Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

Survey On Encryption Schemes used in Clouds

Rajalekshmi V

Computer Science Engineering, SreeBuddha College Of Engineering For Women

Abstract— Cloud computing, is an emerging computer technology that provides users to remotely store their data in a server and provide services on-demand. Since remote data storage is here, data security and privacy is the most critical issues. Users can read, write and store data to cloud. To protect the confidentiality of the data stored, the data must be encrypted using some encryption algorithms. Attribute based encryption (ABE) method is a well-known encryption algorithm used to encrypt data stored in clouds. In this paper, we are going to analyze different variations of encryption schemes used to store data in cloud.

Keywords—Cloud computing; Encryption; Access control; Cipher text; Attribute

I. INTRODUCTION

Cloud computing, is a widely adopted paradigm that offers delivery of services over the internet. Users can store, read, and write their data into clouds. In cloud, sensitive information of different parties are stored normally in remote servers and locations and possibilities of this being exposed to unwanted parties where cloud servers are compromised. The security challenges for cloud computing approach are dynamic and vast. Data location, security and privacy are crucial factors in cloud computing security. Encryption methods, protection for actual hardware, data have any back up, any firewall setup, is information separated from other companies etc. are some of the factors which make sure about the data security in cloud. These services are different for different cloud service providers

The most important facility of cloud is that people need to pay money for the space they used to store data. Also data owner must make access control policies, so that only authorized users can access data. Before providing confidentiality, the data must be encrypted before uploading to the cloud. Traditional public key infrastructure has some disadvantages like storage overhead, need of user's public key etc. By improving some of these disadvantages a number of encryption mechanisms are introduced. The efficiency of these encryption techniques are based on some factors like data confidentiality, fine-grained access control, scalability, user accountability, user revocation, collusion resistant.

In this paper we are analyzing those encryption methods used to store data in clouds starting from the basic traditional public key encryption. Attribute based encryption (ABE) is an important scheme used to encrypt data based on some attributes. There are many variations of ABE are also available.

II. SOME ENCRYPTION SCHEMES

The encryption techniques that we discussed here are public key infrastructure, Identity based encryption, Fuzzy- identity based encryption, Attribute based encryption, etc.

2.1. Public Key Infrastructure

Traditional public key encryption methods uses user's public key to encrypt and private key to decrypt the plain text. It has some disadvantages like (1) storage overhead in which a single plaintext needs different public keys (2) to complete the process data owner needs data user's public key etc.

2.2. IDE

Identity based encryption[2] uses identity of the user. Ones publically known identity is being used as his/her public key whereas corresponding private key is generated from the known identity. IDE requires 4 steps to complete the task.

- Set up algorithm
- Key generation
- Encryption
- Decryption

Set up algorithm generates a master key for the user. By showing and prove his/her identity to private key generator, the key generation algorithm creates a private key for the user. To encrypt the message, the second user knows and uses the first ones identity. To decrypt the message he/she uses her private key.

IDE does not use any CAs, certificates, CRLs etc. The problems of IDE is it needs a secure channel to send the user's private key and also the user's private key is known to private key generator

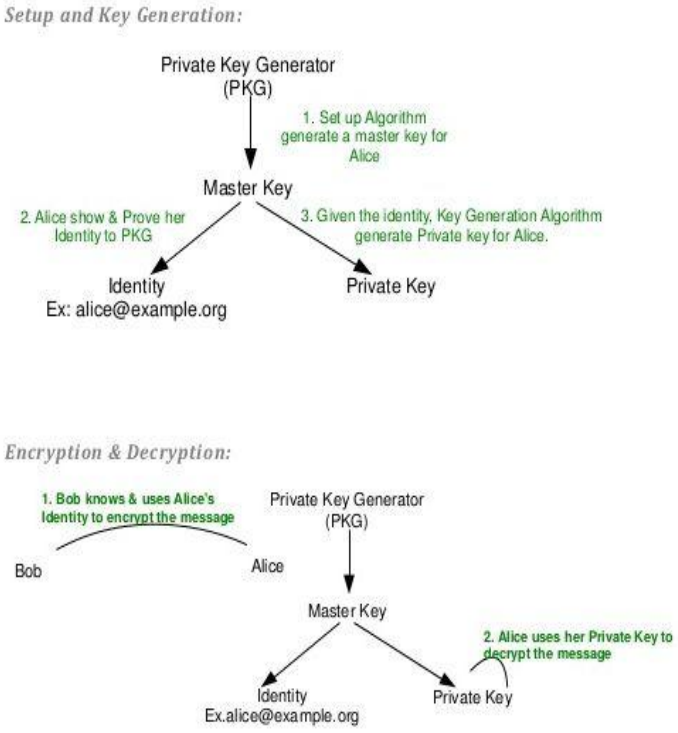

Figure 1. IDE

2.3. Fuzzy- IDE

Fuzzy identity of a person is a set of descriptive attributes which a predefined error tolerance capability[3]. Here, these attributes are used as ones' known public key. Here also 4 steps as described above with some differences.

- Set up algorithm
- Key generation

- Encryption
- Decryption

Given an error tolerance factor d, set up algorithm generates a master key for Alice. Alice's identity w is being decided. Given identity w, key generator algorithm generates Alice's private key.

Charlie can encrypt message with Bob's identity w'. Bob can decrypt M with his private key and Alice can also decrypt m with her private key with ($W \cap W' >= d$)

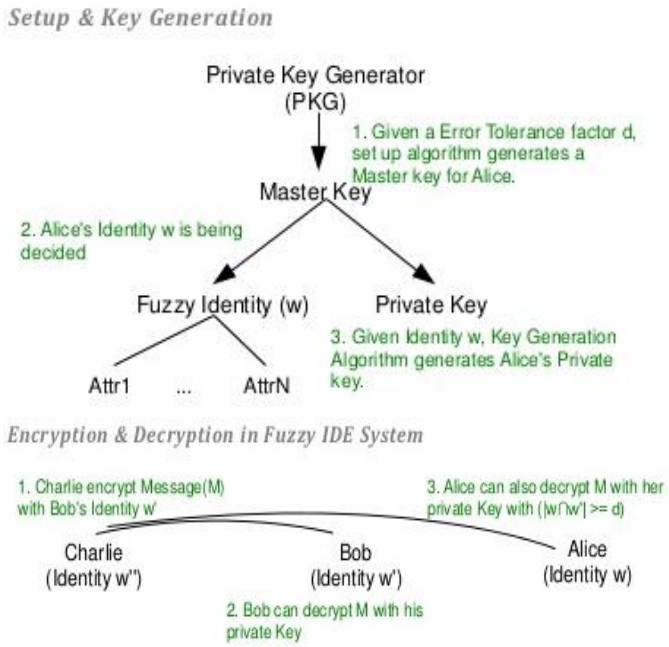

Figure 2. Fuzzy IDE

2.4. Attribute Based Encryption (ABE)

Attribute based encryption method is proposed by Sahai and Waters[4] in 2005. This method provides security and access control in a more efficient way. There are three participants in this schema. Authority, data owner (sender) and data user (receiver). The role of authority is to generate keys for data owners users to encrypt or decrypt data. In ABE, keys are generated according to attributes. These attributes should be predefined which are generated by the authority. The role of data owner is to encrypt data using public key and a set of attributes and that of user's role is to decrypt using private key sent from authority.

Decryption is possible only if the attributes in the user's private key matches with attributes in encrypted data. The data user's private will be permitted to decrypt the encrypted data only if the number of matching at least a threshold value 'd'. In ABE four algorithms are used: Setup, KeyGen, Encrypt and Decrypt .

Setup algorithm, creates a public key and master key. KeyGen algorithm generates a private key for the data user with secret sharing. Encrypt and Decrypt algorithm performs encryption and decryption respectively based on attributes (the country she lives, number of years, position etc). Attribute based encryption prevents collusion attack. Collusion resistant means users cannot combine their attributes to decipher the encrypted data. Since each attribute is related to the polynomial or the random number, different users cannot collude each other. Attribute based encryption has two variation: KP-ABE and CP-ABE

2.4.1. Key Policy Attribute Based Encryption Scheme (KPABE)

KP-ABE was proposed by Goyal [4]in 2006. This is a modified form of ABE. Here encrypted data is described using a set of attributes and access policy is built in user's private key. User's are assigned with an access tree structure over attributes. Nodes of access tree are threshold gates and attributes are leaf nodes. Here also four algorithms are present setup, keygen, encrypt and decrypt.

Since here uses user's private keys for access structure and attributes for attributes for cipher text the keygen algorithm is different from ABE. Thus the decryption algorithm also changes with respect to keygen algorithm.

In keygen algorithm, it takes access structure T and master key MK as input. To decrypt an encrypted message they keygen algorithm provides a secret key SK. Decryption is possible if and only if set of attributes matches T. Decryption algorithm takes SK, T and cipher text as input and output message M if and only if attributes set satisfies the users access structure T.
Disadvantages: KP-ABE achieve fine grained access control and more flexible.
Disadvantages: Encryptor cannot decide who can decrypt the encrypted data. It can only choose attributes.

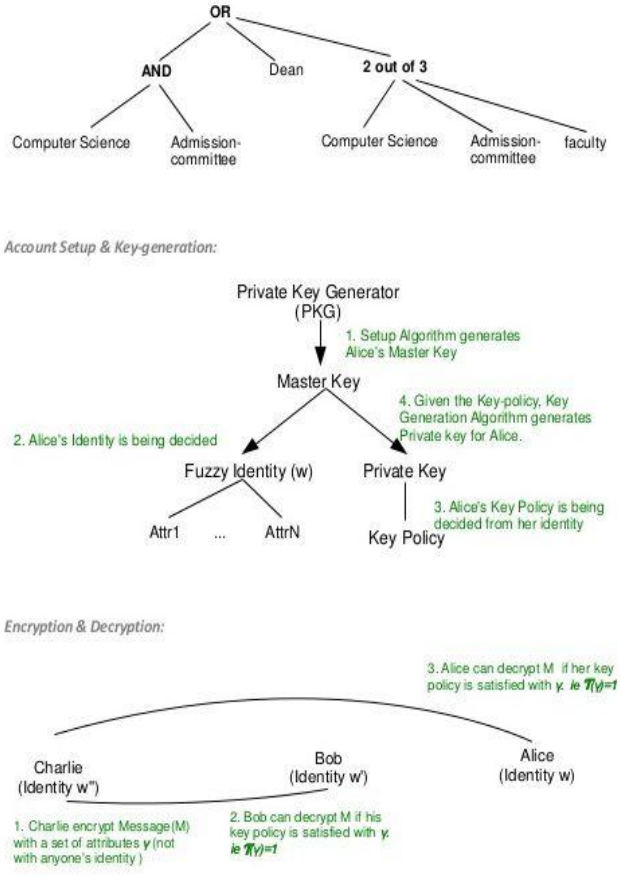

Figure 3. KP-ABE

2.4.2. Cipher Text Policy Attribute Based Encryption scheme (CP-ABE)

In 2007, Bethencourt et al.[5] proposed a cipher text policy attribute-based scheme, and the access policy in the encrypted data (cipher text). The access control method of this scheme is similar to the key policy attribute-based encryption. In key policy attribute-based encryption, the access policy is in user's private key, but the access policy is switched to the encrypted data in cipher text policy attribute-based encryption. And a set of descriptive attributes are associated with the user's private key, and the access policy is built in the encrypted data. The access structure of the encrypted data is corresponding to the user's private key with a set of descriptive attributes. If a set of attributes in

user's private key satisfies the access structure of the encrypted data, the data user can decrypt the encrypted data; if it cannot, the data user cannot obtain the message.

In the access structure of this scheme, it adopts the same method which was depicted in KP-ABE to build. And the access structure built in the encrypted data can let the encrypted data choose which key can recover the data, it means the user's key with attributes just satisfies the access structure of the encrypted data. And the concept of this scheme is very close to the traditional access control scheme. There are five algorithms in this scheme, Setup(), KeyGen(), Encrypt(), Delegate(), Decrypt(). The Delegate algorithm is in addition more than above schemes, and it can input user's private key and regenerate the new one with another attributes which are in a set of attributes of the original user's private key. And this key is equal to the key generated from the authority
The CP-ABE builds the access structure in the encrypted data to choose the corresponding user's private key to decipher data. It improves the disadvantage of KP-ABE that the encrypted data cannot choose who can decrypt. It can support the access control in the real environment. In addition, the user's private key is in this scheme, a combination of a set of attributes, so an user only use this set of attributes to satisfy the access structure in the encrypted data. Moreover, the CP-ABE scheme is applied in the proxy re-encryption field to increase security of this field. The CP-ABE scheme can be applied in the scheme which can achieves proxy re-encryption in cloud environments.

2.4.3. ABE with monotonic access structure

Uses AND gate, OR gate or k out of N threshold gate. This attribute based scheme is proposed by Ostrovsky et al[6]. in 2007 with non monotonic access structure. The access formula of access structure in user's private key can represent any type through attributes such as negative ones. It is different from the previous attribute based encryption scheme. The previous schemes are like KP-ABE scheme, and the access structure in user's private key has monotonic access formula. No negative attributes exist in it. Apart from this, the access structure of this scheme is the same as the access structure of KP-ABE scheme. There is a Boolean formula such as And, OR, and threshold gates in these access structures, but there is a Boolean formula, NOT in access structure of this scheme. However, other schemes do not include it. There is an example for this scheme. If a teacher in department of information management wants to share the data with students, he will set a set of attributes in the encrypted data.

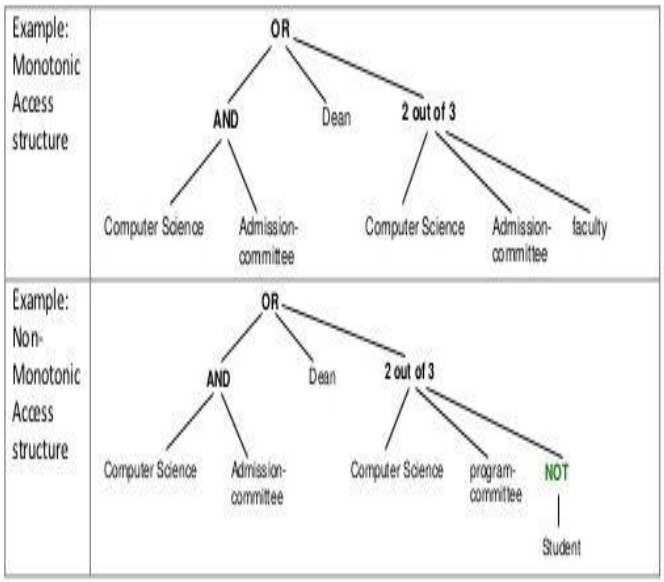

Figure 4. Example for monotonic and non monotonic access structure

2.5. Hierarchical Attribute based Encryption Scheme(HABE)

Hierarchical attribute based encryption which is a combination of hierarchical identity based encryption and cipher text policy based encryption, is proposed by Wang et al, in 2011[7]. To generate keys this scheme uses the property of hierarchical generation of keys in HIBE scheme. DNF (Disjunction normal form) is used to express the access control policy and all attributes in one conjunctive clause. There are five roles in HABE scheme. Cloud storage service, data owner, the root authority and data users. The data owner can store data in cloud storage services and share data with users. The data is encrypted by data owner. The root authority generates system parameters and domain keys to distribute them. Managing domain authority at next level and all users in its domain is carried out by domain authority. Also it can distribute secret keys for users and with their secret keys users can decrypt the encrypted data to obtain the message. The key generation in this scheme adopts a hierarchical method. The root authority generates a root master key for domain authority at the first level. The system public key and the master key of the domain authority at first level are used to create the master keys for the domain authorities at the next level by the root authority or the domain authority at the first level. In addition, the domain authority generates the user identity secret key and the user attribute secret key for the authorized user.

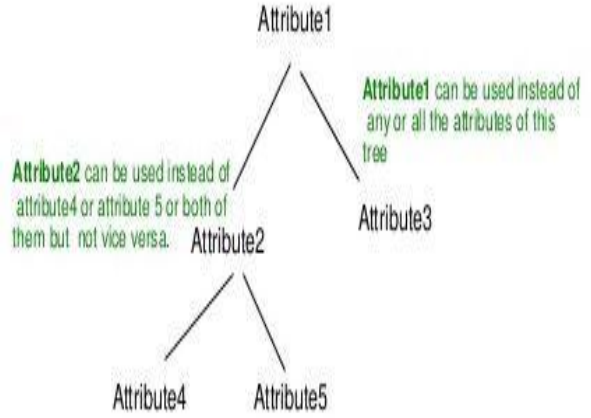

Figure 5. HABE Scheme

2.6. Multi-Authority Attribute based Encryption Scheme(MA-ABE)

MA-ABE was introduced by V Bozovic, D Socek, R Stienwandt and Vil-lanyi [8]. To distribute attributes for users, this scheme uses multiple parties. MA-ABE is composed of k attribute authorities and one central authority. A value dk is assigned to each attribute authority. Here the recipient is defined by a set of attribute not by a single string. One disadvantage of MA-ABE is that each authority attribute set be disjoint and it is complicated.

III. CONCLUSION

Different encryption schemes are discussed in this paper: ABE, KP-ABE, CP-ABE, IDE, FUZZY IDE, HABE, MA-ABE etc. Based on their access policy they are classified. In KP-ABE access policy in the user's private key and in CP-ABE access policy is in the encrypted data. The access structures are predefined in all these schemes i.e. if a user wants to access data and his attribute are not in the access structure, these encrypted data will be re-generated.

The above discussed schemes have some properties: (1) they don't care about the number of users in the system. (2) they are resistant to collusion attack since each attribute has a public key, secret key and a random polynomial (3) only authorized users can satisfy the access policy to decrypt data. (4) Boolean functions are used in access structures for the flexibility in user's access.

REFERENCES

[1] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," Proc. IEEE transactions on parallel and distributed systems , pp. 384- 394, 2014

[2] H. Li, Y.Dai, L. Tian, and H.Yang, "Identity-Based Authentication for cloud computing, " *Proc. First Int'l Conf. Cloud Computing (CloudCom)*, pp. 157-166, 2009

[3] A. Sahaii and B. Waters, "Fuzzy Identity-Based Encryption," *Proc. Ann. Int'l Con. Advances in Cryptology (EUROCRYPT)*, pp. 457-473,2005

[4] V. Goyal, O. Pandey, O. Pandey, A. Sahai, B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," *Proc. ACM Conf. Computer and Comm. Security*, pp. 89-98, 2006.

[5] J. Bethencourt, A. Sahai, and B. Waters, "Cipher text Policy Attribute based Encryption." *Proc. IEEE Symp. Security and Privacy"*, pp.321-334, 2007.

[6] C. Lee, P Shung, M Hwang, "A survey on attribute based Encryption schemes of access control in cloud environments," *Proc. Int'l journal Of Network Security*, pp.231-240, July 2013

[7] G. Wang, Q. Liu, J.Wu, "Hierarchichal Attribute-based Encryption for fine grained access control in cloud strorage services," *Proc. 17th ACM Conf. Computer and Comm. Security(CCS)*, pp 735-737,2010

M.Chase,"Multi-Authority Attribute Based Encryption," *Proc. Fourth Conf. Theory of Cryptography (TCC*), pp.515-524, 2007

