ...
...

Storage Server (Untrusted)

\[ C = Enc(PK, P, M) \]

\[ P = CS AND (PhD OR ALU) \]

\[ S_A \text{ satisfies } P \]

\[ S_B \text{ does not satisfy } P \]

Dept.: CS, EE, ...
Type: PhD Stud., Alumni, ...
Gender: Male, Female
Birth Year: 1980, 1981, ...

M:

\[ M = DEF(\#) \]

\[ S_A = \{CS, PhD\} \]

\[ S_B = \{EE, PhD\} \]
Overview of Access Control Framework

Key Encapsulation Mechanism (KEM) setting

Confidentiality
Primary Access Control
Privacy-preserving AS

Advanced Access Control
Preserve Access Pattern

PR-CP-ABE
Symmetric Encryption
Data Model
ePath ORAM
Data Model

Encrypted data under KEM setting

Used to verify a user’s write permission
By checking decryption ability on a random seed

Three access structure (hide value)
Instance of PR-CP-ABE

- **Master Security Key**
- **Authority (Trust third-party)**
  - Setup
  - KeyGen
- **Cloud Storage**
  - Re-Encrypt
  - SK2
- **Encrypt**
- **Decrypt**
ePath ORAM Protocols

Connection Established

\[ D = \text{Path-ORAM}(\text{read, id, NULL}) \]

\[ P_r, Enc_{k_{\delta}}(data) \]

Connection Established

\[ id, write \]

\[ <A_w, \rho_w>, Enc_{\gamma}(s_w) \]

\[ s'_w \]

\[ s_w \] \(==\) \(s'_w\)?

\[ P_r, Enc_{k_{\delta}}(data), s''_w \in \mathbb{R} \mathbb{Z} \]

\[ Enc_{\gamma}(k'_\delta), Enc_{k_{\delta}}(data'), Enc_{\gamma}(s''_w), s''_w \]

Path-ORAM(write, id, \(D'\))

Time

ePath-ORAM-Read Protocols

ePath-ORAM-Write Protocols
Analysis

• Tricks behind PR-CP-ABE construction
  • *Composite Order Bilinear Groups*
    • Introduce random elements from a subgroup into algorithms to perturb/hide ciphertext components $\leftrightarrow$ attributes
    • Use the property to eliminate random elements

\[
\begin{align*}
  h_r &\in \mathbb{G}_r \\
  h_p &\in \mathbb{G}_p \\
  e(h_r, h_p) &\equiv 1
\end{align*}
\]

• *Re-encrypt technology*
  • Divide the initial secret element $\alpha = \alpha_1 + \alpha_2$
  • One is corresponding to user, the other is for delegation (CSP)
Analysis

• Forward Security
  • *Protects past ciphertext against future compromises of secret keys.*
  • *If attribute is revoked*
    • Users can not update the corresponding private key
    • Thus they can not decrypt again

• Backward Security
  • *A new user joins in an attribute group that satisfies the policy*
  • *Suppose he has a previous ciphertext*
  • *Even if he can update private key, he can not decrypt it*
    • Random elements in previous component D’ ← X → new user’s private key
Analysis

• Key features

<table>
<thead>
<tr>
<th>Schemes</th>
<th>Access Structure (AS)</th>
<th>Immediate Revocation</th>
<th>Privacy-preserving AS</th>
</tr>
</thead>
<tbody>
<tr>
<td>[39]</td>
<td>LSSS Matrix</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>[38]</td>
<td>And-gate</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>[15]</td>
<td>Tree-based</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>[20]</td>
<td>LSSS Matrix</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>[23]</td>
<td>And-gate</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Ours</td>
<td>LSSS Matrix</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Analysis

- Performance
  - As shown in previous experiments.
    - Encryption/decryption → milliseconds level
    - Key Application (network communication) → seconds level

Our scheme makes a compromise on performance for privacy-preserving policy, compared with [39].
However, our scheme’s performance is better than others.
Security Proof

• Methodology
  • Suppose that adversary has advantage to break our scheme
  • Adversary’s advantage $\leftrightarrow$ break q-parallel BDHE assumption
  • However, no-polynomial time algorithm has advantage to break assumption
  • Thus no adversary has advantage to break our scheme

Please find the detail proof in Appendix.
Conclusion

• A novel privacy-preserving attribute-based access control framework
  • *PR-CP-ABE*
    • Privacy-preserving
    • Revocation
    • Security Proof: CPA
  • *ePath-ORAM Protocol*
    • Preserve access pattern
    • Extend PR-CP-ABE to support r/w/o access
• *Features*
  • User-centric data and policy management
  • Immediate privilege revocation
  • Privacy protection
Q & A

Thanks