Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

Attribute Based Encryption to Data for Storage in Cloud

Md. Fayaz and Shaik Reshma,
Affiliated to Department of CSE, DR.K.V.Subba Reddy Women's Engineering College, Kurnool, Andhra Pradesh, India

***Abstract*—**Cloud storage services have become drastically popular. Because of the importance of privacy, many cloud storage encryption procedures have been proposed to protect data from those who do not have access. All such schemes assumed that cloud storage providers are safe and cannot be hacked; however, in practice, some authorities (i.e., coercers) may force cloud storage providers to reveal user secrets or confidential data on the cloud, thus altogether circumventing storage encryption schemes. In this paper, we present our design for a new cloud storage encryption scheme that enables cloud storage providers to create convincing fake user secrets to protect user privacy. Since coercers cannot tell if obtained secrets are true or not, the cloud storage providers ensure that user privacy is still securely protected.

Index Terms— *Encryption, Composite Order Bilinear Group, Attribute-Based Encryption, Cloud Storage*

I. INTRODUCTION

Deniable encryption involves senders and receiverscreating convincing fake evidence of forged data inciphertexts such that outside coercers are satisfied. Notethat deniability comes from the fact that coercers cannotprove the proposed evidence is wrong and thereforehave no reason to reject the given evidence. This approachtries to altogether block coercion efforts sincecoercers know that their efforts will be useless. We makeuse of this idea such that cloud storage providers canprovide audit-free storage services. In the cloud storagescenario, data owners who store their data on the cloudare just like senders in the deniable encryption scheme.Those who can access the encrypted data play the role ofreceiver in the deniable encryption scheme, including thecloud storage providers themselves, who have systemwidesecrets and important information and must be able to decrypt all encrypted and secured data.

II. PREVIOUS WORK ON ABE

ABE a very usefultool for cloud storage services since data sharing is animportant feature for such services. There are so manycloud storage users that it is impractical for data ownersto encrypt their data by pairwise keys. Moreover, it isalso a impractical to encrypt data many times for so manypeople. With ABE, data owners decide only which kindof users can access their encrypted data. Users who can satisfy the conditions are able to decrypt the encrypteddata.

There are two types of ABE, CP-ABE and Key-PolicyABE (KP-ABE). The difference between these two lies in policy checking. KP-ABE is an ABE in which the policyis embedded in the user secret key and the attributeset is embedded in the modified or secret orciphertext. Conversely, CP-ABEembeds the policy into the ciphertext and the user secrethas the attribute set. Goyal et al. proposed the first KPABEin they constructed an expressive way to relateany monotonic formula as the policy for user secretkeys. Bethencourt et al. proposed the first CP-ABE inThis scheme used a tree access structure to expressany monotonic formula over attributes as the policy inthe ciphertext. The first fully expressive CP-ABE wasproposed by Waters in, which used Linear SecretSharing Schemes (LSSS) to build a ciphertext policy.Lewko et al. enhanced the Waters scheme to a fullysecure CP-ABE, though with some efficiency loss, in [13].Recently, Attrapadung et al. constructed a CP-ABE witha constant-size ciphertext in and Tysowski et al.designed their CP-ABE scheme for resource-constrained users in.

III. OUR CONTRIBUTIONS

We construct a deniable CP-ABE scheme that can make cloud storage services more secure. In this scenario, cloud storage service providers are just regarded as simple receivers in other deniable schemes. Unlike most commonly deniable encryption schemes, we do not use translucent sets public key systems to implement deniability. Instead, we adopt the idea proposed with some improvements.We construct our deniable encryption scheme througha different multidimensional space. All data are encrypted intothe multidimensional space. Only with the correct compositionof different dimensions is the original data obtainable.With false composition, encrypted texts will be decrypted topredetermined fake data. The information defining thedimensions is kept securely secret. We make use of order bilinear groups to construct the multidimensionalspace. We also use chameleon hash functions to makeboth true and fake messages convincing after decryption.

Blockwise Deniable ABE.

Most deniable public key procedures are bitwise, which means these schemes can only process one bit a time; therefore, bitwise deniable encryption schemes are inefficient for real use, especially in the cloud storage service case. To solve this problem we designed a hybrid encryption scheme that simultaneously uses symmetric and asymmetric simple encryption. They use a deniably encrypted plan-ahead symmetric data encryption key, while real data are encrypted by a symmetric key encryption mechanism. This will drastically reduces the repeating number from the block size to the key size. Though bitwise deniable encryption is more flexible than block size deniableencryption in ”cooking” fake data.

Deterministic Decryption.

Most deniable encryption techniques have decryption error problems. These errors come from the designed decryption mechanisms uses the subset decision mechanism for decryption.

The receiver determines the decrypted message according to the subset decision result. If the sender chooses an element from the universal set but unfortunately the element is located in the specific subset, then an error occurs. The same error occurs in all selected set- based deniable encryption schemes. One more example is which uses a voting mechanism for decryption. Decryption is correct if and only if thecorrect part overwhelms the false part. Otherwise, the receiver will get the error result.

- **KeyGen**$(MSK, S) \rightarrow SK$: Given set S of attributes, this algorithm chooses $t \in \mathbb{Z}_p$ randomly and outputs the private key as:

$$K = g^{\alpha+at}, L = g^t, \forall x \in SK_x = H(x)^t.$$

- **Decrypt**$(CT, SK) \rightarrow \mathcal{M}$: Suppose that S satisfies the access structure and let $I \subset \{1, \ldots, l\}$ be defined as $I = \{i : \rho(i) \in S\}$. This algorithm finds a set of constants $\{w_i \in \mathbb{Z}_p\}$ such that $\sum_{i \in I} w_i \lambda_i = s$. The decryption algorithm computes

$$e(C', K)/(\prod_{i \in I}(e(C_i, L)e(D_i, K_{\rho(i)}))^{w_i}) = e(g, g)^{\alpha s}$$

and derives $\mathcal{M}$ from the ciphertext.

Consistent Environment

We build a reliable environmentfor our deniable encryption procedure. By reliableenvironment, we means that one encryption technique used in this environmentcan be used for multiple encryption times

without system modifications or updates. The opened receiver proof or identity should look convincing for all cipher or modified texts under thisenvironment, regardless of whether a cipher or modified textis normally encrypted attribute based encrypted or deniably encrypted. Thedeniability of our procedure comes from the secret ofthe partial group or subgroup assignment, which is determined or checked onlyonce in the system setup phase. By the canceling or rechecking property and the proper subgroup assignment, wecan construct the released fake key to decrypt normalcipher or modified texts correctly.

CONCLUSIONS

We proposed a deniable CP-ABE procedure to build an audit-free cloud storage service. The deniability feature makes coercion invalid, and the ABE property ensures the secrecy of secure cloud data sharing with a fine-grained access control mechanism. Our proposed scheme provides a possible way to fight against immoral interference with the right of privacy. We hope more schemes can be created to protect cloud user privacy

References

[1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Eurocrypt, 2005, pp. 457–473.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in ACM Conference on Computer and Communications Security, 2006, pp. 89–98.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in IEEE Symposium on Security and Privacy, 2007, pp. 321–334.

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

[5] A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for attribute-based encryption," in Crypto, 2012, pp. 199–217.

[6] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in Public Key Cryptography, 2013, pp. 162–179.

[7] P. K. Tysowski and M. A. Hasan, "Hybrid attribute- and reencryption- based key management for secure and scalable mobile applications in clouds." IEEE T. Cloud Computing, pp. 172–186, 2013.

[8] Wired. (2014) Spam suspect uses google docs; fbi happy. [Online]. Available: http://www.wired.com/2010/04/cloud-warrant/

[9] Wikipedia. (2014) Global surveillance disclosures (2013present). [Online]. Available: http://en.wikipedia.org/wiki/Globalsurveillance disclosures (2013-present)

[10] (2014) Edward snowden. [Online]. Available: http://en.wikipedia.org/wiki/Edward Snowden

[11] (2014) Lavabit. [Online]. Available: http://en.wikipedia.org/wiki/Lavabit

[12] R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky, "Deniable encryption," in Crypto, 1997, pp. 90–104.

[13] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in Eurocrypt, 2010, pp. 62–91.

[14] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, and C. R`afols, "Attribute-based encryption schemes with constant-size ciphertexts," Theor. Comput. Sci., vol. 422, pp. 15–38, 2012.

[15] M. D¨urmuth and D. M. Freeman, "Deniable encryption with negligible detection probability: An interactive construction," in Eurocrypt, 2011, pp. 610–626.

[16] A. O'Neill, C. Peikert, and B. Waters, "Bi-deniable public-key encryption," in Crypto, 2011, pp. 525–542.

[17] P. Gasti, G. Ateniese, and M. Blanton, "Deniable cloud storage: sharing files via public-key deniability," in WPES, 2010, pp. 31– 42.

[18] M. Klonowski, P. Kubiak, and M. Kutylowski, "Practical deniable encryption," in SOFSEM, 2008, pp. 599–609.

[19] M. H. Ibrahim, "A method for obtaining deniable public-key encryption," I. J. Network Security, vol. 8, no. 1, pp. 1–9, 2009.

Shaik. Reshma, was born in Kurnool City, in 1993. She received the B. Tech degree in Computer Science Engineering from the University of Jawaharlal Technological University, Anantapurand M. Tech degree in Computer Science Engineering from the University of Jawarharlal Nehru Technological University, Anantapur, in 2016.

She is working in Dr K V Subba Reddy College of Engineering for Women as Assistant Professor in Department of Computer Science and Engineering.

MD. FAYAZ, was born in Kurnool City, in 1985. He received the B. Tech degree in Computer Science Engineering from the University of Jawaharlal Technological University, Hyderabadand M. Tech degree in Computer Science Engineering from the University of Jawarharlal Nehru Technological University, Anantapur, in 2015. Working in Dr K V Subba Reddy College of Engineering for Women as Assistant Professor in Department of Computer Science and Engineering.