Security for data sharing in cloud storage using Fine Grained Two Factor Protection mechanism

Ms. Rohini R Rote

Assistant Professor
Computer Department
Samarth Group of Institute, Pune, India

***Abstract*: we propose a two-factor information security insurance component with factor revocability for distributed storage framework. Our framework enables a sender to send an encoded message to a beneficiary through a distributed storage server. The sender just has to know the personality of the beneficiary however no other data, (for example, its open key or its declaration). The beneficiary needs to have two things so as to decode the figure content. The essential thing is his/her puzzle enter set away in the PC. The second thing is a special individual security gadget which associates with the PC. It is difficult to unscramble the figure content without either piece. All the more imperatively, when the security gadget is stolen or lost, this gadget is disavowed. It can't be utilized to decode any figure content. This should be possible by the cloud server which will promptly execute a few calculations to change the current figure content to be un-unscramble capable by this gadget. This procedure is totally straightforward to the sender.**

***Index Terms*—Encryption, decryption, cloud storage system, cloud security, cloud protection, two-factor data security protection.**

I. INTRODUCTION

Sharing large amount of data with several data sharers is a cost-consuming task. In this concept the data owner side is usually proportional to the number of data sharers. The cost of this reduced size of data is of shared data with the help of cloud storage. The data sharer needs upload the data on the cloud and grant the access right to the data sharer. After the sharing data the data sharers can get the data from the cloud instead of the data owner. Regardless of the advantages of information partaking in distributed storage, it additionally acquaints numerous odds with the enemy to get to the common information without approval. To ensure the classification of the common information, the cryptographic plans are normally connected. The security of cryptographic schemes stem from the security of underlying cryptographic key. Currently, the cryptographic key is simply stored in the computer in most of existing cryptographic schemes. Especially, one cipher text in LLS+15 is essentially an identity-based cipher text that can be decrypted by only one user but not a group of users as in data sharing scenario. Recently, sharing of data is most important problem in day todays life. Private data is still difficult to handle in the key concern and an equally striking challenge that reduce the growth of data sharing in cloud. Naive Solution: At rst glance, it seems that we can solve the key exposure and revocation problem in the data sharing scenario by simply replacing the IBE scheme in LLS+15 with the ABE scheme. However, it cannot work well for data sharing in cloud storage due to the contradiction between the inefficiency of LLS+15 and the pay-per-use nature of cloud storage. In LLS+15, once the cloud server receives the encrypted data, it encrypts the data by using a public key encryption (PKE) with a public key corresponding to the user's security device. While when it comes to the data sharing scenario where the cipher text intends for many users, the cloud server would encrypt the data into many cipher texts under many public keys. Furthermore, even the data is shared with one user, it should be decrypted twice. In particular, one is for the IBE encryption, the other is for the PKE encryption. This makes the solution inefficient. There is another potential shortcoming for LLS+15. To realize the key revocation, the key generation centre in LLS+15 needs to store every security devices secret. When the IBE scheme is directly replaced by the ABE scheme, the size of secret will increase. It would be a burden for the key generation centre. 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 devices secret in the key generation centre while solving key exposure and revocation problems and supporting ne-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 primary troubles to make our system function admirably are the means by which the old security gadget is disavowed and how the new security gadget can do decoding legitimately. 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 centre 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 used for secure data storage while our main focus is for secure data sharing. These are two unique functionalities given by various sorts of cryptographic arrangements. We utilize an alternate way to deal with understand the two-factor procedure to tackle the key introduction and key disavowal issues. 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 centre in our proposal does not need to store any other secrets except its own private key. We expressly demonstrate that how the unscrambling is continued without uncovering the mystery put away in the security gadget. While this part isn't referenced in LLS+15. When we make utilization of ABE as IBE, our proposition is more proficient than LLS+15 as far as computational expense and capacity cost.

II. LITERATURE SURVEY

In this section, we brie y review the cryptographic schemes with similar functional-ities needed in the data sharing scenario and explain why they cannot fully achieve our goals.

2.1 Cryptographic schemes dealing with the key exposure problem:In 2002, Dodis et al. proposed a key-insulated public key scheme which is the rest paper dealing with the private key exposure problem. In such a system, there are two keys. One, named master secret key, is stored in a physically secure but computationally limited device (security device); and the other is stored in an insecure device (e.g., computer) while can be updated periodically by using the master secret key. The master secret key and the public key remain the same for all the time. Later on, Dodis et al. introduced the key insulated technique into digital signatures. However, the more frequently the private key updates, the more risk of master secret key exposes. To address this problem, in 2006, Hanaoka et al. introduced the parallel key insulated public key encryption. In further research, there are two independent master secret keys, which significantly reduces the risk of master secret key exposure. But the security proof is obtained in the random oracle model. In 2007, Libert et al. proposed a parallel key insulated public key encryption secure in the standard model. In 2008, Liu et al. applied the key insulated methodology to solve the key exposure problem in ring signature. In all the above schemes, the security device is used to update every users private key periodically. Moreover, once the private key is updated, the security device is not involved in the decryption phase. However, according to the requirements in the data sharing scenario for cloud computing, it is desired that the users private key does not updated in every time period, and the security device should be involved in every decryption phase.

2.2 An E cient Identity-based Short Signature Scheme from Bilinear Pairings(2007).

Hongzhen Du, Qiaoyan Wen present an ID-based signature scheme that is proved to be secure in the random oracle model under the hardness assumption of k-CAA problem. The proposed scheme upholds all desirable properties of previous IBS schemes. It requires general cryptographic hash functions instead of MapToPoint hash function that is ine cient and probabilistic. This scheme requires less computa-tion cost and is signi cantly more e cient than all known IBS schemes also the size of signatures generated by this scheme is approximate 160 bits, which is the shortest ID-based signatures [11].

2.3 Cryptographic schemes with the ne-grained access control: In 2005, Sahai et al.

rst introduced the notionof attribute based encryption (ABE) and further dis-cussed. Later, in 2006, Goyal et al. formalized two complementary avors of ABE: key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In a KP-ABE, the private key is associated with a policy (a boolean formula) and the ciphertext is associated with a set of attributes. While the CP-ABE is the opposite case of KP-ABE. In, the proposed ABE scheme only supports monotonic access structure. Later on, a new KP-ABE scheme sup- porting non-monotonic access structure is proposed by Ostrovsky et al. They also gave a CP-ABE construction based on the technical of where a CP-ABE secure in the random oracle model is proposed. In 2007, Cheung et al. proposed a CP-ABE scheme with non-monotonic access structure in the standard model. Later, many efficient, secure and expressive ABE schemes were proposed. However, by leveraging these schemes can only achieve the ne-grained access control but not revocability and two-factor protection which are required in the data sharing scenario for cloud computing. In 2016, Liu et al. proposed a fine grained two-factor authentication access control system for web-based cloud computing services by using the two-factor and attribute based signature techniques. They focused on building a user authentication with a privacy-preserving, ne-grained and key exposure-resisting way. As a result, Liu et al.s scheme cannot provide ne-grained access control on cipher texts like we do in this paper, and the key revocation is neither in the scope. Furthermore, the cost- consuming zero-knowledge proof technique is applied, which is against the pay-peruse nature of cloud storage. Hence, the methods used cannot be applied in our proposal, and new methods realizing the two-factor technique are desired.

2.4 In 2008, Boldyreva et al.

Cryptographic schemes with revocability: Since the proposed solution in this paper is based on ABE, we would like to review the ABE schemes with revocability. In 2008, Boldyreva et al. introduced a revocable ABE scheme which is extended from their main contribution, a revocable IBE. In their scheme, the non-revoked users need to update their private keys periodically, which is quite inconvenient. To solve this problem, Attrapadung et al. proposed a new ABE scheme with revocability, where the non-revoked users do not need to update their private keys periodically any more, but the sender needs to know the revocation list. To address this problem, in the same year, Attrapadung et al. proposed another ABE scheme, where the authors conclude that there are two methods to let ABE with revocability, namely, direct and indirect methods. The direct revocation requires the sender to know the revocation list during the encryption process, while the indirect revocation requires the non-revoked users to update their private keys periodically. The advantage of direct revocation over the indirect revocation is that the non-revoked users do not need to update their private keys periodically. On the opposite, the advantage of indirect over the direct revocation is that the sender does not need to know the revocation list. They combined both the advantages of direct and indirect revocation methods and proposed the rst hybrid revocable ABE scheme. Later, the fully secure revocable ABE were proposed. They used Composite order bilinear groups to achieve fully secure which is less efcient than the prime order bilinear groups. However, in our proposal, we only need to issue a new security device to revoke the old key without updating all other security devices, and we do not need to maintain a revocation list for all the revoked security devices. As a result, we believe that our scheme provides an alternative approach to tackle the long existing revocability problem of ABE. Another cryptographic privilege supporting revocability is proxy re-encryption (PRE) which was proposed by Blaze et al. In a proxy re-encryption scheme, a proxy (e.g., the semi-trusted cloud) can transform a ciphertext for a user into another cipher. PRE can be formal-ized into two categories in terms of the direction of transformation: bidirectional and unidirectional.

III. SYSTEM ARCHITECTURE

3.1 EXISTING SYSTEM

This is the most convenient mode of encryption for data transition, due to the elimination of key management existed in symmetric encryption. On the off chance that the client has lost his security gadget, his/her relating figure message in the cloud can't be unscrambled until the end of time! That is, the methodology can't bolster security gadget refresh/revocability. As distributed computing turns out to be increasingly developed and there will be more applications and capacity administrations given by the cloud, it is anything but difficult to anticipate that the security for information assurance in the cloud ought to be additionally upgraded. They will be-come more sensitive and important, as if the e-banking analogy. Actually, we have noticed that the concept of two-factor encryption, which is one of the encryption trends for data protection1, has been spread into some real-world applications, for example, full disk encryption with Ubuntu system, ATT two factor encryption for Smartphones2, electronic vaulting and drove cloud-based data encryption3. How-ever, these applications suffer from a potential risk about factor revocability that may limit their practicability.

3.2 PROPOSED SYSTEM

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 sender sends the cipher text to the cloud where the receiver can download it at any time. Our system provides two-factor data encryption protection. So as to unscramble the information put away in the cloud, the client needs to have two things. In the first place, the client needs his/her mystery enter which is put away in the PC. 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. More importantly, our system, for the rst time, provides security device (one of the factors) revocability. Once the security device is stolen or reported as lost, this device is revoked. That is, using this device can no longer decrypt any cipher text (corresponding to the user) in any circumstance. The cloud will immediately execute some algorithms to change the existing cipher text to be un-decryptable by 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. The cloud server cannot decrypt any cipher text at any time. We provide an estimation of the running time of our prototype to show its practicality, using some benchmark results. We also note that although there exist some naive approaches that seem to achieve our goal, that there are many limitations by each of them and thus we believe our mechanism is the rst to achieve all the above mentioned features in the literature.

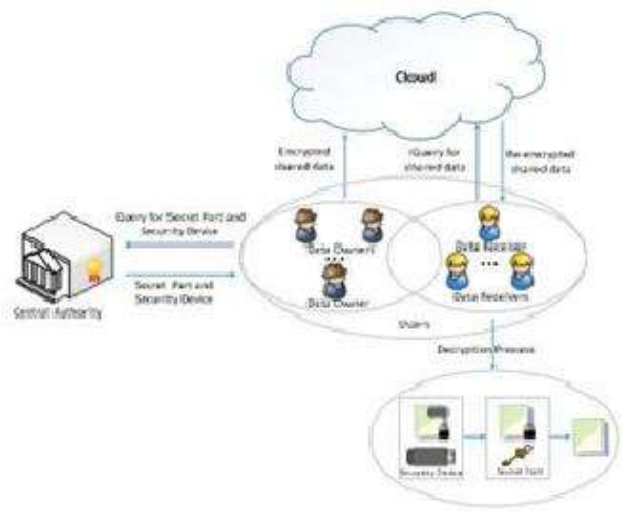

Figure 3.1: Framework Architecture

In Above architecture of CP-ABE based ne-grained two factor data protection framework. There are four entities in our framework. 1)Central Authority (CA) 2)Cloud. 3)Data Owners(DOs). 4)Data Receiver(DRs)

3.2.1 Central Authority

The CA is central and trusted party of this system.CA is responsible for issuing the cryptographic key for every user. This cryptographic key is issuing according to their attribute set and then splitting it into two part(two factor):1) Secret Part Key(SPK) Security Device Key (SDK). CA is also responsible for updating every users security device.

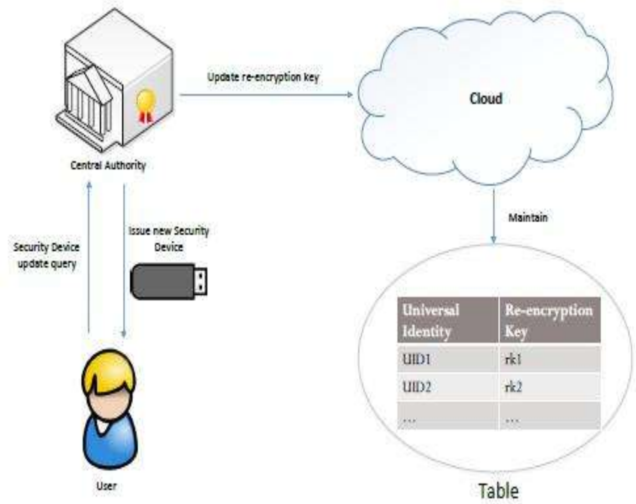

Figure 3.2: SDK update process

3.2.2 Cloud

Cloud is a semi-trust party that store all encrypted share data and maintain table. Table contain the users universal identity (UID) and corresponding re-encryption key when a DR quires for the shared data, the cloud act as proxy to re-encrypt the encrypted share data.

3.2.3 Data Owner

A DO is a user who wants to share data with other users. All the shared data are encrypted by using CP-ABE according to the access policy.

3.2.4 Data Receiver

A DR is a user who can receive the shared data from the cloud. When a DR wants to retrieve the shared data, the cloud restyle does re-encryption and then returns the resulting re-encrypted ciphertext. The re-encrypted ciphertext can be decrypted by using DRs own SPK and SDK, if DRs 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.

3.3 IMPLEMENTATION

Usage is the phase of the task when the hypothetical plan is transformed out into a working framework. In this way it tends to be viewed as the most basic stage in accomplishing a fruitful new framework and in giving the client, certainty that the new framework will work and be viable. The usage organize includes watchful arranging, examination of the current framework and its imperatives on execution, planning of strategies to accomplish changeover and assessment of changeover techniques.

IV. ALGORITHM

5.1 INIT

INIT() (param,msk): On inputting a security parameter , the algorithm (run by the CA) outputs the public parameter param and the master secret key msk.

5.2 KEYGEN

KEYGEN(param,msk,Si) (SPKi,SDKi): On inputting the public parameters param, the master secret key msk and a user UIDi with attribute set Si, the algorithm (run by the CA) outputs the secret part key SPKi and security device key SDKi for the user UIDi.

5.3 REVOCATION

REVOCATION(param,msk,UIDi) (SDKi,rki): It is an interactive algorithm per-formed between the user who wants to revoke his/her security device and the CA. At the end of this algorithm, the CA outputs the new security device key SDKi for the user and the corresponding reencryption key rki for the cloud.

5.4 DATAUPLOAD

DATAUPLOAD(param,policy,m) CT: On inputting the public parameters param, the access structure policy and the message m, the algorithm (run by the DO) outputs the ciphertext CT and uploads it to the cloud.

CONCLUSION

In this paper, we presented a novel two-factor information security assurance mecha-nism for distributed storage framework, in which an information sender is permitted to scramble the information with learning of the character of a beneficiary just, while the recipient is required to utilize the two his/her mystery key and a security gadget to access the information. Our answer not just upgrades the con dentiality of the information, yet in addition o ers the revocability of the gadget so that once the gadget is disavowed, the comparing figure content will be refreshed consequently by the cloud server with no notice of the information proprietor. Moreover, we exhibited the security verification and e ciency examination for our framework.

Bibliography

[1] C.Wang, S. S. Chow, Q.Wang, K. Ren, andW. Lou, Privacy-preserving public auditing for secure cloud storage, Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362375, 2013.

[2] C. Wang, 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. 220232, 2012.

[3] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C.-J. Hu, Dynamic audit ser-vices for outsourced storages in clouds, Services Computing, IEEE Transactions on, vol. 6, no. 2, pp. 227238, 2013.

[4] H. C. Chen, Y. Hu, P. P. Lee, and Y. Tang, Nccloud: a networkcoding- based storage system in a cloud-of-clouds, Computers, IEEE Transactions on, vol. 63, no. 1, pp. 3144, 2014.

[5] B. Libert, J.-J. Quisquater, and M. Yung, Parallel key-insulated public key encryption without random oracles, in Public Key Cryptography PKC 2007. Springer, 2007, pp. 298314.

[6] 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. 19922004, 2016.

[7] Goyal, O. Pandey, A. Sahai, and B. Waters, Attribute-based encryption for ne-grained access control of encrypted data, in Proceedings of the 13th ACM conference on Computer and communications security. Acm, 2006, pp. 8998.

[8] R. Ostrovsky, A. Sahai, and B. Waters, Attribute-based encryption with non-monotonic access structures, in Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 195203.

[9] J. Bethencourt, A. Sahai, and B. Waters, Ciphertext-policy attributebased en-cryption, in Security and Privacy, 2007. SP07. IEEE Symposium on. IEEE, 2007, pp. 321334.

[10] J. Herranz, F. Laguillaumie, and C. R`afols, Constant size ciphertexts in thresh-old attribute-based encryption, in Public Key CryptographyPKC 2010. Springer, 2010, pp. 1934