ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

Multi Attribute-Based Proxy Re-Encryption Method for Cloud Storage Security Improvement and Performance Strategies

K. Pushparaj M.Tech.,, C. Arul Johnsi,

Assistant Professor, Department of Computer Science and Engineering, Chenduran College of Engineering and Technology, Lena Vilaku, Pilivalam (po), Pudukkottai, Tamilnadu, India

M.E. Computer Science and Engineering, Department of Computer Science and Engineering, Chenduran College of Engineering and Technology, Lena Vilaku, Pilivalam (po), Pudukkottai, Tamilnadu, India

ABSTRACT: The main objective of this work is to improve the security towards remote cloud storage and improve the privacy by means of two norms such as Proxy-Reencryption Scheme and Multi-Attribute Based Encryption Logic. Attribute-based encryption (ABE) enables both data security and access control by defining users with attributes so that only those users who have matching attributes can decrypt them. ABE is used in hybrid with a symmetric encryption scheme such as the advanced encryption standard (AES) where data is encrypted with AES and the AES key is encrypted with ABE. The hybrid encryption scheme requires re-encryption of the data upon revocation to ensure that the revoked users can no longer decrypt that data. To re-encrypt the data, the data owner (DO) must download the data from the cloud, then decrypt, encrypt, and upload the data back to the cloud, resulting in both huge communication costs and computational burden on the DO depending on the size of the data to be re-encrypted. In this system, we propose an attribute-based proxy re-encryption method in which data can be re-encrypted in the cloud without downloading any data by adopting both ABE and Syalim's encryption scheme. This scheme reduces the communication cost between the DO and cloud storage and reduces the communication cost by as much as one quarter compared to that of the trivial solution.

KEYWORDS: Cloud service, Quality of service, Security modeling, Performance modeling.

I. INTRODUCTION

In 1998, Blaze, Bleumer and Strauss proposed the concept of proxy re-encryption (PRE), where a semi-trusted proxy can transform a ciphertext for Alice into another ciphertext that Bob can decrypt. However, the proxy can learn nothing about the corresponding plaintext. According to the direction of transformation, PRE schemes can be classified into two types, namely, bi-directional or uni-directional. A PRE scheme is called bidirectional if the proxy can use the reencryption key to divert ciphertexts from Alice to Bob and vice-versa. Otherwise, it is called unidirectional. In unidirectional PRE schemes, the proxy can only transform in one direction. Blaze et al. also gave another method to classify PRE schemes, called multiuse, i.e., the ciphertext can be transformed from Alice to Bob to Charlie and so on; and single-use, i.e., the ciphertext can be transformed only once. Due to its transformation property, PRE schemes can

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

be used in many applications, including simplification of key distribution, key escrow, distributed file systems, multicast, anonymous communication, DFA-based FPRE system, and cloud computation. Recently, the research of cloud email system has become more and more popular in business and organizations as it allows an enterprise to rent the cloud SaaS service to build an email system with less costs and maintenance efforts. Indeed, it is much cheaper and scalable than traditional on premises solution. However, these solutions have a common drawback: the grant of content sharing capability, which is achieved through the generation of re-encryption key.

Up to now, in all of the traditional identity based proxy re-encryption schemes, the generation of re-encryption key is generally divided into two ways: in uni-directional proxy re-encryption scheme, the key is generated by an authorized person A; in bi-directional scheme, it is generated by A and the recipient B. Recently, Wang et al. proposed a new scheme for the re-encryption key generation, where the key is generated by the sender S. This way has the advantage that the sender S can control the authorization granting process by using the random number, which is used in the encryption process to generate the proxy re-encryption key.

In this work, we propose a new identity based proxy re-encryption system. In the new identity based proxy encryption system, the re-encryption key is generated by the sender S, and the process of agency is controlled by S thoroughly. This method can avoid the flaw of the traditional proxy re-encryption, the sender S can control the people who can get the message and the sharing content of the messages.

II. SYSTEM IMPLEMENTATION

A. *Identity based ReEncryption Master*

This module introduces a new scheme called identity based proxy re-encryption system. In the new identity based proxy encryption system, the re-encryption key is generated by the sender S, and the process of agency is controlled by S thoroughly. This method can avoid the flaw of the traditional proxy re-encryption, the sender S can control the people who can get the message and the sharing content of the messages.

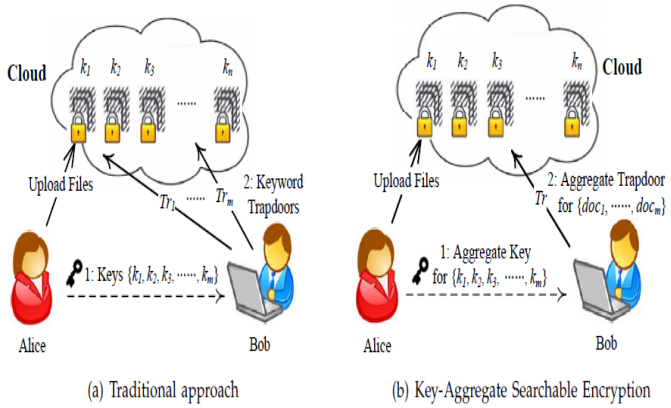

Fig.1 Secured Data Sharing over Cloud

B. *Intelligent Proxy ReEncryption Scheme*

This module can be seen as the dual of the traditional identity based proxy reencryption. In the scheme, the data owner can control sharing capability in a flexible way by using random numbers used in the encryption process. Compared to traditional identity based proxy re-encryption schemes, this scheme has some advantages, and can be more appropriately adapted to some applications for content sharing, such as secure cloud data sharing. Further, it would like

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

to explore other aspects, such as giving formal security proof for our proposal, proposing more efficient schemes and implement the schemes in real Cloud environments, etc.

C. Cloud Manipulation and Security Establishments

Cloud storage has emerged as a promising solution for providing ubiquitous, convenient, and on-demand accesses to large amounts of data shared over the Internet. Today, millions of users are sharing personal data, such as photos and videos, with their friends through social network applications based on cloud storage on a daily basis. Business users are also being attracted by cloud storage due to its numerous benefits, including lower cost, greater agility, and better resource utilization. However, while enjoying the convenience of sharing data via cloud storage, users are also increasingly concerned about inadvertent data leaks in the cloud. Such data leaks, caused by a malicious adversary or a misbehaving cloud operator, can usually lead to serious breaches of personal privacy or business secrets (e.g., the recent high profile incident of celebrity photos being leaked in iCloud).

III. LITERATURE SURVEY

Achieving Secure, Scalable, And Fine-Grained Data Access Control In Cloud Computing - S. Yu, C. Wang, K. Ren. [1] Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine-grained data access control is desired, and thus do not scale well. The problem of simultaneously achieving fine-grainedness, scalability, and data confidentiality of access control actually still remains unresolved.

This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents. We achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Our proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that our proposed scheme is highly efficient and provably secures under existing security models.

Secure Provenance: The Essential Of Bread And Butter Of Data Forensics In Cloud Computing - R. Lu, X. Lin. [2] Secure provenance that records ownership and process history of data objects is vital to the success of data forensics in cloud computing, yet it is still a challenging issue today.

In this paper, to tackle this unexplored area in cloud computing, we proposed a new secure provenance scheme based on the bilinear pairing techniques. As the essential bread and butter of data forensics and post investigation in cloud computing, the proposed scheme is characterized by providing the information confidentiality on sensitive documents stored in cloud, anonymous authentication on user access, and provenance tracking on disputed documents. With the provable security techniques, we formally demonstrate the proposed scheme is secure in the standard model.

Mona: Secure Multiowner Data Sharing For Dynamic Groups In The Cloud – X. Liu, Y. Zhang. [3] With the character of low maintenance, cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Unfortunately, sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud is still a challenging issue, due to the frequent change of the membership. In this paper, we propose a 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. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

revoked users. In addition, we analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments.

Practical Techniques For Searches On Encrypted Data - X. Song, D.Wagner. [4] It is desirable to store data on data storage servers such as mail servers and file servers in encrypted form to reduce security and privacy risks. But this usually implies that one has to sacrifice functionality for security. For example, if a client wishes to retrieve only documents containing certain words, it was not previously known how to let the data storage server perform the search and answer the query, without loss of data confidentiality. We describe our cryptographic schemes for the problem of searching on encrypted data and provide proofs of security for the resulting crypto systems. Our techniques have a number of crucial advantages.
They are provably secure: they provide provable secrecy for encryption, in the sense that the untrusted server cannot learn anything about the plaintext when only given the ciphertext; they provide query isolation for searches, meaning that the untrusted server cannot learn anything more about the plaintext than the search result; they provide controlled searching, so that the untrusted server cannot search for an arbitrary word without the user's authorization; they also support hidden queries, so that the user may ask the untrusted server to search for a secret word without revealing the word to the server. The algorithms presented are simple, fast (for a document of length n, the encryption and search algorithms only need O(n) stream cipher and block cipher operations), and introduce almost no space and communication overhead, and hence are practical to use today.

IV. SYSTEM ANALYSIS

A. Existing System

Revocation of users or their attributes is an indispensable feature of ABE for real-world applications. In real-world situations, users and their attributes change over time within the system. Existing revocation methods of ABE are proposed based on the notion of using ABE to encrypt the data entirely, whereas in actual implementations, hybrid encryption of ABE and symmetric encryption, specifically the advanced encryption standard (AES), are used for efficiency. In hybrid encryption, data is encrypted with AES and the AES key is encrypted with ABE. Because existing revocation methods affect only ABE ciphertext, this fact introduces a problem in which users can keep the AES key prior to revocation and use it to decrypt data even after the users are revoked. Therefore, although existing revocation methods can be applied to revoke users from ABE, re-encrypting data with a new AES key is necessary so that the old AES key can no longer be used.

DISADVANTAGES OF EXISTING SYSTEM

(a) Poor Security by means of Standard Password Generation technique for Encryption and Decryption.
(b) Insecure Authentication Principles.
(c) Easy to guess passwords.

B. Proposed System

In this proposed approach, we propose an attribute-based proxy Reencryption method for revocation in which the DO is no longer required to download any data for re-encryption. By using a symmetric encryption scheme that supports proxy Reencryption in hybrid with ABE, we can perform revocation in the cloud so that a revoked user will no longer be able to decrypt data after revocation. By using a symmetric proxy re-encryption scheme, the data can be reencrypted in the cloud without revealing any data to the cloud. Therefore, in the revocation step, sending only the re-encryption keys and ABE ciphertext to the cloud is required, thus reducing the communication cost between the DO and cloud. Because the re-encrypted ciphertext is encrypted under a completely new set of keys, users cannot decrypt data even if they keep the old symmetric keys or parts of the old ciphertext.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

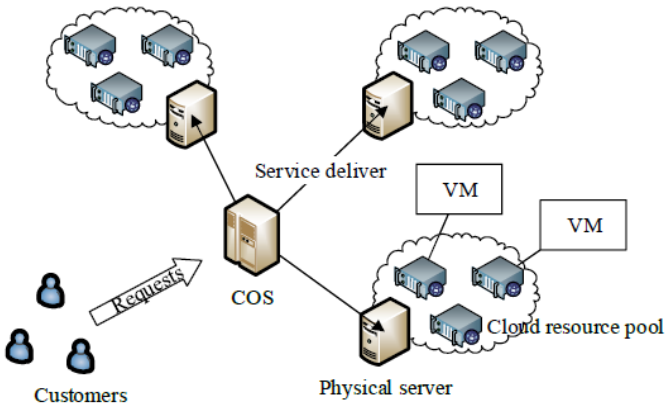

Fig.2 System Architecture

ADVANTAGES OF PROPOSED SYSTEM

(a) High Security establishments by means of Identity based Proxy Encryption Methodology as well as Password Generation technique is based on IBE principles for Encryption and Decryption, so it is highly secured compare to other classical schemes.
(b) Secure Authentication Principles, which generates the password systematically and send to users for precedence, so it is non-guessable.

V. RESULTS AND DISCUSSION

In this section, we provided the simulated results of entire project with its practical proofs. The following figure illustrates the Home Page of the Proposed System.

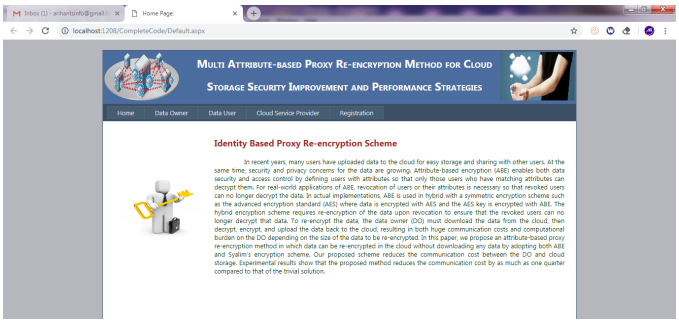

Fig. 3 Home Page

The following figure illustrates the Registration Details of the proposed system.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

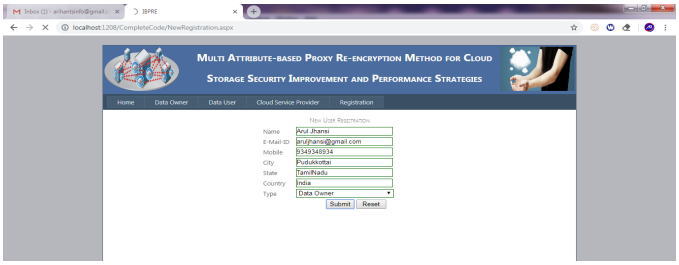

Fig.4 Registration

The following figure illustrates the CSP Authentication Page of the proposed system.

Fig.5 CSP Authentication

The following figure illustrates the View Data User portal of the proposed system.

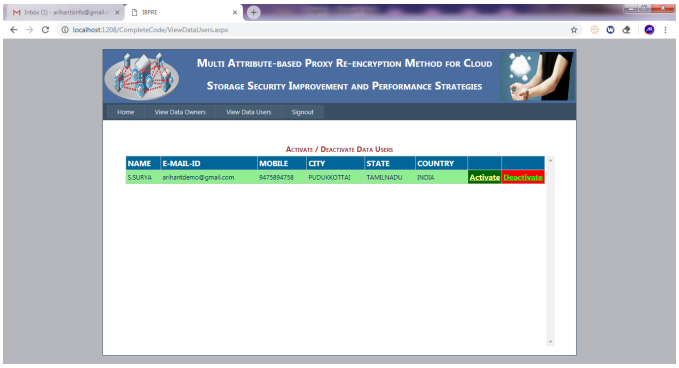

Fig.6 View Data Users

VI. CONCLUSION AND FUTURE SCOPE

In this system, a hierarchical modeling approach and a correlation metric are proposed to study the impact of the security (i.e., malicious attack and security mechanism) on the service performance. The presented modeling approach builds the connection between the security and the service performance through two critical factors. Moreover, the significant impact of different factors, including the security mechanism and service rate on the performance are analyzed through experiments. Experimental results demonstrate that: (a) When the CCS faces serious security issues, redundancy is the easiest and most workable way to improve the service performance. (b) High security is not always

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

the best choice at any moment. (c) When the amount of resources is limited, the correlation between the service performance and the security is inverse.

In future work, we will explore the relevant optimal scheduling algorithms based on this modeling approach to better support service-oriented computing.

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] K. Liang, M. H. Au, J. K. Liu, X. Qi, W. Susilo, X. P. Tran, D. S.Wong, and G. Yang. A dfa-based functional proxy reencryption scheme for secure public cloud data sharing. IEEE Transactions on Information Forensics and Security, vol. 9, no. 10, pp. 1667-1680, 2014.
[8] Kaitai Liang, Joseph K. Liu, Duncan S. Wong, and Willy Susilo. An efficient cloud-based revocable identity-based proxy reencryption scheme for public clouds data sharing. In Miroslaw Kutylowski and Jaideep Vaidya, editors, ESORICS 2014, Part I, volume 8712 of LNCS, pages 257–272, Wroclaw, Poland, September 7–11, 2014. Springer, Berlin, Germany.
[9] Ying Wang, Jiali Du, Xiaochun Cheng, Zheli Liu, and Kai Lin. Degradation and encryption for outsourced png images in cloud storage. International Journal of Grid and Utility Computing, vol. 7, no. 1, pp. 22-28, 2016.
[10] Shuaishuai Zhu and Xiaoyuan Yang. Protecting data in cloud environment with attribute-based encryption. International Journal of Grid and Utility Computing, Vol. 6, No. 2, pp. 91-97, 2015.
[11] Shu Guo and Haixia Xu. A secure delegation scheme of large polynomial computation in multi-party cloud. International Journal of Grid and Utility Computing, Vol. 6, No. 2, pp. 1-7, 2015.
[12] Cristina Dutu, Elena Apostol, Catalin Leordeanu, and Valentin Cristea. A solution for the management of multimedia sessions in hybrid clouds. International Journal of Space-Based and Situated Computing, Vol. 4, No. 2, pp. 77-87, 2014.
[13] Meriem Thabet, Mahmoud Boufaida, and Fabrice Kordon. An approach for developing an interoperability mechanism between cloud providers. International Journal of Space-Based and Situated Computing, Vol. 4, No. 2, pp. 88-99, 2014.
[14] Lihua Wang, Licheng Wang, Masahiro Mambo, and Eiji Okamoto. Identity-based proxy cryptosystems with revocability and hierarchical confidentialities. In Miguel Soriano, Sihan Qing, and Javier Lopez, editors, ICICS 10, volume 6476 of LNCS, pages 383–400, Barcelona, Spain, December 15–17, 2010. Springer, Berlin, Germany.
[15] Xu An Wang, Yunlong Ge, and Xiaoyuan Yang. PRE+: Dual of proxy re-encryption and its application. Cryptology ePrint Archive, Report 2013/872, 2013. http://eprint.iacr. org/2013/872.