Cyber Summer School
Melbourne, 12-13 Feb 2018

Secure Data Sharing in Cloud Computing: Challenges and Research Directions

Willy Susilo

Institute of Cybersecurity and Cryptology
School of Computing and Information Technology
University of Wollongong

Email: wsusilo@uow.edu.au

12 February 2018

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Outline

1 **Background**

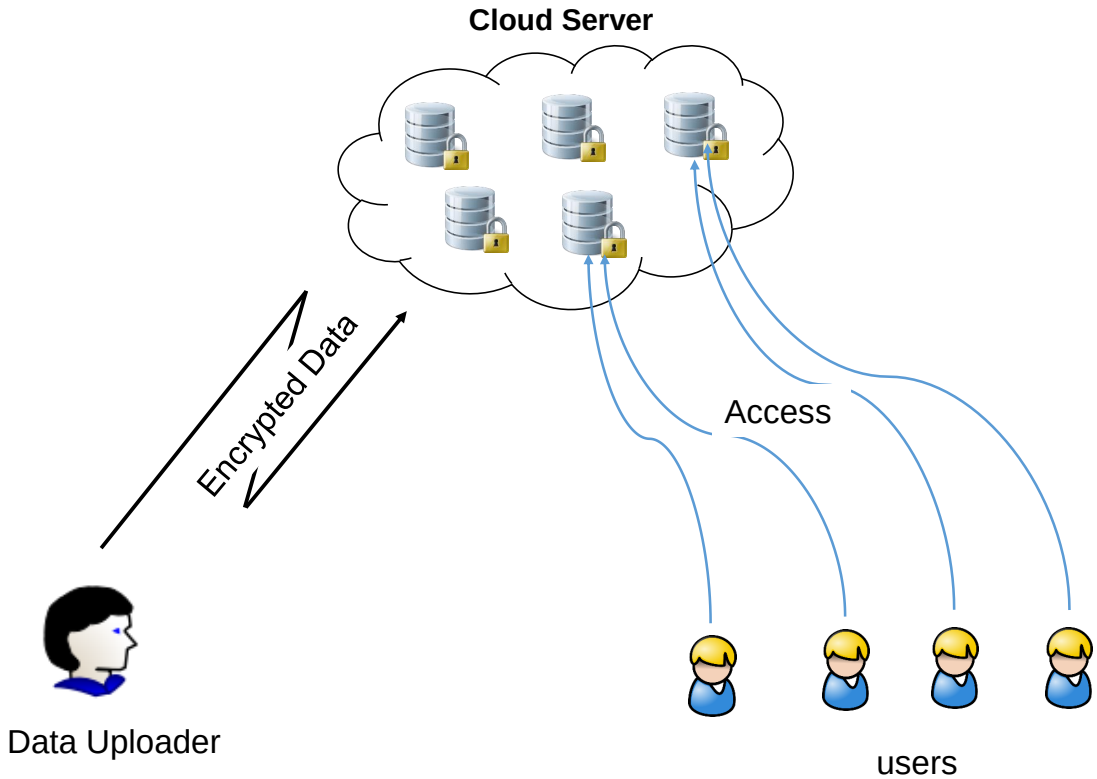
2 Generic Approaches

3 Challenges and Research Directions

4 Our Recent Research Results

5 Conclusion

Data Sharing in Cloud Computing



Challenges:

- How to encrypt data?
- How to decrypt data?

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Outline

Data Sharing via IBE

Identity-Based Encryption(IBE)[BF01]

In the IBE, a data M is encrypted under a specified identity ID such that only the user with matching identity can decrypt the ciphertext.

$$CT = E(mpk, ID, M)$$

If a data owner wants to share a data with a user via IBE, it just encrypts the shared data using the user's identity.

[BF01] Dan Boneh, Matthew K. Franklin: Identity-Based Encryption from the Weil Pairing. CRYPTO 2001: 213-229.

Data Sharing via IBBE

Identity-Based Broadcast Encryption(IBBE)[D07]

In the IBBE, a data M is encrypted under a set of specified identities S such that only the user with identity selected in the data encryption can retrieve the data.

$$CT = E(mpk, S, M)$$

IBBE can be used to share one common data with a group of users efficiently.

[D07] Cécile Delerablée: Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys. ASIACRYPT 2007: 200-215.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Data Sharing via ABE

Attribute-Based Encryption(ABE)[SW05]

- Variant: KP-ABE & CP-ABE

	Data Encryption	Decryption key
KP-ABE	An attribute set	An access policy
CP-ABE	An access policy	An attribute set

- If and only if the attribute set held by a user satisfies the access policy can retrieve the plaintext.
- Without knowing the receivers' identities when performing the data encryption.

[SW05] Amit Sahai, Brent Waters: Fuzzy Identity-Based Encryption. EUROCRYPT 2005: 457-473.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Outline

1 Background

2 Generic Approaches

3 Challenges and Research Directions

4 Our Recent Research Results

5 Conclusion

Challenges and Research Directions

In the IBE,

- One data can only be shared with one user for each encryption.
- The receiver identity must be known when performing data encryption.
- If the receiver privacy is required, how can the user efficiently find the encrypted data which it can decrypt on the cloud?
- ...

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Challenges and Research Directions

In the IBBE,

- All receivers' identities must be known before encrypting the data.
- Once the receivers have been decided and used in the data encryption, how to revoke some of receivers if they are comprised without decryption?
- If the user privacy is required, how can the user efficiently find the encrypted data which it can decrypt on the cloud?
- Achieve collusion resistant when doing user revocation.
- ...

Challenges and Research Directions

In the ABE, the access policy is *fixed*, which might be not suitable for some real life applications.

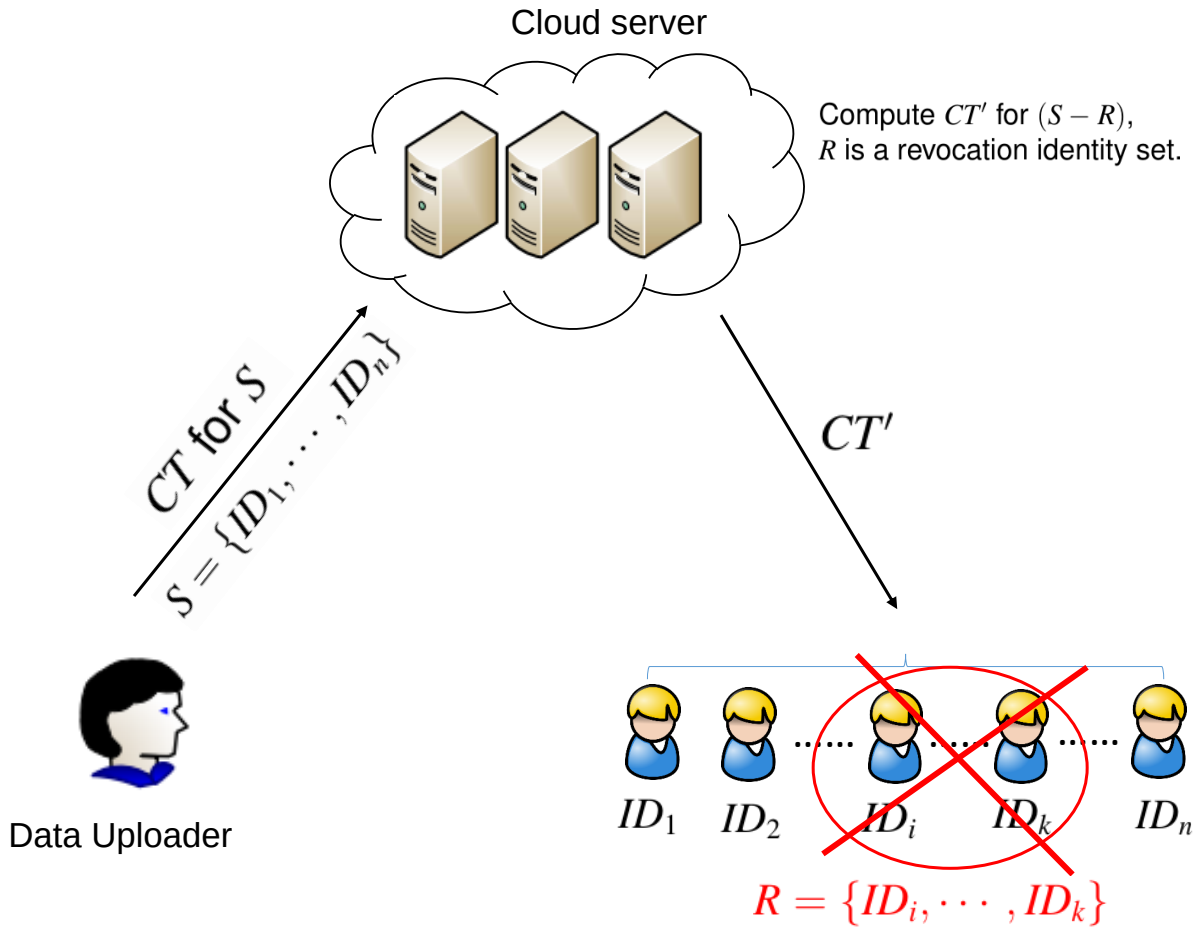
- Achieve scalable access policy.
- Access policy extension
- Access policy update
- Access policy revocation
- Access policy hidden
- Computational efficiency
- Storage or data transmission efficiency
- ...

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Outline

Recipient Revocable Identity-Based Broadcast Encryption

Motivation of RR-IBBE



UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Our RR-IBBE work:

- An extension of IBBE.
- Allow a third party to remove some of receivers stated in the ciphertext without leaking the encrypted data or performing any decryption.
- Constant-size secret key and ciphertext.

Improved Threshold Attribute-Based Encryption

In a (t, n) threshold ABE, users who can decrypt the ciphertext must hold at least t attributes among the n attributes specified in the encryption.

The work of [HLR10] presents the first threshold ABE with constant-size ciphertext.

Limitations of [HLR10]:

- Require to add dummy attributes.
- The computational cost of encryption is linear in the size of selected attribute set and dummy attribute set.

[HLR10] Javier Herranz, Fabien Laguillaumie, Carla Rfols: Constant Size Ciphertexts in Threshold Attribute-Based Encryption. Public Key Cryptography 2010: 19-34

Our work

Propose a new constant-size ciphertext threshold ABE scheme.

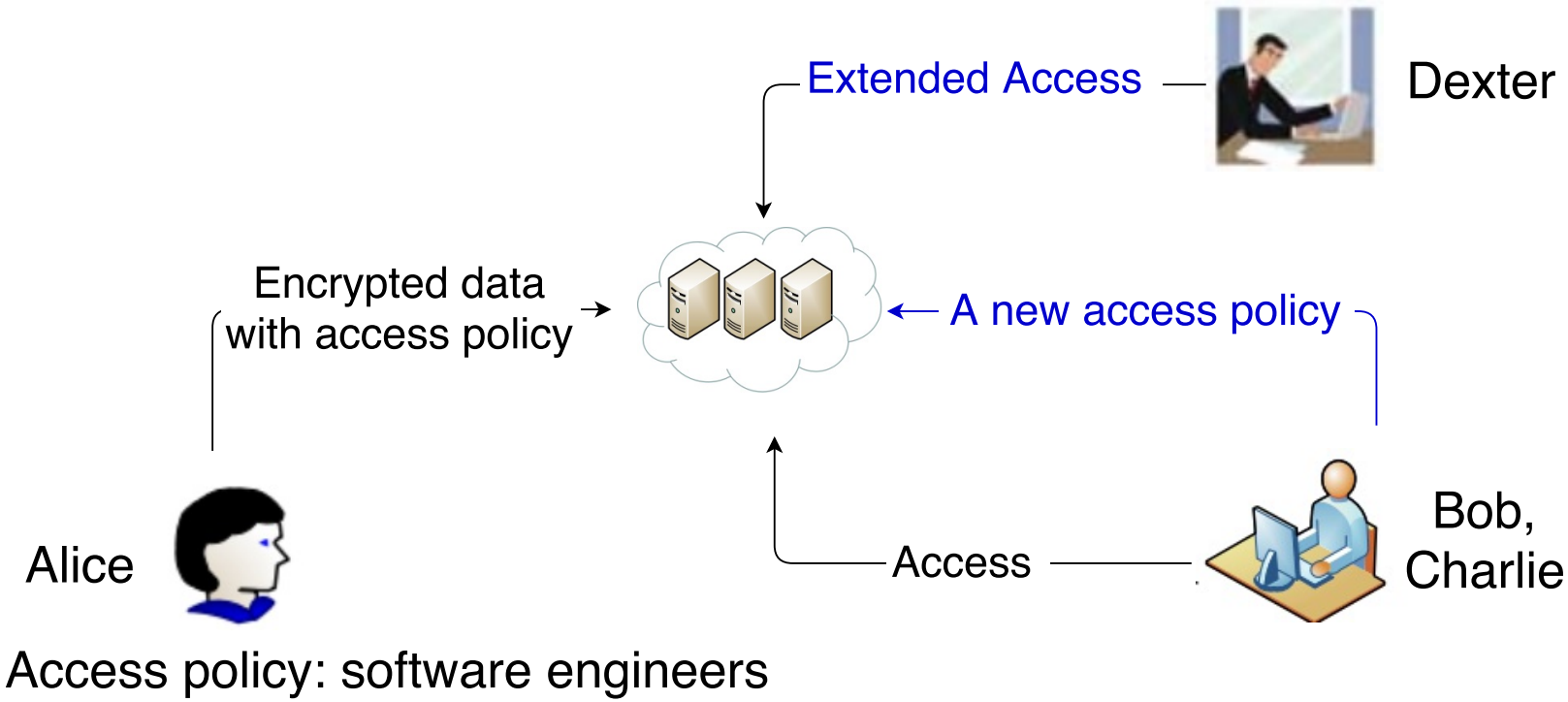
Improvements:

1. Without using any dummy attribute.
2. The computation cost of encryption and decryption is linear in the number of the selected attribute set.
3. Most of the computations can be conducted without the knowledge of the threshold t.
4. The encryptor can change the threshold t without re-computing the overall ciphertext.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Extendable Access Control System with Integrity Protection

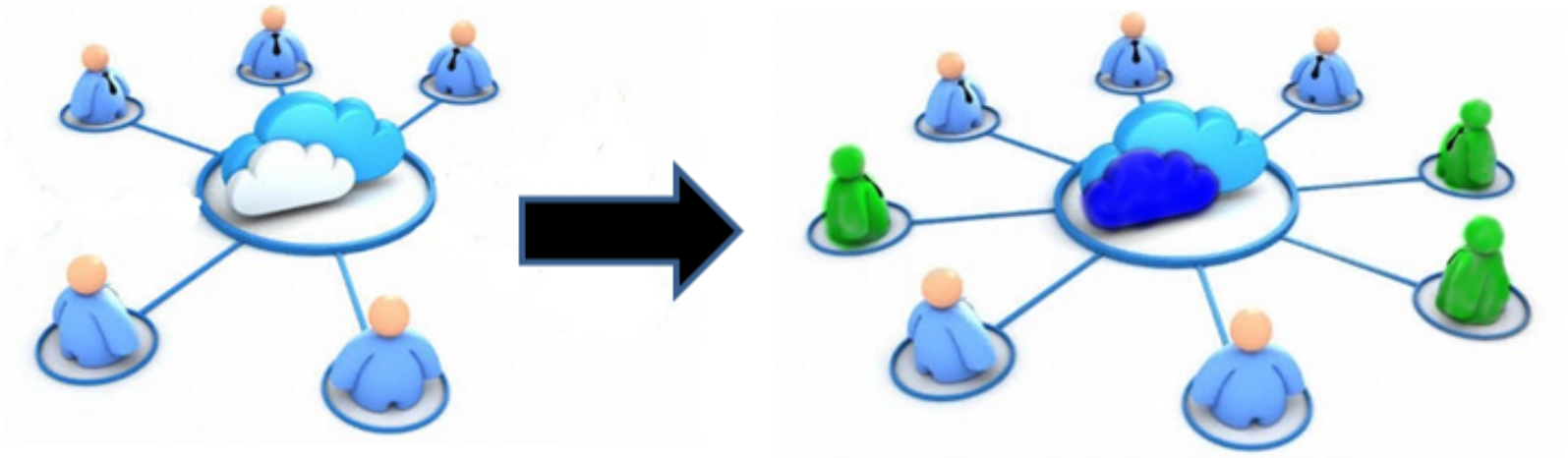
Motivation



How to *EXTEND* the access policy?

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Motivation



- Data on the left is protected with access policy $\mathcal{P}_1$.
- Data on the right is protected with access policy $\mathcal{P}_2 \cup \mathcal{P}_1$.
- Decrypt the ciphertext if satisfying either policy $\mathcal{P}_2$ or $\mathcal{P}_1$.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Trivial Solution

Solution 1

Alice re-uploads the encrypted plaintext with the original access policy and the added access policy.

The extension cannot be done if Alice is out of contact.

Solution 2

Bob downloads the ciphertext, decrypts it, and then re-uploads it with the added policy.

No integrity guarantee between the Alice's plaintext and Bob's plaintext.

Our Solution: EACSIP

We introduce an Extendable Access Control System with Integrity Protection

- Data uploader uploads data under $\mathcal{P}_1$.
  Recipients satisfying the policy $\mathcal{P}_1$ can access the data.
- Any valid recipient can add a new access policy $\mathcal{P}_2$.
  Recipients who satisfy $\mathcal{P}_2$ or $\mathcal{P}_1$ can access the data.
- The cloud server cannot decrypt the ciphertext.
  It checks *integrity* : any recipient who satisfies $\mathcal{P}_2$ can access the same data created by the data uploader.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Public Key Encryption with Equality Test

- Two ciphertexts with different public keys correspond to the same message.
- Dishonest encryptors: even if two ciphertexts pass the equality test, the decrypted messages could be still different.

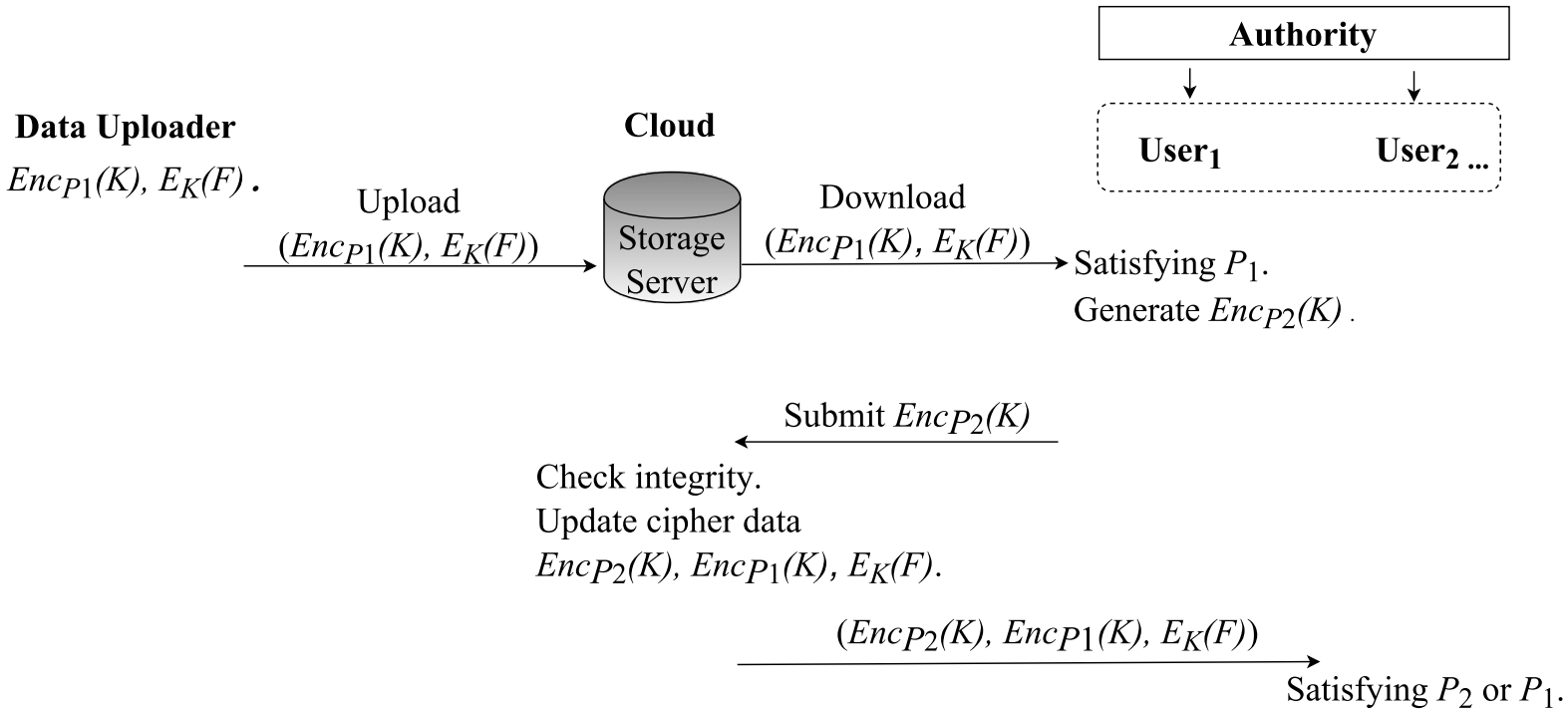
PKEET cannot guarantee the identical decryption result!

Core Technique of EACSIP

Functional Key Encapsulation with Equality Test

- The plaintext is encrypted with a symmetric key.
- The symmetric key is protected with an access policy.
- The original policy and the extended policy correspond to the same key $\rightarrow$ the same decryption result.

EACSIP Architecture



UNIVERSITY OF WOLLONGONG AUSTRALIA

This talk is based on the following works:

- **Willy Susilo**, Peng Jiang, Fuchun Guo, Guomin Yang, Yong Yu, Yi Mu: EACSIP: Extendable Access Control System with Integrity Protection for Enhancing Collaboration in the Cloud. *IEEE Trans. Information Forensics and Security* 12(12): 3110-3122 (2017).
- **Willy Susilo**, Guomin Yang, Fuchun Guo and Qiong Huang. Constant-Size Ciphertexts in Threshold Attribute-Based Encryption without Dummy Attributes. *Information Sciences*. Online 20 November 2017.
- **Willy Susilo**, Rongmao Chen, Fuchun Guo, Guomin Yang, Yi Mu, Yang-Wai Chow: Recipient Revocable Identity-Based Broadcast Encryption: How to Revoke Some Recipients in IBBE without Knowledge of the Plaintext. *AsiaCCS 2016*: 201-210.

Outline

1 Background

2 Generic Approaches

3 Challenges and Research Directions

4 Our Recent Research Results

5 Conclusion

Conclusion

- Present generic approaches for cloud data sharing.
- Show challenges and research directions of data sharing in cloud computing.
- Introduce our recent research results.
  - Recipient revocable IBBE scheme (allow to revoke some of receivers stated in the IBBE ciphertext).
  - Constant-size threshold ABE scheme with using the dummy attributes (improve efficiency).
  - Extendable access control system with integrity protection(the access policy can be extended such that more users are allowed to access the same data).

Thanks & Questions