SURVEY ON TECHNIQUES OF ENCRYPTION FOR CLOUD STORAGE SECURITY

[1]Mrs.K.Ketzial Jebaseeli, [2]Dr.V.G.Rani
[1]Research Scholar, [2]Associate Professor
[1] Department of Computer Science
[1] Sri Ramakrishna college of Arts and science for women Coimbatore, Tamil Nadu, India

Abstract: The cloud service is very suitable to many new companies. Conversely, security issues are being raised based on shared data, since the cloud storage servers and data owners are not in the same domain. Moreover, cloud storage cannot be trusted wholly. As a result, it makes access control more on the shared data a challenging issue that addresses how data owners make certain that their data stored in cloud storage servers are accessed by justifiable users. Cloud computing is considered as an innovatory improvement in data resources management. In addition, cloud data sharing is among the preferred services that are accessible by cloud service providers, which paves the way to data owners for outsourcing their data to cloud data storage servers on the intention of sharing. Cipher text Policy Attribute-Based Encryption (CP-ABE) provides access control in owner's hand in which the secret key of a user and the cipher text are reliant ahead of attributes. Likewise different types of algorithms have been discussed in this paper.

Index terms: **Cloud computing, key policy, Access Control, cipher text policy Attribute.**

I. INTRODUCTION:

The challenges of data security which commences both integral and confidential have been addressed to some point through the implementation of encryption techniques for data on the contrivance or Cloud infrastructure and in transit crosswise the network. On the other hand, such schemes are restricted due to the considerable overhead of administering encryption keys for a huge number of data types, files or documents, to an extensive range of individuals or groups. With the rapid expansion of Cloud computing technology and services there has been found a rush forward in individuals, groups and organizations in uploading data into the Cloud for effortlessness of use or on saving costs. In these circumstances users are capable to share keys to increase on access ahead of their rights. Social networking is a great example where they are vibrant in terms of storage prerequisite by means of cloud. Conversely this lags behind due to the weak security issues and also the use of cloud is not very fast in content sharing networks.

The conventional mechanism is that the data has been encrypted by means of the user's public keys. By the use of these public keys, the owners are able to encrypt the data and then upload the file into the cloud. Whenever the user want to download the file he should decrypt the file with his generated secret key. By decrypting this are problems that arises - like the owner has to search out the public key of the user and the same data is encrypted with diverse public keys which therefore fallsout in storage overhead. The access policy here is utterly based on compliance relationship where the relationship is on edge by user attributes and resource attributes. The attributes may be any information of the user's profession, job roles that is endowed with and is used to give allowance to the access. In CP-ABE the beneficiary can decrypt the data only when the user attribute persuade the access policy and this can be seen as one-to-many public key encryption and the data possessor provides admittance to countless users.

II. LITERATURE SURVEY:

2.1Cipher text Policy Attribute based Encryption :

A cryptographic technique named cipher text policy attribute-based scheme has been explained in the year 2007, Bethencourt et al.[1]. The access policy is built with the data that has been encrypted. A plan was made in [2] for the use of CP-AB technique. In a CP-ABE system, a user's key is in relation with a set of attributes and an encrypted cipher text will specify an access policy over attributes. The first KP-ABE construction has been realized from the monotonic access structures for key policies. Bethencourt et al. proposed the first CP-ABE construction. The construction is only proved secured underneath the generic group model. To prevail above this weakness, Cheung and Newport [3] presented an additional construction that is proved to be secure under the standard model. To accomplish receiver-anonymity, Boneh and Waters proposed a predicate encryption scheme based on the primitive called Hidden Vector Encryption. In this projected scheme data owners need not be alarmed about defining any access policy for users, but just need to define only the access policy for attributes as in the previous ABE schemes. This construction is deprived of private keys that will be identified with a set of descriptive attributes.

2.2 .Key-Policy Attribute-based Encryption :

Key Policy Attribute based Encryption is commenced by VipulGoyal and Omkant Pandey[4] to accomplish fine-grained access control[5] in one- to-many communications. The KeyGen and Decrypt algorithms get fluctuated from the Attribute Based Encryption. In Key-Policy Attribute- based Encryption, clandestine key of the user is cognate with the access structure.The authors have developed a much wealthier type of attribute-based encryption cryptosystem and have demonstrate its applications in different ways. In this system each cipher text is labeled by the encryptor with a set of expressive attributes. Each private key is associated with an access structure that specifically denotes which type of cipher texts the key can decrypt and this is called a scheme Key-Policy Attribute-Based Encryption (KP-ABE), because the access structure is specified in the private key, while the cipher texts are simply labeled with a set of descriptive attributes. Using familiar techniques one can put up a secret-sharing scheme that specifies that a set of parties must assist in order to renovate a secret. For instance, one can specify a tree access structure where the internal nodes consist of AND and OR gates and the leaves consist of different parties. Whichever set of parties that assures the tree can reconstruct the secret.

2.3. Homomorphic Encryption :

Ronald Rivest et al[5] elucidate the Homomorphic encryption concepts. This proposal is applied in the cloud environment to defend the data. These Homomorphic encryption schemes consent to executing computations on the encrypted data. It is only of the highly developed cryptographic technique. In [6] the major shortcoming of homomorphic encryption is explained. It has a dawdling processing time during computation. In 1984 Shamir demanded for a public key encryption method in which the public key can be an illogical string. In such a scheme there are four algorithms: (1) setup generates global system parameters and a master-key, (2) extract uses the master-key to generate the private key corresponding to an arbitrary public key string ID $\in \{0, 1\}*$, (3) encrypt encrypts messages using the public key ID, and (4) decrypt decrypts messages using the corresponding private key.

2.4. Multi-Authority Attribute based Encryption:

Multi-Authority Attribute Based Encryption has been set up by Chase [7] The Multi-Authority Attribute Based Encryption (MA-ABE) is also a cryptographic procedure which consists of many authorities to deal with the attri- butes and the allocation of the secret keys. The users who desire to download the information will ask for the decryption keys from the attribute influence. The attribute key generation is one of the algorithm in MA-ABE. This cryptographic scheme knobs more number of users. Data discretion can be achieved by using this type of practice in cloud environment. This cryptographic scheme picks up security and condenses key management complication which is the most important advantage. The scheme is put together upon a single-authority attribute-based encryption scheme presented earlier by Sahai and Waters. Chase's production [7] uses a trusted central authority that is inherently proficient of decrypting arbitrary cipher texts created within the scheme.

2.5. Attribute-based Encryption :

Attribute-based Encryption is one of the cryptographic techniques used in Cloud Computing Environment. Attribute-based Encryption is first proposed and made into use by Sahai and Waters[8] in the year 2005. The key focus of this Attribute-based Encryption scheme is to endow with security to the data stored in the cloud. The four steps in Attribute Based Encryption are Setup, KeyGen, Encrypt, Decrypt. The users who are authorized can decrypt the information using their personal key. This encryption method crafts the cloud environment more protected. From these solutions it is understood that, the solutions allow any encryptor to indicate access control in terms of several access formula over the attributes in the system[9]. The only work to accomplish the parameters is limited to a proof in the generic group model.

2.6. Symmetric Searchable Encryption:

Symmetric Searchable Encryption is relevant for the atmosphere where the client that searches the data and as well he is liable for generates it. A Single Writer/Single Reader (SWSR) is the resultant from cloud storage terminology. SSE schemes were presented in[10] and improved constructions and security terms were specified in[11] SSE provides sanctuary guarantees which are discussed as (i) the information about the data are concealed until the tokens are exposed. Since token is not revealed, the server learns only the length information. (ii) when the token is provided for a keyword, the server absorbs the document containing the keyword devoid of knowing the keyword. SSE scheme unaccompanied handles the concept of concurrence by pairing with the help of elliptic curves but it is incompetent when applying Asymmetric Searchable Encryption schemes (ASE). Ostrovsky et al. proposed a non-monotonic access structure [12] in 2007, in which the scheme can let each attribute affix primed word in front of them.

2.7. Asymmetric Searchable Encryption (ASE):

Asymmetric Searchable Encryption (ASE) scheme[9] is appropriate for the environment where the client that searches the data is unusual from the one who generates it. This scenario is referred as Many Writer/Single Reader (MWSR). Abundant works have been executed to illustrate how to accomplish more difficult queries in public-key setting like conjunctive searches and range queries[13],[14] Evaluated to SSE scheme, The ASE is suitable for massive amount of setting due to the several writer and reader. ASE provides security warranties which are discussed as (i) the information in relation to the data that are veiled until the tokens are revealed. Since token is not revealed, the server learns only the length information It can also recognize the token and act upon an appropriate search to find out which documents embrace the (known) keyword. It describes a high level,[15] quite a lot of architectures that merge and non-standard cryptographic primitives in order to achieve the goal.

2.8. Identity based Encryption

Identity Based Encryption cryptographic scheme was proposed by Shamini in the year 1984. The most important issue is the lack of ability to build Identity Based Encryption system which is developed on the basis of on RSA. Later on in the year 2001 a proficient Identity Based Encryption has been introduced by Boneh and Franklin[16]. In Identity Based Encryption, the uniqueness of the user plays an imperative role. Only the receiver's identity attribute has to be known by the sender in order to send the encrypted messages. Email Encryption is one of the chief applications for Identity Based Encryption. On the other hand, key revocation is not accomplished in Identity Based Encryption.

The Following table illustrates different encryption techniques based on Access control, Scalability, Flexibility, and Efficiency

Table 1. Cryptographic Algorithm Analysis

Encryption Techniques	Efficiency	Access Control	Scalability	Flexibility
CP-ABE	Avg	High	Avg	High
KP-ABE	Avg	Avg	Avg	High
HE	Low	Low	Avg	Low
ABE	Avg	Avg	High	Avg
MA-ABE	High	Better	High	High
IDE	Low	Low	Avg	Low

III. CONCLUSION:

The extreme main and the vital objective of encryption is to secure your files and data by converting it into encrypted language and also converting into cipher text from plain text. The common accomplishment is that by the use of the above mentioned types of encryption, the cloud storage by a vast data is possibly secured. CP-ABE is mainly based on access management and authorizes a data owner to impose access management supported attributes of data customers while not unambiguously naming the scrupulous information by customers. With the accurate password, the information can be "decrypted" again – translated into its original format. Nevertheless, CP-ABE supports just one privilege level and consequently it is not appropriate for access management to ascendable media. In this paper we presented a basic progress of the CP-ABE and how the access structure is put up in the CP-ABE. Cloud computing is the extremely adaptive technology and mobile devices are fetching prevalent in the above presented CP-ABE access control which helps to get liberated from the computational demanding operations on the cloud server. Symmetric-key algorithms are a group of algorithms for cryptography that use insignificantly related, habitually identical, cryptographic keys for both decryption and encryption. The investigational results be an evidence for that all the encryptions are made easier and is flexible, scalable, user, liability, collision, defiant, user revocation. With the backing of the cloud the quickening of the decryption is augmented but it is still deliberate in some low- end devices because an integrated exponentiation operation is requisited. Assymetric encryption is a type of encryption that arises through the from of pairs. It is also called Public Key Cryptography. These Algorithms also enables vibrant amendment of access policies that supports competent on-demand attribute revocation under tragedic scenarios. Online/offline ABE scheme can be put into operation to perk up the rapidity of key generation and encryption.

REFERENCES

[1] J. Bethencourt, A. Sahai, and B. Waters, Cipher text- policy attribute-based encryption, Proceedings of IEEE Symposium on Security and Privacy, pp. 321V334, 2007.

[2] RajaSekhar B, Kumar S, Swathi Reddy L, PoornaChandar V. CP-ABE Based Encryption for Secured Cloud Storage Access International Journal of Scientific and Engineering Research. 2012; 3(9).

[3] M. S. Hwang and I. C Lin, Introduction to Information and Network Security (4ed, in Chinese), mation and Network Security

(4ed, in Graw Hill. In Taiwan, 2011. .

[4] Goyal V, Pandey O, Sahai A, Waters B. Attribute based encryption for fine-grained access control encrypted data, CCS.

[5] Yu S, Wan C, Ren K, Lou W. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing.

[6] Boneh D, Franklin M. Identity-Based Encryption from the Weil Pairing. Proceedings of Cryptography.

[7] Chase M. Multi-authority attribute based encryption Proceedings of the Theory of Cryptography 2007; 515–

[8] Waters. B, (2008) Ciphertext policy attribute based encryption : An expressive, efficient, and provably

[9] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute based encryption with non-monotonic access structures," in Proceedings

[10] V Bozovic, D Socek, R Steinwandt, and V. I. Villanyi, Multi- authority attribute-based encryption with honest-but-curious central Authority. International Journal of Computer Mathematics, vol. 89, pp. 3, 2012.

[11] Chase M. Multi-authority attribute based encryption Proceedings of the Theory of Cryptography 2007; 515–

[12] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute based encryption with non-monotonic access structures,"

[13] D. Boneh, X. Boyen, and E.-J. Goh. Hierarchical identity based encryption with constant size ciphertext.In R. Cramer, editor, EUROCRYPT, identity based encryption with constant size ciphertext.

[14] Waters. B, (2008) Ciphertext policy attribute based encryption : An expressive, efficient, and provably

[15] Bardin, J., Callas, J., Chaput, S., Fusco, P., Gilbert, F., Hoff, C., Hurst, D., Kumaraswamy, S., Lynch, L., Matsumoto, S., O'Higgins, B., Pawluk, J.Reese, G., Reich, J., Ritter, J., Spivey, J., Viega, J.: Security guidance for critical areas of focus of cloud

[16] Boneh D, Franklin M. Identity-Based Encryption from the Weil Pairing. Proceedings of Cryptography 2001, LNCS, Springer-Verlag. 2001; 2139:213–29.

.