Identity Based Proxy Reencryption with Null Deduplication for Secure Communication in Cloud Environment

Rashmi Dixit, K. Ravindranath

Abstract : Cloud provide services in terms of infrastructure , software , and platform .But data becomes social as it resides on the cloud due which issue raises like security along integrity , duplication etc. The purpose of this work is to enhance the security of data stored on the cloud and improve the privacy along with integrity. Proxy-Reencryption Scheme based on identity is used. Data uploaded by data owner on the cloud is under control of cloud service provider, Data may be in motion or rest In this case for uploaded data needs of security and privacy is growing gradually. Attribute-based encryption (ABE) cater one and the other, access control as well as data security by specifying users with attributes so that particular user is able to decrypt data by matching attributes. In real-world applications of ABE, cancellation of users or their attributes is needed so that such users is no longer able decrypt the data. ABE is used in hybrid along with symmetric encryption scheme such as the Advanced Encryption Standard (AES). In this the data is encrypted with AES and the AES key is encrypted with ABE. Again Encryption performs on on ciphertext which is uploaded in the cloud, the data owner (DO) must requires more communication cost as well as computational burden as data download from the cloud, then decrypt, encrypt, and again upload the data back to the cloud

Keywords: Deduplication, Attribute Based Encryption (ABE), Cloud Service Storage, Proxy Re-Encryption, Advanced Encryption Standard, AES.

I. INTRODUCTION

Cloud Computing, a powerful storage place medium which allows the users to use infrastructure, software and platform depending upon the requirements. but if we take a look at the problems while uploading data over the cloud, We already know that the cloud infrastructure is powerful devices but facing problem from internal and external threats for data integrity .Second, once data is deployed in the cloud ,it is under the control of CSP, and we cannot fully trust on them .And getting data from cloud after checking integrity also not easy due to the expensiveness in I/O and transmission cost besides the network. Owner cannot detect data exploitation time to time and sometime it might be too late to recover the data loss or damage. Encryption is one of technique to provide security but only encryption cannot completely solve the problem as data may move from one cloud to another cloud as control on hands of another CSP.

With storage its really important to preserve the data with secured manner without any issues. But the problem arises when the same data stored in the cloud by different user or client, at that time deduplication have equal weight age. So while preserving the data into the cloud care will be taken for the issues such as deduplication problems, security threats and ownership schemes. Above all security is more important while deploying data into the cloud.

A Proxy based authentication scheme is introduced to avoid unauthorized users to get access to the server to use data along with powerful encryption scheme called Advanced Encryption Standard (AES) algorithm for securing the data from any attack more at the same time to maintain the data integrity by means of eliminating duplicate records. Two powerful algorithms, Proxy Authentication and AES will work together along with server-side deduplication scheme to control access to outsourced data. And by handling randomized meet encryption and secure ownership group key distribution the ownership changes dynamically.

This combination avoids loss of data and at the same time revoke users by storing inherited data legitimately-but-curious on cloud storage server. The proposed work gives guaranty of integrity of data in the environment of inconsistency attacks. The efficiency analysis validates that the proposed scheme is powerful than the existing schemes, while the additional computational overhead is unimportant.

Below figure represent basic uploading of data with encryption. While uploading different user may user encryption key to convert data into encrypted format.

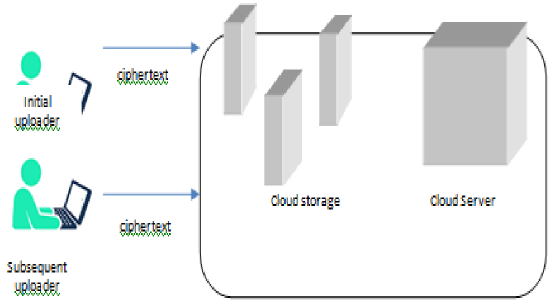

Fig. 1 Traditional Data uploading Model over Cloud Server

In ABE[8] , user or attribute cancellation is the basic characteristic in real-world applications. Changing of users or their attributes is the basic need or the thing which is constant over system.

Revised Manuscript Received on April 12, 2019.

Ms Rashmi Dixit, Research Scholar, Department of CSE, Koneru Lakshmaiah Education Foundation, Guntur, AP, India

K. Ravindranath, Associate Professor, Department of CSE, Koneru Lakshmaiah Education Foundation, Guntur, AP, India

For example, if any one user is mischievous, then it may be directly cancelled otherwise as a choice their attribute directly change from the system before decryption . In the existing revocation methods, hybrid ABE is proposed along with private encryption, i.e the advanced encryption standard (AES). In hybrid encryption, data is encrypted with AES and the AES key is encrypted with ABE.

Because extant cancellation system alter only ABE encrypted text, but users can carry their AES key and even after cancellation they can use it to decrypt data. So its important to reencrypt data with new key, so that the previous AES key is no available for use.

II. LITERATURE REVIEW

Though Cloud computing is an emerging trend which allow to share resoueses but at the same time it brings forth many new challenges for data security and access control This paper focuses on such challenges by combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Proposed scheme also allow user to define privileges[1] A sharing of data in secure multi-owner data sharing scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. [2]The simple algorithms are proposed for with O(n) time complexity using stream cipher and block cipher techniques with almost no space and communication overhead[3] Searchable symmetric encryption (SSE) allows a party to outsource the storage of its data to another party (a server) in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research in recent years. In this paper we show two solutions to SSE that simultaneously enjoy the following properties[4] Two variants of the basic scheme which differ in the efficiency of search and storage. [5] The scheme suitable with present IBE with no additional work for key generation and also allows multiple re-encryptions. [6]

III. SYSTEM DESIGN

In the proposed method , re encryption keys generated at user side using old keys and new keys are send to cloud storage server .Ciphertext is reencrypted using reencryption key before sending to receiver along with Attribute Based Encryption (ABE) Scheme, which derive keys from the hash of plaintext and Store it to server. While generating rencyprion key identity of user is used this is in addition

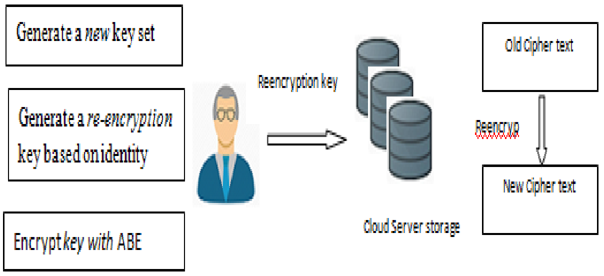

Fig. 2 Proxy Re Encryption Scheme Model

An identity based proxy Reencryption method along with Symmetric encryption scheme is used that backing proxy Reencryption in hybrid with ABE, Specifically, we implement a scheme using private encryption in which data will reencrypted using key generated based on user own identity .Proxy is an entity who works for reencryption. Adding a symmetric scheme to provides a facilty of process of reencryption in the cloud environment with their own attributes so no need or cost of any extra things.

User Authorization and Authentication

Proxy is an entity who provides user verification and approval. Signature constructed by proxy where an user gives credits of signing authority to proxy , and which continued by proxy Assume

User Rashmi [Sender – Initial Signer] with attested key Pair { PR_{Rashmi} & PU_{Rashmi} }

Proxy Entity P with valid Key Pair { PR_p & PUp }

Let RW be Rashmi's information document based on "warrant partial delegation scheme ", which has linguistic data including the authenticate signer's integrity, a few clues about the proxy entity (for example the identity), duration of delegation validity, the eligibility of messages on which the proxy signer can sign, etc

Now Rashmi sign with her own key PR_{Rashmi} on information document RW

Then Rashmi transmit that data to the Proxy Entity P for sign

This schemes adds integrity verification depending upon type of data storage systems, data dynamics is not possible. For complete and powerful design along with security it is important to integrate theses two components .Before uploading data which we refer as text, is converted into ciphertext based on Attribute based Encryption where key provided by data owner himself at both sides. Here cloud storage is acted as semi trusted server .At receiver side user along with attribute key and key provided by data owner decrypt the ciphertext to get original data. But the problem is with data integrity.

IV. ALGORITHM

New Registration for User/Owner

1. Enter all information about user/owner in given respective textbox.
2. Check email id is not existed.
3. Select type of user (user/owner).
4. Clicking on submit button it will store in cloud server storage.

Cloud Service Provider Authentication

1. On the CSP side CSP controls user authentication by using activate / deactivate action.
2. If user is active then that user can share data on the cloud or upload / download the data.
3. If user is deactivated then they could not share data on the cloud.

Encryption of Data (Upload file)

1. At the owner side select data file.
2. Generates AES key using owner identity value and master key.
3. Generates Re-encryption key using owner identity value and AES key.
4. Encrypt that data file using Cryptographic encryption method and AES key.
5. Then encrypted data and Re-encryption key send to the cloud server storage.

Re-encryption of Data

1. At the cloud proxy side fetch the ciphertext from database
2. Re-encrypt the data using Cryptographic encryption method and Re-encryption Key.
3. Store re-encryption data on the cloud server storage.

Decryption of Data (Download Data)

1. Check data is existed on cloud or not.
2. If Data existed then Fetch Re-encrypted data from cloud storage
3. Decrypt file using cryptographic decryption method and AES Key.

V. RESULTS & DISCUSSION

A. Performance Analysis

Here, performance of the system is evaluated by monitoring system when it is accessed by multiple users in Ethernet LAN with 100Mbps speed of underlying network and 2.87Mbps downloading, 3.61 uploading speed and the device configuration is 32-bit OS, x64-based Intel i3 processor with 2.27 GHz of processing speed.

Table. 1 Time analysis

System File size	Existing System	Proposed system
1 Mbps	250	175
5 Mbps	700	500
10 Mbps	1000	800
15 Mbps	1500	1000

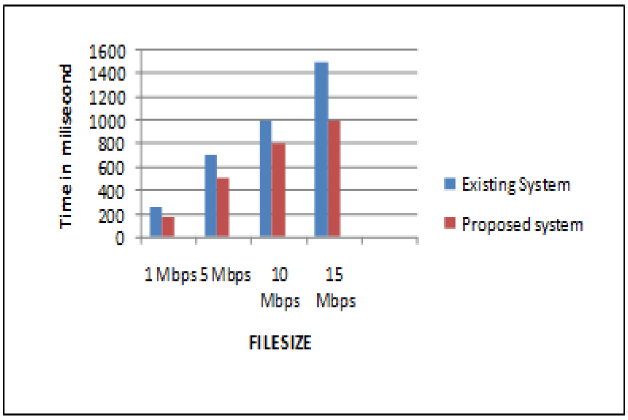

Fig. 3 Chart for Time Analysis

B. Security Module

Encryption techniques can be used for security of the cloud storage provider. Also, the security in between the CSP and the user can be improved by utilizing powerful key sharing and authentication processes. Providing Identity Based Key exposure resilient auditing scheme in the proposed system it shows more secure for cloud storage.

Table. 2 Security Analysis

System Security attacks	Existing System	Proposed System
Malicious Attack	60	10
Password Attack	40	4.4
Denial-of-service Attack	30	1.8
Malware Attack	20	2.8

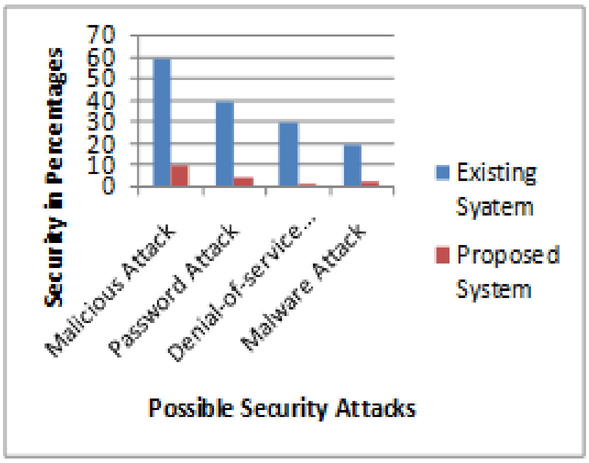

Fig. 4 Security Analysis chart

VI. CONCLUSION

In this system, providing guarantee towards distant cloud repository and advances the isolation by means of Proxy-Reencryption Scheme. In Identity based Proxy Reencryption (IBPRE) design user who holds can dominate distribution in a malleable way by using arbitrary ways encryption process. This scheme has an edge over the other and can be more accordingly used to some applications for comfortable sharing in protected cloud data environment. The advantage of this scheme is that it consumes communication cost and time of encryption and decryption method by proposing an attribute-based proxy re-encryption method in re-encryption of data in the cloud without loading any data

REFERENCES

1. Matt Blaze, Gerrit Bleumer, and Martin Strauss. Divertible protocols and atomic proxy cryptography. In Kaisa Nyberg, editor, EUROCRYPT'98, volume 1403 of LNCS, pages 127–144, Espoo, Finland, May 31 – June 4, 1998. Springer, Berlin, Germany.
2. Anca Ivan and Yevgeniy Dodis. Proxy cryptography revisited. In NDSS 2003, San Diego, California, USA, February 5–7, 2003. The Internet Society.

3. Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. In NDSS 2005, San Diego, California, USA, February 3–4, 2005. The Internet Society.
4. 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, vol. 9, no. 1, pages 1–30. 2006.
5. Yun-Peng Chiu, Chin-Laung Lei, and Chun-Ying Huang. Secure multicast using proxy encryption. In Sihan Qing, Wenbo Mao, Javier Lopez, and Guilin Wang, editors, ICICS 05, volume 3783 of LNCS, pages 280–290, Beijing, China, December 10–13, 2005. Springer, Berlin, Germany.
6. J. Shao, P. Liu, G. Wei, and Y. Ling. Anonymous proxy reencryption. Security and Communication Networks, vol. 5, no. 5, pp. 439-449, 2012.
7. Matthew Green, Giuseppe Ateniese Identity-Based Proxy Re-encryption, Proceeding ACNS '07 Proceedings of the 5th international conference on Applied Cryptography and Network Security, Pages 288 - 306 , Zhuhai, China — June 05 - 08, 2007
8. R.K.Dixit ,K.Ravindranath “Encryption techniques and access control model “,Internation journal of Engineering and Technology ,Vol. no. 7 – March 18
9. Sattar J Aboud and 2 Mohammad Al-fayoumi “PROXY SIGNATURE SCHEME FOR WARRANT PARTIAL DELEGATION” Pg No. 107 Vol 1