International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 3 Issue: 11
ISSN: 2454-4248
447 – 450

Enhance Data Security Protection for Data Sharing in Cloud Storage System

Swetha Gadde
Asst. Prof, Dept. Of. IT
R.V.R &J.C COLLEGE OF ENGINEERING
Guntur, India
ursgadde@gmail.com

Dr.Paras Nath Singh
Professor, Dept. Of.CSE
CMRIT
Bangalore, India
drpn.singh@cmrit.ac.in

Abstract— Cloud computing technology can be used in all types of organizations. 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 any place. Another advantage of cloud storage is data sharing between users. By sharing storage and networks with many users it is also possible for unauthorized users to access our data. To provide confidentiality of shared sensitive data, the cryptographic techniques are applied. So protect the data from unauthorized users, the cryptographic key is main challenge. In this method a data protection for cloud storage 1) The key is protected by two factors: Secret key is stored in the computer and personal security device 2) The key can be revoked efficiently by implementing proxy re-encryption and key separation techniques. 3) The data is protected in a fine grained way by adopting the attribute based encryption technique. So our proposed method provides confidentiality on data.

Keywords- *Two-factor, cloud storage,security,revocability,proxy re-encryption, aaribute-based encryption*

*****

I .INTRODUCTION

Cloud computing provides low cost, high quality, flexible and scalable services to users. The main advantage of cloud storage [1] is data sharing. Sharing huge data with several data shares it cost consuming task, while this cost could be reduced to the size of shared data with the help of cloud storage. While transmitting data between users, protect the sensitive data from unauthorized users. In classical cryptography schemes

Symmetric encryption: In this encryption single key is used for both encryption and decryption.

Asymmetric encryption: In this encryption different public and private keys are used for both encryption and decryption. To provide the confidentiality of shared data the cryptographic techniques are applied. In cryptographic schemes, to protect and revoke the key is main important. To protect the secret key, it is stored in the computer it can be revealed by some viruses [2]. To deal with key exposure problem, many techniques have been proposed such as public key technique [3] [4]. The security protection is sufficient if the computer is isolated from an opening network. If the computer is in the opening network, there exists a need to enhance the security protection. In [5] proposed two factor data security protection. To enhance the security protection the key is divided into two parts. One part is stored in user's computer and other one is stored in security device. An analogy is e-banking security. Many e-banking applications require a user both password and security device named as "two factor" to login system for money transfer. The purpose of using two factors is to enhance the security protection for access control. Once the security device is lost, it could be revoked by using proxy re- encryption technique. Sender sends an encrypted message to the cloud. The cloud server receives the encrypted data, again encrypts the data by using public key encryption with public key corresponding to the users security device. The receiver decrypts the cipher text from the cloud. The sender encrypted twice, one for Identity based encryption (IBE) and other one is public key encryption (PKE).This makes solution inefficient. In proposed framework old security device is revoked and how the new security device can do decryption properly. To revoke the old security device the cloud updates the old cipher text before sending to the user by using proxy re-encryption technique. When the receiver requests the new security device, the user should give a secret to the key generation center to generate the new secret which can be used to decrypt the updated cipher text. Here the cloud can be act as proxy.

Main Contributions:

1)In this method propose an efficient and secure communication. The data can be stored in the cloud. The cloud service provider (CSP) provides the assurance to the users with strong evidence. The CSP is store all data and this data can not be leaked to unauthorized parties. It provides confidentiality on data . The proposed scheme against attacks.

2) In proposed method the security device is revoked. Once the security device is lost, the user requests the new security device, which can be used to decrypt the updated cipher text.

3) Here the cloud can update the all existing cipher text by using proxy re-encryption technique.

II . RELATED WORK

Several cryptographic schemes have been introduced to protect data in data sharing scenario. Initial cryptographic scheme is dealing with key exposure problem Doids et al. [3] provided a key-insulated public key scheme dealing with public key exposure problem. In this system there are two keys named as master key is stored in a physically secure and other

 ISSN: 2454-4248
447 – 450

key is public key stored in insecure device that is computer while can be updated periodically by using master secret key. The more private key updates, the high risk of master key exposes.

To address this problem Hanaoka et al. [6] provides key insulated public key encryption. In [6] there are two independent master keys are used. These are reduces the high risk of master secret key exposure. In all the schemes the security device is used to update the every user's private key. Once the private key is updated periodically there is no need of security device is in decryption phase. In cloud computing data sharing between users is main important thing. In cloud computing user's private key is does not updated in every time period. The security device is used in every decryption phase.

Blaze et al. in [7] provides another crypto system supporting revocability is proxy re-encryption. In this a proxy can transform a cipher text for a user into another cipher text that another user can decrypt it. PRE can learn the length of the cipher text. To increase the efficiency and security of PRE the schemes were proposed [8]-[12]. Boldyreva et al. [13] provides a revocable attribute based encryption (ABE) from revocable identity based encryption (IBE). In this scheme non revoked users need to update private keys periodically. This method is most inconvenient. To solve this problem, Attrapadung et al. [14] provides a new ABE scheme with revocability, where the non revoked users do not need to update the private keys periodically but sender needs to know the revocation list. To solve this problem Attrapadung et al. [15] proposed another ABE with revocability scheme named direct and indirect methods. In direct revocation method sender need to know the revocation list during the encryption and main advantage is non revoked users need not to update their private keys. In indirect revocation requires non revoked users need to update their private keys periodically and advantage is sender need not to know the revocation list. Combined both advantages and disadvantages fully secure revocable ABE proposed in [16], [17].Here need to maintain a revocation list for all security devices. Our method is to issue a new security device to revoke the old key without updating all other security devices. Combining the ABE and PRE techniques it cannot support the two factor protection.

III. SYSTEM DESIGN

To design and implement efficient data storage in cloud the following design goals are maintained.

a) **Data security :** Whenever sender send data to the cloud provides security to that data. Examples for data security include encryption,backups.

b) **Cloud storage :** Cloud storage provides are in charge of maintain the data information an accessible,open and the physical environment secured. It is responsible for storing all the cipher text (for receiver to download). The cloud acts as proxy to re-encrypt all past and future ciphertext corresponding to the new device. That is old device is revoked. The cloud server cannot decrypt any cipher text at any time.

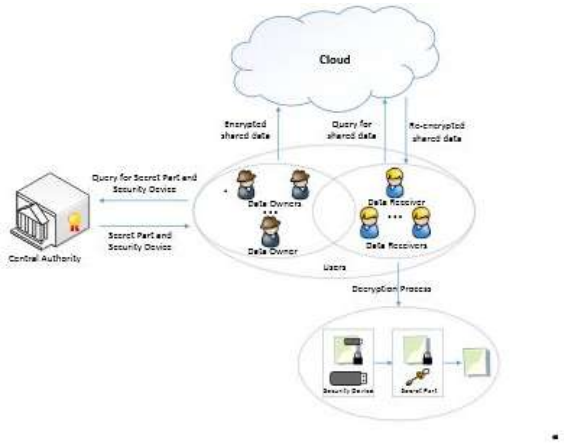


Fig 1: Overall System Architecture

Design Goals:

Provide two factor data protection mechanism for cloud storage with revocability. Issuing the secret key to each user according to their attribute list and splitting the key into two parts (two factors): one is Secret Part Key (SPK) stored in computer and other named as Security Device Key (SDK) is stored in security device. The Key Generation Center (KGC) is in control for making keys where the key generation control is capable to produce a partial private key for all users in partial private key extract.

System Model:

Four different entities proposed in our framework are as follows

- Central Authority
- Cloud
- Data owner
- Data receiver

a) Central Authority (CA): It is trusted party which is responsible for issuing cryptographic key for every user and splitting the key into two parts : One is called as Secrect Part Key (SPK) stored in a computer and other part is named Security Device Key(SDK) stored in security device. And CA is responsible for updating every user's security device.In fig.2 if security device is lost the user sends the query to the CA then the CA issues new securitydevice to the user and corresponding re-encryption key that will be sent to the cloud.The re-encryption key is used to update the cipher texts to make a new SDK works. The generation of re-encryption requries the information about the old SDK. In this proposal the CA does not need to store any secret for users.

 ISSN: 2454-4248
447 – 450

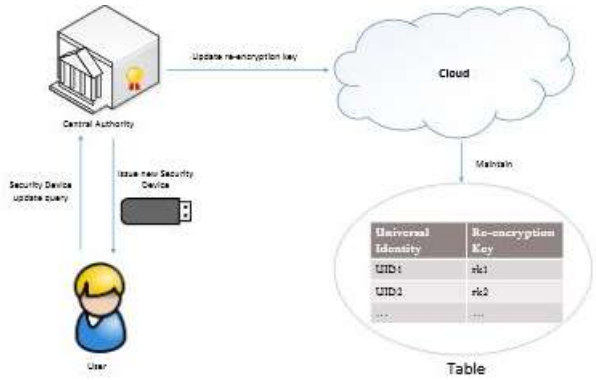


Fig. 2: The process of SDK update

b) Cloud: The cloud is a semi-trust party that stores all encrypted shared data and maintains a Table containing the user's universal identity (UID) and corresponding re-encryption key. Whenever the data receiver queries for a shared data the cloud acts as proxy and to re-encrypt the encrypted shared data by using data receiver's corresponding re-encryption key and returns the re-encrypted shared data to data receiver.

c) Data Owner (DO): A DO is a user sends the data with other (DRs). The encrypted data is uploaded into the cloud. All the shared data are encrypted by using Cipher text Policy-Attribute Based Encryption (CP-ABE).

d) Data Receiver (DR): The DR is a user to receive the data from the cloud. Whenever the receiver wants to retrieve the data from cloud, the cloud firstly does the re-encryption and returns the resulting re-encrypted cipher text. The re-encrypted cipher text can decrypted by using the DRs own SPK and SDK. Once the security device is lost the DR can revoke it and obtain a new security device through interacting with CA.

IV.PROPOSED SOLUTION

In the proposed method key is stored into two parts, one stored in computer and other one is stored in security device. In which the sender is allowed to encrypt the data with the knowledge of receiver. The receiver required to use both keys to access data. If the security device is lost, the central authority issues a new security device to the receiver. The cloud acts a proxy to re- encrypted the encrypted shared data by using receivers corresponding re- encryption key and returns re-encrypted shared data to receiver.

A) Setup phase: Setup phase is generated by the data account holder to establish an account on an un-trusted cloud server. In This module the user's requirement is to transfer the data to the cloud server. To transfer the data to the receiver first sender have to enroll the first. The receiver decrypts the data from the cloud server by using secret key. In this phase generates all the public parameters and master secret key used. Public parameters are shared with all parties into the system including data sender and receiver and the master key is kept secret to the central authority.

Algorithm: Setup phase algorithm

Step 1: Start
Step 2: The data owner initialize the generation of public and private keys
Step 3: The user will upload the data file on cloud server
Step 4: End

B) Key Generation Phase: In this the central authority will generate the secrets including SPK and SDK for all the registered users according to the attribute set.

C) Revocation: In this phase if the security device is lost the user obtain a new security device key from CA. The CA also generates the re-encryption key and gives it to the cloud with UID's via secure and authenticated channel. The cloud will maintain the all user ids and re-encryption key. The cloud will update the Table with UID'S and re-encryption keys.

D) Data Upload: In this phase, the data owner will encrypt the shared data according to the sharing policy and upload the resulting cipher texts to the cloud.

E) Data Download: In this phase, the receiver will download the shared data from the cloud. The data receiver queries the cloud for the cipher text with universal identity (UID). The cloud first checks if the data receiver security device has been updated. If not, the cloud returns the cipher text to the receiver directly. Otherwise the cloud will transform the cipher text under the receiver's encryption key.

F) Data Reveal: In this phase, the data receiver will decrypt the re-encrypted cipher text by using secret key and security device SDK.

V. PRELIMINARIES

Here revise some basic terminologies used in security proof

A) Bilinear maps: Let G_1 and G_2 are denoted by multiplicative cycle groups. Let p be the prime number and generators of G_1 and G_2 are g1 and g2. The map is e: G_1 X G_2 said to be a bilinear mapping it holds the following

Input: Text
Output: Encrypted and decrypted data

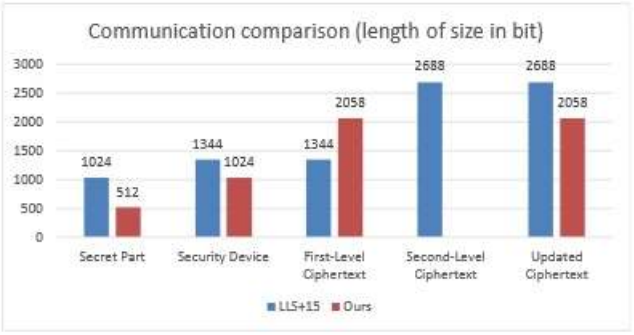
a) e is bilinear for all a, b belongs to Z_p
b) e is non-degenerate , that is e(g1,g2) !=1GT
c) e is efficiently computable.

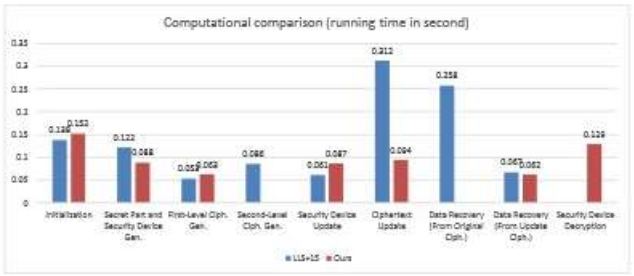
VI .Results

Fallowing performance has been measured based on various factors and issues. The existing work suffers from secret key. In our system is security protection system with revocability in terms of computational and communicational cost except the communication cost of the first-level cipher text and computational cost of security device update. Our system requires additional computation cost in security device generation and update. This is because security device revocability. Communication comparison our system is better except the communication cost of the first-level cipher text. The computational comparison is our scheme does not need to

 ISSN: 2454-4248
447 – 450

generate or recover the second-level cipher text, which can reduce the much computation time. Cipher text update phase is also much more efficient in our scheme. The proposed method achieves data protection with much less computational.





VII. Conclusion

In the proposed method find the solution to protect the data of a user from unauthorized access of control and data security for cloud storage. The secret key can be stored in two parts, one can be in computer and another can be stored in security device. Only one of them is kept in secret the proposed method remains secure and provides confidentiality on data. In proposed method encrypt the data and revocability of security device.

REFERENCES

[1] 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.

[2] "Encryption threat,"http://searchsecurity.techtarget.com/tip/ Encryption-key-virus-threat.

[3] Y. Dodis, J. Katz, S. Xu, and M. Yung, "Key-insulated public key cryptosystems,"in Advances in Cryptology EUROCRYPT 2002. Springer,2002, pp. 65–82.

[4] ——, "Strong key-insulated signature schemes," in Public Key Cryptography–PKC 2003. Springer, 2002, pp. 130–144.

[5] J. Liu, K. Liang, W. Susilo, J. Liu, and Y. Xiang, "Two-factor data security protection mechanism for cloud storage system," Computers, IEEE Transactions on, vol. 65, no. 6, pp. 1992–2004, 2016.

[6] G. Hanaoka, Y. Hanaoka, and H. Imai, "Parallel key-insulated public key encryption," in Public Key Cryptography-PKC 2006. Springer, 2006, pp. 105–122.

[7] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in Advances CryptologyłEUROCRYPT'98. Springer, 1998, pp. 127–144.

[8] A.-A. Ivan and Y. Dodis, "Proxy cryptography revisited." in NDSS, 2003.

[9] 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 (TISSEC), vol. 9,no. 1, pp. 1–30, 2006.

[10] R. Canetti and S. Hohenberger, "Chosen-ciphertext secure proxy reencryption,"in Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 185–194.

[11] B. Libert and D. Vergnaud, "Unidirectional chosen-ciphertext secure proxy re-encryption," in Public Key Cryptography–PKC 2008. Springer,2008, pp. 360–379.

[12] J. Shao and Z. Cao, "Cca-secure proxy re-encryption without pairings,"in Public Key Cryptography–PKC 2009. Springer, 2009, pp. 357–376.

[13] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proceedings of the 15th ACM conference on Computer and communications security. ACM, 2008, pp. 417–426.

[14] N. Attrapadung and H. Imai, "Conjunctive broadcast and attribute-based encryption," in Pairing-Based Cryptography–Pairing 2009. Springer, 2009, pp. 248–265.

[15] ——, "Attribute-based encryption supporting direct/indirect revocation modes," in Cryptography and Coding. Springer, 2009, pp. 278–300.

[16] J.-l. Qian and X.-l. Dong, "Fully secure revocable attribute-based encryption,"Journal of Shanghai Jiaotong University (Science), vol. 16,pp. 490–496, 2011.

[17] F. Zhang, Q. Li, and H. Xiong, "Efficient revocable key-policy attribute based encryption with full security," in Computational Intelligence and Security (CIS), 2012 Eighth International Conference on. IEEE, 2012, pp. 477–481.