IPHV8I3008X
International Journal Of Advanced Research and Innovation -Vol.8, Issue .III
ISSN Online: 2319 – 9253
Print: 2319 – 9245

SECURE DATA RECORDS SHARING IN CLOUD COMPUTING USING REVOCABLE-CAPACITY DISTINGUISHING PROOF BASED ABSOLUTELY ENCRYPTION

#1HEENA KOUSER, M.Tech Student,
#2BOORLA SRINIVAS, Associate Professor,
Dept of CSE,
MOTHER THERESSA COLLEGE OF ENGINEERING & TECHNOLOGY, PEDDAPALLI, T.S.,INDIA.

ABSTRCT: Distributed computing gives an adaptable and helpful path for information sharing, which brings different advantages for both the general public and people. Be that as it may, there exists a characteristic resistance for clients to straightforwardly outsource the mutual information to the cloud server since the information regularly contain important data. In this manner, it is important to put cryptographically upgraded get to control on the common information. Personality based encryption is a promising crypto graphical primitive to fabricate a reasonable information sharing framework. Be that as it may, get to control is not static. That is, the point at which some client's approval is lapsed, there ought to be a component that can expel him/her from the framework. Thus, the repudiated client can't get to both the beforehand and consequently shared information. To this end, we propose a thought called revocable-capacity character based encryption (RS-IBE), which can give the forward/in reverse security of ciphertext by presenting the functionalities of client renouncement and ciphertext refresh at the same time. Besides, we introduce a solid development of RS-IBE, and demonstrate its security in the characterized security display. The execution examinations demonstrate that the proposed RS-IBE plot has focal points as far as usefulness and productivity, and hence is attainable for a commonsense and financially savvy information sharing framework. At last, we give execution aftereffects of the proposed plan to show its practicability.

Keywords: *Cloud Computing, Data Sharing, Revocation, Identity-Based Encryption, Cipher Text Update, Decryption Key Exposure.*

I. INTRODUCTION

Cloud computing is a worldview that gives massive computation limit and huge memory space at a low cost. It empowers clients to get proposed benefits independent of time and location across multiple platforms (e.g., cell phones, PCs), and in this manner conveys extraordinary accommodation to cloud clients. Among various administrations gave by distributed computing, distributed storage administration, for example, Apple's iCloud , Microsoft's Azure and Amazon's S3 , can offer a more adaptable and simple approach to share information over the Internet, which gives different advantages to our general public . In any case, it additionally experiences a few security threats, which are the primary concerns of cloud clients. Firstly, outsourcing information to cloud server suggests that information is out control of clients. This may bring about clients' hesitation since the outsourced information normally contain important and sensitive data. Secondly, information sharing is frequently actualized in an open and hostile environment, and cloud server would become a target of attacks. Surprisingly more terrible, cloud server itself may uncover clients' information for unlawful benefit. Thirdly, information sharing is not static. That is, the point at which a client's approval gets expired, he/she should no longer possess the privilege of accessing the previously and subsequently shared data. Therefore, while outsourcing information to cloud server, clients additionally need to control access to these information such that only those currently authorized users can share the outsourced data.

Obviously, such a data sharing system can provide confidentiality and backward secrecy. Furthermore, the method of decrypting and re-encrypting all the shared data can ensure forward secrecy. However, this brings new challenges. Note that the process of decrypt-then-re-encrypt necessarily involves users’ secret key information, which makes the overall data sharing system vulnerable to new attacks. In general, the use of secret key should be limited to only usual decryption, and it is inadvisable to update the ciphertext periodically by using secret key. Another challenge comes from efficiency. To update the ciphertext of the shared data, the data provider has to frequently carry out the procedure of download-decrypt-encrypt- upload. This process brings great communication and computation cost, and thus is cumbersome and undesirable for cloud users with low capacity of computation and storage. One method to avoid this problem is to require the cloud server to directly re-encrypt the ciphertext of the shared data. However, this may introduce ciphertext extension; namely, the size of the ciphertext of the shared data is linear in the number of times the shared data have been updated. In addition, the technique of proxy re-encryption can also be used to conquer the aforementioned problem of efficiency.

Unfortunately, it also requires users to interact with the cloud server in order to update the ciphertext of the shared data.

Our Contribution. Our contribution consists of two parts. First, we separate the Boldyreva et al. security model and the security level of the BF-RIBE by introducing a new realistic threat, which we call decryption key exposure, and also show that all previous RIBE schemes, except the BF-RIBE, are vulnerable to decryption key exposure.3 That is, we show that the Boldyreva et al. security model does not fully capture the exact notion for security of the BF-RIBE scheme. Roughly speaking, the Boldyreva et al. security model allows an adversary to obtain any secret keys of a chosen identity. The only one restriction is that if the adversary obtains skID∗ of the challenge identity ID∗ , then ID∗ should be revoked before the challenge time T ∗ . This model is a natural extension of the security of the ordinary IBE scheme . However, does this security model formalize all realistic threats ? For example , if the short -term decryption key dkID ,T (T≠ T ∗) is leaked, is the RIBE scheme still secure? The answer to this question may naturally appear to be 'yes' since the adversary can obtain secret keys of any chosen identity, and the decryption key can be generated from a secret key and (public) key update. But to show this thinking is wrong, we give an exceptional attack (decryption key exposure), wherein an adversary is allowed to obtain a decryption key dkID∗,T with the condition T/= T ∗ . This setting is based on the similar attitude of key-insulated PKE [16], where it is desired that no information of the plaintext is revealed from a ciphertext even if all (short-term) decryption keys of a "different time period" are exposed. This kind of attack is not covered by the Boldyreva et al. security model; that is, the adversary may obtain not a secret key skID∗ but a decryption key dkID∗,T , and ID∗ can still be alive in the system in the challenge time period T ∗≠ T. However, we can easily show that the BF-RIBE is still secure against decryption key exposure since every decryption key in the BF-RIBE is a private key with a distinct identity (ID, T) in the Boneh-Franklin IBE scheme.

Next, we revisit approaches to achieve (adaptively secure) scalable RIBE schemes, and propose a simple RIBE scheme by combining the (adaptively secure) Waters IBE scheme [39] and the (selectively secure) Boneh-Boyen IBE scheme [8]. This is the first scalable RIBE scheme with decryption key exposure resistance, and is more efficient than previous (adaptively secure) scalable RIBE schemes. Surprisingly, our construction does not require any additional efficiency cost for achieving decryption key exposure resistance. In particular, our construction has the shortest ciphertext size and a fastest decryption algorithm even compared with all scalable RIBE schemes without decryption key exposure resistance. Table 1 gives a detailed comparison with previous (efficient pairing-based) schemes. From our standard model RIBE construction, we can easily obtain more efficient RIBE construction in the random oracle model, by replacing both the Waters hash and the Boneh-Boyen hash into cryptographic hash functions that are modeled as random oracles. Our construction is natural in the sense that its security can be reduced to the original (non-revocable) Waters IBE scheme. However, in [28], Libert and Vergnaud mentioned that this kind of simple construction using the original Waters IBE scheme will face with the difficulty in the security proof, and they circumvented this by using a variant of the Waters IBE scheme [29] instead of the original.4 We resolve this difficulty by carefully dealing with the means of assigning nodes of a binary tree to each user, which we call random node assignment technique. This allows us to circumvent the difficulty, and is explained in section 4. Surprisingly, such a simple construction is secure against decryption key exposure. The main difference between ours and previous constructions is the re-randomizable property of the decryption key, whereas decryption keys use the same randomness used in the secret key in all previous constructions.

II. RELATED WORK

Public key and private key are used to encryption and decryption respectively in this paper, AES algorithm as well as KUNode algorithm is used. Normally forward secrecy or backward secrecy provided for security. In this paper, Forward secrecy is used for advanced security. Revoke user can't access the previous or subsequent data so that revocable identity based encryption technique is used. Data providers upload the files into storage server using the encryption technique. For the encryption key is used and this key provide by the key authority. Key authority is responsible for sending the key to data provider. In this paper, random function used for generating the key to encryption as well as decryption. Storage server stores the files which are uploaded by data provider. And users download or access the file as per their need. Download the file is done through decryption process. In this paper, time quantum also provided for downloading the data. Firstly for downloading file key will be send and this key is send again key authority. If key will be match between data provider and user then user will authorized to download the data. Else key does not match then the user cannot download the file. After matching key OTP will be send to the user. At this stage, time limit should be provided because of more security for accessing the data using cloud computing. Within a time period user can type the OTP. If OTP is type within time then user can access this file. Else time period is expired then user cannot access this file. And one more condition is that, if OTP is wrong then user enters into revoke list .In this paper, extra mechanism provided for the secure data sharing in cloud computing.

Recently, several functional encryption (FE) schemes, which are generalizations of the IBE scheme, have been proposed [23, 36], and the revocation capability in FE has also been studied [3, 4, 34]. The revocation method used in [4, 34] differs from RIBE contexts; the senders carry out the revocation, so it does not require any private key update procedures on the recipient's side. In [3] Attrapadung and Imai considered two different ways for revocation method; one is similar to that in [4, 34], and the other is similar to that in RIBE schemes. However, decryption key exposure is not considered in [3], so achieving revocation capabilities in FE with decryption key exposure resistance would be an interesting future area of study. All revocable IBE schemes use a strategy in which only decryption keys of users who are not revoked in a time period T can be updated in time period T. This strategy is similar to those for cryptosystems against key exposure such as key-insulated PKE [16, 6, 27] and IBE [22, 21, 40, 41], forward secure encryption [12], and intrusion-resilient PKE [15]. However, these systems require a secure channel between a user and a key issuer or do not support scalability.

III. SYSTEM DESIGN

In this system first data provider upload the file. And upload file convert into the encrypted format using key encryption algorithm. I.e. AES algorithm. Then storage server responsible not only storing the data or files but, also give permission for unrevoked user to access the data or files through cloud computing.

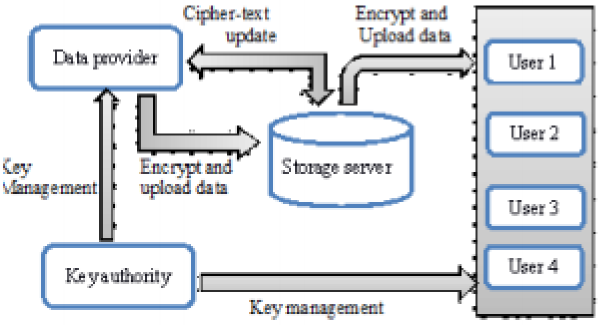

Figure-1: System Architecture

User send request for accessing data permission to data provider via storage server. Then key authority generates the key as per user requested data. These generated key is send to user. After receiving key, data provider key and user key will be match. If key will be match then user is authorized to download the data. Else it cannot the file. After matching of key again OTP will be send to user for extra security. User can write the OTP within time period. Again user will write the OTP within a time period. Then user can download the required file successfully. Else it cannot download the needed file. This whole process provide large security in cloud computing. In this paper, extra security for data sharing in cloud computing should be provided. There for sharing data through cloud computing is securely.

3.1 Data Provider

Data provider is working as a cloud and it provides important data. Cloud computing is based on internet computing it provides data and resources to the computer very securely. This model is for enabling ubiquitous to share a pool of configurable computing resources for e.g. Server, application, and computer network. For obtaining information user request to the data provider then data provider accept the request of the user and then work on data analysis. Next data is encrypting by the data provided by using the key and sequence key provide by key authority. The Time quantum is also set by data provider. Key updating can be done by data provider.

3.2 Number Of User

Multiple users can access their data from cloud at a one time. Each user have different key for decryption. Each user can access the data in particular time quantum. Users can access meaningful information from cloud. Key authority manager provide the key to user for decryption purpose. In this paper, additional thing is OTP, and time period is provided for the writing the key.

3.3 Storage Server

In the data sharing concept storage server is most important module. The storage data store the huge amount of data. This data is securely store in storage server. The storage server is securely store the data. It also store encrypted data and key which used for data encryption. When the user requires his data, user requests to the storage server. There are two keys used for encryption and decryption purpose. Data sharing can be done by this server.

3.4 Key Authority

The key which is used for encryption as well as decryption is generated by key authority. There are two algorithm is used for key generation. KUNodes algorithm and RS_IBE algorithm these two algorithms are used for key authority. In this paper, matching a key is important for security. Key authority generates the key and it will provide to the user as well as data provider. And both key matched to each other for sharing the secure data in cloud computing.

IV. REVOCABLE IDENTITY-BASED ENCRYPTION

We basically used two level hierarchical construction and it is not difficult to extend our construction to three level hierarchical construction (but revocation capability is allowed only for the first level). Therefore, we can apply the well-known Naor transformation from an IBE scheme to a signature scheme. More precisely, from the three level hierarchical construction, we can obtain a scalable identity-based signature scheme, where the first level is for identity, the second level is for time period, and the third level is for message. For better efficiency, we can apply the same transformation used in the previous paragraph to here, and then obtain an efficient RIBS scheme in the random oracle model.

The concept of identity-based encryption was introduced by Shamir and conveniently instantiated by Boneh and Franklin. IBE eliminates the need for providing a public key infrastructure (PKI). Regardless of the setting of IBE or PKI, there must be an approach to revoke users from the system when necessary, e.g., the authority of some user is expired or the secret key of some user is disclosed. In the traditional PKI setting, the problem of revocation has been well studied and several techniques are widely approved, such as certificate revocation list or appending validity periods to certificates. However, there are only a few studies on revocation in the setting of IBE. Boneh and Franklin first proposed a natural revocation way for IBE. They appended the current time to the ciphertext, and non-revoked users periodically received private keys for each time from the key authority. Unfortunately, such a solution is not scalable, since it requires the key authority to perform linear work in the number of non revoked users. In addition, a secure channel is essential for the key authority and non-revoked users to transmit new keys. To conquer this problem, Boldyreva, Goyal and Kumar introduced a novel approach to achieve efficient revocation. They used a binary tree to manage identity such that their RIBE scheme reduces the complexity of key revocation to logarithmic (instead of linear) in the maximum number of system users. However, this scheme only achieves selective security. Subsequently, by using the aforementioned revocation technique, Libert and Vergnaud proposed an adaptively secure RIBE scheme based on a variant of Water's IBE scheme, Chen et al. constructed a RIBE scheme from lattices. Recently, Seo and Emura proposed an efficient RIBE scheme resistant to a realistic threat called decryption key exposure, which means that the disclosure of decryption key for current time period has no effect on the security of decryption keys for other time periods. Inspired by the above work and Liang et al. Introduced a cloud-based revocable identity-based proxy re-encryption that supports user revocation and ciphertext update. To reduce the complexity of revocation, they utilized a broadcast encryption scheme to encrypt the ciphertext of the update key, which is independent of users, such that only non-revoked users can decrypt the update key. However, this kind of revocation method cannot resist the collusion of revoked users and malicious non-revoked users as malicious non-revoked users can share the update key with those revoked users. Furthermore, to update the ciphertext, the key authority in their scheme needs to maintain a table for each user to produce the re-encryption key for each time period, which significantly increases the key authority's workload.

V. FORWARD-SECURE CRYPTOSYSTEMS

In 1997, Anderson [28] introduced the notion of forward security in the setting of signature to limit the damage of key exposure. The core idea is dividing the whole lifetime of a private key into T discrete time periods, such that the compromise of the private key for current time period cannot enable an adversary to produce valid signatures for previous time periods. Subsequently, Bellare and Miner provided formal definitions of forward-secure signature and presented practical solutions. Since then, a large number of forward-secure signature schemes [29], [30], [31], [32], [33] has been proposed. In the context of encryption, Canetti, Halevi and Katz [34] proposed the first forward-secure public-key encryption scheme. Specifically, they firstly constructed a binary tree encryption, and then transformed it into a forward-secure encryption with provable security in the random oracle model. Based on Canetti et al's approach, Yao et al. [35] proposed a forward-secure hierarchical IBE by employing two hierarchical IBE schemes, and Nieto et al. [36] designed a forward-secure hierarchical predicate encryption. Particularly, by combining Boldyreva et al.'s [20] revocation technique and the aforementioned idea of forward security1, in CRYPTO 2012 Sahai, Seyalioglu and Waters [37] proposed a generic construction of so-called revocable storage attribute-based encryption, which supports user revocation and ciphertext update simultaneously. In other words, their construction provides both forward and backward secrecy. What must be pointed out is that the process of ciphertext update of this construction only needs public information. However, their construction cannot be resistant to decryption key exposure, since the decryption is a matching result of private key and update key.

V. METHODOLOGY

We introduce a notion called revocable storage identity-based encryption (RS-IBE) for building a cost-effective data sharing system that fulfills the three security goals. More precisely, the following achievements are captured in this paper:

- We present a concrete construction of RS-IBE. The proposed scheme can provide confidentiality and backward/forward secrecy simultaneously.
- We prove the security of the proposed scheme in the standard model, under the decisional ℓ-Bilinear Diffie-Hellman Exponent (ℓ-BDHE) assumption. In addition, the proposed scheme can withstand decryption key exposure.

The proposed scheme is efficient in the following ways:

1. They utilized the idea to provide the forward secrecy of Cipher Text, rather than secret key as in the original case.
2. our scheme achieves forward security under the assumption that the encrypted data is stored in the cloud and users do not store the encrypted/decrypted data locally.

- The procedure of Cipher Text update only needs / public information. Note that no previous identity-based encryption schemes in the literature can provide this feature;
- The additional computation and storage complexity, which are brought in by the forward secrecy, is all upper bounded by O(log(T)2), where T is the total number of time periods.

VI.CONCLUSION

Cloud computing brings great convenience for people. Particularly, it perfectly matches the increased need of sharing data over the Internet. In this paper, to build a cost-effective and secure data sharing system in cloud computing, we proposed a notion called RS-IBE, which supports identity revocation and ciphertext update simultaneously such that a revoked user is prevented from accessing previously shared data, as well as subsequently shared data. Furthermore, a concrete construction of RS-IBE is presented. The proposed RS-IBE scheme is proved adaptive-secure in the standard model, under the decisional ℓ-DBHE assumption. The comparison results demonstrate that our scheme has advantages in terms of efficiency and functionality, and thus is more feasible for practical applications.

REFERENCES

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, —A break in the clouds: towards a cloud definition,‖ ACM SIGCOMMComputer Communication Review, vol. 39, no. 1, pp. 50–55, 2008.

[2] iCloud. (2014) Apple storage service. [Online]. Available: https://www.icloud.com/

[3] Azure. (2014) Azure storage service. [Online]. Available: http://www.windowsazure.com/

[4] Amazon. (2014) Amazon simple storage service (amazon s3). [Online]. Available: http://aws.amazon.com/s3/

[5] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, —Social cloud computing: A vision for socially motivated resource sharing,‖Services Computing, IEEE Transactions on, vol. 5, no. 4, pp. 551–563,2012.

[6] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, —Privacypreserving public auditing for secure cloud storage,‖ Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013.G. Anthes, —Security in the cloud,‖ Communications of the ACM, vol. 53, no. 11, pp. 16–18, 2010.

[7] K. Yang and X. Jia, —An efficient and secure dynamic auditing protocol for data storage in cloud computing,‖ Parallel and DistributedSystems, IEEE Transactions on, vol. 24, no. 9, pp. 1717–1726, 2013.

[8] B. Wang, B. Li, and H. Li, —Public auditing for shared data with efficient user revocation in the cloud,‖ in INFOCOM, 2013Proceedings IEEE. IEEE, 2013, pp. 2904–2912.

[9] S. Ruj, M. Stojmenovic, and A. Nayak, —Decentralized accesscontrol with anonymous authentication of data stored in clouds,‖Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2,pp. 384–394, 2014.

[10]X. Huang, J. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu, and J. Zhou, —Cost-effective authentic and anonymous data sharingwith forward security,‖ Computers, IEEE Transactions on, 2014, doi:10.1109/TC.2014.2315619.

[11]C.-K. Chu, S. S. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng,—Key-aggregate cryptosystem for scalable data sharing in cloud storage,‖ Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 468–477, 2014.

[12]A. Shamir, —Identity-based cryptosystems and signature schemes,‖ in Advances in cryptology. Springer, 1985, pp. 47–53.

[13]D. Boneh and M. Franklin, —Identity-based encryption from the weil pairing,‖ SIAM Journal on Computing, vol. 32, no. 3, pp. 586–615, 2003.

[14]W. Aiello, S. Lodha, and R. Ostrovsky, —Fast digital identity revocation,‖ in Advances in Cryptology–CRYPTO 1998. Springer,1998, pp. 137–152.

[15]D. Naor, M. Naor, and J. Lotspiech, —Revocation and tracing schemes for stateless receivers,‖ in Advances in Cryptology– CRYPTO 2001. Springer, 2001, pp. 41–62.