International Journal of Engineering Research and General Science Volume 3, Issue 6, November-December, 2015
ISSN 2091-2730

Secure data sharing using attribute-based broadcast encryption in cloud computing

Mrs. Komal Jagdale[1], Prof. Asha Pawar[2]

[1]PG Scholar, Department of Computer Engineering, ZCOER, Pune, Maharashtra

[2]Assistant Professor, Department of Computer Engineering, ZCOER, Pune, Maharashtra

Abstract— Data owner outsource the data due to cost reduction and poor management to the cloud which provide data as a service. Data owner then lose control over the data, because cloud service provider becomes a third party provider. Traditionally, data owner encrypt the data and export it to the cloud seems a good approach. But it has some drawbacks like decryption computation overhead, revocation of user and privacy preserving. A secure and flexible attribute-based broadcast encryption (EP-ABBE), which reduce the decryption computation overhead by partial decryption, and protect user privacy. Based on EP-ABBE, efficient and privacy preserving data sharing scheme in cloud computing was presented, where data owner can flexibly encrypt the data using access policy and implicit user index set. User revocation can be achieved by dropping revoked user's index from the user index set, with very low computation cost and the privacy of user can be protected.

Keywords— Cloud service provider, Encryption, Decryption, Broadcast encryption, Ciphertext, Revoke user, Attribute key.

INTRODUCTION

Cloud computing is most emerging paradigms in the field of information technology. Cloud computing has benefits ,such as scalability, reduced costs, flexibility, increased operational efficiencies, hence people inclined to outsource their personal data to the cloud. Cloud service provider is semi-trusted which arise concerns of security and privacy. Before outsourcing data to semi trusted cloud for data security, it will be encrypted. Data owner may face problem in using public key encryption and identity based encryption. Encrypted cipher text using public key or identity can be decrypted by private key of corresponding user.

In broadcast encryption (BE) broadcaster choose a subset of privileged users to send a cipher text from all recipients dynamically. But it is hard to support flexible, fine-grained access control policies. Attribute based encryption (ABE) make possible to achieve fine grain access control over encrypted data using access policies and credited attributes among the secret keys. Cipher text policy attribute based encryption (CP-ABE) which is theoretically similar to the role-based access control models, which makes possible to data owner to modify access policy number of attributes that the user possesses in order to decrypt the cipher text. But it has some drawbacks like user revocation.

Attribute based broadcast encryption (ABBE) address the problem of user revocation. It encrypts the broadcast data using expressive access policy with or without specifying the receiver. Data decryption scheme is time consuming since it required large number of pairing operations.

In EP-ABBE, it reduces decryption computation of user and protects user privacy. The data owner can enjoy the flexibly of encrypting personal data using a specified access policy and a user index set which is a list of selected users' indexes. Thus, only the users whose index are in index set and attributes satisfy the access policy can access the personal data. In EP-ABBE scheme achieves efficient user revocation by dropping user index from the user index set of cipher text. The data owner does not need to update the secret key of non-revoked user, which has very low computation cost and is more efficient compared with current attribute-based data sharing schemes.

RELATED WORK

ABE is used in data sharing schemes for fine grain access control. Liang et al. used Attribute Based Encryption to protect data security in mobile social networks [1]. In specific time slot it enables a trusted authority to revoke a specific user's data decryption capability. But drawback of this scheme, revoked user is able to access the encrypted data even if it does not hold the attribute any more until the next expiration time. Li et al. proposed a secure sharing of personal health record in cloud computing based on ABE [2]. Immediate revocation is achieved in which multi-authority work together to re-encrypt cipher texts and update unrevoked users' attribute secrete keys. This scheme requires extra communication cost and it is inefficient. Hur et al. proposed a data outsourcing scheme using CP-ABE in which immediate user revocation is achieved in attribute level [3]. But on the downside there is amount of data redundancy because cipher texts must be re-encrypted many times for different attribute groups. ABBE was proposed by David et al. [4]. In this scheme broadcasters can encrypt data with access policy and receiver those who present in receivers list and satisfy the access policy that can decrypt cipher text. Asim et al. proposed a reversed ABBE scheme [5], in which the broadcaster encrypts the data according to the access policy and the list of the identities of revoked users rather than the authorized users' identities. Only the users with the attributes that satisfy the access policy and their identities are not in the list of revoked users would be able to decrypt the cipher text.

SYSTEM MODEL

The system model of data sharing scheme based EP-ABBE consists of the following entities, as shown in Fig. 1.

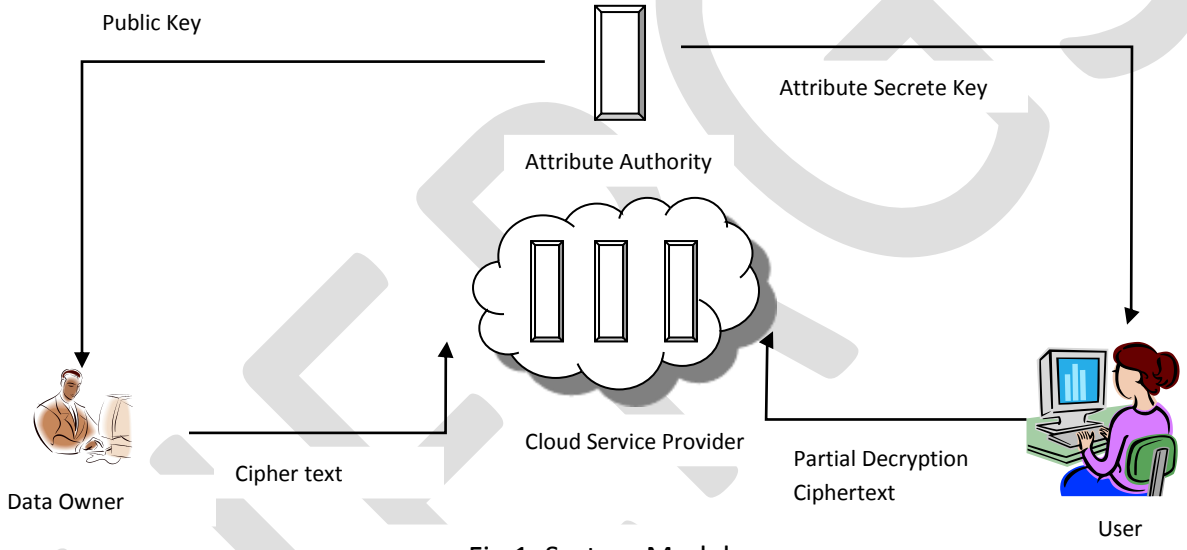

Fig.1. System Model

1. **Attribute authority**: Attribute authority is trusted attribute centre, which is responsible for assigning attributes to user and generating user's attribute secret key which corresponds to the user's attributes.
2. **Cloud service provider**: Cloud service provider is the semi-trusted entity .This entity provides data outsourcing service. Data owner outsource the encrypted data to cloud through cloud service provider. The CSP is also responsible for partially decrypting the cipher text for the users.
3. **Data owner**: It is an entity who needs to outsource data to cloud storage provided by CSP, for the purpose of using low-cost and energy-efficient storage resources. The data owner encrypts the data with the specified obfuscated access policy and a user index set before outsourcing.
4. **User**: User is an entity who wants to access the data. After receiving attribute secret key from attribute authority, user generates attribute key to delegate decryption computation to CSP. If a user possesses a set of attributes satisfying the access policy and his index is in the user index set, he can recover data from partial decrypted cipher text.

WORKING MODEL

Working model of data sharing scheme is describe as follows:

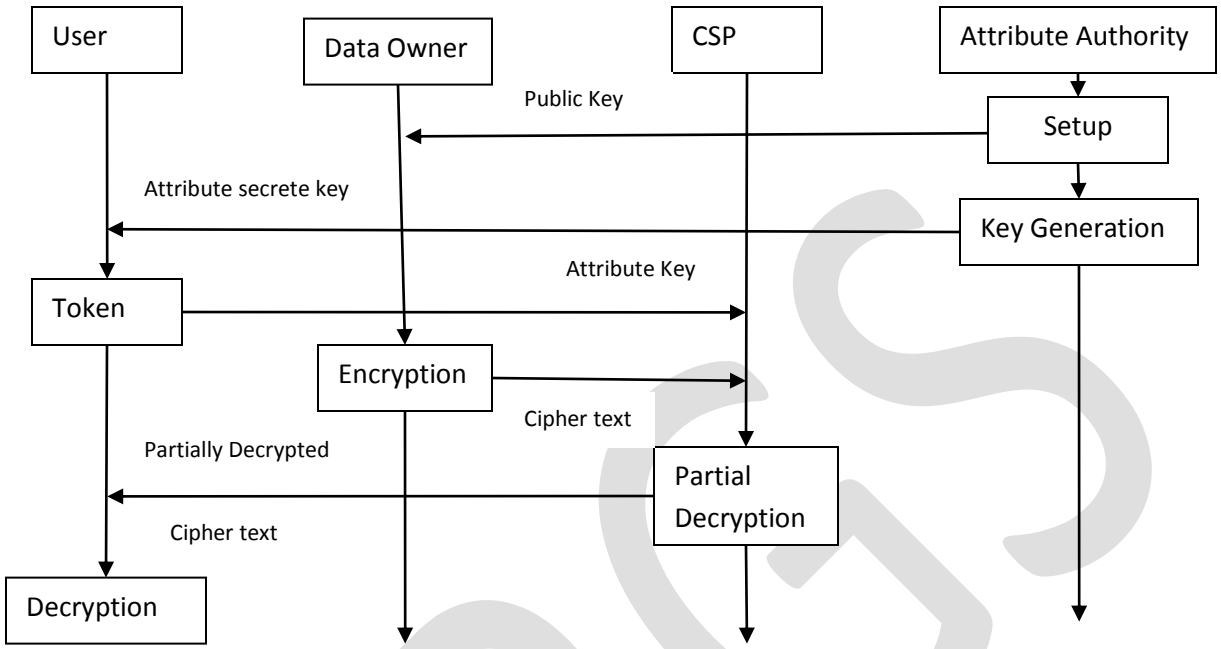

Fig.2. Working Model

SYSTEM SETUP

The attribute authority runs setup algorithm to select a bilinear group G_1 of prime order q and generator g, and the bilinear map e :G_1 X $G_1 \rightarrow G_2$. Then the attribute authority chooses random, $\alpha, \beta \in Z_q$, and defines the hash function H :$\{0,1\}^* \rightarrow G_1$:$G_1 \rightarrow G_2$. Let N = {1, 2,...,n} denotes the set of all user indexes [6]. The system public key K_P is published as: $K_p = \{g^{\alpha}, ..., g^{\alpha n}\}, g^{\beta}$ The master secret key K_M is kept secret by attribute authority and is constructed as: $K_M = (\alpha, \beta)$

KEY GENERATION

The attribute authority runs key generation algorithm to choose a random $\gamma \in Z_q$ for a user with the user index d $\in$ N, and chooses random $\gamma_j \in Z_q$ for each $a_j \in S$ where S denotes the attribute set of user. Then the attribute secret key K_{AS} is computed as:
$K_{AS} = (D= g^{\alpha\beta+\gamma}, \{D_j = g^{\gamma} H(j)^{\gamma j}, D'_j = g^{\gamma j}, D''_j = H(j)_{\beta}\}_{j \in S}\})$

The attribute authority delivers the attribute secret key K_{AS} to the user in a secure manner. The user runs token generation algorithm to choose a random $t \in Z_q$, and generates the attribute key K_A as: $K_A = (\{\check{D}_j = (Dj)1^{/t}\}, \check{D}'_j = (D'^{1/t}_j, D''_j)_{j \in S}\})$

Then, the user sends K_A to CSP, and keeps the D secretly.

TOKEN GENERATION

The user takes his K_{AS} as input, and outputs the attribute key K_A which is sent to CSP.

ENCRYPTION

The data owner takes K_P, user index set U which is the set of selected users' indexes, the access policy T and plaintext M as input, and outputs the cipher text C_T which contains the obfuscated T. Thus only the user whose index is in the index set U and attributes satisfy the access policy that can access the data.

PARTIAL DECRYPTION

The C_{SP} takes as input a cipher text C_T, the user's attribute key K_A and user index d. It outputs a partially decrypted cipher text CTP. The C_{SP} first generates the user's obfuscated attribute set S′ with K_A, then C_{SP} computes C_{TP} with K_A if the S′ satisfies the obfuscated T of the cipher text C_T and d is in the user index set U.

DECRYPTION.

The user takes as input a partially decrypted cipher text C_{TP} and the attribute secret key K_{AS}, outputs the message M.

USER REVOCATION

The data owner can revoke the user from the user index set U. Upon receiving the revoked user index R from data owner, the CSP first generates C'_0 . Then the CSP replaces C_0 in the cipher text with C'_0 , and generates the re-encrypted cipher text C'_T . CSP cannot generate I for the revoked user in user index R. Thus, the revoked user cannot decrypt the re-encrypted cipher text.

CONCLUSION

Modified structure of attribute based broadcast encryption which is named as EP-ABBE is explained. EP-ABBE reduces the decryption computation overhead of user and protects user privacy by obfuscating access policy of ciphertext and user's attributes. A flexible and secure data sharing scheme in cloud computing was presented using EP-ABBE based scheme. Using this scheme data owner can encrypt data with a specified access policy and the user index set. Also using this scheme efficient user revocation is performed by dropping user's index from the user index set of the encrypted data. This scheme can protect user privacy as well.

REFERENCES:

[1] Liang X, Li X, Lu R, et al. An efficient and secure user revocation scheme in mobile social networks. Proceedings of the IEEE Global Communications Conference (GLOBECOM'11), Dec 5−9, 2011, Houston, TX, USA. Piscataway, NJ, USA: IEEE, 2011: 5p
[2] Li M, Yu S, Zheng Y. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Transactions on Parallel and Distributed Systems, 2013, 24(1): 131−143
[3] Hur J, Noh D K. Attribute-based access control with efficient revocation in data outsourcing systems. IEEE Transactions on Parallel and Distributed Systems, 2011, 22(7): 1214−1221
[4] Lubicz D, Sirvent T. Attribute-based broadcast encryption scheme made efficient. Advances in Cryptology: Proceedings of the 1st International Conference on Cryptology in Africa (AFRICACRYPT'08), Jun 11−14, 2008
[5] Junod P, Karlov A. An efficient public-key attribute-based broadcast encryption scheme allowing arbitrary access policies. Proceedings of the 17th ACM Conference on Computer and Communications Security (CCCS'10), Oct 4−8, 2010, Chicago, IL, USA. New York, NY, USA: ACM, 2010: 13−24
[6] Asim M, Ibraimi L, Petkovic M. Ciphertext-policy attribute-based broadcast encryption scheme. Communications and Multimedia Security: Proceedings of the 12th IFIP TC 6/TC 11 International Conference on Communications and Multimedia Security (CMS'11), Oct 19−21, 2011, Ghent, Belgium. LNCS 7025. Berlin, Germany: Springer-Verlag, 2011: 244−246
[7] Hur J. Improving security and efficiency in attribute-based data sharing. IEEE Transactions on Knowledge and Data Engineering, 2013, 25(10): 2271−2282
[8] Cecile D. Identity-based broadcast encryption with constant size ciphertexts and private keys. Advances in Cryptology:Proceedings of the 13th International Conference on the Theory and Application of Cryptology and Information Security(ASIACRYPT'07), Dec 2−6, 2007, Kuching, Malaysia.LNCS 4833.Berlin,Germany: Springer-Verlag, 2007: 193−215
[9] Zhou Z, Huang D. On efficient ciphertext-policy attribute based encryption and broadcast encryption.Proceedings of the 17th ACM Conference on Computer and Communications Security(CCCS'10), Oct 4−8, 2010, Chicago, IL, USA. New York, NY,USA:ACM, 2010: 753−755
[10] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data. Proceedings of the 13th ACM Conference on Computer and Communications Security (CCCS'06), Oct 30−Nov 3, Alexandria, VA, USA. New York, NY, USA: ACM, 2006: 89−98
[11] Hur J, Koo D, Hwang S O, et al. Removing escrow from ciphertext policy attribute-based encryption. Computers and Mathematics with Applications, 2013, 65(9): 1310−1317
[12] Liang X, Li X, Lu R, et al. An efficient and secure user revocation scheme in mobile social networks. Proceedings of the IEEE Global Communications Conference (GLOBECOM'11), Dec 5−9, 2011, Houston, TX, USA. Piscataway, NJ, USA: IEEE, 2011: 5p
[13] Li M, Yu S, Zheng Y. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Transactions on Parallel and Distributed Systems, 2013, 24(1): 131−143