International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

Two Dimensional Security in Cloud Data Sharing with Factor Revocability Mechanism

E. Dhivyaprabha, B. Goutham Sabaries, T. R. Dharanish, R. Srikanth, N. Sathya Nackiran
Sri Krishna College of Technology/Computer Science & Engineering Department, Coimbatore, Tamil Nadu, India

ABSTRACT

In the two dimensional security in cloud data sharing with factor revocability mechanism. This system allows a sender to send an encrypted message to a receiver through a cloud storage server. The sender only needs to know the identity of the receiver but no other information (such as its public key or its certificate). The receiver needs to possess two things in order to decrypt the cipher text. The first thing is his/her secret key stored in the computer. The second thing is a unique personal security device which connects to the computer. It is impossible to decrypt the cipher text without either piece. More importantly, once the security device is stolen or lost, this device is revoked. It cannot be used to decrypt any cipher text. This can be done by the cloud server which will immediately execute some algorithms to change the existing cipher text to be un-decryptable by this device. This process is completely transparent to the sender. Furthermore, the cloud server cannot decrypt any cipher text at any time. The security and efficiency analysis show that our system is not only secure but also practical.

Keywords : Cloud Storage, Data Sharing, Key-Aggregate Encryption And Decryption, Device Revocation

I. INTRODUCTION

Cloud storage is gaining popularity recently. In enterprise settings, we see the rise in demand for data outsourcing, which assists in the strategic management of corporate data. CLOUD storage is a model of networked storage system where data is stored in pools of storage which are generally hosted by third parties. There are many benefits to use cloud storage. The most notable is data accessibility. Data stored in the cloud can be accessed at any time from any place as long as there is network access. Storage maintenance tasks, such as purchasing additional storage capacity, can be offloaded to the responsibility of a service provider. Another advantage of cloud storage is data sharing between users. If Alice wants to share a piece of data (e.g., a video) to Bob, it may be difficult for her to send it by email due to

the size of data. Instead, Alice uploads the file to a cloud storage system so that Bob can download it at anytime. Despite its advantages, outsourcing data storage also increases the attack surface area at the same time. For example, when data is distributed, the more locations it is stored the higher risk it contains for unauthorized physical access to the data. By sharing storage and networks with many other users it is also possible for other unauthorized users to access your data. This may be due to mistaken actions, faulty equipment, or sometimes because of criminal intent. A promising solution to offset the risk is to deploy encryption technology. Encryption can protect data as it is being transmitted to and from the cloud service. It can further protect data that is stored at the service provider. Even there is an unauthorized adversary who has gained access to the cloud, as the data has been encrypted, the adversary cannot get any information about the plaintext. Asymmetric encryption allows the encryptor to use only the public information (e.g., public key or identity of the receiver) to generate a cipher text while the receiver uses his/her own secret key to decrypt. This is the most convenient mode of encryption for data transition, due to the elimination of key management existed in symmetric encryption. It is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including

data storage space, networks, computer processing power, and specialized corporate and user applications.

II. METHODS AND MATERIAL

1. Key Aggregate Cryptosystem

Key-aggregate system, user can covert a plain text or encrypt a message using a public-key and the ids of the cipher text classes called class the cipher text classes are divided into different divisions. Data owner's has a secret that are called masters-secret key which has the collection of other keys and it holds as a single key it provides high security for the keys and the keys can be easily retrieval. The secret key is an aggregate key which has compact and similar to extract key for a single class the extract key is used to extract the keys for different set of classes. The extract key is an aggregate key which is compact and similar to the secret key for a single class; it aggregates power of their keys. A key-aggregate encryption cryptosystem includes five algorithmic steps such as Setup, KeyGen, Extract, Encrypt, Decrypt, in which the owner establishes the parameter by using Setup and generates the public /masters key pair by using Key Generation. Files are encrypted using Encrypt. The owner uses their provided secret keys to provide a Decryption key for a cipher text classes that are produced by Extract. The provided keys are sending to the data Receivers safely through their mails. Those User having an aggregate key uses the key files for decryption through cipher text using Decrypt.

A. Symmetric Key Encryption:

Symmetric key encryption, the encryption and decryption keys are similar data owner wants to share data to the other party and then they should give their secret keys to the encryptions.

B. Asymmetric Key Encryption:

The key produced by asymmetric encryption for both encrypt and decrypt are different. These encryption methods are used for many applications.

C. System Architecture:

Data owner encrypted and stores the files in cloud storage. According to the Data Requester the files are to be decrypt using aggregate key. The files are to be selected and store in cloud using their id and the password if the user is valid it will allow the user to store and retrieve the file.

The user login into the cloud the user will select the files that are to be uploaded. The files are uploading using the different keys to be encrypted. The master secret key and the symmetric key are to generate the secret keys. Using their keys user will decrypt the file. The single keys are generated for the different file the combination of key are to make the single aggregate Key. According to the user the files that they needed are to be decrypt using the aggregate key. The aggregate has the cipher text and the message and index and the set of indexes are combined together.

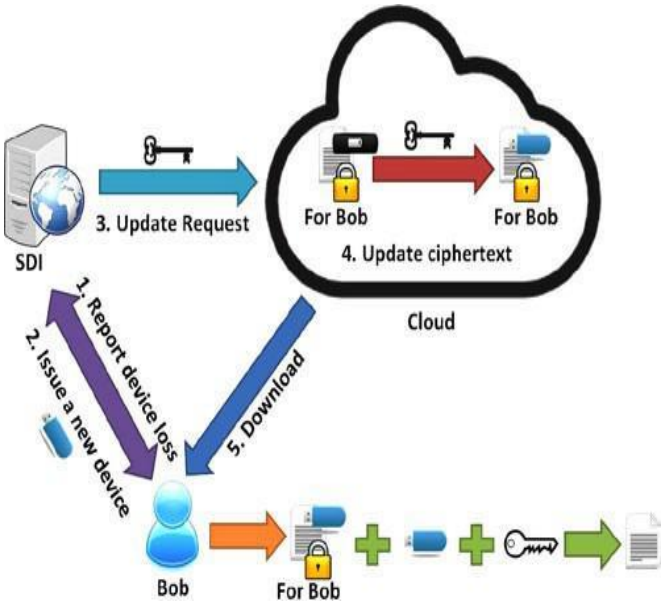


Figure 1 (a) : Ordinary Data Sharing

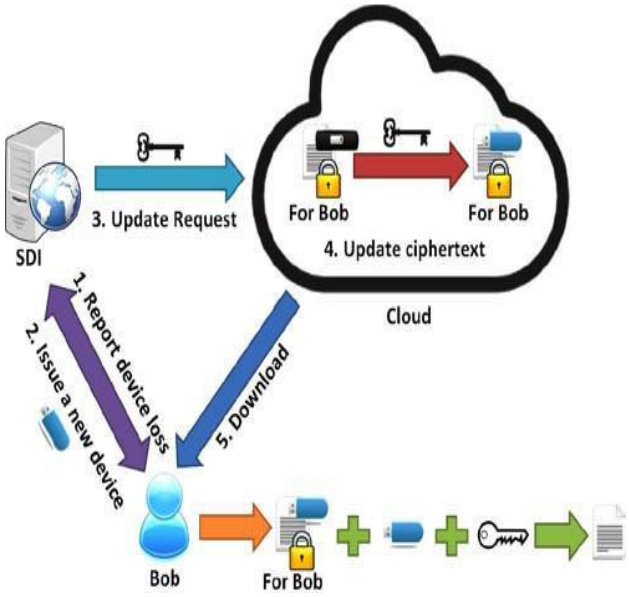


Figure 2 (b): Update ciphertext after issuing a new security device

2. Existing System

Data sharing is an important functionality in cloud Storage. For example, bloggers can let their friends view a subset of their private pictures; an enterprise may grant her employees

access to a portion of sensitive data. The challenging problem is how to effectively share encrypted data. Of course users can download the encrypted data from the storage, decrypt them, then send them to others for sharing, but it loses the value of cloud storage. Users should be able to delegate the access rights of the sharing data to others so that they can access these data from the server directly. However, finding an efficient and secure way to share partial data in cloud storage is not trivial. Transferring these secret keys inherently requires a secure channel, and storing these keys requires rather expensive secure storage. Now days the data sharing can be accessible with the asymmetric key encryption only Like Private key and public Key mechanism.

Disadvantages of Existing System:

1. If the user has lost his/her security device, then his/ her corresponding ciphertext in the cloud cannot be decrypted forever! That is, the approach cannot support security device update/revocability.
2. The sender needs to know the serial number/ public key of the security device, in additional to the user's identity/public key. That makes the encryption process more complicated.

3. Proposed System

The proposal is a novel two-factor security protection mechanism for data stored in the cloud. Our mechanism provides the following nice features: 1) Our system is an IBE (Identity-based encryption)- based mechanism. That is, the sender only needs to know the identity of the receiver in order to send an encrypted data (cipher text) to him/her. No other information of the receiver (e.g., public key, certificate etc.) is required. Then the user needs to possess two things. First, the user needs to have his/her secret key which is stored in the computer. Second, the user needs to have a unique personal security device which will be used to connect to the computer (e.g., USB, Bluetooth). It is impossible to decrypt the cipher text without either piece. 2) More importantly, our system, for the first time, provides security device (one of the sender sends the cipher text to the cloud where the receiver can download it at anytime. 3) Our system provides two-factor data encryption protection. In order to decrypt the data stored in the cloud, the factors) revocability.

III. RESULTS AND DISCUSSION

MODULES
The implementation has 5 Modules,
Private Key Generator
Security Device Issuer
Sender Module
Receiver Module
Cloud Server

A. Module Description

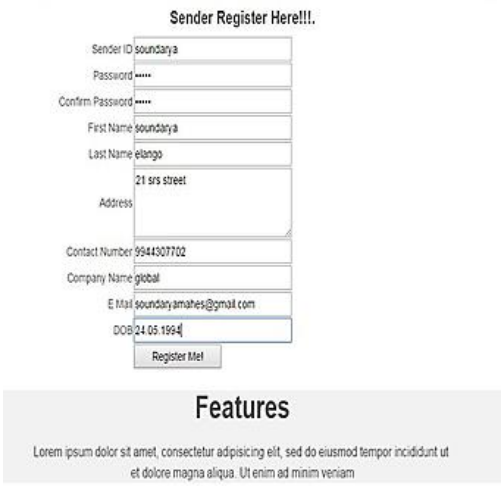
1) **Private Key Generator:**

It is a trusted party responsible for issuing private key of every user. **Key generation** is the process of generating keys in cryptography. A key is used to encrypt and decrypt whatever data is being encrypted/decrypted.

2) Security Device Issuer (SDI):

It is a trusted party responsible for issuing security device of every user. A secure device is issued to each user who are registered on the cloud. This device is used to verify the user for storing and downloading the files from the cloud storage.

3) Sender:



The sender (and the creator) of the cipher text only knows the identity (e.g., email address) of the receiver but nothing else related to the receiver. After the user has created the cipher text, they send to the cloud server to let the receiver for download.

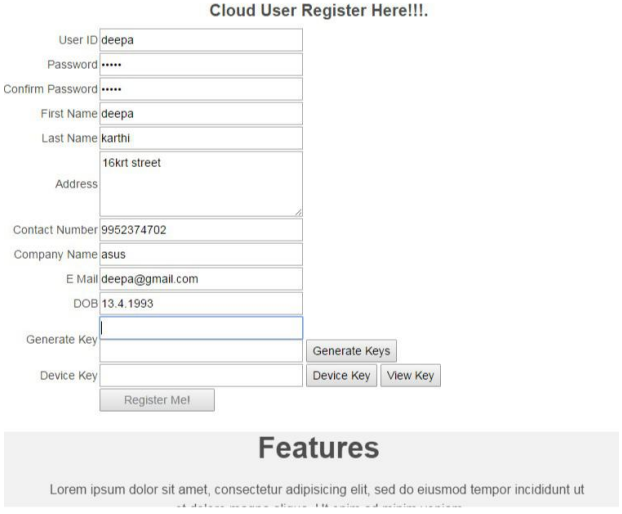


Figure 2

4) Receiver

The receiver of the cipher text has a unique identity (e.g., email address). The cipher text is stored on cloud storage while the user can download it for decryption. The receiver has a private key (stored in his computer) and a security device (that contains some secret information related to his identity). They are given by the PKG. The decryption of cipher text requires both the private key and the security device.

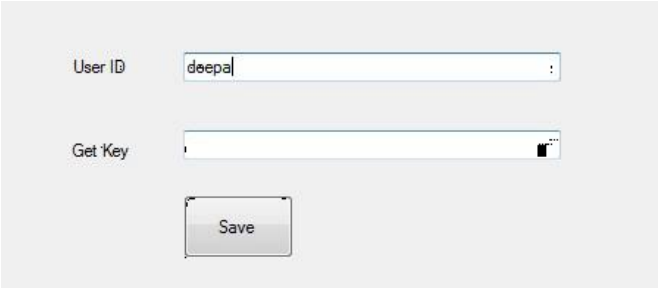


Figure 3

5) **Cloud Server**

The cloud server is responsible for storing all cipher text (for receiver to download). Once a user has reported lost of his/her security device (and has obtained a new one from the PKG), the cloud acts as a proxy to re-encrypt all his past and future cipher text corresponding to the new device. That is, the old device is revoked.

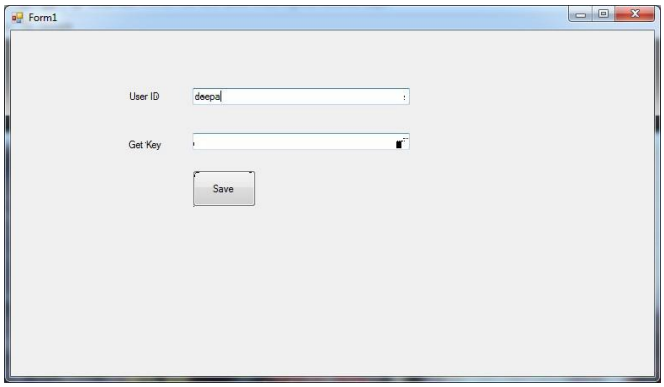


Figure 4

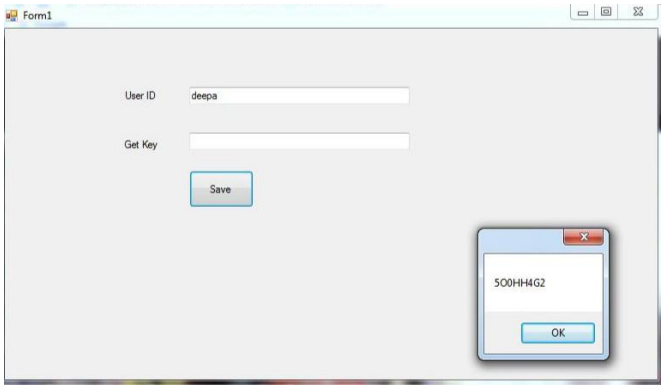


Figure 5

IV.CONCLUSION

We introduced a novel two-factor data security protection mechanism for cloud storage system, in which a data sender is allowed to encrypt the data with knowledge of the identity of a receiver only, while the receiver is required to use both his/her secret key and a security device to gain access to the data. Our solution not only enhances the confidentiality of the data, but also offers the revocability of the device so that once the device is revoked, the corresponding cipher text will be updated automatically by the cloud server without any notice of the data owner. Furthermore, we presented the security proof and efficiency analysis for our system.

V. REFERENCES

[1]. A. Akavia, S. Goldwasser, and V. Vaikuntanathan, "Simultaneous hardcore bits and cryptography against memory attacks," in Proc. 6th Theory Cryptography Conf., 2009, pp. 474–495.

[2]. S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in Proc. 9th Int. Conf. Theory Appl. Cryptol., 2003, pp. 452–473.

[3]. M. H. Au, J. K. Liu, W. Susilo, and T. H. Yuen, "Certificate based (linkable) ring signature," in Proc. Inf. Security Practice Experience Conf., 2007, pp. 79–92.

[4]. M. H. Au, Y. Mu, J. Chen, D. S. Wong, J. K. Liu, and G. Yang, "Malicious KGC attacks in certificateless cryptography," in Proc. 2nd ACM Symp. Inf., Comput. Commun. Security, 2007, pp. 302–311.

[5]. M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., 1998, pp. 127–144.

[6]. A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proc. ACM Conf. Comput. Commun. Security, 2008, pp. 417– 426.

[7]. D. Boneh, X. Ding, and G. Tsudik, "Fine-grained control of security capabilities," ACM Trans. Internet Techn., vol. 4, no. 1, pp. 60–82, 2004.

[8]. D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in Proc. 21st Annu. Int. Cryptol. Conf., 2001, pp. 213–229.

[9]. R. Canetti and S. Hohenberger, "Chosen-ciphertext secure proxy re-encryption," in Proc.

ACM Conf. Comput. Commun. Security, 2007, pp. 185–194.

[10]. H. C. H. Chen, Y. Hu, P. P. C. Lee, and Y. Tang, "NCCloud: A network- coding-based storage system in a cloud-of-clouds," IEEE Trans. Comput., vol. 63, no. 1, pp. 31–44, Jan. 2014.