Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption

[1]Kishore Babu V, [2]R Amutha

[1]PG Student, [2]Research Scholar
AMCEC Bengaluru.

***Abstract*— Cloud computing provides a flexible and convenient way for data sharing, which brings various benefits for both the society and individuals. But there exists a natural resistance for users to directly outsource the shared data to the cloud server since the data often contain valuable information. Thus, it is necessary to place cryptographically enhanced access control on the shared data. Identity-based encryption is a promising cryptographical primitive to build a practical data sharing system. However, access control is not static. That is, when some user's authorization is expired, there should be a mechanism that can remove him/her from the system. Consequently, the revoked user cannot access both the previously and subsequently shared data. To this end, we propose a notion called revocable-storage identity-based encryption (RS-IBE), which can provide the forward/backward security of ciphertext by introducing the functionalities of user revocation and ciphertext update simultaneously.**

I. INTRODUCTION

CLOUD computing is a paradigm that provides massive computation capacity and huge memory space at a low cost [1]. It enables users to get intended services irrespective of time and location across multiple platforms (e.g., mobile devices, personal computers), and thus brings great convenience to cloud users. Among numerous services provided by cloud computing, cloud storage service, such as Apple's iCloud [2], Microsoft's Azure [3] and Amazon's S3 [4], can offer a more flexible and easy way to share data over the Internet, which provides various benefits for our society [5], [6]. However, it also suffers from several security threats, which are the primary concerns of cloud users [7]. Firstly, outsourcing data to cloud server implies that data is out control of users. This may cause users' hesitation since the outsourced data usually contain valuable and sensitive information. Secondly, data sharing is often implemented in an open and hostile environment, and cloud server would become a target of attacks. Even worse, cloud server itself may reveal users' data for illegal profit. Thirdly, data sharing is not static. That is, when a user's authorization gets expired, he/she should no longer possess the privilege of accessing the previously and subsequently shared data. Therefore, while outsourcing data to cloud server, users also want to control access to these data such that only those currently authorized users can share the outsourced data.

A natural solution to conquer the problem is to use cryptographically enforced access control such as identity-based encryption (IBE).

II. CLOUD SECURITY

Besides, to overcome the above security threats, such kind of identity-based access control placed on the shared data should meet the following security goals:

A. Data confidentiality:

Unauthorized users should be prevented from accessing the plaintext of the shared data stored in the cloud server. In addition, the cloud server, which is supposed to be honest but curious, should also be deterred from knowing plaintext of the shared data.

B. Backward secrecy:

Backward secrecy means that, when a user's authorization is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the subsequently shared data that are still encrypted under his/her identity.

C. Forward secrecy:

Forward secrecy means that, when a user's authority is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the shared data that can be previously accessed by him/her. the plaintext of the subsequently shared data that are still encrypted under his/her identity.

III. RIBE OPERATION

The concept of identity-based encryption was introduced by Shamir [13], and conveniently instantiated by Boneh and Franklin [14]. 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 [15], [16], [17], [18], [19], 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 [14] first proposed a natural revocation way for IBE. They appended the current time period to the ciphertext, and non-revoked users periodically received private keys for each

time period 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 [20] 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 [21] proposed an adaptively secure RIBE scheme based on a variant of Water's IBE scheme [22], Chen et al. [23] constructed a RIBE scheme from lattices.Recently, Seo and Emura [24] 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 [25], Liang et al. [26] 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 [27] 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 nonrevoked 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. However, this may introduce ciphertext extension, namely, the size of the ciphertext of the shared datais linear in the number of times the shared data havebeenupdated. In addition, the technique of proxy re- encryptioncan also be used to conquer the problemofefficiency.

IV. REVOCABLE IDENTITY-BASED ENCRYPTION

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.

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.

[16] C. Gentry, "Certificate-based encryption and the certificate revocation problem," in Advances in Cryptology–EUROCRYPT 2003.Springer, 2003, pp. 272–293.

[17] V. Goyal, "Certificate revocation using fine grained certificatespace partitioning," in Financial Cryptography and Data Security.Springer, 2007, pp. 247–259.

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

[19] S. Micali, "Efficient certificate revocation," Tech. Rep., 1996.

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

[21] B. Libert and D. Vergnaud, "Adaptive-id secure revocable identitybased encryption," in Topics in Cryptology–CT-RSA 2009. Springer, 2009, pp. 1–15.

[22] ——, "Towards black-box accountable authority ibe with short ciphertexts and private keys," in Public Key Cryptography–PKC2009. Springer, 2009, pp. 235–255.

[23] J. Chen, H. W. Lim, S. Ling, H. Wang, and K. Nguyen, "Revocable identity-based encryption from lattices," in Information Security andPrivacy. Springer, 2012, pp. 390–403.

[24] J. H. Seo and K. Emura, "Revocable identity-based encryption revisited: Security model and construction," in Public-Key Cryptography–PKC 2013. Springer, 2013, pp. 216–234.

[25] ——, "Efficient delegation of key generation and revocation functionalities in identity-based encryption," in Topics in Cryptology– CT-RSA 2013. Springer, 2013, pp. 343–358.

[26] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloudbased revocable identity-based proxy re-encryption scheme for public clouds data sharing," in Computer Security-ESORICS 2014.Springer, 2014, pp. 257–272.

[27] D.-H. Phan, D. Pointcheval, S. F. Shahandashti, and M. Strefler, "Adaptive cca broadcast encryption with constant-size secret keysand ciphertexts," International journal of information security, vol. 12,no. 4, pp. 251–265, 2013.

[28] R. Anderson, "Two remarks on public-key cryptology (invited lecture)," 1997.

[29] M. Bellare and S. K. Miner, "A forward-secure digital signature scheme," in Advances in Cryptology–CRYPTO 1999. Springer, 1999,pp. 431–448.

[30] M. Abdalla and L. Reyzin, "A new forward-secure digital signature scheme," in Advances in Cryptology–ASIACRYPT 2000. Springer, 2000, pp. 116–129.

[31] A. Kozlov and L. Reyzin, “Forward-secure signatures with fast key update,” in Security in communication Networks. Springer,2003, pp. 241–256.

[32] X. Boyen, H. Shacham, E. Shen, and B. Waters, “Forward-secure signatures with untrusted update,” in Proceedings of the 13th ACMconference on Computer and communications security. ACM, 2006,pp. 191–200.

[33] J. Yu, R. Hao, F. Kong, X. Cheng, J. Fan, and Y. Chen, “Forwardsecure identity-based signature: security notions and construction,” Information Sciences, vol. 181, no. 3 pp. 648–660, 2011.

[34] R. Canetti, S. Halevi, and J. Katz, “A forward-secure public-key encryption scheme,” in Advances in Cryptology–Eurocrypt 2003.Springer, 2003, pp. 255–271.

[35] D. Yao, N. Fazio, Y. Dodis, and A. Lysyanskaya, “Id-based encryption for complex hierarchies with applications to forward security and broadcast encryption,”.