Large data transaction market system design using proxy re-encryption technology based on elliptic curve cryptography

Won-Bin Kim
LSware Inc.
Republic of Korea
wbkim29@lsware.com

Seung-Chan Back
LSware Inc.
Republic of Korea
davidback@lsware.com

YongJoon Joe
LSware Inc.
Republic of Korea
eugene@lsware.com

Dong-Myung Shin
LSware Inc.
Republic of Korea
roland@lsware.com

ABSTRACT

Proxy re-encryption technology has been proposed to share data securely and efficiently. The proxy re-encryption technology has the advantage that the original content of the data or the sender's secret information is not exposed during the data sharing process. Thus, data can be shared securely and accurately even in untrusted environments. In this study, the market system for transacting large amounts of data was designed as proxy re-encryption, and the operation of proxy re-encryption was configured with elliptic curve encryption to increase the efficiency of the operation.

KEYWORDS

Data Market, Large Data, Elliptic Curve Cryptography, Proxy Re-encryption

1 INTRODUCTION

Data sharing technology uses a method that provides the right to decrypt the encrypted data after encrypting the data. Therefore, symmetric key encryption and asymmetric key encryption, which are representative encryption methods, are used respectively or mixed. However, these methods have a problem in that the original content of the data is exposed or the private key/private key is exposed during the data transmission process. Therefore, various research groups have been carried out to solve these problems.

Proxy re-encryption technology is a technology that can safely transmit data decryption rights to a third party without exposing data and encryption keys. In general, when the authority to decrypt encrypted data is provided to a third party through an agent, the agent decrypts the encrypted data and then performs the encryption process for the designated recipient. However, this method is difficult to achieve unless the agent is completely trusted because the agent can know the contents of the data source. Such proxy re-encryption technology is generally designed based on public key encryption technology and has an encryption-re-encryption-decryption process. Therefore, since decryption is not performed in the agent's processing stage, the agent cannot know the contents of the data source.

In this study, we design proxy re-encryption technology using elliptic curve encryption technology and design a market system that can trade large amounts of data based on proxy re-encryption technology.

2 RELATED WORK

2.1 Data Sharing based on Encryption

To securely share data, data encryption is required. However, a separate method is required to delegate authority so that the receiver can decrypt the data encrypted by the sender. In general, symmetric key encryption and asymmetric key encryption are used individually or in combination. As shown in Figure 1, a total of four methods can be used. However, each method has the following characteristics and problems.

a. **Symmetric key encryption:** This method encrypts and shares data using only a symmetric key. This method requires relatively few operations and communication, but requires direct key transfer between the sender and the receiver. Therefore, there is a difficulty in key distribution.
b. **Asymmetric key encryption:** This method encrypts and shares data using only an asymmetric key. Therefore, the difficulty of key distribution, which is the problem of ***a. Symmetric key encryption***, can be solved. However, if the sender cannot know the receiver at the time the data is encrypted, data cannot be encrypted.
c. **Asymmetric key encryptions with proxy's asymmetric key pair:** This method uses asymmetric key encryption repeatedly to encrypt and share data. This method uses a method in which the proxy decrypts the sender's ciphertext and re-encrypts it again with the

receiver's public key. Therefore, it is possible to solve the difficulty of key distribution in ***a. Symmetric key encryption*** and ***b. Asymmetric key encryption***. However, there is a problem that the proxy can know the contents of the data source.

d. **Asymmetric key encryption with symmetric key decryption:** This method uses a combination of asymmetric key encryption and symmetric key encryption to encrypt and share data. This method also solves the difficulty of key distribution as in ***c. Asymmetric key encryptions with proxy's asymmetric key pair***. However, like ***c. Asymmetric key encryptions with proxy's asymmetric key pair***, there is a problem that the proxy can know the contents of the data source.

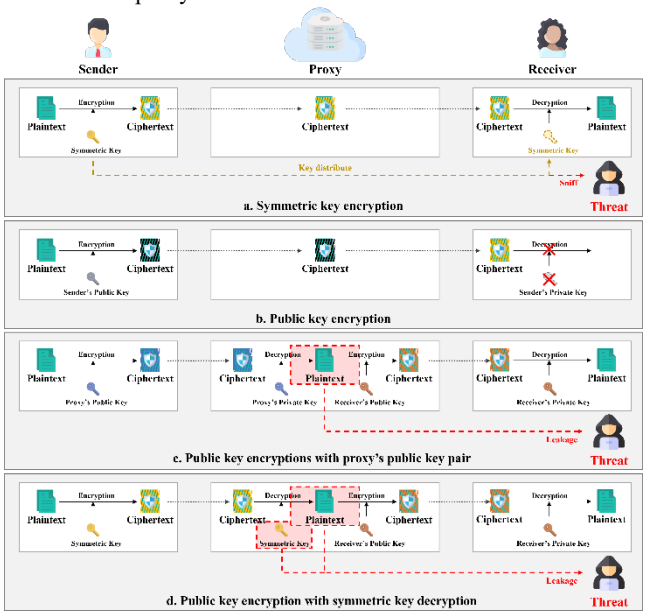

Figure 1: Problems of data sharing technique using symmetric key and asymmetric key encryption

Therefore, to solve this problem, a data sharing technology based on proxy re-encryption has emerged.

2.2 Proxy Re-encryption

In 1998, M. Blaze, G. Bleumer, and M. Strauss proposed Proxy Re-encryption (PRE), a technology that transforms data through a proxy and delivers data securely to the receiver as shown in Figure 2 [1]. This technology converts data encrypted with the sender's public key into data encrypted with the receiver's public key at the proxy. In this process, the private keys of the sender and receiver are not exposed, and the original data is not exposed because data decryption is not performed. By using proxy re-encryption, data can be safely stored in cloud storage, and data can be shared efficiently by converting it to the recipient's ciphertext at the request of the recipient. Currently, research on various sharing methods using proxy re-encryption technology is being conducted[2-4].

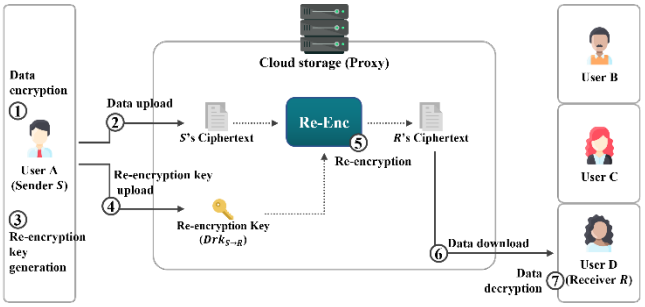

Figure 2. Basic form of proxy re-encryption

3 PROPOSED SCHEME

3.1 System Model

The system proposed in this study was designed based on proxy re-encryption, and the resulting system model is shown in Figure 3.

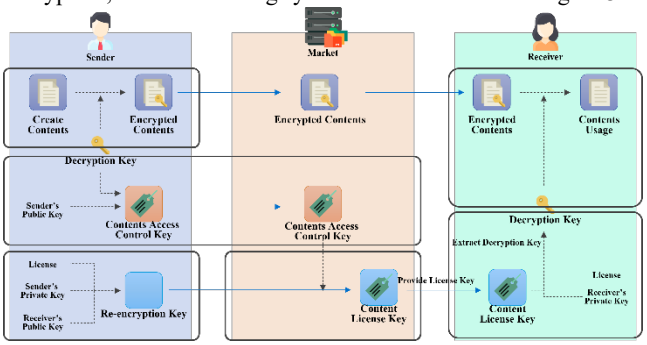

Figure 3: Proposed system model

3.2 Main Protocol

The system proposed in this study is mainly composed of five parts. *Details on this are as follows.*

3.2.1 Setup Phase. This is the phase in which the system administrator defines parameters to be commonly used within the system. In this phase, common functions, elliptic curves, parameters, etc. are determined and disclosed by the system administrator.

3.2.2 Key Generation Phase. This is the phase that performs key generation between the key generation center and the user. In this phase, a public key is generated through mutual communication between the user and the key generation center, and a private key corresponding to the public key is generated.

3.2.3 Encryption Phase. This is the phase in which the sender encrypts the data. In this phase, the user encrypts data with their public key, and then uploads the encrypted data to the market.

3.2.4 Re-encryption Phase. This is a phase in which the receiver requests data, the sender generates a re-encryption key for the receiver and delivers it to the market, and then the market re-encrypts the sender's cipher text. In this phase, the market changes the sender's cipher text to the receiver's cipher text without revealing the sender's private key and original data to the market.

3.2.5 Decryption Phase. This is the phase in which the receiver decrypts the data delegated from the sender. In this phase, the receiver can decrypt data using only his/her private key.

4 CONCLUSIONS

In this study, ECC-based proxy re-encryption technology was used to design a market for large-scale data transaction. Proxy re-encryption technology can delegate the decryption authority of encrypted data from the data owner to a third party without exposing the original data content and sensitive sensitive information. Such a technology can completely solve the problems that appear in the existing methods using symmetric key encryption and asymmetric key encryption. Therefore, even in a completely unreliable environment, it can be applied to the market for trading large amounts of data to provide safety. As a result, this study makes it possible to provide trust with security even in a trustless environment.

ACKNOWLEDGMENTS

This research is supported Year 2021 Copyright Technology R&D Program by Ministry of Culture, Sports and Tourism and Korea Creative Content Agency (Project Name : Development of content copyright protection and application technology for digital holographic printers, Project Number: 1375027291, Contribution Rate: 100%)

REFERENCES

[1] M. Blaze, G. Bleumer and M. Strauss, "Divertible protocols and atomic proxy cryptography." International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1998.

[2] Lei Xu, Xiaoxin Wu, and Xinwen Zhang. Cl-pre: a certificateless proxy re-encryption scheme for secure data sharing with public cloud. In Proceedings of the 7th ACM symposium on information, computer and communications security, pages 87–88, 2012.

[3] Xiaoxin Wu, Lei Xu, and Xinwen Zhang. Poster: a certificateless proxy re-encryption scheme for cloud-based data sharing. In Proceedings of the 18th ACM conference on computer and communications security, pages 869–872, 2011.

[4] Kang Yang, Jing Xu, and Zhenfeng Zhang. Certificateless proxy re-encryption without pairings. In International Conference on Information Security and Cryptology, pages 67–88. Springer, 2013.