Secured Access Control System on Cloud Disk Based on Cryptography

PROJECT PLAN

Student	:	Chow Chi Ling (3035072832)
Supervisor	:	Dr. Lucas Hui
Course	:	COMP4801 Final Year Project
Project Code	:	FYP16007
Date	:	October 2, 2016

CONTENTS

1 Background 2
1.1 Current Situation 2
1.2 Theoretical Background 2
1.2.1 Types of Attribute Based Encryption 2
1.2.2 Implementation 3
2 Objective 3
3 Methodology 4
3.1 openEHR Framework 4
3.2 Libfenc Library 4
4 Schedule 4
5 Bibliography 5

1 BACKGROUND

1.1 CURRENT SITUATION

Usage of cloud computing has been growing rapidly recently. Statistics have shown that there is a steady increase in adoption of cloud solutions for enterprises, from 57% respondents in 2012 to 72% of respondents in 2015. Despite the rising popularity, security remains one of the top challenges, such as tackling unauthorized access and data protection issues. [2]

In the enterprise situation, files and data are usually encrypted and are shared and accessible by certain groups of staffs only. This could be securely encrypted by conventional cryptography, such as the public key infrastructure. However, this could require much computation power. If there are a large number of staffs sharing the same piece of information, the number of encryption computation could be very huge. As cloud is also often used together with mobile devices, with limited processing power and storage space in mobile devices, cryptographic protection is even more challenging.

Under this situation, attribute based encryption (ABE), a relatively younger cryptography, could possibly be a better alternative. Encryption and decryption are calculated based on attributes of individuals and a specified access control policy. Therefore, people with different secret keys would be able to decrypt the same ciphertext if the supplied attributes match the specified access control policy. This could allow more flexibility in information sharing while protecting from unauthorized access. Moreover, more recent researches have proposed outsourcing ABE which breaks the decryption process into stages, thereby reducing the computation power requirements.

1.2 THEORETICAL BACKGROUND

1.2.1 Types of Attribute Based Encryption

Attribute based encryption (ABE) was introduced by Sahai and Waters in 2005. The two major components in ABE are attributes and access control policy. Attribute is the characteristic of a piece of information or a user. A piece of information or a user may be identified by a set of attributes. On the other hand, access control policy is the specification of the set of attributes that users must satisfy in order to decrypt the ciphertext. It is organized in tree based data structure. [1]

ABE can be classified into two types, namely ciphertext-policy attribute based encryption (CP-ABE) and key-policy attribute based encryption (KP-ABE).

In CP-ABE, each user is associated with a set of attributes and is represented in their secret key. During the encryption, ciphertext is associated with the access control policy specified by the sender. All users possessing a secret key with attributes satisfying the access control policy specified in the ciphertext would be able to decrypt and get the message.

On the contrary, in KP-ABE, user's secret key is associated with the access control policy while the ciphertext is associated with a set of attributes specified by the sender. Users would be able to decrypt a ciphertext if the ciphertext contains attributes that satisfy the access control policy specified in his secret key.

1.2.2 Implementation

Since 2005, there are various related works in ABE. Implementation methods are slightly different, but they comprise of the four basic steps described below. [3],[4],[5]

1. Setup

Public key and the master secret key are generated.

2. Key Generation

In CP-ABE, individual secret key is generated from a set of attributes.

In KP-ABE, individual secret key is generated from an access control policy.

3. Encryption

In CP-ABE, message is encrypted by the sender from the public key and an access control policy to give the ciphertext.

In KP-ABE, message is encrypted by the sender from the public key and a set of attributes to give the ciphertext.

4. Decryption

Ciphertext is decrypted by the user who possesses a valid secret key.

2 OBJECTIVE

The project would focus on the implementation of ciphertext-policy attribute based encryption (CP-ABE) in the context of electronic health record system. The project aims at achieving the following objectives:

1. To protect electronic health records by CP-ABE
2. To support operations on mobile devices
3. To develop convenient management of access control policy and attributes for CP-ABE

3 METHODOLOGY

The project would make use of the following development tools.

3.1 OPENEHR FRAMEWORK

The openEHR Framework is an international open standard governing systems related to electronic health records. The standard is developed and continuously maintained by a large group of professionals. Many organizations, including commercial and research projects, are conforming to the standard and hence it is internationally accepted.

3.2 LIBFENC LIBRARY

Libfenc is an open source library with implementation of several functional encryption including both CP-ABE and KP-ABE. A few versions of ABE schemes were implemented in the library.

4 SCHEDULE

Date	Milestones	Deliverables
2 October 2016	Completion of Phase 1	Detailed Project Plan Project Web Page
9-13 January 2017	First Presentation	
22 January 2017	Completion of Phase 2	Preliminary Implementation Detailed Interim Report
16 April 2017	Completion of Phase 3	Finalized Tested Implementation Final Report
18-21 April 2017	Final Presentation	

5 BIBLIOGRAPHY

[1] "Introduction to Attribute Based Encryption (ABE)," [Online]. Available: http://gleamly.com/article/introduction-attribute-based-encryption-abe.

[2] IDG Enterprise Marketing, "Clound Computing Survey 2015," 17 11 2015. [Online]. Available: http://www.idgenterprise.com/resource/research/2015-cloud-computing-study/.

[3] S. Banescu, H. Ideler and S. Posea, "Personal Health Record System Protected using CP-ABE".

[4] J. Li, X. Huang, J. Li, X. Chen, Y. Xiang and IEEE, "Securely Outsourcing Attribute-Based Encryption with Checkability," *IEEE Transactions on Parallel and Distributed Systems,* vol. 25, no. 8, pp. 2201-2210, 2014.

[5] F. Xhafa, J. Li, G. Zhao, J. Li, X. Chen and D. S. Wong, "Designing Cloud-Based Electronic Health Record System with Attribute-Based Encryption," Springer Science+Business Media New York, New York, 2014.