ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

A Fine-Grained Two-Factor Protection Mechanism for Data Sharing in Cloud Storage

Sivagami[1], K.Charulatha[2], K.Nandhini[2], L.Thamizhselvi[2]

Assistant Professor, Department of Information Technology, Velammal Institute of Technology, Chennai, Tamil Nadu, India[1]

Department of Information Technology, Velammal Institute of Technology, Chennai, Tamil Nadu, India[2]

ABSTRACT: Data sharing in cloud storage is receiving substantial attention in Information Communications Technology, since it can provide users with efficient and effective storage services .To protect the confidentiality of the shared sensitive data, the cryptographic techniques are usually applied. However, the data protection is still posing significant challenges in cloud storage for data sharing. Among them, how to protect and revoke the cryptographic key is the fundamental challenge. To tackle this, we propose a new data protection mechanism for cloud storage, which holds the following properties. 1) The cryptographic key is protected by the two factors. Only if one of the two factors works, the secrecy of the cryptographic key is held. 2) The cryptographic key can be revoked efficiently by integrating the proxy re-encryption and key separation techniques. 3) The data is protected in a fine-grained way by adopting the attribute based encryption technique. Furthermore, the security analysis and performance evaluation show that our proposal is secure and efficient, respectively.

KEYWORDS: revocability, fine-grained, attribute based encryption, proxy re-encryption, cloud storage

I. INTRODUCTION

The development and deployment of cloud-based applications have gained tremendous impetus in the industry and research community in recent years. Cloud storage is the most successful cloud-based applications, since it matches the huge data sharing demands. Sharing huge data with several data sharers is a cost-consuming task, and the cost on the data owner side is usually proportional to the number of data sharers. The only thing is the data sharer needs to do is to upload the data to the cloud and grant the access right to the data sharer. To protect the confidentiality of data the cryptographic schemes are applied. The security of cryptographic schemes stem from the security is underlying in the cryptographic key. Now, the cryptographic key is simply stored in the computer. The cryptographic key exposure and revocation problems in cloud storage are unrevealed by two factor mechanism. The cryptographic key is divided into two parts. One is kept in user's computer and the other is stored in a security device (e.g., smart card) Hence, the "two-factor" is named. Furthermore, once the user's security device was either lost or stolen, it could be revoked by using the proxy re-encryption technique.

Recently, the data sharing is rising concern While privacy is still the key concern and an equally striking challenge that reduce the growth of data sharing in cloud .

II. LITERATURE SURVEY

1.*cong wang ,member of IEE*-the security in cloud sharing in this study enabling public audit ability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

2.W*enjing lou senior member of IEE*- the security in cloud storage in this study provides flexible distributed storage integrity auditing mechanism, utilizing the homomorphic token and distributed erasure-coded data. The proposed design allows users to audit the cloud storage with very lightweight communication and computation cost. The auditing result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization, i.e., the identification of misbehaving server

3. *Devi Parvathy Mohan, Gnanamani college of engineering*- this study provides a traditional approach developed a dynamic audit service for verifying the integrity of an un trusted and outsourced storage. An audit service is constructed based on the techniques, fragment structure, random sampling, and index-hash table, supporting provable updates to outsourced data and timely anomaly detection. The method based on probabilistic query and periodic verification for improving the performance of audit services. The audit service is performed by TPA monitoring

4. *Priya J. Khindre, Matoshri Pratishthan Group of Institutions*, this study proposed an essential security requirement that 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 owners 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.

III. PROPOSED SYSTEM

we integrate the attribute-based encryption technique, proxy re-encryption technique, and the key separation technique to remove the use of PKE and the storage of security device's secret in the key generation center while solving key exposure and revocation problems and supporting fine-grained access control.. However, all the cipher texts in our proposed framework are ABE cipher texts.. When the user requests the new security device, the user should give a secret to the key generation center to generate a new secret which can be used to decrypt the updated cipher texts. Fig. 1 shows the architecture of our CP-ABE based fine grained two-factor data protection framework. There are four main entities in our framework: Central Authority (CA), Cloud, Data Owners (DOs) and Data Receivers (DRs) Central Authority (CA): The CA is a trusted party which is responsible for issuing the cryptographic key for every user according to their attribute set and then splitting it into two parts (two-factor): One, called as Secret Part Key (SPK), is assumed to be stored in a potential-insecure place (e.g., computer). The other, named as Security Device Key (SDK) is stored in a physically-secure but computationally limited device (security device).The CA is also responsible for updating every user's security device (and the corresponding SDK). Specially, in the SDK update phase, the CA generates a new SDK that is stored in a security device and the corresponding re encryption key that will be sent to the cloud.

FRAME WORK AND DESIGN GOAL:

In this section, we formalize the system model and attack models considered in this paper, and identify the design goals. There are four main entities in our framework: Central Authority (CA), Cloud, Data Owners (DOs) and Data Receivers (DRs) .

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

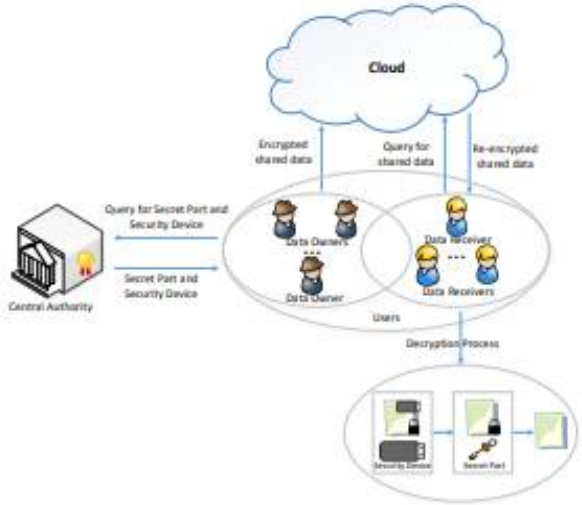

Fig. 1: Architecture of our framework

• **Central Authority (CA):** The CA is a trusted party which is responsible for issuing the cryptographic key for every user according to their attribute set and then splitting it into two parts (two-factor): One, called as Secret Part Key (SPK), is assumed to be stored in a potential-insecure place (e.g., computer). The other, named as Security Device Key (SDK) is stored in a physically-secure but computationally limited device (security device). Furthermore ,the CA is also responsible for updating every user's security device (and the corresponding SDK). Specially, in the SDK update phase, the CA generates a new SDK that is stored in a security device and the corresponding re encryption key that will be sent to the cloud.

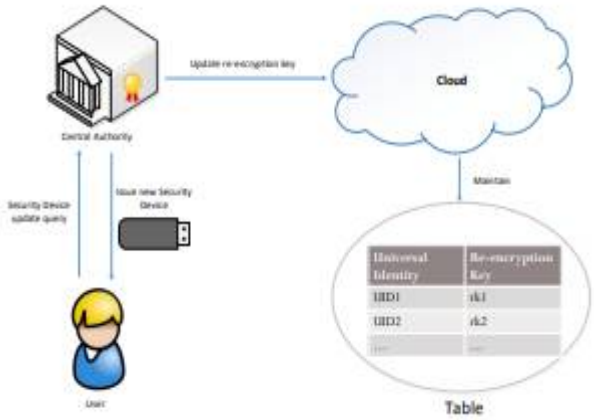

Fig. 2: The process of SDK update

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

Note that the re-encryption key is used to update the cipher texts to make the new SDK work, while the generation of the re-encryption key requires the information of the old SDK. As mentioned before, one of the advantages of our proposal is that the CA does not need to store any secrets for users. In this case, the way that the CA simply issue an update key to update the old SDK cannot work due to the absent of the old SDK (the security device may be stolen or lost). To solve the problem, we use SPK to retrieve SDK instead. (See Section IV for more details.)

• **Cloud:** The cloud is a semi-trust party that stores all encrypted shared data and maintains a table T able containing the users' universal identity (UID) and corresponding re-encryption key. When a DR queries for the shared data, the cloud acts as a proxy to re-encrypt the encrypted shared data by using DR's corresponding re-encryption key and returns the re-encrypted shared data to DR.

• **Data Owner (DO):** A DO is a user who wants to share data with other users (DRs). All the shared data are encrypted by using CP-ABE according to the access policy. • Data Receiver (DR): A DR is a user who can receive the shared data from the cloud. When a DR wants to retrieve the shared data, be decrypted by using DR's own SPK and SDK, if DR's attribute set satisfies the access policy of the shared data. Note that SDK is never revealed out of the security device during the decryption, while a partial decryption process using SDK would be executed in the security device. Once the security device is lost or stolen, DR can revoke it and obtain a new security device through interacting with CA.

OUR TECHNIQUE:

To solve the shortcomings of the naive solution, we integrate the attribute-based encryption technique, proxy re-encryption technique, and the key separation technique to remove the use of PKE and the storage of security device's secret in the key generation center while solving key exposure and revocation problems and supporting fine-grained access control. In LLS+15, the cipher texts are of two formats. One is the IBE cipher text, the other is the PKE cipher text. However, all the cipher texts in our proposed framework are ABE cipher texts. The main difficulties to make our framework work well are how the old security device is revoked and how the new security device can do decryption properly. To revoke the old security device, we need that the cloud updates the old cipher texts before sending them to the user by using proxy re-encryption technique. When the user requests the new security device, the user should give a secret to the key generation center to generate a new secret which can be used to decrypt the updated cipher texts. Compared to LLS+15, our proposed solution has the following properties.
• LLS+15 is mainly targeted for secure data storage while our main focus is for secure data sharing. These are two different functionalities provided by different types of cryptographic solutions.
• We use a different approach to realize the two-factor technique to solve the key exposure and key revocation problems. As a result, only one kind of cipher texts exists in our solution, which makes our solution easier to understand and implement. Furthermore, the key generation center in our proposal does not need to store any other secrets except its own private key
. • We explicitly show that how the decryption is proceeded without revealing the secret stored in the security device. While this part is not mentioned in LLS+15.
• When we make use of ABE as IBE, our proposal is more efficient than LLS+15 in terms of computational cost and storage cost.

SECURITY MODEL:

In our system, we assume that the CA is a trusted party. As the existing literatures dealing with the security in cloud computing we assume that the cloud is honest but-curious. In particular, the cloud could only launch passive attacks and would not collude with other users. Furthermore, it will definitely follow the proposed protocol. In our proposal, it will update the cipher texts before sending them to users. We also assume that the security device is tamper-resistant. In this paper, we consider the following attack model, which is mainly due to the two-factor requirement.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

• **Type-1:** The adversary can obtain SPK; revoked SDK's of the target user, while it cannot have the corresponding current SDK.

• **Type-2:** The adversary can obtain all SDK's for all the time of the target user, while it cannot have the corresponding SPK.

DESIGN GOALS:

Considering the aforementioned framework architecture and security model, our design goal is to present fine-grained two-factor data protection mechanism for cloud storage with revocability. Specifically, the follow
• Fine-grained. The fine-grained access control is always a desired requirement for the data sharing scenario.
• Revocable. The secrets used to decrypt the cipher texts can be revoked.
• Secure. The proposed system should be resilient to Type1 and Type-2 attacks.
• Practical. The underlying encryption, decryption and SDK update procedures should be effective and efficient.ing design goals should be satisfied: 2CTr,i and CT are of the same format,

IV. RESULT

The numerical and experimental comparison between these two schemes Here modify LLS+15 from CCA-secure to CPA-secure by removing the parts related to the CCA security since our scheme is CPA-secure. Most of the related parts are due to the FO transformation, we can also use this method to make our scheme CCA-secure.We denote te, te1 and tp as the time for one exponentiation in G and G1, and one pairing, respectively. We also let jGj, jZpj and jG1j as the bit length of an element in G, Zp and G1, respectively. jWj denotes the bit length of the AND gate, and denotes the length of security parameter. Again, to make the comparison relatively fair, we set the attribute number in the system, the access structure and the private key to 1.The number of user's attributes are relatively small in real world.

V. CONCLUSION

In this paper, the proposal is a fine-grained two-factor data protection for cloud storage. The two-factor is realized by separating the secret key into two parts, one can be stored in a potential-insecure place, and the other is stored in a tamper resistant device. Only if one of them is kept secret, the proposal remains secure. Furthermore, with the help of CPABE and PRE, we obtained the fine-grained access control on encrypted. data and the revocability of tamper resistant device, respectively

REFERENCES

[1] J. K. Liu, M. H. Au, X. Huang, R. Lu, and J. Li, "Fine-grained two factor access control for web-based cloud computing services," IEEE Transactions on Information Forensics and Security, vol. 11, no. 3, pp.484–497, 2016.
[2] C. Zuo, J. Shao, G. Wei, M. Xie, and M. Ji, "Chosen cipher text secure attribute-based encryption with outsourced decryption" in Australasian Conference on Information Security and Privacy. Springer, 2016 , pp.495– 6 based storage system in a cloud-of-clouds," Computers, IEEE Transactions on, vol. 63, no. 1, pp. 31–44, 2014
[3]C.Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure. cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013
[4] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C.-J. Hu, "Dynamic audit services for outsourced storages in clouds," Services Computing, IEEE Transactions on, vol. 6, no. 2, pp. 227–238, 2013.
[5] C., Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," Services Computing, IEEE Transactions on, vol. 5, no. 2, pp. 220–232, 2012.
[6] L. Xu, X. Wu, and X. Zhang, "Cl-pre: a certificateless proxy re-encryption scheme for secure data sharing with public cloud," in Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security. ACM, 2012, pp. 87–88.
[7] 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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

[8] A. De Caro and V. Iovino, "jpbc: Java pairing based cryptography," in Proceedings of the 16th IEEE Symposium on Computers and Communications ISCC 2011. Kerkyra, Corfu, Greece, June 28 - July 1: IEEE,2011, pp. 850–855

[9]B. Waters, "Ciphertext-policy attribute-based encryption: An expressive,
efficient, and provably secure realization," in Public Key Cryptography–PKC 2011. Springer, 2011, pp. 53–70.

[10] J. Herranz, F. Laguillaumie, and C. R`afols, "Constant size ciphertexts in threshold attribute-based encryption," in Public Key Cryptography–PKC 2010. Springer, 2010, pp. 19–34.

[11] N. Attrapadung, B. Libert, and E. De Panafieu, "Expressive key-policy attribute-based encryption with constant-size ciphertexts," in Public KeyCryptography–PKC 2011. Springer, 2011, pp. 90–108.

[12]Y. Rouselakis and B. Waters, "Practical constructions and new proof methods for large universe attribute-based encryption," in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM, 2013, pp. 463–474.

[13]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.