IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

Improved Data Security Protection Mechanism for Cloud Storage using Two Factors

Ravali Kolli[1], Swetha Mile[2], Shreya Shetty[3], Sharana Jyothi B[4], Chandrakala. B.M[5]

Student, Department of Information Science and Engineering, Dayananda Sagar College of Engineering, Bangalore, Karnataka, India[1,2,3,4]

Associate Professor, Department of Information Science and Engineering, Dayananda Sagar College of Engineering, Bangalore, Karnataka, India[5]

Abstract: This system proposed an improve data security protection mechanism for cloud using two components. In this system sender sends an encrypted message to a receiver with the help of cloud system. The sender requires to know identity of receiver but no need of other information such as certificate or public key. To decrypt the cipher text, receiver needs two parts. The first thing is a unique personal security device or some hardware device connected to the computer system. Second one is private key or secrete key stored in the computer. Without having these two things cipher text never decrypted. The important thing is the security device lost or stolen, then cipher text cannot be decrypted and hardware device is revoked or cancelled to decrypt cipher text.

Keywords: cloud storage system, cloud security, cloud protection, two-factor data security protection.

I. INTRODUCTION

There are such a large number of advantages, to store the information in the cloud storage. Information in the cloud storage server can be facilitated whenever and wherever as long as network access. Cloud service provider gives services to the cloud users, they can get any amount of more resources any time. It provides no risk of data Storage maintenance tasks, such as acquiring additional storage capacity, can be unloaded to the responsibility of a service provider. Easy to information sharing between numerous clients. In the event that sender needs to share a bit of information, for example, video, text, audio and so forth to receiver it might be troublesome for sender to send it by email because of the size of information. Instead of that sender transfers the data into the cloud storage after that receiver can easily download anytime from any place. Cloud storage typically refers to an offer object storage services like Microsoft Azure and Amazon S3 Storage. There are different significant challenges in cloud computing for securing data, provision of services and storage of data in the internet from different types of attacks. Cloud computing provides an including space for data storage, computer processing power, shared pool of resources, networks, user applications and specialized corporate. Cloud computing is a more sophisticated. It is easy to forecast that the security for data protection in the cloud storage should be improve. In any cases, these applications go through a potential risk about component revocability that may limit their possibility. An expandable and flexible Two-Component encryption mechanism is really more appropriate in the term of cloud computing that prompt our System. Cloud computing is a common term for anything that involves scalable services, delivering hosted services like accessing, data sharing, etc. over the web on demand basis. Generally, user share various types of documents through cloud storage networking application like Drop box, cloud me, Google drive. Citrix Cloud computing is known as an alternative to traditional technology due to its low-maintenance and better resource-sharing capabilities. The main goal of cloud computing is to provide high performance energy of computing for various field like military and research organization for performing billions of computations. The essential security requirement can be attained by combining both the cryptographic cloud storage along with searchable encryption scheme. In cloud system overall cost of data storage is less as it does not require managing and maintaining expensive hardware. In which data owner firstly encrypt all data before storing on a cloud in such way that only user whom having decryption keys can be decrypt or fetch the data.

II. RELATED WORK

In [1] proposed an architecture that ensures the privacy of data stored in cloud storage. The proposed architecture can directly applicable to existing clouds without any modifications or any changes in cloud database. It can be process that connects directly to an encrypted cloud database without an intermediate devices or systems with geographically distributed clients and it also allowed executing independent and operations including those changing the database structure.The proposed systemeliminates the limit on scalability, and availability properties of cloud based solutions.

DOI10.17148/IJARCCE.2017.6505

In [2] described unidirectional proxy re-encryption schemes. This scheme is with chosen cipher text security in the standard model. The two contribution of this proposed system is fitted a unidirectional extension of the Canetti–Hohenberger security model and another one is how to change the scheme to attain security. It provides additional properties like as non-interactive temporary delegations.

In [3] proposed a solution for problem of efficiently delegating in key revocation [4] and generation in Identity Based Encryption (IBE) scheme. In this paper proposed realization of RHIBE, it is constructed based on the scheme called Boneh-Boyen HIBE (BB-HIBE) scheme. The size of cipher text and revocation cost was same for both RHIBE and BB-HIBE schemes. But in RHIBE allows hierarchical structure of entities and selective ID was protected under Decisional Bilinear Diffie-Hellman (DBDH) assumption.

In [5] proposed new definition and security models for single-hop Identity-Based Proxy Re-Encryption (IBPRE) systems. This system holds the property of IBPRE along with conditional re-encryption technique. This new IBPRE overcome two problems are extension of IBPRE to support conditional re-encryption and construction of CCA-secure unidirectional single hop IBPRE without random oracles.

In [6] presented a security definition against chosen cipher text attack (CCA). This definition was for the purpose of certificate less proxy re-encryption. The proposed security model was allowed to adaptively corrupt users. After the corruption of security model and it displayed some proofs to show that a challenges involved in the construction of secure CL-PRE. Finally proved RCCA was secured in random oracle model.

In [7] proposed a solution for constructing a multi-use unidirectional IBPRE scheme problem by converting non-anonymous hierarchical identity-based encryption (NaHIBE) with strongly CPA security to CCA-secure and collusion-resistant multi-use unidirectional IDbased proxy re-encryption MUIBPRE. This technique tries to satisfy the security requirements are CCA security and collusion resistance.

In [8] proposed an approach to protect user’s privacy data in cloud environment. This approach explained the compression applied in secret keys in public key cryptosystem to handle the cloud storage by supporting delegation of secret keys in various cipher text classes. This approach is more flexible and efficient than hierarchical key assignments. The hierarchical key assignments analysed privileges of all key-holders if they allocate the same privileges it saved their space for privileges. The proposed approach used key-aggregate cryptosystem encryption technique where the cipher texts were categorized into various classes.

In [9] proposed an effective third party auditor (TPA) for privacy preserving public auditing to secure a cloud storage system. This technique allows without learning the data content in a cloud environment an external auditor audit user’s outsourced data by using privacy-preserving auditing protocol. This technique used random masking andhomomorphic linear authenticator as privacy-preserving auditing protocol. Thus this technique removed burden for cloud user‘s and expensive task in cloud.

In [10] presented a proxy-based storage system called NCCloud for fault-tolerant multiple-cloud storage. This system was developed on functional minimum-storage regenerating a network a network-coding- based storage scheme. This proposed system used less repair traffic than redundancy as in traditional erasure codes that sustain less monetary cost due to data transfer. This system removes the encoding operations within the storage nodes during repair thus it reduced the repair traffic in the cloud.

In [11] proposed a short and efficient Certificate Based Signature (CBS) scheme to improve level of trust in cloud environment. This scheme was need one group element for public key and the signature size and it reduced the public information to one group elements for each and every user in the cloud environment. This key size is smaller than the PKI based signature scheme because it needs one group element for generation of public key and the another group element is needed for the certificate.

In [12] proposed an approach that overcomes the problem in Attribute-Based Encryption (ABE). In this introduced a cipher text delegation procedure that re-encrypted a cipher text based on the public information and analysed the problem of revocable in existing Attribute-Based Encryption technique. Based on the analysis it is necessary for first fully secure construction, it modifies an existing Attribute-Based Encryption scheme. Thus this approach was used for revocation on stored data.

In [13] proposed a two-factor data security protection mechanism for cloud storage system. In this proposed mechanism sender sends their data to receiver with an encrypted message. The receiver decrypts the message with the help of secret key of the computer and unique personal security device. If the device is stolen by someone it can be revoked by implementing some algorithms to change the cipher text. This technique is more transparent to the sender.

DOI10.17148/IJARCCE.2017.6505

Table I: Comparison of cloud data security techniques [14].

Ref no	Title	Merits	Demerits
[1]	Distributed, concurrent, and independent access to encrypted cloud databases	Eliminates intermediate proxies and doesn't need modifications in the database structure	Encrypted database results negligible overhead
[2]	Unidirectional Chosen-Cipher text Secure Proxy Re-Encryption	Mild complexity assumptions in bilinear groups	The problem of securely obfuscating CCA-secure re-encryption
[3]	Efficient Delegation of Key Generation and Revocation Functionalities in Identity-Based Encryption	It reduced excessive workload	It has more complicating key distributing method
[5]	A CCA-Secure Identity-Based Conditional Proxy Re-Encryption without Random Oracles	It provides security against adaptive identity and adaptive condition chosen-cipher text attacks	CHK transformation to achieve CCA Security seems un widely
[6]	Towards a Secure Certificate less Proxy Re- Encryption Scheme	computation time for an exponentiation and a bilinear pairing is lesser than IB-PRE scheme	Results are based on honest list created by challenger
[7]	Multi-use unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption	CCA security is high	Cipher text size and decryption time will be increased with the number of translations.
[8]	Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage	This approach do not need to set a very high number of classes to have better compression	The cipher text size is dependent on the maximum number of cipher text classes
[9]	Privacy-Preserving Public Auditing for Secure Cloud Storage	Removes cloud user's burden and expensive task	privacy-preserving public auditing protocol is not used in multi-user setting
[10]	NC Cloud: A Network-Coding-Based Storage System in a Cloud-of-Clouds	Reduced the repair traffic	It leads to bad repair if don't check the rMDS property
[11]	Short and Efficient Certificate-Based Signature	The computation requirement of CBS is very light	It requires both the public key and user identity for encryption.
[12]	Dynamic Credentials and Cipher text Delegation for Attribute-Based Encryption	It satisfies strong efficiency guarantees with consideration of the lifetime of the database.	It creates inconvenience once the current period key is lost
[13]	Two-Factor Data Security Protection Mechanism for Cloud Storage System	Provides confidentiality of data and revocability of the device	It affects from the largest price in Updated Cipher text Size

III. EXISTING AND PROPOSED SYSTEM

A. Existing System

There exists cryptographic primitive called “leakage-resilient encryption”. The security of the scheme is still guaranteed if the leakage of the secret key is up to certain bits such that the knowledge of these bits does not help to recover the whole secret key. However, though using leakage resilient primitive can safeguard the leakage of certain bits, there exists another practical limitation. Say,a part of the secret key is stored into the security device. If the device gets stolen, then the user needs a replacement to continue to decrypt his corresponding secret key. One of the solution is to copy those bits (that in the stolen device) to the replaced device by the private key generator (PKG).

This approach can be easily achieved. Nevertheless, there exists security risk. If the adversary (who has stolen the security device) can also break into the computer where the other part of secret key is stored, then it can decrypt all cipher text corresponding to the victim user. The most secure way is to cease the validity of the stolen security device.

DOI10.17148/IJARCCE.2017.6505

Disadvantages of Existing System**:**

1. If the user has lost his security device, then his/ her corresponding cipher text 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.

B. Proposed System

This paper describes a novel two-factor security protection mechanism for data stored in the cloud. This mechanism provides the following nice features:

1)The 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 sender sends the cipher text to the cloud where the receiver can download it at any time.

2) The system provides two-factor data encryption protection. In order to decrypt the data stored in the cloud, 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 and NFC). It is impossible to decrypt the cipher text without either piece.

3) More importantly, the system, for the first time, provides security device (one of the factors) revocability. When the security device is stolen/lost, this device is revoked. That is, using this device you can no longer decrypt any cipher text. The cloud will immediately execute some algorithms to change the existing cipher text to beun-decryptableby this device. While, the user needs to use his new/replacement device (together with his secret key) to decrypt his/her cipher text; this process is completely transparent to the sender.

4) The cloud server cannot decrypt any cipher text at any time.

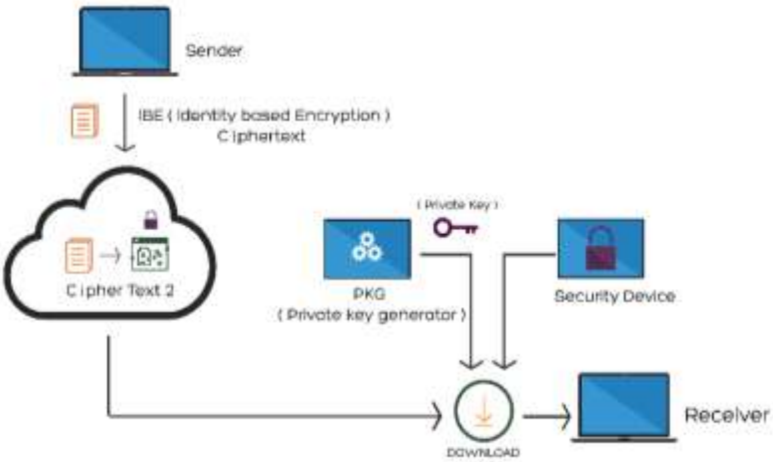

Fig. 1: Ordinary data sharing.

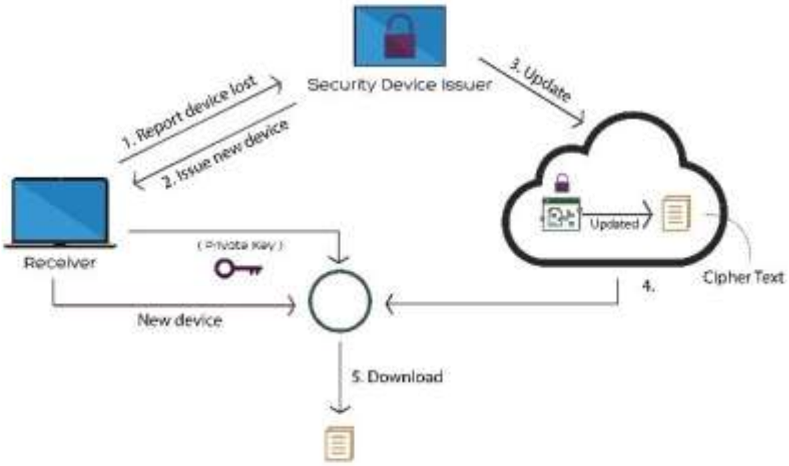

Fig. 2: Update cipher text after issuing a new security device.

DOI10.17148/IJARCCE.2017.6505

Advantages of Proposed System:

1. The 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.
2. The cloud server cannot decrypt any cipher text at any time.

IV. IMPLEMENTATION

In this implementation we have 5 Modules,

1. Private Key Generator
2. Security Device Issuer
3. Sender Module
4. Receiver Module
5. Cloud Server Module

Module Description:

1. Private Key Generator:

A Private Key Generatoris a trusted party responsible for issuing the private key for every user.

2. Security Device Issuer (SDI):

ASecurity Device Issuer is a trusted party responsible for issuing security device for every user.

3. Sender:

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

4. Receiver:

This user is the receiver of the cipher text and has a unique identity (e.g., email address). The cipher text is stored on cloud storage while he/she 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.

5. Cloud server:

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

V. CONSTRUCTION

The construction of such a system includes the following phases-

1. Setup Phase –

The setup phase generates all public parameters and master secret key used throughout the execution of system.

2. Key and Issued Phase –

A SDI and a PKG will respectively generate a security device and a secret key for a registered user ID in secure channel such that the user can combine the security device with the secret key to obtain the plain message after decrypting.

3. First-Level Cipher text Generation-

A data sender encrypts a data under the identity of a data receiver, and further sends the encrypted data to the cloud server.

4. Second-Level Cipher text Generation –

After receiving the first-level cipher text of a data from the data sender, the cloud server generates the second-level cipher text.

5. Device Update –

Once a device of a user needs to be updated due to some incidences (e.g. it is either lost or stolen), the user first reports the issue to the SDI. The SDI then issues a new device for the user.

6. Cipher text Update –

The SDI notifies the cloud server to update the cipher text of the user by sending a special piece of information.

7. Data Recovery –

A data receiver uses a decryptionkey and a device to recover the data.

DOI10.17148/IJARCCE.2017.6505

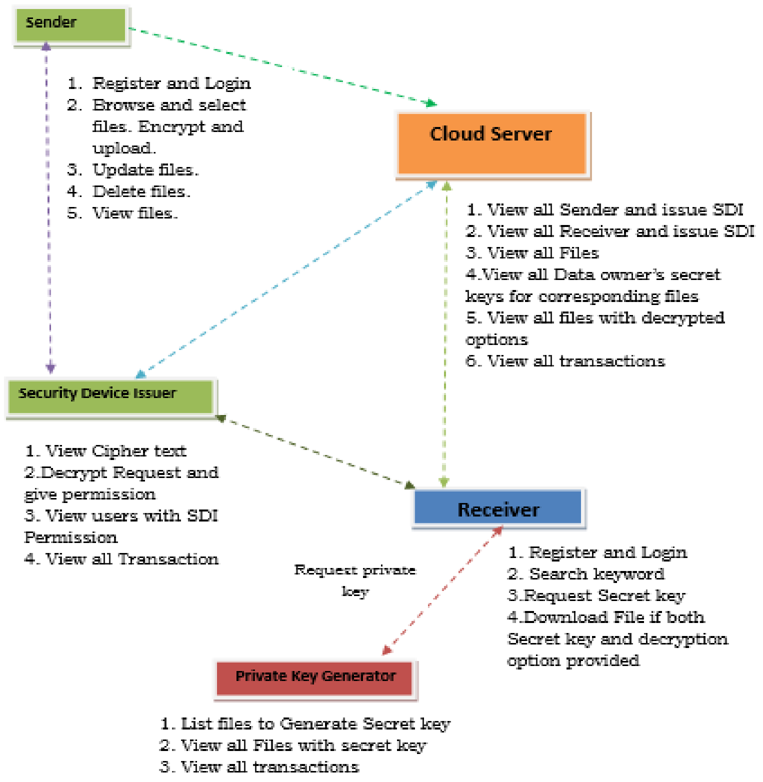
Sender
1. Register and Login
2. Browse and select files. Encrypt and upload.
3. Update files.
4. Delete files.
5. View files.
Cloud Server
1. View all Sender and issue SDI
2. View all Receiver and issue SDI
3. View all Files
4.View all Data owner's secret keys for corresponding files
5. View all files with decrypted options
6. View all transactions
Security Device Issuer
1. View Cipher text
2.Decrypt Request and give permission
3. View users with SDI Permission
4. View all Transaction
Receiver
1. Register and Login
2. Search keyword
3.Request Secret key
4.Download File if both Secret key and decryption option provided
Request private key
Private Key Generator
1. List files to Generate Secret key
2. View all Files with secret key
3. View all transactions

Fig 3: Architecture of System.

VI. CONCLUSION

Various techniques are available to provide security for cloud storage data. Among them, two-Factor Data Security Protection mechanism only provides confidentiality of the data and revocability for cloud data by using secret key and unique personal device. The efficiency and security analysis show that the system is secure as well as practically implemented

REFERENCES

[1] L. Ferretti, M. Colajanni, M. Marchetti. Distributed, concurrent, and independent access to encrypted cloud databases. IEEE transactions on parallel and distributed systems, 2014; 25(2), 437-446.

[2] B. Libert, D. Vergnaud. Unidirectional chosen-ciphertext secure proxy re-encryption. IEEE Transactions on Information Theory. 2011; 57(3), 1786-1802.

[3] J. H. Seo, K. Emura. Efficient delegation of key generation and revocation functionalities in identity-based encryption. In: Cryptographers' Track at the RSA Conference. Springer Berlin Heidelberg. 2013; 343-358.

[4] R. R. Pavithra, V. R. Nagarajan. A survey on certificate revocation scheme using various approaches. Indian Journal of Innovations and Developments. 2016; 5(5), 1-3..

[5] K. Liang, Z. Liu, X. Tan, D. S. Wong, C. Tang. A CCA-secure identity-based conditional proxy re-encryption without random oracles. In: International Conference on Information Security and Cryptology. Springer Berlin Heidelberg. 2012; 231-246. .

[6] H. Guo, Z. Zhang, J. Zhang, C. Chen. Towards a secure certificateless proxy re-encryption scheme. In: InternationalConference on Provable Security. Springer Berlin Heidelberg. 2013; 8209, 330-346..

[7] J. Shao, Z. Cao. Multi-use unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption. Information Sciences, 2012; 206, 83-95.

[8] C.K. Chu, S.S. Chow, W.G. Tzeng, J. Zhou, R.H. Deng. Key-aggregate cryptosystem for scalable data sharing in cloud storage. IEEE Transactions on Parallel and Distributed Systems. 2014; 25(2), 468-477.

[9] C. Wang, S.S. Chow, Q. Wang, K. Ren, W. Lou. Privacy-preserving public auditing for secure cloud storage. IEEE Transactions on computers. 2013; 62(2), 362-375.

[10] H.C. Chen, Y. Hu, P.P. Lee, Y. Tang. NCCloud: a network-coding- based storage system in a cloud-of- clouds. IEEE Transactions on Computers, 2014; 63(1), 31-44.

[11] J.K. Liu, F. Bao, J. Zhou. Short and efficient certificate-based signature. In: International Conference on Research in Networking. Springer Berlin Heidelberg. 2011; 167-178.

[12] A. Sahai, H. Seyalioglu, B. Waters. Dynamic credentials and cipher text delegation for attribute-based encryption. In: Advances in Cryptology–CRYPTO 2012. Springer Berlin Heidelberg. 2012; 199-217.

[13] J.K. Liu, K. Liang, W. Susilo, J. Liu, Y. Xiang. Two-Factor Data Security Protection Mechanism for Cloud Storage System. IEEE Transactions on Computers, 2016; 65(6), 1992-2004.

[14]M. Vimala,K.Vishnukumar. A survey on data security mechanism for cloud storage system, 2016.

DOI10.17148/IJARCCE.2017.6505