International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER
SSRN

IJIEMR Transactions, online available on 13th Jan 2023. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=ISSUE-1

DOI: 10.48047/IJIEMR/V12/ISSUE 01/79

Title **A Secure Data Sharing Proxy with Accountable Re-Encryption**

Volume 12, Issue 1, Pages: 851-855

Paper Authors
CH.VIJAYKUMAR, S.RAMYA, V.DEEKSHITHA SREE, K.SAIRAM, G.RAHUL

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

A Secure Data Sharing Proxy with Accountable Re-Encryption

[1]CH.VIJAYKUMAR, [2]S.RAMYA [3]V.DEEKSHITHA SREE, [4]K.SAIRAM, [5]G.RAHUL
[1]ASSOCIATE PROFESSOR, [2,3,4,5]STUDENT, [1,2,3,4,5]DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, ACE ENGINEERING COLLEGE, HYDERABAD

ABSTRACT:
For exchanging encrypted information in cloud service, proxy re-encryption (PRE) offers a potential approach. When outsourced data Alice wants to provide data end user Bob access to her encrypted information, Alice creates a re-encryption key and delivers it to the public cloud (proxy). With the help of this key, the proxy may convert Alice's decryption into Bob's without knowing the underlying ciphertexts. Despite the fact that current Alice's secret key can be prevented from being obtained by the proxy using PRE methods malicious packets with Bob, it is unavoidable that the substitute and Bob will be able to acquire and disseminate Alice's decryption skills owing to PRE's fundamental functionality. Even worse, the malicious proxy can claim that it hasn't revealed the decrypt tools, and there's very little chance that it will be discovered. . To solve this issue, we provide the idea of Accountable Periodically Re (APRE), wherein a judge program can determine whether or not the intermediary is innocent if it is charged with decryption capacity of Alice is distributed through reencryption key misuse. Our non-interactive APRE mechanism is then demonstrated to be secure and transparent using the standard model's DBDH assumptions. Our final demonstration shows how it can be upgraded to be secure.

KEYWORDS: IBE, APRE, Proxy, CCA, Security

I. INTRODUCTION:

In the digital age, cloud computing and sharing data have quickly become essential components of consumer-focused software like Amazon S3, iCloud, Dropbox, Microsoft SkyDrive, and Google Drive . Additionally, a growing number of people's record - keeping systems rely on cloud platforms for data collection, archiving, and sharing. It is possible, for example, to outsource personal medical records (PHR) services to second cloud service providers such as Windows HealthVault, PatientsLikeMe, and ELGA, which enhances data storage efficiency and facilitates data synchronization among institutions. Online security challenges associated with cloud services, including their popularity challenges, including privacy, despite its ease and attractiveness. which are the main issues for users that use such services. Before uploading user data to the cloud, it is customary to encrypt it. However, in such a situation, data exchange between users can be challenging. The data controller can obviously obtain the substitution cipher, decode it with his personal encryption key, and then encrypt it for each individual receiver. However, it is impractical since such activities significantly raise the processing and transmission costs for the data owner. This method also has the drawback of requiring the data owner to remain online at all times. In 1998, Blaze et al. I PRE techniques can prevent the proxy from accessing Alice's private key by means of plan, which are the main issues for users that use such services. Before downloading user data to the cloud, it is customary to encrypt it. However, in such a situation, data exchange between users can be challenging. The data owner can simply download that ciphertext, decode it with his personal encryption key, and then encrypt it for each individual receiver. However, it is unsustainable since those activities significantly raise the processing and transmission costs for the data owner. This method also has the drawback of requiring the data owner to remain online at all times. In 1998, Blaze et al. introduced proxy re encryption (PRE) as a solution to the problem of data exchange. In a PRE plan, A proxy can change a ciphertext meant for Alice (the micro manager) into another ciphertext that Bob can decipher by using detailed (The re encryption key) information (delegatee) .PRE offers a wide range of beneficial applications in addition to cloud data sharing and disclosure systems, such as email forwarding, shared file systems, administration of digital rights, and distributed files systems.A sample PRE application for cloud data exchange is shown in Fig. 1. Alice, a research company and acquirer, may want to keep the She obtains encrypted material from a cloud

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

server and provides it to her paying clients. Remember that Alice .Alice owns the data and doesn't want anyone, not even the cloud server, to have access to it without their permission. When preparing, For validation, Alice, Bob, and proxy must send the other the credentials and public keys. Sally uses encryption is used for all stages of processing personal data, and a cloud server is used to keep the decryption. Before sharing her encrypted data, Alice prepares a re-encryption key and uploads it to the cloud server.. The cloud server alters Alice's ciphertexts at Bob's request and sends them his way. Stopping the proxy from discovering any information about the encrypted messages is the main goal of the classic PRE security model. To realize the application requirement illustrated in the aforementioned example, however, is insufficient. Due to Condenser mics built-in functionality, Bob and the public cloud can jointly access Alice's decoding ability and keep it on any transmitters, such as a decrypt a tool or programme. Therefore, if Alice's decryption abilities were advertised both online and off, she could lose a lot of money.. The "re-encryption key addiction to drugs" is a common term used to describe this problem.." If a decoded message is compared to a fish, a decoding device can be used to catch fish; therefore, it is far riskier to distribute an illicit decryption equipment than it is to send out a a solitary message Even worse, there is no likelihood that law enforcement will be able to detain the hostile server. more specifically, because Alice has the ability to decrypt as well, the decryption device itself cannot be utilized to prove beyond a reasonable doubt who is guilty.

II. LITERATURE SURVEY:

[1] **Ateniese et al. [10],** who also proposed the idea of non-transferability. They did not address the issue of how to build a non-transferable PRE scheme. Several papers have since been published with the goal of fixing this issue.

[2] **Blaze et al[3] .'s** original PRE concept was first proposed CPA secure PREs] and CCA secure PREs are two examples Several more PRE schemes, such as type-based (conditional) PREs, forward secure PRE, and PRE for key revocation and rotation, have also been proposed. Since the proxy is presumed to be somewhat honest in all of the aforementioned schemes, the PRE scheme's re-encryption key misuse problem cannot be resolved.

[3] Libert and Vergnaud [36] in which the delegator could identify a malicious proxy who revealed the re encryption key to a third party. Their work makes the assumption that the delegator is trustworthy and that he or she cannot leak the revealed re-encryption key. Instead of making such an assumption in this research, the intention is to identify malevolent delegators or malicious proxies.

[4] Later, Guo et al. [19] and Hayashi et al. [37] tried to provide more lenient definitions of non-transferability. Regrettably, their security model was unable to stop every attempt to transmit decrypt rights. Furthermore, Hayashi et a approach's is susceptible to an attack on the forgeability of re-encryption keys, according to Isshiki et al. , and the security assumption used in their proofs can be easily addressed. A concrete construction based on two primitives—an indistinguishability obfuscator for circuits and a k-unforgeable authentication scheme—was recently proposed by Guo et al., who also formalized the idea of non-transferability. Although have explored the transferability issue in proxy re-encryption, their work lacks a formal security model and security proof.

[5] Changbo Hu et.al Ateniese et al. first proposed the idea of non-transferability in 2005 as a means of reducing the aforementioned issue of misuse of re-encryption keys. When Bob and a proxy conspire to transfer Alice's decrypt right, as a cost, Bob has to reveal his own decoding capability. This is how ou pas protects Alice's "advantage" in outsourcing her decryption right. Before Guo et al. provided a generic architecture employing basis of lack obfuscation and unforgeable authentication as main techniques, creating a non-transferable PRE method had long always been open problem. Non-transferability proactively discourages harmful users and it effectively solves the issue of misuse of re-encryption keys. However, it still falls short in the aforementioned particular cloud data sharing scenario.

[6] Shamir A Image recognition system based on computer vision for identifying offensive and noncompliant images large data sets has been proposed by Shreyas Gandhi et.al.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

III. RESULTS & DISCUSSION:

Sl.No	Author	Technology Used	Remarks
1	Ateniese	Introduced the notion of non-transferability.	They did not address the issue of how to build a non-transferable PRE scheme.
2	Blaze	Many efforts have been made to improve the security of the ciphertexts since PRE was first introduced, including the development of CPA secure PREs and CCA safe Pres.	They present atomic proxy crypto, in which secret data (messages or signatures) for one key are converted into encrypted message for a further key using an instantaneous proxy function and a public proxy key. Proxy functions may be used in unknown environments after proxy keys have been generated and brought to light.
3	Libert and Vergnaud	Vergnaud and Libert They provided a detectable proxy re-encryption scheme that allowed the delegator to spot an unreliable proxy that had given the re-encryption key to a third party.	Their work makes the assumption that the delegator is trustworthy and that he or she cannot leak the disclosed re-encryption key.
4	Later, Guo et al. and Hayashi et al	Author tried to provide looser definitions of non-transferability	Regrettably, their security model was unable to stop every attempt to transmit decryption rights. Furthermore, Isshiki et al. noted that the security premise used in Hayashi et a proofs 's can be focus and emphasis, making Hayashi et a scheme's susceptible to the forgeability exploit of re-encryption keys.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

5	M. Green and G. Ateniese,	ID-based proxy reencryption (IBPRE) includes data transfer in a 1 : 1 manner between a sender and receiver.	Only its data owner inside this project has the ability to decode or re encrypt material that has been encrypted using that owner's public key.
6	Shamir	the handling of certificates for conventional public key infrastructure.	IBE has a problem with key escrow since private key generators (PKG) can decode all hash codes and distribute private keys at whim without being noticed.

IV. CONCLUSION:

Because of the nature of PRE schemes, the main worries for users of cloud data sharing services have been the capacity for intermediary and any delegate to collaborate in order to derive and share the delegator's decrypt power. In order to address this issue, we presented the responsible PRE concept in this study. We initially defined the idea of responsible PRE, where the judge method can determine which proxy is misusing its re-encryption key. Then, we gave the first responsible.

V. ACKNOWLEDGEMENT:

The authors appreciate the guidance and time that our guides Mrs. D. Ashwini and Mrs. Soppari Kavitha have given us. We also wish to express our sincere thanks to Dr.M. V. Vijaya Saradhi, Head of the Department of Computer Science and Engineering at Ace Engineering College, for his valuable time and support.

REFERENCES:

[1]. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage,"
in NDSS, 2005.

[2]. M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in Advances in Cryptology-EUROCRYPT'98. Springer, 1998, pp. 127–144

[3]. B. Libert and D. Vergnaud, "Towards black-box accountable authority IBE with short ciphertexts and private keys," in Public Key Cryptography–PKC 2009. Springer, 2009, pp. 235–255.

[4]. R. Hayashi, T. Matsushita, T. Yoshida, Y. Fujii, and K. Okada, "Unforgeability of re-encryption keys against collusion attack in proxy re-encryption," in Advances in Information and Computer Security. Springer, 2011, pp. 210–229

[5]. G. Ateniese, K. Fu, M. Green, and S. Hochenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in NDSS, 2005.

[6]. A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in cryptology. Springer, 1984, pp. 47–53. [43] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in Advances in Cryptology-CRYPTO 2001. Springer, 2001, pp. 213–229 .

[6]. C. Cocks, "An identity-based encryption scheme based on quadratic residues," in Cryptography and coding. Springer, 2001, pp. 360–363. [45] V. Goyal, "Reducing trust in the PKG in identity-based cryptosystems," in Advances in Cryptology-CRYPTO 2007. Springer, 2007, pp. 430– 447.

[7] V. Goyal, S. Lu, A. Sahai, and B. Waters, "Black-box accountable authority identity-based encryption," in Proceedings of the 15th ACM conference on Computer and communications security. ACM, 2008, pp. 427–436.

[8] B. Libert and D. Vergnaud, "Towards black-

box accountable authority IBE with short ciphertexts and private keys," in Public Key Cryptography–PKC 2009. Springer, 2009, pp. 235–255.

[9] A. Sahai and H. Seyalioglu, "Fully secure accountable-authority identitybased encryption," in Public Key Cryptography–PKC 2011. Springer, 2011, pp. 296–316.

[10] A. Kiayias and Q. Tang, "Making any identity-based encryption accountable, efficiently," in Computer Security–ESORICS 2015. Springer, 2015, pp. 326–346