iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VI **Month of publication:** June 2023

DOI: https://doi.org/10.22214/ijraset.2023.53822

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

Accountable Proxy Re-Encryption for Secured Data Sharing

V. Bhuvaneshwari[1], S. Shakthieswari[2], R. Supraja[3], R.Youkashree[4]
[1]*B.E., M.E., B.Ed., Assistant Professor/CSE,* [2, 3, 4]*Final Year, Computer Science Engineering Department, Achariya College of Engineering Technology*

Abstract: ***Proxy re-encryption (PRE) provides a promising solution for encrypted data sharing in public cloud. When data owner Alice is going to share her encrypted data with data consumer Bob, Alice generates a re-encryption key and sends it to the cloud server (proxy); by using it, the proxy can transform Alice's ciphertexts into Bob's without learning anything about the underlying plaintexts. Despite that existing PRE schemes can prevent the proxy from recovering Alice's secret key by collusion attacks with Bob, due to the inherent functionality of PRE, it is inevitable that the proxy and Bob together are capable to gain and distribute Alices decryption capabilities. Even worse, the malicious proxy can deny that it has leaked the decryption capabilities and has very little risk of getting caught. To tackle this problem, we introduce the concept of Accountable Proxy Re-Encryption (APRE), whereby if the proxy is accused to abuse the re-encryption key for distributing Alice's decryption capability, a judge algorithm can decide whether it is innocent or not. We then present a non-interactive APRE scheme and prove its CPA security and accountability under DBDH assumption in the standard model. Finally, we show how to extend it to a CCA secure one.***

I. INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.

The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

II. LITERATURE SURVEY

The paper titled "Divertible protocols and atomic proxy cryptography" by M. Blaze, G. Bleumer, and M. Strauss introduces the concept of divertibility as a protocol property and presents a definition of protocol divertibility applicable to arbitrary two-party protocols. The authors propose a sufficiency criterion for divertibility, which extends beyond the traditional notion and encompasses protocols like blind signature protocols and Diffie-Hellman key exchange.

The paper also introduces the concept of atomic proxy cryptography, which involves utilizing an atomic proxy function and a public proxy key to convert ciphertexts from one key to another. The authors provide atomic proxy functions for discrete-log-based encryption, identification, and signature schemes. However, the existence of atomic proxy functions for all public-key cryptosystems remains uncertain.

Furthermore, the paper delves into the relationship between divertibility and proxy cryptography, examining how these concepts interact within secure communication protocols.

The paper titled "A Certificateless Proxy Re-Encryption Scheme for Secure Data Sharing with Public Cloud" by L. Xu, X. Wu, and X. Zhang proposes CL-PRE, a certificateless proxy re-encryption scheme designed for secure data sharing with a public cloud. In CL-PRE, the data owner encrypts shared data in the cloud using an encryption key. The encrypted data is then transformed by the cloud and distributed to authorized recipients based on access control policies.

©IJRASET: All Rights are Reserved

One of the distinguishing features of CL-PRE is its utilization of re-encryption keys derived from the data owner's private key and the recipients' public keys. This approach eliminates the key escrow problem associated with identity-based cryptography and removes the need for certificates. By ensuring data and key privacy from semi-trusted clouds, CL-PRE maximizes the utilization of cloud resources, thereby reducing the computational and communication costs for the data owner.

To address the challenges of running a proxy in a public cloud environment, the paper further proposes two enhancements: multi-proxy CL-PRE and randomized CL-PRE. These additions improve the security and robustness of the CL-PRE scheme. The authors also implement all CL-PRE schemes and evaluate their security and performance aspects.

The paper titled "Two Secure Anonymous Proxy-Based Data Storages" by O. Blazy, X. Bultel, and P. Lafourcade addresses the challenge of privacy protection in shared storage systems that employ unidirectional proxy re-encryption (PRE). While PRE enables efficient and secure storage, it currently requires users to disclose their identity and query to the proxy, compromising their privacy. In response, the authors propose two secure data storage systems that allow authorized users to access the encrypted data content anonymously.

The first scheme presented in the paper corresponds to a pay-per-download economic model. In this scheme, users are required to pay for each file they download. This approach ensures privacy by allowing users to access the content without revealing their identity or queries to the proxy.

The second scheme adopts a subscription-based economic model. Users pay a monthly fee to gain unlimited access to all their files stored in the system. This model also maintains anonymity, allowing users to retrieve their files without exposing their identity or queries.

By introducing these two secure data storage systems, the authors aim to provide privacy-preserving solutions that enable authorized users to access their encrypted data without compromising their anonymity. The schemes offer different economic models, catering to different user preferences and needs.

The paper titled "Generally Hybrid Proxy Re-Encryption: A Secure Data Sharing among Cryptographic Clouds" by P. Xu, J. Xu, W. Wang, H. Jin, W. Susilo, and D. Zou addresses the challenge of securely sharing data among different Proxy Re-Encryption (PRE) schemes in a cryptographic cloud environment. While several PRE schemes have been proposed for specific applications, ensuring secure data sharing across different PRE schemes has not been addressed in a general manner. The existing PRE schemes differ significantly in terms of algebraic systems and public-key types, making it challenging to achieve interoperability.

To address this challenge, the authors of this paper propose a Generally Hybrid Proxy Re-Encryption (GHPRE) scheme. They begin by unifying the definitions of existing PRE and Public Key Encryption (PKE) schemes and further standardize their security definitions. By considering a uniformly defined PRE scheme and a uniformly defined PKE scheme as building blocks, the GHPRE scheme is constructed. The scheme leverages the concept of temporary public and private keys to facilitate secure data sharing between the underlying PRE and PKE schemes. Importantly, the GHPRE scheme is not limited to a specific combination of schemes and can work between any two PRE schemes. Furthermore, the GHPRE scheme can be seamlessly deployed even when the underlying PRE schemes are being implemented. By proposing the GHPRE scheme, the authors contribute to achieving secure data sharing among cryptographic clouds by providing a general solution that bridges the gap between different PRE schemes. The scheme's flexibility and compatibility make it a promising approach for enabling secure and flexible data sharing in cryptographic cloud environments. The paper titled "Fine-grained Two-Factor Protection Mechanism for Data Sharing in Cloud Storage" by C. Zuo, J. Shao, J. K. Liu, G. Wei, and Y. Ling addresses the challenge of data protection in cloud storage for data sharing. While cryptographic techniques are commonly used to protect shared sensitive data, challenges remain, particularly in safeguarding and revoking cryptographic keys. To overcome these challenges, the authors propose a new data protection mechanism for cloud storage with several key properties. The proposed mechanism employs a two-factor protection approach for cryptographic keys. The secrecy of the key is maintained only if one of the two factors is successfully authenticated. This enhances the confidentiality of the cryptographic key and provides an additional layer of security.

Efficient key revocation is achieved through the integration of proxy re-encryption and key separation techniques. This enables the efficient revocation of cryptographic keys when necessary, ensuring data security even in scenarios where access permissions need to be modified.

To achieve fine-grained data protection, the mechanism adopts attribute-based encryption techniques. This allows data to be protected based on specific attributes, enabling granular control over access to the encrypted data.

The proposed mechanism is evaluated through security analysis and performance evaluation, demonstrating its effectiveness and efficiency. The analysis confirms the security of the mechanism, while the evaluation highlights its computational efficiency and suitability for practical implementation.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

III. EXISTING SYSTEM

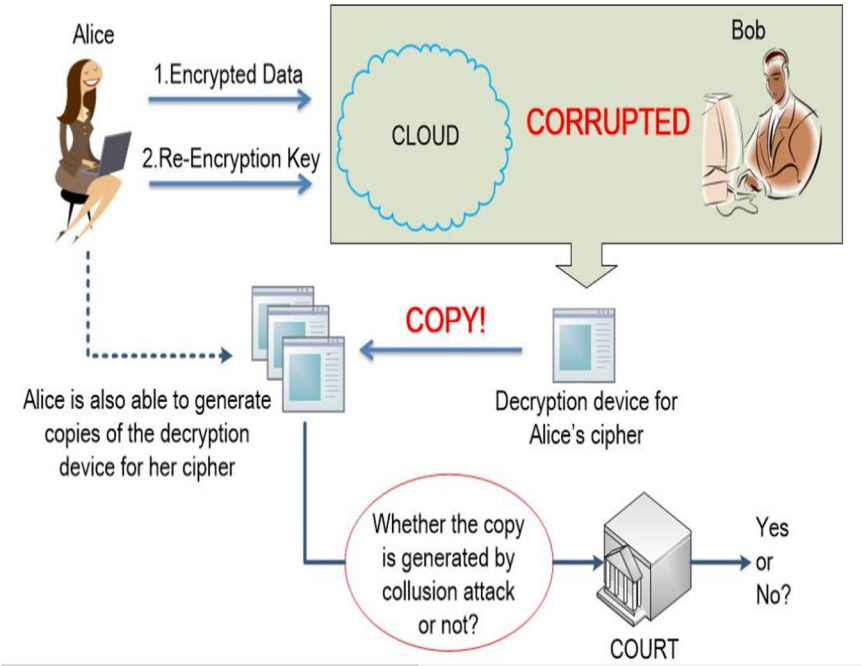
Hayashi et al. and Guo et al. attempted to give relaxed notions of non-transferability. Unfortunately, their security model could not capture all attacks of decryption rights' transference. Moreover, Isshiki et al. pointed out that Hayashi et al.'s scheme is vulnerable to the forgeability attack of re-encryption keys and the security assumption employed in their proofs can be solved efficiently. Recently, Guo et al. formalized the notion of non-transferability and proposed a concrete construction building on two primitives: an indistinguishability obfuscator for circuits and a k-unforgeable authentication scheme. The transferability issue in proxy re-encryption has also been considered, but their work lacks formal security model and security proof. The existing system approach also suffers from a limitation that the data owner has to be on-line all the time. Due to the inherent functionality of PRE, the cloud server and Bob together are able to obtain Alice's decryption capability and keep it on any form of carriers, such as a decryption program or a decryption device. Therefore, Alice's decryption capability could be sold online and offline, which makes Alice suffering serious economic losses. This weakness is also called re-encryption key abuse problem. The existing system security model could not capture all attacks of decryption rights' transference.

IV. PROPOSED SYSTEM

In this proposed system, we explore a new approach to resolve the existing trust problem. In particular, we introduce the concept of accountable PRE (APRE), where a convincing proof can be provided from which a judge can make a decision about who is guilty. Therefore, if the proxy (colluded with any delegatee) re-distributes a decryption device, it will have the risk of being caught and sued. In this paper, we design the re-encryption key as a signature on the proxy's public key. Informally, the secret key of the proxy plays the role of salt in the above analysis. Hence, the unforgeability of the underlying signature implies the proxy can not forge another re-encryption key to remove its key pair's information. Simultaneously, the delegator has no knowledge about the secret key of the proxy. As a result, a decryption device created by using the re-encryption key can be distinguished from the one generated by the delegator.

The proposed system is CPA secure, secure against malicious proxy and secure against malicious delegator under the DBDH assumption in the standard model. The judge algorithm is public, that is, anyone can run the judge algorithm with no additional secret needed. The re-encryption key generation process is non-interactive and thus communication cost can be saved. The proposed system is of great practical significance to restrict misbehavior of the proxy.

V. SYSTEM ARCHITECTURE



©IJRASET: All Rights are Reserved

VI. IMPLEMENTATION

A. *Modules Description*

1) *Data Owner:* In Data Owner module, Initially Data Owner must have to register their detail. After successful registration data owner can login and upload files into cloud server with encrypted keywords and hashing algorithms. He/she can view the files that are uploaded in cloud. Data Owner can approve or reject the file request sent by data users. After request approval data owner will send the secret key and verification object through mail. Whenever data owner wants to audit their uploaded file, He/she can send request to court.
2) *Delegator:* In Delegator module, Initially Delegator must have to register their detail. After successful registration Delegator can login and search all the files upload by data owners. He/she can send request to the files and then request will send to the data owners. If data owner approve the request then Delegator will receive decryption key in registered mail.
3) *Court:* In Court module, whenever receives auditing request from data owner, the court can generate the auditing proof to respected data owner.
4) *Cloud Server:* Cloud Server provides a public platform for data owners to store and share their encrypted data. The cloud provider doesn't conduct data access control for owners. The encrypted data can be downloaded freely by any data users. We have used DriveHQ cloud service provider for the storage of files in the cloud part.

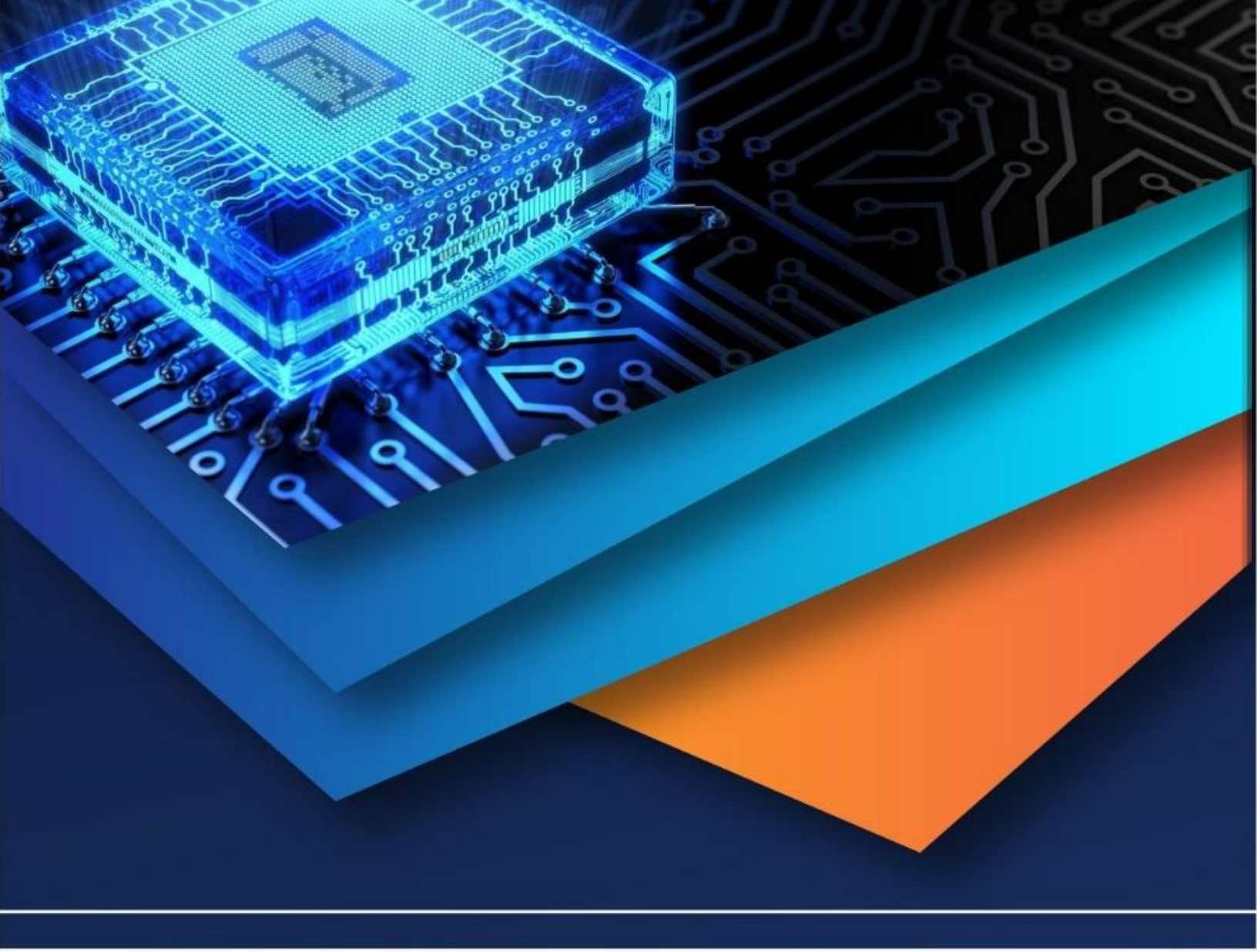
VII. CONCLUSION

Due to the nature of PRE schemes, proxy and any delegate can collude to derive and distribute the delegator's decryption capability, which has been the major concerns for users utilizing cloud data sharing services. In this paper, we introduced the concept of accountable PRE to resolve this problem. We first formalized the notion of accountable PRE, in which the proxy that abuses its re-encryption key can be identified by the judge algorithm. Then, we presented the first accountable PRE scheme which is non-interactive and public accountable and proved its CPA security and accountability under DBDH assumption in the standard model. When compared with previously related schemes, our scheme offers better performances. A worthwhile direction is to propose an efficient generic transformation with accountable properties of PRE, which may potentially stimulate the adoption of PRE schemes in practice.

REFERENCES

[1] "Amazon S3." [Online]. Available: http://aws.amazon.com/s3/
[2] Covert, "Google Drive, iCloud, Dropbox and more compared: What's the best cloud option?" [Online]. Available: http://gizmodo.com/5904739
[3] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in Advances in Cryptology-EUROCRYPT' 98. New York, NY, USA: Springer, 1998, pp. 127–144.
[4] L. Xu, X. Wu, and X. Zhang, "A certificateless proxy re-encryption scheme for secure data sharing with public cloud," in Proc. 7th ACM Symp. Inf. Comput. Commun. Secur., 2012, pp. 1–10.
[5] O. Blazy, X. Bultel, and P. Lafourcade, "Two secure anonymous proxy-based data storages," in Proc. SECRYPT, 2016, pp. 251–258.
[6] P. Xu, J. Xu, W. Wang, H. Jin, W. Susilo, and D. Zou, "Generally hybrid proxy re-encryption: a secure data sharing among cryptographic clouds," in Proc. 11th ACM Asia Conf. Comput. Commun. Secur., 2016, pp. 913–918.
[7] C. Zuo, J. Shao, J. K. Liu, G. Wei, and Y. Ling, "Fine-grained twofactor protection mechanism for data sharing in cloud storage," IEEE Trans. Inf. Forensics Secur., vol. 13, no. 1, pp. 186–196, Jan. 2018.
[8] S. Myers and A. Shull, "Practical revocation and key rotation," in Proc. Cryptographers Track RSA Conf., 2018, pp. 157–178.
[9] R. Canetti and S. Hohenberger, "Chosen-ciphertext secure proxy re-encryption," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 185–194.
[10] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. Netw. Distrib. Syst. Secur. Symp., 2005.
[11] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," ACM Trans. Inf. Syst. Secur., vol. 9, no. 1, pp. 1–30, 2006.
[12] J. Zhang, Z. Zhang, and H. Guo, "Towards secure data distribution systems in mobile cloud computing," IEEE Trans. Mobile Comput, vol. 16, no. 11, pp. 3222–3235, Nov. 2017.
[13] G. Taban, A. A. Cardenas, and V. D. Gligor, "Towards a secure and interoperable drm architecture," in Proc. ACM Workshop Digit. Rights Manage., 2006, pp. 69–78.
[14] C. Borcea, Y. Polyakov, K. Rohloff, G. Ryan, et al.,"Picador: End-to- end encrypted publish–subscribe information distribution with proxy re-encryption," Future Generation Comput. Syst., vol. 71, pp. 177–191, 2017.
[15] Y. Polyakov, K. Rohloff, G. Sahu, and V. Vaikuntanathan, "Fast proxy re-encryption for publish/subscribe systems," ACM Trans. Privacy Security, vol. 20, no. 4, 2017, Art. no. 14.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)