International Journal of Computer Science and Engineering Communications
Vol.3, Issue 3, 2015, Page.1069-1075
ISSN: 2347–8586
www.scientistlink.org

An Efficient Re-encryption Scheme for Secure and Scalable Data Storage in Cloud

[1]V. Monishaa, [2]N.R. Rejin Paul
[1] PG Student, [2]Assistant Professor
Department of CSE, Velammal Institute of Technology, Chennai, India,
v.aishmon@gmail.com ,nrrejinpaul@gmail.com

Abstract: Cloud computing confers strong economic advantages, but many clients are reluctant to implicitly trust a third-party cloud provider. Cloud provider is also not directly entrusted with key material, but naive schemes often prove difficult to scale. The confidentiality of data stored in cloud platform must be protected from being read in the clear by cloud provider. This work focuses on the Improvement of existing traditional attribute-based encryption scheme to allow only authorized users to access the cloud data based on possession of right attributes and also a model based on the principle of dynamic data re-encryption is applied, to a cloud computing system in a unique way to provide more security to the user data stored. The idea is proposed to be efficient for resource-constrained mobile users by delegating computation and requests to a cloud provider or trusted authority, without compromising security. Also, a backup of stored data is done by a separate server accompanied by an automated auditing service while retrieving to support exact delivery of data.

Keywords

Mobile Computing, Based Encryption, Cryptography, Scalability, Secure Communication.

1. Introduction

CLOUD computing offers the advantages of highly scalable and reliable storage on third-party servers. Its economical pay-per-use model typically results in a small fraction of the cost of deploying the same computing resources in-house. Outsourcing data to the cloud are beneficial for reasons of economy, scalability, and accessibility, but significant technical challenges remain. Sensitive data stored in the cloud may be read by a cloud provider without the knowledge of the client.

A cloud administrator may not be trusted despite the presence of contractual security obligations, if data security is not further enforced through technical means. An additional risk is that sensitive data may be intercepted by an unauthorized party despite safeguards promised by the provider. In short, although outsourcing data to the cloud is economically attractive for long-term large-scale storage, it does not immediately offer any guarantee on data integrity and confidentiality. Therefore, it is necessary to ensure the users that the confidentiality of their data stored in cloud is preserved at all times. Also, any protocol providing additional security must not add burdensome costs to users those who access cloud applications via resource-constrained mobile devices such as smartphones and tablets; specifically, the number of transmissions and the amount of computation must be minimized. Another important requirement is for data to be addressable with fine-grained access controls on the record-level or finer, to provide flexibility. A single user log-in is largely insufficient in today's complex data retrieval tasks.

The main contributions of the proposed work are as follows:

1. A protocol for secured storage of outsourced data in cloud provider is provided. The provider is prevented from reading sensitive data stored; only authorized users may do so based on qualification through possession of the right attributes without arbitration by the data owner. The protocol is designed to be efficient for resource-constrained mobile users by delegating computation and requests to a cloud provider or trusted authority, where appropriate, without compromising security.

2. An improvement is made over a traditional attribute-based encryption scheme, such that responsibility over key generation is divided between a mobile data owner and a trusted authority; the owner is relieved of the highest computational and messaging burdens.

3. Additional security is provided through a group keying mechanism; the data owner controls access based on the distribution of an additional secret key, beyond possession of the required attributes. This additional security measure is an optional variant applicable to highly sensitive data subject to frequent access.
4. Re-encryption process administered by a trusted authority without involvement of the data owner permits efficient revocation of users; provides more security to the cipher text from CSP.
5. Additionally, automatic backup of cipher text is performed; supports exact delivery of data while retrieving.
In Section 2, related work on proposed protocol schemes is presented. In Section 3, the proposed algorithm for attribute-based encryption and re-encryption suitable for mobile users of the cloud is presented. In Section 4, detailed explanation about each module is presented.

2. Related Work

The technique of ciphertext-policy attribute-based encryption (CP-ABE) **[3]** offers numerous advantages. It allows a user to obtain access to encrypted data in the cloud based on the possession of certain attributes determined in advance by data owners. These pre-determined attributes satisfy an access structure defined in the cloud, rather than the possession of a key **[4]** that must be disseminated to all interested parties in advance. This scheme based on CP-ABE relies upon the data owner granting access permission through an access tree, does not require his or her constant availability.
Our related work proposes the merging of ABE with proxy re-encryption, allowing fine-grained access control of resources while offloading re-encryption activity to the cloud provider **[4]**. It has numerous differences to the scheme that will be proposed. The data owner is involved in generating a key for each new user that joins or leaves the system, rather than offloading this task; it is not only a prohibitive cost for a mobile user, but also impractical due to the user's mobility. Another difference is that a secret key must be regenerated and redistributed for each user, in lazy fashion, whenever user revocation occurs, rather than allowing users to upgrade a common group key, which reduces the communication cost and results in higher efficiency. Furthermore, the re-encryption occurs due to attribute redefinition and the scheme is based on key-policy attribute-based encryption (KP-ABE) and not CP-ABE, where the ciphertext is associated with a policy.
A multiauthority system has been proposed **[5]** that uses attribute-based access control to avoid the single point of failure of a single key authority, and relies upon the data owner communicating with attribute authorities to generate multiple encryption keys for hosted content. The costs of communicating with multiple authorities and storing multiple keys could become prohibitive for mobile users. Li *et al.* **[6]** proposed an attribute revocation method for multi-authority ABE systems, but their methods are only for KP-ABE systems. In a related work **[6]**, each user submits multiple secret keys issued by authorities to a server to generate a decryption token for each ciphertext that is used in concert with the user's global secret key to perform a decryption. The same costs associated with multiple authorities apply, however, and such authorities complicate and add to the expense of system engineering. The authors are unaware of a similar scheme where fine-grained operations in attribute-based cryptography have been reassigned across system components to minimize the workload of mobile users; nor are other techniques found with performance benchmarked on commercial mobile and cloud systems, as herein, useful in assessing real-world viability.

3. Proposed Model

In this section, we describe the system model for a secure storage of data in cloud provider.

3.1. System model

The system model of the proposed work is shown in Figure 1.
A mobile user may act as *data owner* and decide the access privileges for the data that he/she uploads to the cloud by specifying the attributes that inherently grants permission. The *Manager* is a trusted authority situated behind an organization's firewall and form a part of private cloud belonging to the client; it is completely independent of the CSP; considered fast and scalable. It may maintain a database of private key information relating to set of authorized mobile users. Inside the cloud, the ciphertext of user data is stored. This user data may periodically undergo cryptographic transfo-rmation, such as re-encryption from one version of cipher text to another.

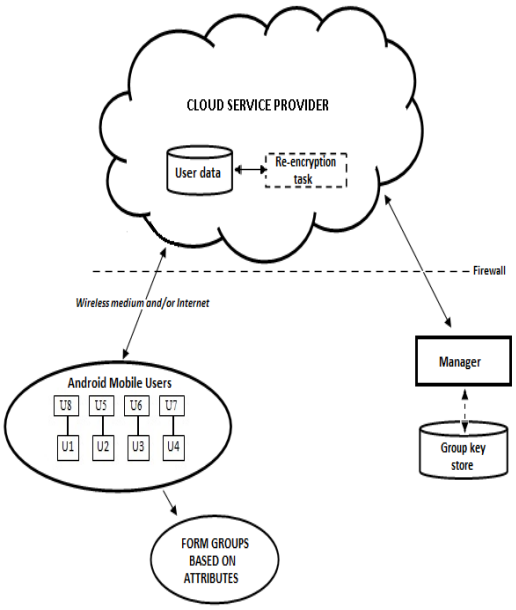

Figure 1. System Model

A highly scalable system envisioned, where users may number potentially in more numbers.

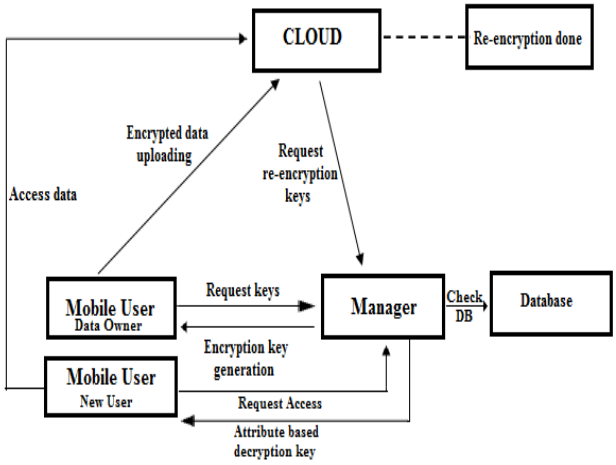

Figure 2. Block Diagram of Proposed System

Possible applications of the secure data outsourcing approach suggested here include highly collaborative enterprise services, secure data storage and retrieval, and social networks.

3.2. Trust Model

The cloud provider will generally obey a communications protocol will not deny service to any authorized party. At the same time, a cloud administrator may read or modify the contents of user data stored in the cloud without the knowledge of client for nefarious reasons. Thus, data stored in the cloud should remain encrypted at all times, and any required transformation of it should not reveal the plaintext in the process.

The manager is a trusted authority within the system and is administered under the domain of the users in question; it is completely independent of the CSP. It is sufficiently trusted to authorize access to the cloud and to contain key material as necessary; however, to minimize the risk of it being compromised, a user will only share as much of its own key material with the manager as is necessary in the security scheme utilized. Additionally backup of the stored ciphertext accompanied with an auditing service while retrieving supports exact delivery of the data.

International Journal of Computer Science and Engineering Communications
Vol.3, Issue 3, 2015, Page.1069-1075
ISSN: 2347–8586
www.scientistlink.org

4. Proposed Algorithm

The proposed algorithm for user data encryption, re-encryption, and key generation is now described.

- Improvements are proposed to the basic functions of the original CP-ABE scheme.
- The mobile data owner and cloud entity co-operate to jointly compute keys; reduces the amount of computation for data owner.
- Proxy-based re-encryption has been integrated with CP-ABE so that the cloud provider may perform automatic data re-encryption; prevents the cloud provider to decode the user data that it permanently stores; permits efficient revocation of users. This dual-encryption scheme is a hybrid approach combining cryptographic techniques that offers greater flexibility in access control.
- The Key generation operation proposed is performed by manager; reduces communication cost for the users. The proposed technique is now described as follows:

Preliminary: Any mobile user that acts as the self-elected data owner ***U0*** of plaintext message *m*, which is user data that are desired to be encrypted and shared in the cloud may wish to protect their shared data.To protect the highly sensitive data, the encryptor restricts user membership requirements based on possession of right attributes A.

4.1. Encryption

A Manager acts as a trusted entity; computes a symmetric key ***K0*** to encrypt the owner's data. The encrypted cipher text ***C0*** is uploaded in the cloud; meanwhile the backup of stored cipher text is performed at the backup memory.

TABLE 1. Comparison of Proposed Algorithm to Related Work

Characteristic	**Protocol in [4]**	**Protocol in [5]**	**Protocol in [6]**	**Protocol herein**
System model:	Owner, CSP	Owner, Multiple Authorities	Owner, Authority	Owner, Manager, CSP
Cryptographic technique	KP-ABE (requiring access structure for user)	ABE	Attribute- Based Cryptography	CP-ABE + Proxy Re-encryption
Participating actors in user data encryption task	Data owner	Data owner, Attribute authorities	Multiple Authorities	Data owner, Manager, CSP jointly (to offload owner's computation)
Participating actors in user re-encryption keygen task	Data owner	—	—	Data owner or Manager, by delegation

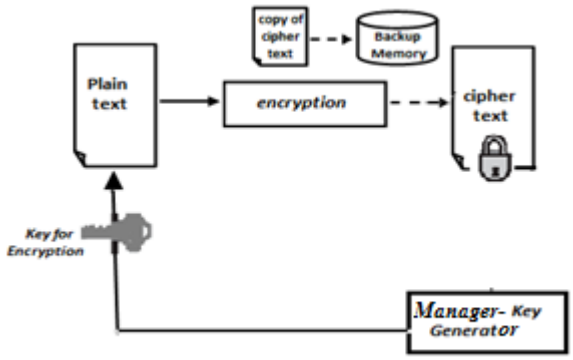

Figure 3. Encryption

The encryption algorithm takes as input the key ***K0*** and encrypts a message *m* as follows:

$$C0 = K0(m)$$

The Manager may create a group public key K0; this key is a shared secret key for restricted subset of users Ur, which is distributed to each user on demand. (manager shares this secret key based on attributes)

4.2. Re-Encryption

Whenever a user leaves the authorized membership of restricted user group ***Ur***, the user's access rights to the ciphertext must be revoked. When this occurs, a new version ***Kx*** of the secret group key GSK is normally distributed by the manager to the remaining authorized users in restricted user group based on demand through a secure offline channel whenever data access is required. The CSP is then requested to perform a re-encryption operation on demand so that its stored ciphertext can no longer be decoded using the prior version of the key.

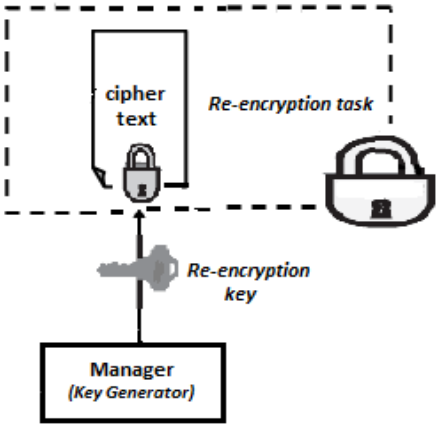

Figure 4. Re-Encryption

The ciphertext is re-encrypted from one version ***C0*** to another version ***Cx***, given a re-encryption key ***RK0→x*** transmitted by the manager.

$$Cx = RK0 \rightarrow x\ (K0(m))$$

The CSP is unable to decode the ciphertext during the re-encryption process as it has no knowledge of the old key ***K0*** and the new key ***Kx***.

4.3. Key Generation

Irrespective of which party performed the encryption, the manager executes a data secret key(DSK) generation algorithm that takes as input the set of attributes to decrypt the ciphertext. The data owner is not involved in the key generation and need not remain available at that time. The manager distributes a DSK to each authorized user holding the required attributes, without requiring the participation of the data owner.

4.4. Decryption

Any user that is authorized, by virtue of holding the required attributes, may download the ciphertext C from the cloud and decrypt it, as the recipient. The decryption routine takes as input the ciphertext and data secret key DSK obtained from the manager. If the access tree is satisfied by attributes A(that determined the data secret key DSK); and if the ciphertext is optionally encoded with the public key ***K0*** of the restricted user group Ur, then the recipient may utilize the secret key ***Kx*** to decrypt the downloaded ciphertext.

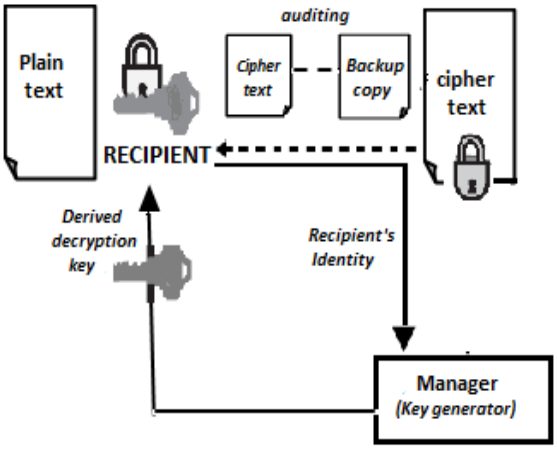

Figure 5. Decryption

The message *m* can be decrypted as follows:

$$m = K_x(C_x)$$

During decryption process, while downloading the ciphertext from cloud, auditing is performed [in terms of bytes] at the back-end for the exact delivery of data.

5. Discussion

5.1. Security Analysis

The proposed scheme offers a dual level security by combining CP-ABE with Proxy re-encryption Scheme.

In this case, the encryptor of a message may restrict its eligible leadership by selecting a required set of attributes; only the users possessing the required attributes will be distributed with shared secret key inorder to access the stored ciphertext. Furthermore, Proxy Re-encryption inside the cloud environment is a very high level security as it just transforms ciphertext from one form to another; to prevent any third party attackers or the provider to read the ciphertext stored inside it. At all times, the interception of any key components over the network will not yield useful information to the attacker, as no private keys are transmitted in the clear.

5.2. Performance Analysis

The data owner must only perform exponentiation operations during its key generation phases, while the manager performs the more expensive pairing operation. The keys are efficiently managed and distributed by the manager.

6. Conclusion and Open Directions

A system has been proposed for secure data outsourcing applications, that permits only authorized users to access secure content in the cloud based on the possession of right attributes; reduces the computation and communication cost for data owner by delegating the operation of key distribution to the manager. Additionally, the system allows re-encryption to occur for providing more security to sensitive data stored in the cloud environment. Furthermore, the system proposed promises exact delivery during retrieval of data. One limitation of our proposed system is that it is proved secure under the generic group heuristic. An important endeavour would be to prove a system secure under a more standard and non-interactive assumption.

References

[1] P.K. Tysowski and M.A. Hasan, "Hybrid Attribute-Based Encryption and Re-Encryption for Scalable Mobile Applications in Clouds," Technical Report 13, Centre for Applied Cryptographic Research (CACR), Univ. of Waterloo, 2013.

[2] Piotr.K. Tysowski and M. Anwarul. Hasan, "Hybrid Attribute and Re-Encryption-Based Key Management for Secure and Scalable Mobile Applications in Clouds," IEEE Transactions on Cloud Computing (DEC'13), pp. 172-185, 2013.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy (SP '07), pp. 321-334, 2007.

[4] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM '10, pp. 534-542, 2010.

[5] K. Yang and X. Jia, "Attributed-Based Access Control for Multi-Authority Systems in Cloud Storage," Proc. IEEE 32nd Int'l Conf. Distributed Computing Systems (ICDCS), pp. 536-545, 2012.

[6] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attributebased encryption," *IEEE Trans. Parallel Distrib. Syst.*, 2012.

[7] J. Hur and D.K. Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.

[8] K. Yang, X. Jia, K. Ren, and B. Zhang, "DAC-MACS: Effective DataAccess Control for Multi-Authority Cloud Storage Systems," Proc. IEEE INFOCOM, pp. 2895-2903, 2013.

[9] G. Zhao, C. Rong, J. Li, F. Zhang, and Y. Tang, "Trusted Data Sharing over Untrusted Cloud Storage Providers," Proc. IEEE Second Int'l Conf. Cloud Computing Technology and Science (CLOUDCOM '10), pp. 97-103, 2010.

[10] P.K. Tysowski and M.A. Hasan, "Towards Secure Communication for Highly Scalable Mobile Applications in Cloud Computing Systems," Technical Report 33, Centre for Applied Cryptographic Research (CACR), Univ. of Waterloo, 2011.