Scenario of Cipher text Policy Attribute Based Encryption for Secure Data Sharing

Y.Sobhan Babu,
Research Scholar,
Shri Venkateshwara University

Dr Duvvuri B K Kamesh,
Professor,
St. Martin's Engineering College.

Abstract-The most emerging technologies today life has become faster. Now a day people want to store their data and share without having to worry about how they internally work. Now a day attribute based encryption has a major role in data sharing by providing great security and access control on data. This can be achieved by encryption and decryption of data. Policy over attributes has been defined along with access tree structure. Access structure is a process used in security systems, which helps in sharing the resources in secured manner .The access tree structure defines way of accessing the resources by the heterogeneous parties need to work together to get a resource. CP-ABE is a very complex access control method on encrypted data .The CP-ABE provides match between user's private key and cipher text then only decryption is possible. In the cipher text-policy attribute-based encryption scheme, each user's private key (decryption key) is tied to a set of attributes representing that user's permissions. We implement a multiple level authority CP-ABE technique to recover data in a secured manner. Each and every one of the multiple local key authorities distributes partially customized attribute keys to the clients.

Keywords: Attribute Based Encryption, Key Policy Attribute Base Encryption, Cipher Text –Attribute Based Encryption.

I. INTRODUCTION

A sender can encrypt data for a policy written over attributes issued by different authorities. A receiver in the system should be able to decrypt if their attributes satisfy the policy specified by the cipher text. In addition, the system should be able to express complex policies and not require coordination amongst the authorities. One stumbling block of conventional encryption schemes is that this data can be only shared by any user with the decryption key can decrypt the data. [M. S. Sarath Chandra, K. Raghava Rao and Mohammed Ali Hussain , Vol 9(5), DOI: 10.17485/ijst/2016/v9i5/84915, February 2016].

1.1 Data Encryption And Decryption

The translation of data into a secret code is called Encryption. It is the most effective way to achieve data security. Reading encrypted file needs a secret key or password that enables us to decrypt it. Encrypted data is referred to as cipher text. [M. S. Sarath Chandra, K. Raghava Rao and Mohammed Ali Hussain , Vol 9(5), DOI: 10.17485/ijst/2016/v9i5/84915, February 2016].There are two main types of encryptions. Asymmetric encryption A cryptographic system that uses two keys , a public key known to everyone and a private or secret key known only to the recipient of the message. Symmetric encryption, A type of encryption where the same key is used to encrypt and decrypt the message.

1.2 Key In Cryptography

The functional output of the special algorithm called as cryptographic algorithm or the cipher can be described by the key which is the piece of the information. A cryptographic key is a string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa. This key remains private and ensures secure communication.[Brent Waters,"Ciphertext-Policy Attribute-Based Encryption an Expressive, Efficient, and Provably Secure Realization", Mar 2011, In Public Key Cryptography (Vol. 6571, pp. 53-70].A cryptographic key is the core part of cryptographic operations. Many cryptographic systems include pairs of operations, such as encryption and decryption.

1.3 Access Tree Structure

The study of Security systems is one of the core issues in data storing and sharing. This can be done with the help of Access structures. So Access structure plays a key role in the study of secure data systems, where the heterogeneous parties need to work together to get a resource. The study of the special security systems in which the number of systems working together for releasing a particular resource uses a specific structures are called as Access structures. The clients that get their access granted are called as qualified parties. They are also called as qualified groups. The resource can also be a job that a multiple people can perform together. The job may be digital signatures or the message encryption and decryption. In general the access structures functionality is the way of monotonic structures. If there is a availability of subset SUB1 in the access structure ,then all sets(s1,s2,s3,..) that belong to the set SUB1 must be an active part of the access structure.

1.4 Threshold Policy Access Control

Database ones stored in Secured system can be accessed by multiple users for multiple purposes. The access control or rules or policy will changes from one user to other user. Different users access the same database. Every database must be restricted from unauthorised users. The Threshold Policy Access Control sets the accessing authorities to the users based on the level of user. Threshold Policy Access Control can decide that, who can access particular data from the database and how much extent users can access the data from the database. It sets policies according to the access based on user attributes. It is one the key role of Cipher text Attribute based Encryption.

1.5 Attribute-Based Encryption

In 2004, Sahai and Waters presented a revolutionary encryption system. This idea can be applied to a class of protocols called Attribute-Based Encryption (ABE). The idea of having a variable number of attributes as an identity comes from the need of sharing a secret in well-ordered process. This is a one to many encryption techniques in which the encryption and decryption of the data is based on the attributes. In this method the user's secret key and the Cipher text are linked with the set of attributes. The decryption of the information can be only possible when the user's attributes and the cipher text's attributes are identical. Decryption is possible only if there is a threshold T number of matching attributes. Along with these features there is an additional feature called as Collusion Resistance. The user holding multiple attributes can get access only if at least one individual key provides access. [Amit Sahai and Brent Waters, "fuzzy Identity –Based Encryption " , Vol 3494,457-473,2005].This method has a drawback with attribute-based encryption. The problem is that the data owner needs to encrypt the data with all the public keys of all the users so that they can access the data.

For a concrete model of this case, suppose the set of attributes have been assumed in an University : "JNTUA", "Computer Science"," Hod of Cse" ,"Exam branch", "office clerk". If the result policy of a student is defined so that ,the result can be read by exam branch and office clerk belongs the JNTUA ,and at the same time the Hod of cse and student can read it at any time ,then the Boolean expression can capture the Policy:

(Hod of Cse or Student) or [(Exam Branch or Office Clerk) and JNTUA] , The student result can also be linked with other attributes like University Location or University code. The access of student result will only be granted to those private key holders having enough attributes to satisfy the access policy. The attributes that are initially described as alphanumeric strings can be uniquely mapped to group elements by means of a special hash function that maps arbitrary strings to elements in either the group G1 or G2. As it was described above, the access policy is specified through a Boolean formula, which is transformed to an access structure that can be implemented using a linear secret-sharing scheme (LSSS) as described by Waters.

1.6 Key Policy Attribute-Based Encryption

The modified form of the attribute-based encryption is Key-Policy Attribute-based Encryption (KP-ABE). The threshold gates will be the nodes of the access tree of this a type of attribute-based encryption. In this type the leaf nodes of the access tree are associated with the attributes. There will be a secret key for every user. Now the keys associated with the access structure should be equal to the user's secret key; then only the user can decrypt the message. It is generally a one to many communications.

1.7 Cipher Text-Policy Attribute-Based Encryption

In this type unlike Key Policy Attribute-based encryption the cipher text is associated with the access policy and the user will be associated with the set of attributes. The user will be able to get access to the text only if the user's set of attributes satisfies the access policy of the cipher text. This is the main difference between the CP-ABE and KP-ABE. [J Bettencourt, Admit Sahai, and Brent Waters, "Cipher text-Policy Attribute-Based Encryption". SP'07. IEEE Symposium on. IEEE, 2007] . The access structure of this is same as the key policy. In the cipher text-policy attribute-based encryption scheme, each user's private key (decryption key) is tied to a set of attributes representing that user's permissions. When a cipher text is encrypted, a set of attributes is designated for the encryption, and only users tied to the relevant attributes are able to decrypt the cipher text.

1.7.1 CP-ABE Methodology

Here the function of dispersing the key authorities from a central authorities to another location are partially faithful, we can make sure that they are put away from attaining the actual data that sender wishes to protect in the external storage node by themselves, but still they must be capable of distributing secret keys to the clients. To protect this quite a bit tricky achievement, we are implementing 2PC protocol on the key authorities, who have their own master secret keys and can distribute autonomous keys to the clients. The 2PC protocol restricts these local key authorities from gaining access to each of the other local key authorities' secret keys, therefore, none of them can achieve the ability to produce the complete set of user secret keys by themselves. Therefore, we can assume that these key authorities cannot access the secret keys of all other users and this leads to conclusion that keys authorities do not collude with one another.

II. RELATED WORK

In standard public key cryptography a file can be encrypted along with a public key. The file is decrypted with the help of secret key. This method can be suitable for predefined groups. If a new member is added to the existing group in such case standard public key cryptography is not suitable. To overcome this problem Identity Based Encryption was introduced by Amit Sahai and Brent Waters[11] named as Attribute based encryption and further modified by Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters for the purpose of encryption and decryption of required data based on key attributes of different users known as key policy. Attribute based encryption schemes are KP-ABE and CP-ABE.

In KP-ABE Encryptor needs to apply set of attributes on cypher text, Private key is connected with access tree structure. The access tree structure decides which type of cipher text the key can decrypt[3]. This is complicated to implement it in real time. "Key policy attribute based encryption"- here private keys are associated with an access tree and its cipher text is associated with users attributes.

In this paper our aim is to implement a method with the help of CP-ABE for providing more security for the data. In this concept access tree structure is designed by the Sender. Every file is uploaded with the set of attributes, which are under the control of Sender. Sender or Owner can select certain set of attributes before sending the file. Here the attributes belongs to the user, so that others cannot access or cannot identify the linked attributes.

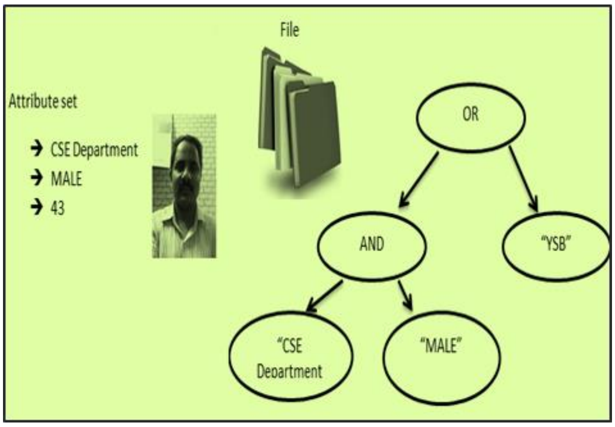

Figure 1 : Cypher text-Policy Based Encryption Access structure

This method can be applied on required set of users. The data access condition is represented with a specific policy. The End Users can decrypt the file if the set of attributes satisfies the represented policy.

III. PROPOSED METHODOLOGY

We implement a multiple level authority CP-ABE technique to send and receive data in a secured manner.

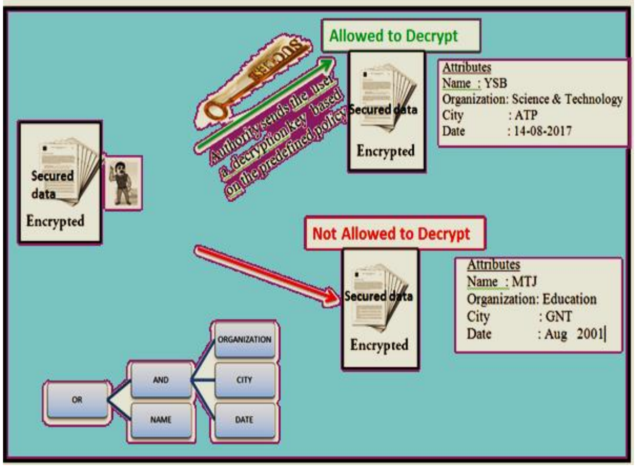

Figure 2 Architecture of CP-ABE

Each and every one of the multiple local key authorities distributes partially customized attribute keys to the clients. Where every attribute key of the client can be updated instantaneously. In our system security and scalability of the system can be improved.

CP-ABE scheme needs two components for client secret key. They are a Personal unique key and multiple attribute keys. The personal keys are unique to each client, which are helpful for Collusion resistant. In our proposed scheme, a personal key is released, succeeded by multiple attribute keys. We can avoid the key security problems.

In our concept plain text is encrypted via Advanced Encryption Standard (AES) encoding scheme, which can be used at both the sender and receiver sides and the same key is used for both ciphering and deciphering the plain text. In our simulation, client also employs the same AES scheme to decrypt the encrypted data

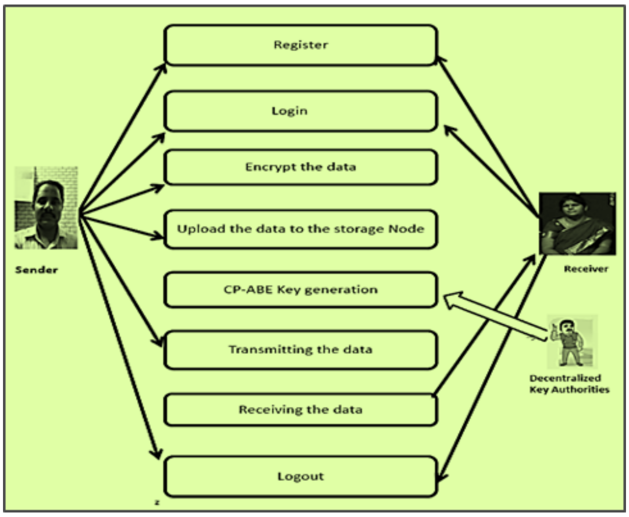

Figure 3 : Implementation of cypher text policy based Encryption (Use case Diagram)

.

IV. CONCLUSION

Secured communication in the hostile environment can be successfully achieved through this implementation. In this paper, we've designed an efficient data recovery scheme based on CP-ABE methodology via Advanced Encryption Standard (AES) encoding scheme, making security the utmost prioritized characteristic. DES (data encryption Standard) was 56 bit key ,which was mainly used to design hardware but we use AES encryption algorithm, which helps to provide an efficient design of both hardware as well as software.

REFERENCES

[1] M. S. Sarath Chandra, K. Raghava Rao and Mohammed Ali Hussain " An Efficient - Scheme for Facilitating Secure Data Sharing in Decentralized Disruption Tolerant Networks"- Vol 9(5), DOI: 10.17485/ijst/2016/v9i5/84915, February 2016.

[2] Sneha Chandrashekhar Parit, Dr. Rashmi Rachh,"Ciphertext Policy Attribute Based Encryption**",** IRJET Volume: 04 Issue: 04 | Apr -2017.

[3] Vipul Goyal, Omkant Pandeyy, Amit Sahaiz, Brent Waters, " Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data", Oct 30, 2006 , volume 3027 of LNCS pages 207-222.

[4] Mahaling G. Salimath , Pavana S. Baligar, Sharada K. S, Rajeshwari Banni "Secure Data Retrieval Of Attribute Based Encryption Policy System " , Volume 5 Issue 11 (November 2016).

[5] Brent Waters,"Ciphertext-Policy Attribute-Based Encryption an Expressive, Efficient, and Provably Secure Realization", Mar 2011, In Public Key Cryptography (Vol. 6571, pp. 53-70).

[6] Walunj Pratap, Bhagwan Kurhe ," Survey of Attribute Based Encryption Schemes", IJETT) – Volume 47 Number 2 May 2017.

[7] S. Roy, M. Chuah, "Secure Data Retrieval Based on Ciphertext Policy Attribute-Based Encryption (CP-ABE) System for the DTNs", Lehigh CSE Tech8.S8 (2009): 542-8.

[8] Sherley Codio ," Ciphertext-Policy Attribute-Based Encryption (CP-ABE)", Mar 31, 2011.

[9] Yi-mu Ji, Jie Tana, Hai Liu, Yan-peng Sun, Jia-bang Kang, Zizhuo Kuang , Chuanxin Zhao "A Privacy Protection Method Based on CP-ABE and KP-ABE for Cloud Computing", JOURNAL OF SOFTWARE, VOL. 9, NO. 6, JUNE 2014.

[10] Mis.M.Jerusha Blessy, Prof.D.V.Rajesh Babu,"Ensured Data Recovery For Localized Interruption Sympathetic Military Networks", IJITR ,Volume No.5, Issue No.2, February – March 2017, 5926-5932.

[11] Amit Sahai and Brent Waters, "fuzzy Identity –Based Encryption " , Vol 3494,457-473,2005.

[12] J Bettencourt, Admit Sahai, and Brent Waters, "Cipher text-Policy Attribute-Based Encryption", SP'07 IEEE Symposium on. IEEE,2007.