An Authentication and Revocation Approach to Proxy Re-encryption in a Distributed File System.

Matthias, D.[1]

Department of Computer Science, Rivers State University.

Port Harcourt, Nigeria.

matthias.daniel@ust.edu.ng [1]

Charles, Davidba[2]

Department of Computer Science, Rivers State University.

Port Harcourt, Nigeria.

charlesdavidba@yahoo.com [2]

Anireh, V. I. E.[3]

Department of Computer Science, Rivers State University.

Port Harcourt, Nigeria

anireh.ike@ust.edu.ng [3]

Abstract: The cloud can serve as a distributed file system and storage facility where data can be shared conveniently. For security and confidentiality/privacy purpose the data is encrypted and the proxy acts as an emissary to re-encrypt the already encrypted data to a receiver without having to give out the data provider’s private key. Furthermore, this work adopted an authentication and revocation mechanism whereby only receivers with certain attributes can have access to the ciphertext and the data provider has absolute power over his data as he can either send a revocation command to the proxy to delete the policy and therefore stop re-encrypting data to that particular recipient or revoke access to a particular file or both. This work combines the advantages of unidirectional proxy re-encryption with attribute based authentication technique, thus achieving attributes authentication before re-encryption. Moreover, this work finally proves that the system is secure and would significantly enhance the system security level.

Keywords: Authentication, big data, privacy-preserving, proxy re-encryption, revocation, cloud.

1 Introduction

Big data is one of the main stream technologies at the core of concern in IT. The term big data is used to depict a large amount of data which could either be structured, unstructured or semi-structured that can be processed to extract information; though they are too intricate to be dealt with by traditional data processing application software.

Today, more individuals, businesses, organizations including government and governmental agencies prefer to store their data on the cloud. Cloud computing is the on demand availability of computer system resources, particularly data storage and computing power, without direct active management by the user. The term is normally used to describe data centers available to many users over the Internet. The cloud provides various advantages such as less cost, 24 hours 7 days a week availability, flexibility in capacity, all over functioning**,** automated updates on software, security**,** carbon footprint**,** enhanced collaboration, control on the documents, and is easily manageable**.**

Cloud computing is emerging as an unavoidable choice for internet based applications and services. It is a distributed computing architecture where the computing resources such as hardware, software, processing power are delivered as a service over a network infrastructure. The cloud computing model permits the users to access information and other resources from anywhere that a network connection is available.

In cloud computing all data are stored on distributed servers at remote location. The remote locations are data centers. The client can purchase or rent, such as handling time, network bandwidth, disk storage and memory [1]. Data owners can remotely store their data in the cloud and no longer possess the data locally. Cloud computing migrates the application software and database to the large data center, where the data management and services may not be fully trustworthy [2].

A cloud storage system is a distributed storage system [3] that comprises of many independent storage servers. The function of distributed storage systems is to store data confidentially and reliable over long periods of time [4]. The crucial clarification behind the elevation of the innovation cloud computing is as a result of the convenience that they provide to different newly developed applications and for enterprises. The information that are stored in the cloud is been accessed a huge number of times and is often subjected to changes.

The blend of big data and cloud computing reaps more for individuals, businesses, agencies, including the government. Big data is all about dealing with the massive scale of data whereas Cloud computing is about infrastructure. However, the simplification offered by big data and Cloud technology is the major motive for their tremendous enterprise adoption. Also, both the technologies are in the stage of evolution but their combination leverages scalable and cost-effective solution in big data analytics. The advantages of big data in cloud encompass improved analysis, simplified infrastructure, lowering of cost and virtualization.

Cloud services and applications may require all standard security functions including data confidentiality, integrity, privacy, robustness and access control. A significant aspect of cloud storage servers is that, it gives rise to a number of security threats. The first thing people consider before transferring data to the cloud is whether the cloud storage is secure or not because they wouldn’t want their data to be peeped without their consent. There are several cryptographic (the art of protecting information by transforming it into an unreadable format) methods to secure the data stored in cloud storage systems. Asymmetric or public key encryption is a cryptographic system that uses two keys, a public key which is known to everyone and a secret or private key which is known distinctly to the recipient of the message; in other words, public key encryption is a mechanism designed for data providers to encrypt/ hide data for security purposes.

However, public key encryption does not enable multi-sharing of cipher text without exposing the secret key of the data provider, hence, the need of applying a semi-trusted proxy to re-encrypt the cipher text, data can be shared without exposing information to the third party. Proxy re-encryption is a relatively new data encryption technique devised notably for distributed data and file security. The goal of proxy re-encryption is allowing the re-encryption of one cipher text to another cipher text without relying or trusting the third party that performs the transfer. In circumstances where one user wishes for another user to decrypt a message using its own or a new secret key instead of the first user's secret key.

Proxy re-encryption is a confidential means and technique for a user to store and share data [5]. A user can encrypt the file with a public key and then store the cipher text in a trusted server. When a receiver arrives, the sender can delegate a re-encryption key associated with the particular receiver to the trusted server as a proxy. Then the proxy re-encrypts the initial cipher text to the desired receiver. The purpose of proxy re-encryption schemes is to prevent the disclosure of the keys involved in re-encryption and the plaintext that should be re-encrypted to the proxy.

Due to the limitation of physical storage space came the need to store and transmits data on the cloud. Data owners therefore encrypt their data to ensure further privacy/confidentiality of data, but encrypted data using public key encryption possess a problem were the data cannot be sent to another receiver without revealing the senders secret key hence the need for a proxy to re-encrypt the cipher text which is to be sent to the receiver and also authenticate data receivers for verification processes in order to enhance security and the need to revoke users if found to be malicious or if the wrong data was sent. In this work, we consider a situation where data providers can verify the authenticity of receivers before proxy re-encryption and data providers also have the ability to revoke users rights so they can no longer access the cipher text; and during the authentication process if receivers attributes do not match that of the cloud provider there would be no more communication between the data provider and the receiver.

The sections that follow in this paper are structured as follows: in Section 2 we present the related works. In section 3 we would look at system analysis of the existing and proposed work. We gave the module description in Section 4. While, section 5 talks about the experimental analysis. Finally, in section 6 we conclude the work.

2 Related Works

Privacy of data is probable one of the greatest issues for organizations that make use of big data. The most every now and again utilized solution as regards securing data privacy in a Big Data framework is cryptography. Cryptography has been utilized to guard information for a tremendous amount of time. The indispensable goal of cryptography is to allow two people, commonly referred to as Alice and Bob, to speak over an insecure channel in such a way that an adversary, Oscar, cannot comprehend what is being stated/said. Encryption is a special kind of cryptographic technology that enforces access control over outsourced data [6].

The proxy re-encryption schemes were proposed by [7] and [5]. Proxy re-encryption is a cryptographic primitive which translates ciphertexts from one encryption key to some other encryption key. It very well may be utilized to advance encoded messages without uncovering the clear texts to the potential users. The re-encryption protocol ought to be key unbiased to abstain from compromising the private keys of the sender and the beneficiary. The major advantage of this PRE scheme [8] is that they are unidirectional (i.e., Alice can delegate to Bob barring Bob having to delegate to her) and don't require delegators to disclose their entire secret key to anybody.

This new cryptographic primitive permits a semi-trusted proxy with explicit information (a.k.a. re-encryption key) to transform a ciphertext under a public key into another ciphertext with the same plaintext under another public key. However, the proxy cannot get the plaintext. Two techniques where given by the above to classify PRE schemes. One is according to the allowed times of transformation. If the ciphertext can be transformed from Alice to Bob, then from Bob to Carol, and so on, then the PRE scheme is multi-use; else, it is single-use. The other method is according to the allowed direction of transformation. If the re-encryption key can be used to transform the ciphertext from Alice to Bob, and vice versa, then the PRE scheme is bidirectional; else, it is unidirectional. The Uni-Directional Schemes are further classified as Identity based PRE, Attribute Based PRE, Ciphertext-Policy Attribute based PRE, Conditional PRE, Time based PRE, while the Bi-directional Schemes are further classified as Type based PRE and Threshold based PRE.

Identity-based PRE is a scheme proposed by [9] in which senders encrypt messages using the recipient’s identity (a string) as the public key. An Identity Based Proxy Re-encryption scheme is an extended Identity Based Encryption scheme. The identity-based proxy re-encryption (IB-PRE) schemes enables a proxy to translate an encryption under Alice’s identity into one computed under Bob’s identity. The proxy uses proxy keys, or re-encryption keys, to perform the translation barring being capable to study the plaintext. Also, no information on the mystery keys of Alice and Bob can be deduced from the proxy keys.

Both PRE and IB-PRE is constrained to single receiver. If there should arise an occurrence of different receivers then the particular system is compelled to utilize PRE or IB-PRE more than one times. Subsequently to escape this issue, the concept of broadcast PRE (BPRE) was introduced by [8]. BPRE which runs the system equivalent to PRE and IB-PRE, however, in a significantly more fulfilling way.

Since the introduction of proxy re-encryption many schemes with different properties have been proposed. These schemes can be roughly categorized into two classes: public key infrastructure based (PKI-based), and identity based (ID-based).

The first PKI-based PRE scheme was proposed by [5] the scheme is proven-secure against chosen-plaintext attacks (CPA). In view of the modified CHK conversion [10] and [11] proposed the first chosen ciphertext secure (CCA-secure) multi-use bidirectional PRE scheme in the standard model. Recently, [12] proposed a new CCA-secure multi-use bidirectional PRE scheme without pairings in the standard model. However, there is no unidirectional PRE scheme proposed in the works referenced above and these three bidirectional schemes experience the ill effect of collusion attacks.

By using key sharing technique, two efficient single-use unidirectional PRE schemes are proposed in [13] and [14]. Howbeit, they experience the ill effects of collusion attacks. The first collusion-resistant PRE schemes are proposed by [9] and [15] based on public key encryption with double trapdoors (strong and weak private keys).

However, these schemes are solely CPA-secure. [16] proposed the first replayable chosen ciphertext secure (RCCA-secure) and collusion-resistant PRE scheme in the standard model. [17], and [18] proposed CCA-secure and collusion-resistant PRE schemes in the random oracle model. [19] and [20] proposed CCAsecure and collusion-resistant PRE schemes in the standard model. Notwithstanding, every one of these schemes are single-use and unidirectional.

Regarding the ID-based PRE, [13] proposed the first unidirectional IBPRE schemes, which are CCA-secure with single-useability and CPA-secure with multi-useability. They left that designing a CCA-secure multi-use unidirectional IBPRE (MUIBPRE) scheme as a problem. Later, [21] proposed a RCCA-secure MUIBPRE scheme. Recently, [22] proposed the first CCA-secure MUIBPRE scheme in the random oracle model. However, all the above three MUIBPRE schemes suffer from the collusion attack, and none of them is CCA-secure in the standard model. [23] propose an MUIBPRE scheme with CCA security and collusion resistance in the standard model, with the conversion from strongly CPA-secure and non-anonymous hierarchical identity-based encryption to CCA-secure and collusion-resistant MUIBPRE. The resulting scheme from the conversion offers answers to the hassle proposed in [13] and [22]. That is, they propose the first CCA-secure and collusion-resistant MUIBPRE scheme in the standard model and furthermore refine the security definition for MUIBPRE i.e. the security definition contains the CCA security and collusion resistance.

3 System Analysis: Existing System

The existing system uses a pre-authentication approach where users with certain attributes can have access to the data. The system ensures that the pre-authentication mechanism would essentially enhance the system security level. It was designed to be anonymous by means of getting rid of the linkage between the data and the identity (using an anonymous mechanism). It also allows for data to be shared conditionally. The present system considers a situation where users of the cloud center have the access to decide who to share with the data. Data providers can verify the authenticity of receiver's, Once receiver's attributes do not meet the conditions, providers will not communicate with him anymore and he can't acquire the data as well. The present system can grant multi-dimension privacy protection including data, user identities and attributes; this enhances the protection of user privacy.

MH-IBCPRE can realize conditional share and protect user's privacy from CCA, chosen plaintext attack, collusion attacks and tracing attacks.

Proposed system:

We propose a system where data providers can authenticate the receivers of the data and just those with the desired attributes can be granted access to the ciphertext. The proposed system gives data providers/owners the option to revoke (withdraw) authenticated users of access rights and they would no longer be capable to access the ciphertext or a revocation command can be given to the proxy to stop re-encrypting data for a certain user. Revocation in this context means from this point henceforth, any newly generated data will no longer be shared with a certain recipient. Revocation is a property to change the access rights of users when unexpected events occur such as malicious behavior etc. The system would also enable multi sharing over encrypted data. We used MH-IBCPRE and attribute-based encryption to enable data security and access control.

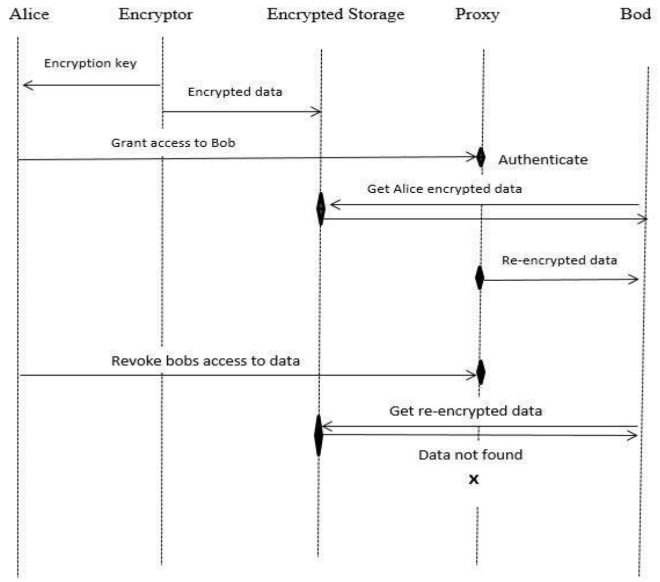

Figure 1: Revocation Workflow to Deny Access to File

Advantages of proposed system:

i. This system meets the demand of flexibility and privacy preserving.

ii. Reduces communication cost and computational burden by ensuring the proxy re-encrypt the ciphertext instead of the data provider downloading the data from the cloud, then decrypt, encrypt and upload the data back to the cloud.

iii. The data provider has the option of revoking a user/users from accessing his data or/and also give a revocation command so as the proxy would stop re-encrypting data for a certain recipient.

iv. The ability to authenticate and revoke users gives the data provider control over the data at his possession.

4 Module Description

In this section, we present the algorithms for our proxy re-encryption scheme with which we used in the system construction.

i. Setup: this is run by a trusted party that takes as input a security parameter and generates the global parameters.

ii. Key generation: this generates the public key pk_i and the secret key sk_i for user$_i$.

iii. Re key-generation: on inputting parameter, the private key of user$_i$ and the public key of user$j$, this would output re-encryption key R_{i}, j that can be used to re-encrypt a ciphertext which can be decrypted by useri and then generate a ciphertext which can be decrypted by userj.

iv. Encryption: input the public key pk, and message M and output the ciphertext CT.

v. Re-Encryption: takes the ciphertext CT and re-encryption key R_{i}, j as input, and output new ciphertext CT′.

vi. Decryption: takes the ciphertext c' and the private key as input, and output the message M.

5 Experimental Analysis

The results in this research focalized on the comparison of some different proxy re-encryption schemes and their execution times. We compared some PRE schemes based on the time of their encryption, re-encryption and decryption. The compared schemes are [5], [15], [24], [25] and ours. The comparison was based on experimental performance on execution times. Table 1 shows the cost in ms. of the main operations of the selected PRE schemes. These figures were measured at the mean cpu time of 10.000 executions for each operation. Note however, that the results of these experiments are highly dependent on implementation issues such as choice of programming language, parameters(type of curve, size of fields, type of pairing etc.), the underlying libraries and the use of pre-processing. For this reason, any comparative analysis based on these figures has to consider these aspects.

Table 1: Experimental Performance of Several Proxy Re-encryption Schemes (in ms)

Scheme	Encryption	Re-encryption	Decryption
[5]	11.07	11.48	11.21
[15]	22.76	83.52	13.76
[24]	22.52	22.29	11.89
[25]	155.27	386.93	443.87
OURS	7.89	11.34	8.03

6 Conclusion

In this paper, we propose a framework of privacy preserving for unidirectional sharing over encrypted data in big data context. Our framework adopted an authentication and revocation approach to proxy re-encryption system which ensures that only users whose attributes have been verified are permitted to obtain the data and also revocate users who need not have access to the data. Therefore, this model have proved to have added an additional level of security for encrypted data for encrypted data sharing.

REFERENCES

1. A. G. Dimakis, P. G. Godfrey, Y. Wu, M. J. Wainwright and K. Ramchandran,, "Network Coding for Distributed Storage Systems", IEEE, pp. 4539-4551, 2010.
2. C. Wang, W. Qian, R. Kui and L. Wenjing, "Ensuring Data Storage Security in Cloud Computing", pp.1-9, 2009.
3. P. Druschel and A. Rowstron, A Large Scale, Persistent Peer-to-Peer Storage Utility, Proc. Eighth Workshop Hot Topics in Operating System, pp. 75-80, 2001.
4. Q. Tang, Type-Based Proxy Re-Encryption and Its Construction, Proc. Ninth International Conf. Cryptology in India, pp. 130-144, 2008.
5. G. B. M. Blaze and M. Strauss, Divertible Protocols and Atomic Proxy Cryptography in Proc. Advance Cryptology, pp. 127–144, 1998.
6. S. Sundareswaran, A. C. Squicciarini and D. Lin, Ensuring Distributed Accountability for Data Sharing in the Cloud, IEEE Transactions on Dependable and Secure Computing, vol. 9(4), 2012, pp. 556–568.
7. M. Mambo and E. Okamoto, Proxy cryptosystems: Delegation of the Power to Decrypt Ciphertexts, IEICE Transactions on Fundamentals Electronics Communication Computer Science, vol. 80(1), 1997, pp. 54–6,.
8. C. K. Chu, J. Weng, S. S. M. Chow, J. Zhou, and R. H. Deng, Conditional proxy broadcast re-encryption in Proc. 14th Australasian Conf. Inf. Security Privacy, pp. 327-342, 2009.
9. G. Ateniese, F. Kevin, G. Matthew and H. Susan, Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage; In Proceedings of the 12th Annual Network and Distributed System Security Symposium, pp. 29-44, 2005.
10. R. Canetti, S. Halevi, and J. Katz, Chosen-Ciphertext Security from Identity-Based Encryption, in: EUROCRYPT 2004, LNCS, vol. 3027, pp. 207–222, 2004.
11. R. Canetti, and S. Hohenberger, Chosen-Ciphertext Secure Proxy Re-Encryption, in: ACM CCS, 2007.
12. T. Matsuda, R. Nishimaki, and K. Tanaka, (2010). CCA Proxy Re-Encryption without Bilinear Maps in the Standard Model, in: PKC 2010, LNCS, vol. 6056, pp. 261–278.
13. M. Green and G. Ateniese, Identity-based Proxy Re-encryption: Application Cryptography Network Security Lecture Notes Computer Science, vol. 4521, 2007, pp. 288– 306.

14. J. Weng, R. H. Deng, S. Liu, K.. Chen, J. Lai and X. Wang, Chosen-Ciphertext Secure Proxy Re-Encryption Schemes without Pairings, in: CANS 2008, LNCS, vol. 5339, pp.1–17.
15. G. Ateniese, K.. Fu, M. Green, and S. Hohenberger, Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage, ACM Transactions on Information and System Security (TISSEC) vol. 9 (1), 2006, pp. 1–30.
16. B. Libert and D. Vergnaud, Unidirectional Chosen-Ciphertext Secure Proxy Re-Encryption. International Conference on Cryptology in Africa, Vol. 4939, 2008, pp.360–379.
17. J. Shao and Z. Cao, CCA-Secure Proxy Re-Encryption without Pairings. In Proceedings of the 12th International Conference on Practice and Theory in Public Key Cryptography: PKC'09, 2009, pp. 357–376.
18. S. M. C. Sherman, W. Jian, Y. Yanjiang and H. D. Robert, Efficient Unidirectional Proxy Re-encryption, International Conference on Cryptology, vol. 6055, 2010, pp.316-332.
19. P. L. J. Shao and Y. Zhou, "Achieving Key Privacy without Losing CCA Security in Proxy Re-encryption: J. System Software, vol. 85(3), 2011, pp.655–665.
20. J. Weng, M. Chen, Y. Yanjiang, D. Robert, K. Chen, and B. Feng, CCA-Secure Unidirectional Proxy Re-encryption in the Adaptive Corruption Model without Random Oracles. Science China Information Science, vol. 53, 2010, pp. 593-606.
21. C. Chu and W. Tzeng, Identity-based Proxy Re-encryption without Random Oracles. Information Security Lecture Notes Computer Science vol. 4779, 2007, pp.189–202.
22. H. Wang, Z. Cao, W. Licheng, Multi-use Unidirectional Identity-based Proxy Re-encryption Schemes. Inf. Sci. vol. 180(20), 2010, pp.4042-4059.
23. G. W. J. Shao, P. Liu, and Y. Ling, Anonymous Proxy Re-encryption: Security Communication Network, Vol. 5(5), 2012, pp.439–449.
24. J. Weng, H. D Robert, S. Liu and K.. Chen, Chosen ciphertext secure bidirectional proxy re-encryption schemes without pairings. Information Sciences, vol. 180(24), 2010, pp. 5077–5089.
25. B. Libert and D. Vergnaud,. Unidirectional Chosen-Ciphertext Secure Proxy Re-Encryption. Information Theory, IEEE Transactions on, vol. 57(3), 2011, pp. 1786–1802.
26. L. Guo, J. Sun, C. Zhang, and Y. Fang, A privacy-preserving Attribute-based Authentication System for Mobile Health Networks: IEEE Transaction on Mobile Computer, vol. 13(9), 2014, pp. 1927–1941.
27. K.. Wang, J. Yu, X. Liu and S. Guo, A Pre-authentication Approach to Proxy Re-encryption in Big Data, IEEE, 2017.