Attribute Based Encryption in Cloud Computing

Devi.T, N.Deepa, Kodikalla Preetham Krishna, P.Mohit Sai

Abstract: Cloud acts as a database for huge amount of data. It allows users to store the information or data related items in the cloud storage and allows them to use/ their data via network connection. There are different types of cloud, Public private hybrid and community. In case of public cloud the user rents the storage and stores the data in it. There exist some trust issues in storing data in the cloud since there are many untrusted users who also rented the cloud and there is need for the encryption of data there are many ways to encrypt the data the new trend in encryption is attribute based encryption. The main advantage in attribute based encryption is that it depends on the attributes of the user which differs vastly from one user to another. This paper explains about the use of attribute based encryption in cloud and how it differs from the other encryption algorithms and it advantages over other algorithms. This paper also explains about the cipher-text policy in ABE in various aspects.

Keywords: Cloud, privacy, attribute based encryption, cipher-text, encryption algorithms etc

I. INTRODUCTION

Cloud provides the users a new dimension to store and access information resources in various forms. It is the on-demand usage of network resources especially data resources and pay as peruse metering service. It can be also defined as the huge data centers where authorised users can access to the data stored in it. The cloud provides different types of services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS). SaaS is a set of programs which are predefined and are suitable for the naive users where the users don't need any knowledge about the programming and other things. IaaS is a advanced set of service where the user should have knowledge about programming, create a platform based application and use it and it is not suitable for naive users. PaaS gives the users a platform to create an application and run it the users should need computer knowledge. These are service models and there also exist some deployment models they are public cloud, private cloud, community cloud and hybrid cloud. Public cloud is shared by many users based on their data requirements it is generally used by small companies.

Private cloud is owned by a single organisation. These are generally used by large companies whose data requirements are high. Community model is shared between users whose data requirements are similar and hybrid cloud is a mixture of any two models of the above. There exist some privacy issues when the data is stored in the cloud. So the data is encrypted and the encrypted data is stored in the cloud and while data is accessed by the user, the data is decrypted. There are many ways to encrypt the data some of them are:

Hashing

Hashing is a one of a kind of encryption where it uses, fixed-length key for a plain text or informational collection. Each "hash" is exceptional so minor changes to that message would be difficult to follow. When the text is encoded by using this technique, it can't be turned deciphered.

Symmetric techniques

Symmetric encryption techniques are commonly called as private-key cryptography, due to the fact that the key used to encode and decipher the plaintext and it is needed to stay secure,. By using this technique, a sender scrambles the plaintext with one key, sends the ciphertext the collector uses the same key to decode the information.

Unbalanced techniques

Unbalanced technique of encryption, in relation to the past technique since it utilizes two keys for encryption or ciphering the data. With this technique, an public key is unreservedly known to everybody and is required to scramble messages, and another private key is required to decode messages.

However, these encryption techniques are useful only for ensuring the secrecy of information, but the control of access of data items is not possible. The ABE is an open key encryption method that ensures the data security which is shared among multiple users in which one can get advantages of both access control and privacy. In ABE, data is encoded into ciphertext using attributes and decoded by the help of secret or private key of a user. This is classified into two different types based on the attributes choosing. They are KPABE and CPABE. The classification and explanation of ABE is described in the below figure 1.

Revised Manuscript Received on July 13, 2019.

Devi.T, Assistant Professor, Saveetha School of Engineering, SIMATS, Chennai

N.Deepa, Assistant Professor, Saveetha School of Engineering, SIMATS, Chennai

Kodikalla Preetham Krishna, Assistant Professor, Saveetha School of Engineering, SIMATS, Chennai

P.Mohit Sai, Assistant Professor, Saveetha School of Engineering, SIMATS, Chennai

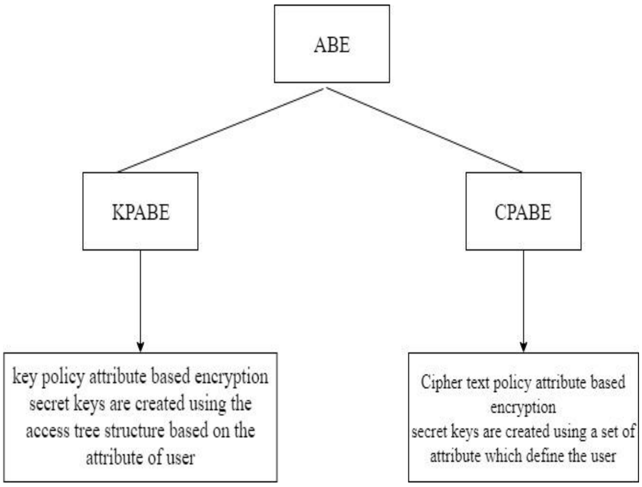
ABE
KPABE
CPABE
key policy attribute based encryption secret keys are created using the access tree structure based on the attribute of user
Cipher text policy attribute based encryption
secret keys are created using a set of attribute which define the user

Fig. 1 ABE Classification

II. LITERATURE REVIEW

[1] Sahai et al initiated this idea of ciphertext attribute based encryption in cloud environment he proposed this system as the method of cryptography in which the key is open for the securing the document data in the cloud. In his paper the encrypted information is based on the characteristics it also produces itself a mystery key which is important for this encryption. **[2] Goyal et al**. proposed the key based attribute based encryption in which the cryptography is a fine grained sharing of the scrambled information. The structure used in the system is based on the access tree structure. **[3] Ostrovskyet al**. proposed the new method called non-monotonic structure which is used for encryption of both positive and negative properties it used three logic gates AND, NOT and OR for ranging the access structure of the data. **[4] Lewkoetalim** showed that the strategy used in his paper is very small size of the private keys which underpins the non-authorized users. **[5] Attrapadung et al** proposed the usage of the steady size ciphertext it relies upon the traits quality which is a huge task required per quality. **[6] Wang et al** initiated the consistent size encryption of plaintext for access structures of data. This paper is based on communicate encryption plot. Both the works are specifically secure yet not completely verified by the experts so this is not much consistent.**[7] Lai et al** proposed crafted by consistent access structures of data with completely safe and quick decoding

III. PROPOSED SYSTEM

In our proposed system the private keys are generated using a algorithm and the encryption is based on the access tree structure. To encrypt the message ‘m’ we need to take some attributes of the user and construct a access tree structure and encrypt the message based on the access tree. The leaves of the access tree are properties or attributes of the user. To decode the message we need the same access tree and reconfigure the message. We used a recursive algorithm for the repeated reciphering the text based on the access tree attributes. It is not easily done by using a recursive algorithm and the help of access tree as the key and the attributes of the user the message is decrypted.

The following steps are followed for the key generation

1. Finding the set of attributes of the user which are unique
2. Developing an access tree structure for generating keys
3. The ends of the access tree are the nodes and the attributes
4. With the help of the access tree structure, the plaintext is converted into encrypted language.
5. By using the recursive algorithm and merging the message is decrypted back to the original form.

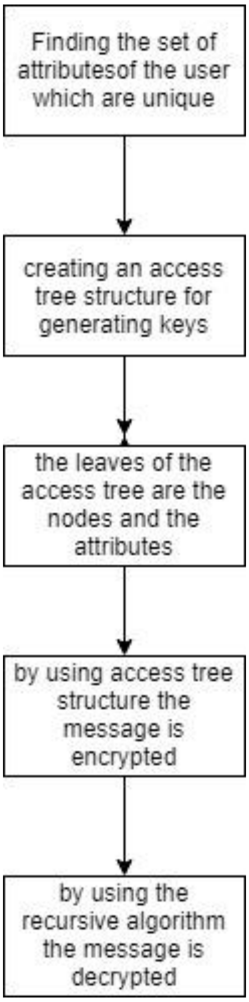
Finding the set of attributesof the user which are unique
creating an access tree structure for generating keys
the leaves of the access tree are the nodes and the attributes
by using access tree structure the message is encrypted
by using the recursive algorithm the message is decrypted

Fig. 2 Flowchart for the attribute based encryption

IV. IMPLEMENTATION

While using the recursive algorithms we need to bring the merge pairing concept using a private key attribute we create repeated recursive algorithms for the decryption of each node each function is declared in it by usage of repeated recursion all the nodes will be decrypted with the selected private key and the original message is traced back. We need to merge the pairings Which can be done through the combing the set of attributes by using this merging technique the time needed for the decryption can be decreased due to this the ABE can have the greater application in the future.

V. CONCLUSION AND FUTURE ENHANCING

We created a new algorithm for ABE system where the secret key is based on the user which differs from one person to another vastly thereby creating a innumerable number of private keys in it by using the access tree structures this method is a key dependent attribute based encryption algorithms and also used some of the concept of ciphertext policy ABE for the recursive algorithms in the decryption process.

REFERENCES

1. A. Sahai, B. Waters, Fuzzy identity-based encryption, in: Theory and Applications of Cryptographic Techniques, Springer Berlin Heidelberg, 2005, pp. 457-473. https://doi.org/10.1007/11426639_27
2. V. Goyal, O. Pandey, A.Sahai, 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, ACM, 2006, pp. 89-98. https://doi.org/10.1145/1180405.1180418
3. R. Ostrovsky, A.Sahai, B. Waters, Attribute-based encryption with non-monotonic access structures, in: ACM Conference on Computer and Communications Security Computer and communications security, ACM, 2007, pp. 195-203. https://doi.org/10.1145/1315245.1315270
4. A. Lewko, A. Sahai, B. Waters, Revocation systems with very small private keys, in: Security and Privacy (SP), IEEE, 2010, pp. 273-285. https://doi.org/10.1109/SP.2010.23
5. N. Attrapadung, B. Libert, E. De Panafieu, Expressive key-policy attribute-based encryption with constant-size ciphertexts, in: Public Key Cryptography, Springer Berlin Heidelberg, 2011, pp. 90108. https://doi.org/10.1007/978-3-642-19379-8_6
6. C.J. Wang, J.F.Luo, A key-policy attribute-based encryption scheme with constant size ciphertext, in: Eighth International Conference on Computational Intelligence and Security (CIS), IEEE, 2012, pp. 447-451. https://doi.org/10.1109/CIS.2012.106
7. J. Lai, R. H. Deng, Y. Li, J. Weng, Fully secure key-policy attribute-based encryption with constant-size ciphertexts and fast decryption, in: Proceedings of the 9th ACM Symposium on Information Computer and Communications Security, ACM, 2014, pp. 239-248. https://doi.org/10.1145/2590296.2590334
8. M. Chase, Multi-authority Attribute Based Encryption, in: In Theory of Cryptography Conference, vol. 4392, Berlin Heidelberg, 2007, pp. 515–534. https://doi.org/10.1007/978-3-54070936-7_28
9. M. Chase, S.S. Chow, Improving privacy and security in multi-authority attribute-based encryption, in: Proceedings of 16th ACM Conference Computer and Communications Security, ACM, 2009, pp. 121-130. https://doi.org/10.1145/1653662.1653678
10. J. Han, W. Susilo, Y. Mu, and J. Yan, Privacy-preserving decentralized key-policy attribute-based encryption, IEEE Trans. Parallel Distrib. Syst. 23(11) (2012) pp. 2150–2162. https://doi.org/10.1109/TPDS.2012.50