Cyber Summer School
Adelaide, 21-22 March 2019

Securing Cloud Storage: Challenge and Research Directions

Willy Susilo

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

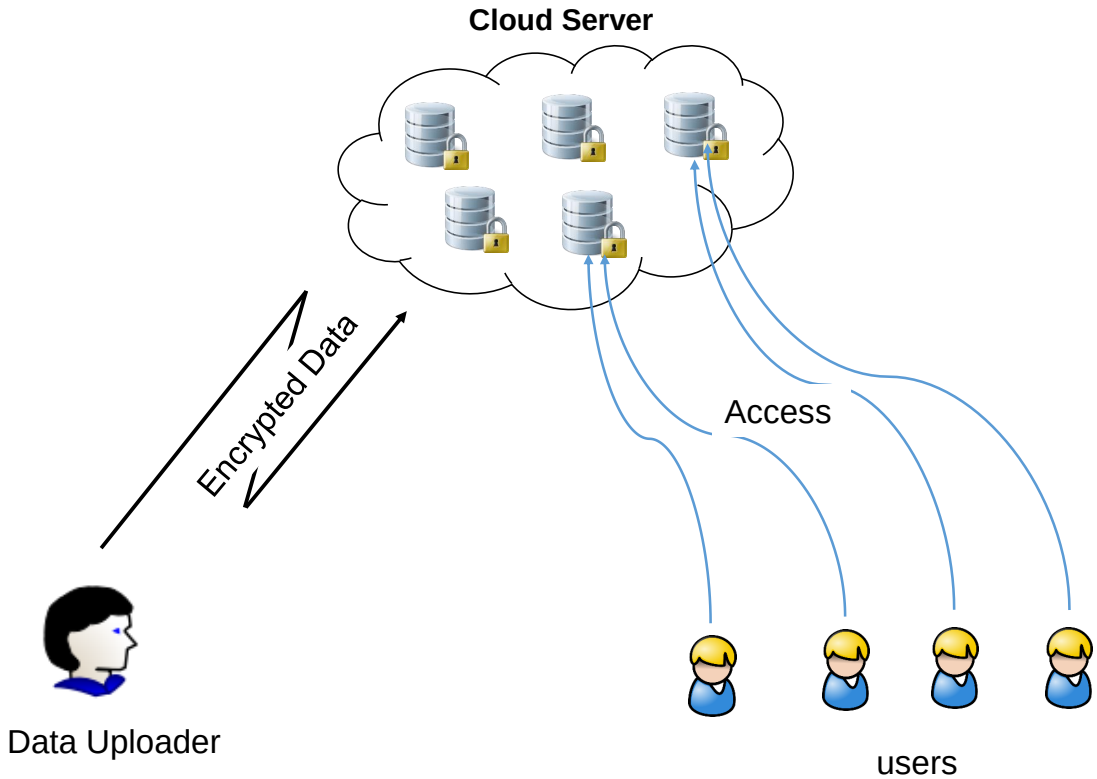
Email: wsusilo@uow.edu.au

22 March 2019

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Outline

Data Sharing in Cloud Computing



Challenges:

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

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.

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.

Outline

1 Background

2 Generic Approaches

3 Research Challenges and Future Directions

4 Conclusion

Issues and Challenges

Theory vs. Practice

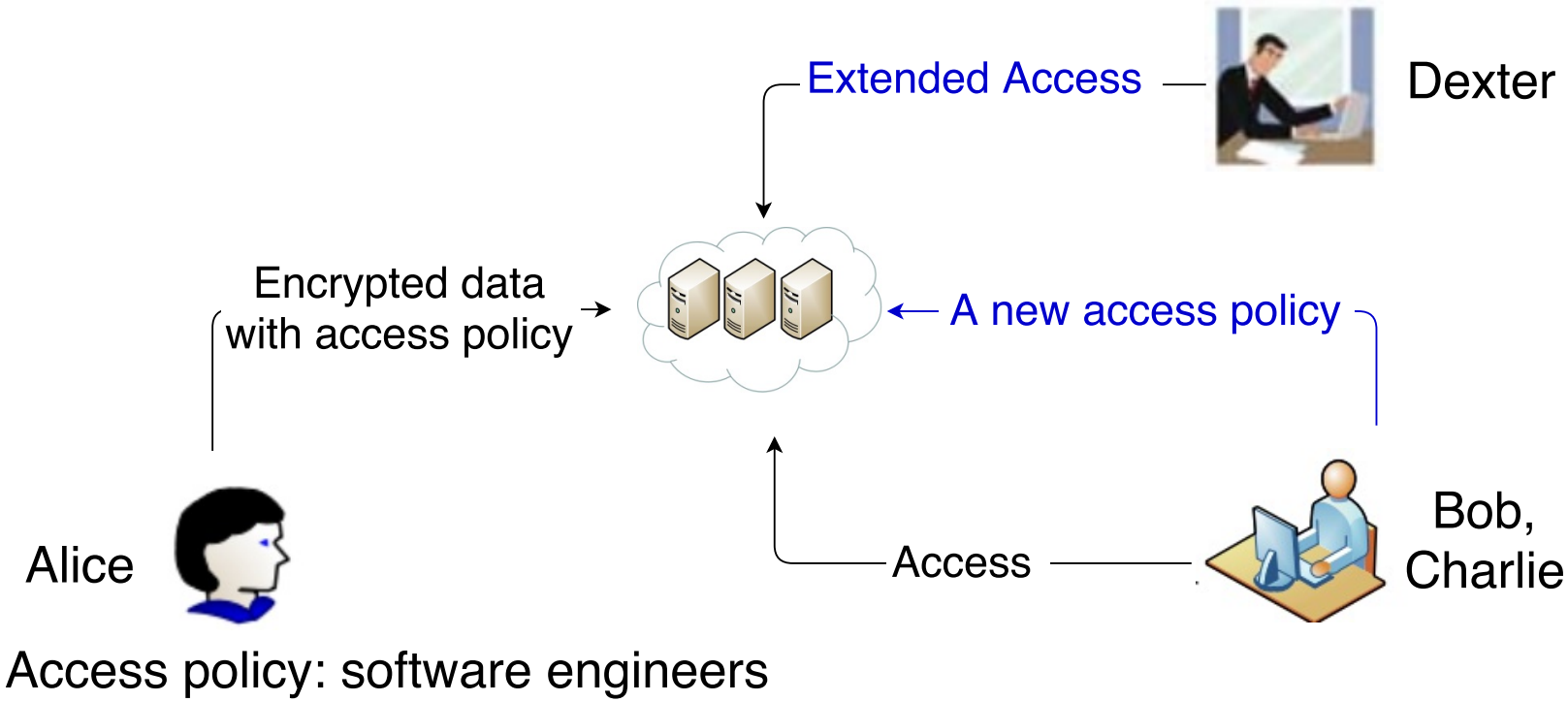
Challenges and Research Directions

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
- ...

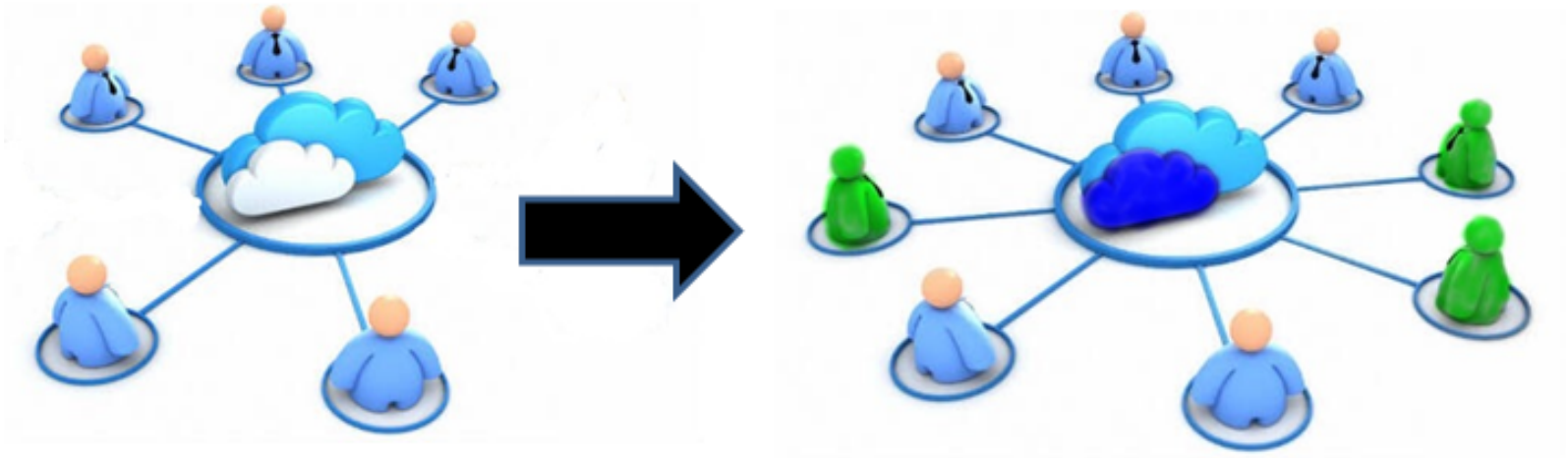
Extendable Access Control System with Integrity Protection

Motivation



How to *EXTEND* the access policy?

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 $\mathcal{P}_1$.

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.

EACSIP Framework

We introduce an Extendable Access Control System with Integrity Protection

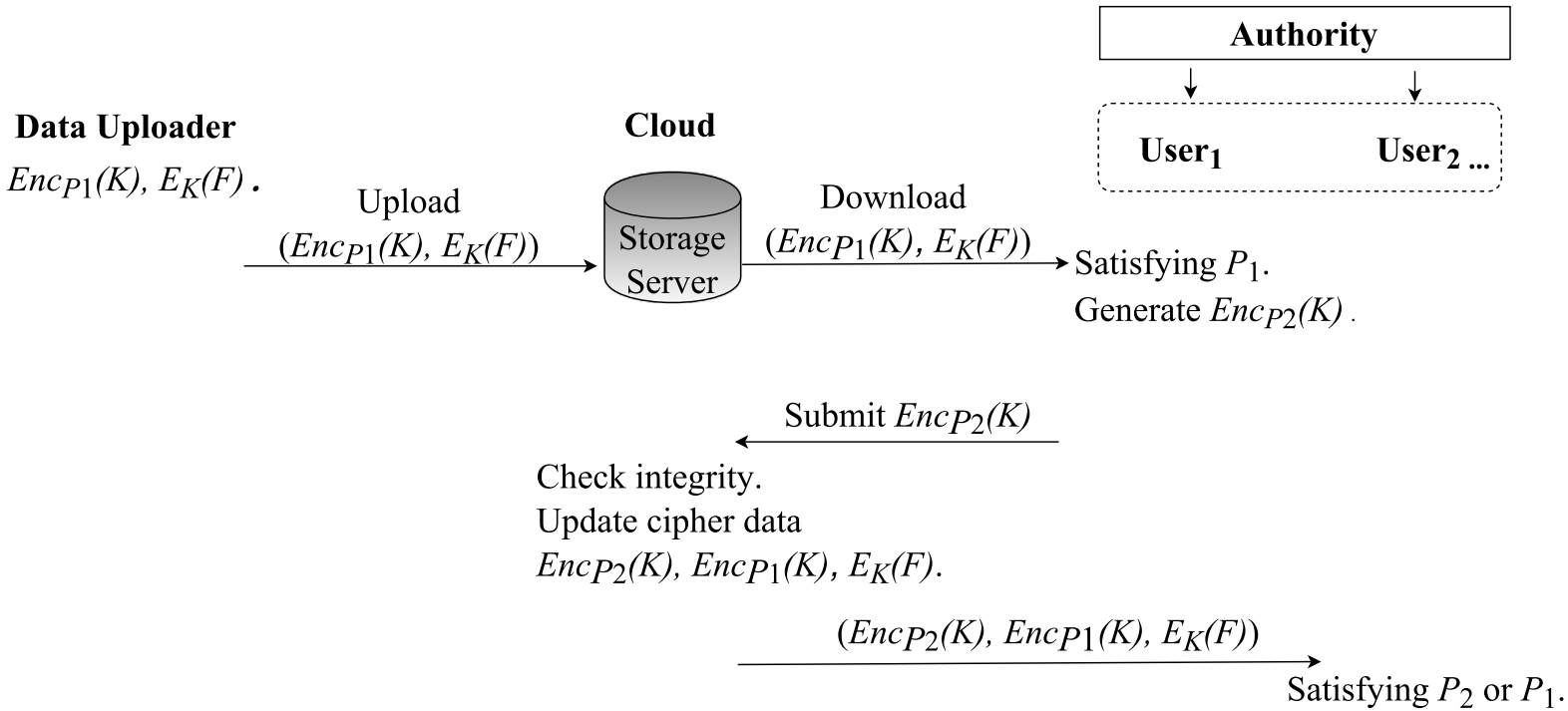
- Data uploader uploads data under $\mathcal{P}_1$.
  Recipients satisfying the policy $\mathcal{P}_1$ can access the data.
- Any valid recipient can add a new access policy $\mathcal{P}_2$.
  Recipients who satisfy $\mathcal{P}_2$ or $\mathcal{P}_1$ can access the data.
- The cloud server cannot decrypt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

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



Complete framework can be found in:

- **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).

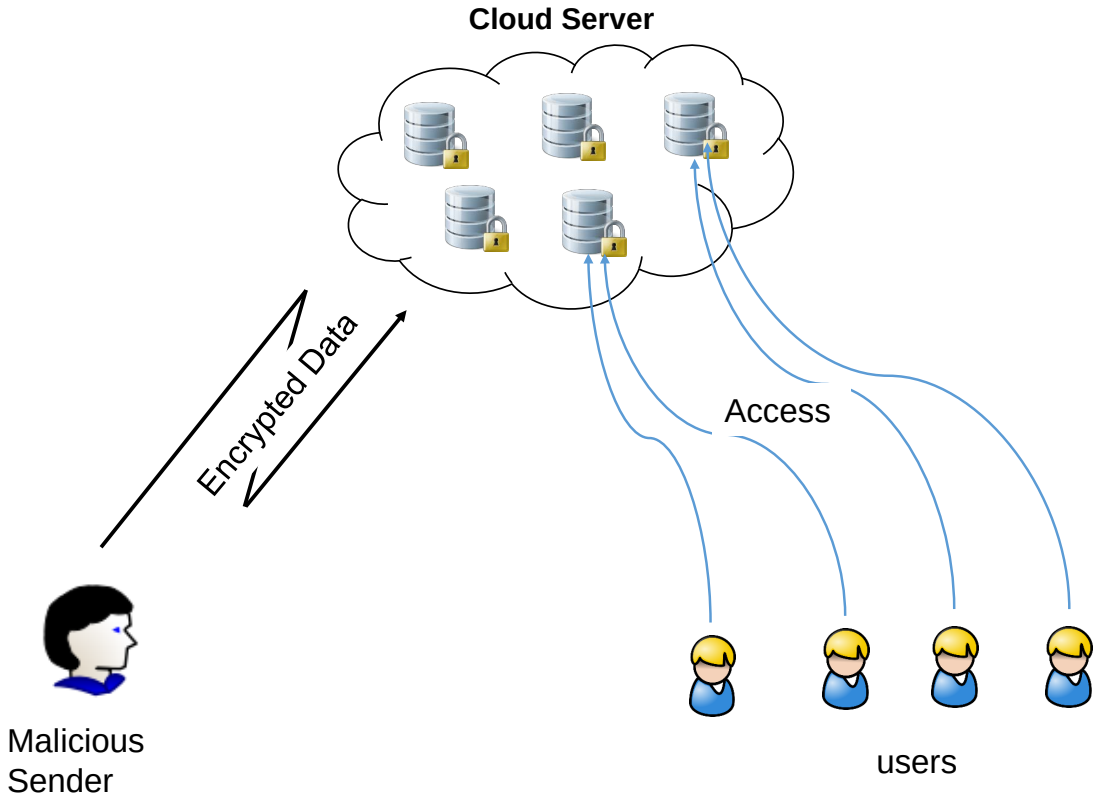
Future direction:

- Post-quantum secure EACSIP.
- Functional Key Encapsulation with Equality Test in Post-quantum setting.

New Other Research Challenges:

- Involvement of Malicious Senders.
- Subversion.
- Searchable Encryption.

Malicious Senders



What can a malicious sender do?

Disadvantages of having malicious senders

- Filling cloud storage with useless data.
- Damaging Cloud's Reputation.
- Subversion.

The issue is due to the "honest-but-curious" model assumption of the cloud. If the cloud is trusted, then there is no issue.

Outline

1 Background

2 Generic Approaches

3 Research Challenges and Future Directions

4 Conclusion

Conclusion

- Cloud Data Sharing: Theory vs. Practice
- Challenges and research directions of data sharing in cloud computing.

Thanks & Questions