4th International Conference on Recent Development in Engineering Science, Humanities and Management
National Institute of Technical Teachers Training & Research, Chandigarh, India (ESHM-17)
2nd April 2017, www.conferenceworld.in ISBN: 978-93-86171-19-1

A SURVEY ON REVOCABLE IDENTITY-BASED ENCRYPTION IN CLOUD COMPUTING

Kedar G. Pathare[1], Prof. P. M. Chouragade[2]

[1]*Computer Science and Engineering, Government College of Engineering, Amravati, (India)*

[2]*Computer Science and Engineering, Government College of Engineering, Amravati, (India)*

ABSTRACT

Cloud computing provides convenient way for data sharing for users. But sometime users may need to outsourced the shared data to cloud server though it contain valuable information. Security has always been a big concern when it comes to data sharing in cloud computing. Thus it is necessary to place cryptographically enhanced access control on the shared data. The paper discuss about a promising cryptographical primitive for data sharing in cloud which is Identity-based encryption. We first introduce the revocable-storage identity-based encryption scheme which provides both forward and backward security of ciphertext. Then we will have glance at all the techniques that have been used for implementation of identity-based encryption so for. Finally we conclude the paper.

Keywords - Cloud Computing, Data Sharing, Identity-Based Encryption, Revocation

I. INTRODUCTION

Cloud computing is technology that provides high computational capability and high memory space at low cost. It gives users various services irrespective of time and location across various platforms. Cloud computing brings great convenience for users. Cloud service providers offer flexible and efficient way to share data over internet which provides various benefits but also vulnerable to various security threats which is a primary concern of users.

Cloud user may need to outsourced the shared data to cloud server though it contain valuable or sensitive information. Outsourced data is out control of users. Cloud servers can also become victim of attacks. In the worst case cloud server may reveal user data in public for illegal profit. In cloud sharing system if users authorization is revoked he/she should no longer be able to access data previously shared to him/her. While outsourcing data to cloud, users should be control access to the data so that only authorized users can share outsourced data. Identity-based encryption (IBE) is access control scheme which provides solution to all the aforementioned problems. Identity-based encryption also meets data confidentiality, forward secrecy and backward secrecy. In this paper we will discuss previous techniques that has been used for the implementation of identity-based encryption.

To overcome the aforementioned security threats in previous section identity-based encryption scheme should meet following security goals.

- Data Confidentiality

Unauthorized users should not be allowed to access the plaintext of the shared data stored in cloud storage. Even Cloud service provider should also be deterred from knowing the plaintext of the shared data.

ISBN: 978-93-86171-19-1

- Backward Secrecy

Backward secrecy means that, if user's secret key is compromised or his/her authorization is expired, he/she should not be able to access the plaintext of the subsequently shared data that was earlier encrypted under his/her identity.

- Forward Secrecy

Forward secrecy means that, if user's secret key is compromised or authorization is expired, he/she should not be able to access the plaintext of shared data that was previously accessed by him/her.

The above security goals should be conquer in the Identity-based encryption scheme. We also note that some security issues like authenticity and availability of shared data are equally important in the practical data sharing system [8], [9], [10], [11], [12].

II IDENTITY-BASED ENCRYPTION SCHEME

Identity-based encryption (IBE) is an effective alternative for public-key encryption, which removes the need of Public Key Infrastructure (PKI). In Identity-based encryption scheme the sender does not need to get the public keys and the certificates of the receiver for the encryption, because the identities like emails or IP address together with common public attributes are sufficient for encryption. The private keys are generated by private key generator (PKG) which is a trusted third party. The idea of identity-based cryptography was introduced in 1984 by Shamir[14]. But it was conveniently instantiated by Boneh and Franklin in 2001[15], building on the progress in elliptic curves with bilinear pairings. A first scheme for IBE was based on the bilinear Diffie-Hellman assumption in the random oracle model by Boneh and Franklin [15]. In IBE schemes private key generator is essential for creating private keys for all users and because of that it is performance bottleneck for organization with large number of users.

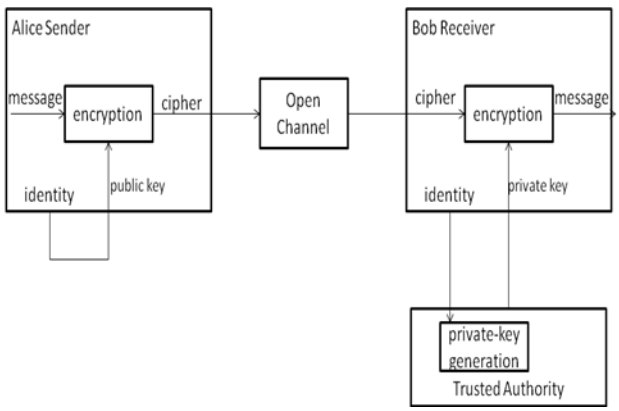

Figure 1 Shamir's IBE concept in 1984

The above figure 1 [41] shows architecture of Identity-based encryption scheme by Shamir in 1984. Figure illustrates the working of encryption and decryption using IBE scheme.

III REVOCABLE IDENTITY-BASED ENCRYPTION SCHEME

Revocation capability is important for IBE as well as PKI setting. If the authority of some user is expired or the secret key is compromised there must be an approach to revoke user from the system. In the traditional PKI setting, the revocation problem has been well studied [16], [17], [18], [19], [20] and various techniques are

ISBN: 978-93-86171-19-1

widely approved, such as appending validity periods to certificates or certificate revocation list. But there are only few studies on the revocation in identity-based encryption scheme. First natural revocation way for Identity-based Encryption was proposed by Boneh and Franklin [15]. They concatenated the current time period to the ciphertext and non-revoked users received private keys from the key authority periodically. But such solution was not scalable as it required the key authority to perform linear work in the number of non-revoked users. In addition, a secure channel is required between key authority and non-revoked users to transfer new generated keys. To overcome this problem, Boldyreva, Goyal and Kumar [21] introduced a novel approach for the efficient revocation. The reduce the complexity of Revocable Identity-based encryption scheme to logarithmic in the maximum number of users by using binary tree to manage identity. Later by using the above revocation technique, Libert and Vergnaud [22] proposed an adaptively secure Revocable Identity-based scheme based on variation of Water's IBE scheme[23], Chen et al. [24] created RIBE scheme from lattices.

Seo and Emura [25] proposed an effective RIBE scheme which was resistant to decryption key exposure problem, that means though decryption key for current time period exposed would not have effect on the security of decryption keys for other time periods. Later Liang et al. [26] introduced a cloud-based RIBE proxy re-encryption that allows user revocation and ciphertext update. They utilized a broadcast encryption scheme [28] to encrypt the ciphertext of the update key, which is independent of users, such that only non-revoked users can decrypt the update key it also reduce the complexity of revocation. But this revocation method cannot oppose 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 needs to maintain a table for users to produce the re-encryption key for each time period which increases the workload of key authority.

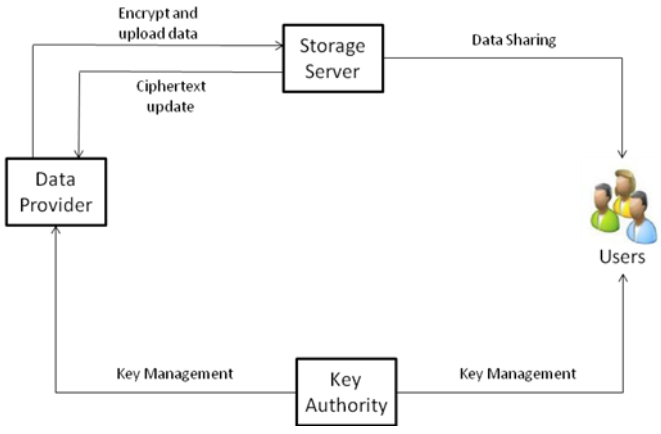

Figure 2 Natural RIBE-based data sharing system

Revocable Identity-based Encryption scheme enables sender to concatenate the current time period to the ciphertext such that only receiver can decrypt the ciphertext if and only if he/she is not revoked out of the system at that time period. Figure 2 [1] shows the working of natural RIBE-based data sharing system.

Step 1. The data provider first decides the users who can share the data, then data provider encrypt the data under the identities of users and uploads the ciphertext of the shared data to cloud storage.

Step 2. When users wants to get the shared data, they download and decrypt the ciphertext. However the plaintext of the shared data is not available to unauthorized users of cloud server.

ISBN: 978-93-86171-19-1

Step 3. If user authorization is expired then data provider can download the ciphertext of the shared data and then decrypt-then-re-encrypt the shared data such that unauthorized user is prevented from accessing the plaintext of the shared data and then upload re-encrypted data to the cloud storage.

Obviously, above data sharing system can provide confidentiality and backward secrecy. It also ensures forward secrecy by implementing the method of decrypting and then re-encrypting of all the shared data. Since decrypt-then-re-encrypt requires users secret key information this makes whole data sharing system vulnerable to attacks. Another challenge comes from efficiency. As data provide has to frequently carried out decrypt-then-re-encrypt procedure to update the ciphertext to prevent from shared data from revoked users. This brings high computational cost and it is cumbersome and undesirable for cloud users. The technique of proxy re-encryption scheme can be used to overcome the aforementioned problem.

IV FORWARD-SECURE CRYPTOSYSTEM

Anderson [29] introduced the idea of forward security in the setting of signature to prevent the key exposure. The idea was dividing the private key into T discrete time periods, such that compromise of the private key for current time period will not allow to produce valid signature for previous time periods. Later formal definitions of forward-secure signature and practical solutions were provided by Bellare and Miner. Since then, various forward-secure signature schemes [30], [31], [32], [33], [34] has been created.

In the context of encryption, Canetti, Halevi and Katz [35] proposed the first forward-secure public-key encryption scheme. They firstly created a binary tree encryption and then transformed it into a forward-secure encryption with security in the random oracle model. Yao et al.[36] proposed a forward -secure hierarchical IBE based on Canetti et al's approach. Nieto et al. [37] designed a forward-secure hierarchical predicate encryption scheme. Combination of Boldyreva et al's revocation technique and Nieto et al's technique in CRYPTO 2012 Sahai, Seyaioglu and Waters [21] proposed a generic construction called as revocable storage attribute-based encryption, which supports the user revocation and ciphertext update simultaneously. Their scheme provides both forward and backward secrecy. Ciphertext updating of this aforementioned schemes only needs public information. However this schemes should not be resistant to decryption key exposure, since the decryption is a matching result of private and update key.

V CONCLUSION

The above schemes if applied to cloud computing can increase the security of the cloud storage. Identity-based encryption scheme can give access control to the user hand though the data is outsourced to the cloud servers. Revocable-Identity based encryption can prevent the shared data be accessed by revoked users from the system. Some advancements in the previous RIBE scheme is required to reduce the complexity and computational cost at the cloud servers.

REFERENCES

[1] Jianghong Wei, Wenfen Liu, Xuexian Hu, "Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption", IEEE Transactions on Cloud Computing, Vol. 14, No. 8, August 2015

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

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

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

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

[6] 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.

[7] 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.

[8] G. Anthes, "Security in the cloud," Communications of the ACM, vol. 53, no. 11, pp. 16–18, 2010.

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

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

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

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

[13] 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. 2168-7161

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

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

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

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

[18] 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.

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

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

[21] 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.

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

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

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

[25] 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.

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

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

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

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

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

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

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

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

[34] 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.

[35] 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.

[36] D. Yao, N. Fazio, Y. Dodis, and A. Lysyanskaya, "Id-based encryption for complex hierarchies with applications to forward security and broadcast encryption," in Proceedings of the 11th ACM conference on Computer and communications security. ACM, 2004, pp. 354–363.

[37] J. M. G. Nieto, M. Manulis, and D. Sun, "Forward-secure hierarchical predicate encryption," in Pairing-Based Cryptography–Pairin 2012. Springer, 2013, pp. 83–101.

ISBN: 978-93-86171-19-1

[38] A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for attribute-based encryption," in Advances in Cryptology–CRYPTO 2012. Springer, 2012, pp. 199–217.

[39] B. Waters, "Efficient identity-based encryption without random oracles," in Advances in Cryptology–EUROCRYPT 2005. Springer, 2005, pp. 114–127.

[40] B. Lynn. (2014) Pbc library: The pairing-based cryptography library. [Online]. Available: http://crypto.stanford.edu/pbc/

[41] Liqun Chen "Identity-Based Cryptography", Hewlett-Packard Laboratories. www.sti.uniurb.it/events/fosad06/papers/Chen-fosad06.pdf