INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES

ISSN 2454-9924 Volume: 1 Issue: 1(2015)

Role Check Secured User Data Access with Attribute-based Encryption, Dynamic Key Generation & User Revocation System

D. Arthy #1, T. Priya Rathika Devi *1

Mailam Engineering College, Mailam #1, *1

dhakshina.arthy@gmail.com #1

Abstract

Attribute-based encryption (ABE) describes a mechanism for complex process control over secured data. The previous method only store the data in the cloud any user can access the data. In the proposed system the data is Stored in the Remote Cloud. Data Owner can share the Data and it's Key to the Permitted Users. Data Sharing is achieved for three types of Users. 1. User Based 2. Role Based (Position / Role), 3. Attribute (Experience). In the modified concept of the Project is Data is uploaded by the Data Owner based on Public Key, Secret Key, Global Key and Group Key. Public Key is randomly generated. Secret Key & Group Key is generated via our Role / Attribute. For both User Name & Designation is used. Global Key is generated randomly. We encrypt the uploaded file using AES Algorithm. User Revocation is also developed in this Part. If a user is moving out of the Group or removed out of the Group, Key is altered and the new Key is mailed to the Present Members. During Data Download, apart from verifying all the Keys, Token is generated as E Mail, which is used for further Authentication.

Key Words: Group key, Attribute, Encryption, Randomly, Secret key

1 Introduction

CLOUD computing is a very fascinating computing paradigm, in which computation and storage are moved away from terminal devices to the cloud. This new and popular paradigm brings important revolutions and makes bold innovations for the manner in which enterprises and individuals manage, distribute, and share content. By outsourcing their information technology capabilities to some cloud service providers, cloud users may achieve significant cost savings. There is widespread public concern about cloud computing, that is, how to ensure cloud users' data security. Part of the outsourced data is sensitive, should be accessed by authorized data consumers at remote locations. For instance, in a university, one of its colleges uploads its (encrypted) development projects to the university cloud, and wants to give only the administrative personnel of the university and the faculty of this college the privilege to access the encrypted projects. This is a very natural scenario in our real life when we use cloud storage systems. Cryptographic technology is an essential manner to achieve this goal. For example, Attribute-Based Encryption (ABE), a special kind of powerful functional encryptions, contributes to access control over encrypted data. The notion of ABE was first introduced by Sahai and Waters. Depending on how to deploy the access control policy, there are two different kinds of ABE systems. That is, Key-Policy Attribute-Based Encryption (KP-ABE) and its dual notion, Cipher text-Policy Attribute-Based Encryption (CP-ABE). In a CP-ABE scheme, every cipher text is associated with an access policy, and every user's private key is associated with a set of attributes. While in a KPABE scheme, cipher texts are labeled with sets of attributes and access policies over these attributes are associated with users' private keys. In an ABE system, decryption operation requires that the set of attributes should match the access policy. Given its expressiveness, ABE is regarded as one of the most natural and important technologies for realizing data access control in the cloud. However, in most existing ABE schemes, one of the main efficiency drawbacks is that the size of the cipher text and the decryption overhead (computational cost) grow with the complexity of the access policy. This becomes critical barriers in applications running on resource-limited devices. For instance, the college adopts a pairing-based ABE scheme to encrypt its development projects and uploads the generated ABE cipher text to the university cloud. An authorized administrative officer of the university, who is on a business ship, wants to look up the encrypted development projects of the college through his (resource-limited) mobile phone. He then wants to download and decrypt the ABE cipher text. Since the cipher text might have a large size and the pairing operations in decryption procedure are usually expensive for a resource-limited device, he has to wait for a long time and sometimes even aborts the decryption procedure. To remarkably eliminate the cipher text size and the decryption overhead for users in ABE systems, a new method for efficiently and securely outsourcing decryption of ABE cipher texts was put forth by Green et al. Fig. 1 illustrates their ABE system with outsourced decryption. More concretely, in their ABE system with outsourced decryption, the key generation algorithm is modified to produce two keys for a user. The first one is a short El Gama type secret key, called the retrieving key rk, and it must be kept private by the user.

2 Related Work

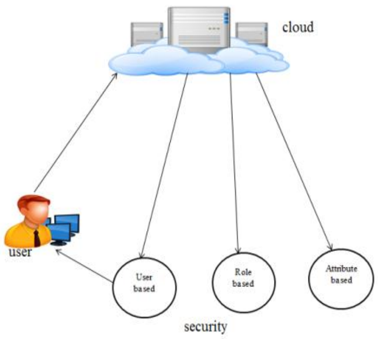
The existing concept only store the data in the cloud any user can access the data. Here it provides some drawback to the existing concept. They are, Congestion occurring, Less security, Less effective, Low connectivity

3 Proposed Work

In the proposed work the data is Stored in the Remote Cloud. Data Owner can share the Data and it's Key to the Permitted Users. Data Sharing is achieved for three types of Users. 1. User Based 2. Role Based (Position / Role), 3. Attribute (Experience). In the modified work of the Project is Data is uploaded by the Data Owner based on Public Key, Secret Key, Global Key and Group Key. Public Key is randomly generated. Secret Key & Group Key is generated via our Role / Attribute. For both User Name & Designation is used. Global Key is generated randomly. We encrypt the uploaded file using AES Algorithm. User Revocation is also developed in this Part. If a user is moving out of the Group or removed out of the Group, Key is altered and the new Key is mailed to the Present Members. During Data Download, apart from verifying all the Keys, Token is generated as E Mail, which is used for further Authentication. I this, it provides some benefits are,

- Avoid Congestion
- User friendly
- High security
- More effective

4 Architecture



5 Methodologies

5.1 User Registration

If the user wants to access the data from the server, they should have an account with that server. Without having an account they aren't able to access the files are view the details. So first the user will create an account with that server by providing the necessary information like Username, Password, DOB, Address and Phone number. Once this information is provided by the user, server will get that information and stored it into the database for future purpose.

5.2 Cloud Server

Cloud Data Service Provider will contain the large amount of data in their Data Storage. Also the Cloud Service provider will maintain the all the User information to authenticate the User when are login into their account. The User information will be stored in the Database of the Cloud Service Provider. Also the Data Server will redirect the User requested job to the Resource Assigning Module to process the User requested Job. The Request of all the Users will process by the Resource Assigning Module. To communicate with the Client and the with the other modules of the Network, the Data Server will establish connection between them. For this Purpose we are going to create a User Interface Frame. Also the Cloud Service Provider will send the User Job request to the Resource Assign Module in Fist in First out (FIFO) manner.

5.3 Data upload with Data sharing

Although the Cloud Computing is vast developing technology, In security point of view the it need more growth. To overcome this disadvantage, we implementing two types of Cloud. Once is Public Cloud and another one is Private Cloud. In Private the patient will set the access privileges' for each and every user they wish. In Public Cloud, the Cloud Server will set the access privileges' for each and every user based on their designation. So that legitimate users can view the data stored in the cloud only up to their privilege level. They aren't allowed to view the data beyond their privileges'.

5.4 Three Layer User Access Control

In the three layer user access control system, the data is stored in the remote cloud. Data owner can share the data and its key to the permitted users. Data sharing is achieved for three types of users 1.User Based, 2.Role Based (Position/Role), 3.Attribute (Experience)

5.5 Request with Two Third Authentications

In this module is to share the data across the user using multiparty two third authentication schemes. Using this scheme new user can send the request to the data owner as well as permitted users. Either owner or two third o permitted user authenticates (SMS alert to the owner) the request, data is forwarded to the requested new user in case of non-sensitiveness and also shared to rest of the user based on the sensitiveness specified by the data owner.

6 Common constructions about Outsourced data

In this section, we shall give generic constructions of CPA secure and RCCA-secure ABE systems with verifiable outsourced decryption from CPA-secure ABE system with outsourced decryption respectively. Note that our constructions can be also applied to selectively CPA secure ABE systems with outsourced decryption. And then, the resulting ABE systems with verifiable outsourced decryption are only selectively CPA-secure/RCCA-secure as well. Unlike the technique of separately encrypting an extra random message and then using this random message to commit to the true message in, the method adopted in our CPA-secure construction is encrypting a message and a random value together and then committing to the message by using the random value. Our method brings significant benefits. First, our construction is generic, and it has more compact cipher text and less computational costs. Second, such a generic CPA-secure construction can be transformed into a generic RCCA-secure construction more naturally.

6.1 Common CPA-Secure Construction

Now, we give the generic construction of CPA-secure ABE with verifiable outsourced decryption from CPA-secure ABE with outsourced decryption. As we have said, in this construction, we employ a commitment scheme to verify the correctness of the outsourced decryption.

6.2 Moving on to Generic RCCA-Secure Construction

In this subsection, we give the generic construction of RCCA-secure ABE with verifiable outsourced decryption from CPA-secure ABE with outsourced decryption. Suppose that we shall construct an ABE scheme with verifiable outsourced decryption to work with a universe U. A set W of dummy attributes, which is disjointed from U, is used in the construction. The underlying CPA-secure ABE scheme with outsourced decryption is then required to work with universe U [W]. A dummy attribute set S W is associated to an encapsulation string com of an encapsulation scheme.

7 Conclusion

From this, Role Check Secured User Data Access with Attribute-based Encryption, Dynamic Key Generation & User Revocation System has been implemented. We have presented generic constructions of CPA-secure and RCCA-secure ABE with verifiable outsourced decryption from CPA-secure ABE with outsourced decryption, respectively. Note that the techniques involved in RCCA-secure construction can be applied in generally constructing CCA secure ABE from CPA-secure ABE. We have instantiated the CPA-secure construction in the standard model. Also of importance is the fact that a RCCA-secure ABE scheme with verifiable outsourced decryption in the standard model can be easily obtained from our generic RCCA-secure construction. We have then implemented our CPA-secure instantiation. The experimental results show that, compared with the existing selectively CPA-secure system, our instantiation has more compact cipher text and less computational costs. Additionally in future, the system enhances its performance and efficiency by reducing time consumption and cost.

8 References

[1] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption," in Proceedings of the 29th Annual international conference on Theory and Applications of Cryptographic

Techniques, ser. EUROCRYPT'10. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 62–91.

[2] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology EUROCRYPT 2005, ser. Lecture Notes in Computer Science, R. Cramer, Ed. Springer Berlin Heidelberg, 2005, vol. 3494, pp. 457–473.

[3] B. Waters, "Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization," in Proceedings of the 14th international conference on Practice and theory in public key cryptography conference on Public key cryptography, ser. PKC'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 53–70.

[4] D. Boneh, A. Sahai, and B. Waters, "Functional encryption: Definitions and challenges," in Theory of Cryptography, ser. Lecture Notes in Computer Science, Y. Ishai, Ed. Springer Berlin Heidelberg, 2011, vol. 6597, pp. 253–273.

[5] D. Boneh and J. Katz, "Improved efficiency for CCA-secure cryptosystems built using identity-based encryption," in Topics in Cryptology - CT-RSA 2005, ser. Lecture Notes in Computer Science, A. Menezes, Ed. Springer Berlin Heidelberg, 2005, vol. 3376, pp. 87–103.

[6] E. Fujisaki and T. Okamoto, "Secure integration of asymmetric and symmetric encryption schemes," in Advances in Cryptology CRYPTO '99, ser. Lecture Notes in Computer Science, M. Wiener, Ed. Springer Berlin Heidelberg, 1999, vol. 1666, pp. 537–554.

[7] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in Proceedings of the 17th ACM conference on Computer and communications security, ser. CCS '10. New York, NY, USA: ACM, 2010, pp. 735–737.

[8] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proceedings of the 2007 IEEE Symposium on Security and Privacy, ser. SP '07. Washington, DC, USA: IEEE Computer Society, 2007, pp. 321–334

[9] J. Lai, R. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Transactions on Information Forensics and Security, vol. 8, no. 8, pp. 1343–1354, Aug 2013.

[10] J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. D. Rubin, "Charm: a framework for rapidly prototyping cryptosystems," Journal of Cryptographic Engineering, vol. 3, no. 2, pp. 111–128, 2013.

[11] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," Parallel and Distributed Systems, IEEE Transactions on, vol. 22, no. 7, pp. 1214–1221, 2011.

[12] L. Cheung, J. A. Cooley, R. Khazan, and C. Newport, "Collusionresistant group key management using attribute-based encryption," Group-Oriented Cryptographic Protocols, p. 23, 2007.

[13] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of abe ciphertexts," in In: Proceedings of the 20th USENIX Conference on Security, SEC 2011. San Francisco, CA, USA: USENIX Association, Berkeley, 2011.

[14] R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology, revisited (preliminary version)," in Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing, ser. STOC '98. New York, NY, USA: ACM, 1998, pp. 209–218.

[15] S. Jahid, P. Mittal, and N. Borisov, "Easier: encryption-based access control in social networks with efficient revocation," in Proceedings of the 6th ACM Symposium on Information, Computer andCommunications Security, ser. ASIACCS '11. New York, NY, USA: ACM, 2011, pp. 411–415.

[16] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non monotonic access structures," inProceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07. New York, NY, USA: ACM, 2007, pp. 195–203.

[17] S. Muller, S. Katzenbeisser, and C. Eckert, "Distributed attributebased encryption," in Information Security and Cryptology — ICISC 2008, P. J. Lee and J. H. Cheon, Eds. Berlin, Heidelberg: SpringerVerlag, 2009, pp. 20–36.

[18] S. Yamada, N. Attrapadung, G. Hanaoka, and N. Kunihiro, "Generic constructions for chosen-ciphertext secure attribute based encryption," in Public Key Cryptography - PKC 2011, ser. Lecture Notes in Computer Science, D. Catalano, N. Fazio, R. Gennaro,

and A. Nicolosi, Eds. Springer Berlin Heidelberg, 2011, vol. 6571, pp. 71–89.

[19] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ser. ASIACCS '10. New York, NY, USA: ACM, 2010, pp. 261–270.

[20] T. Okamoto and K. Takashima, "Fully secure functional encryption with general relations from the decisional linear assumption," in Proceedings of the 30th Annual Conference on Advances in Cryptology, ser. CRYPTO'10. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 191–208.

[21] T. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in Advances in Cryptology – CRYPTO '91, ser. Lecture Notes in Computer Science, J. Feigenbaum, Ed. Springer Berlin Heidelberg, 1992, vol. 576, pp. 129–140.

[22] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proceedings of the 13th ACM conference on Computer and communications security, ser. CCS ’06. New York, NY, USA: ACM, 2006, pp. 89–98.