ATTRIBUTE BASED ENCRYPTION SCHEME BY RING SIGNATURE IN CLOUD COMPUTING

[1]KETHAVATH SAMBASIVA NAIK and [2] K.F BHARATI

[1]M.Tech (student), Department of CSE, JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY, ANANTAPUR, ANDHRA PRADESH

[2]ASSISTANT PROFESSOR, Department of CSE, JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY, ANANTAPUR, ANDHRA PRADESH

ABSTRACT- Formally, Cipher text-policy attribute-based encryption (CP-ABE) technique has been implemented in multilevel hierarchy in well known areas like healthcare and military. The drawback is that representation of the relaxed records in multilevel hierarchy is not explored. To access the shared files in layered structure, encryption technique CP-ABE is implanted such that hierarchal files can be accessed in single access structure. However, single access structure improves the efficiency of time and storage cost of shared files. In generally, user doesn't provide their personal information in service based applications due to privacy issues. To access such applications flexibly and to reduce potential issues, CP-ABE scheme is adopted successfully

Keywords: Cloud computing, data sharing, file hierarchy, ciphertext -policy, attribute-based encryption, ring signature.

I. *INTRODUCTION:*

The expanding of system innovation and portable terminal, online information sharing has resources to get consistency. for example, Facebook and twitter . In the interim, distributed computing is to be clear amongst the most encouraging application stages to seize the delicate growing of information sharing. In distributed computing, to protect information from Spilling, clients need to scramble their insights earlier than being shared. Access control is vital as it miles the essential line of resistance that stops unapproved a get right of access to the mutual realities. As of late, characteristic based totally encryption (ABE) has been pulled in a lot additional considerations for the reason that it can hold data protection and perceive astounding grained, one-to-many, and no intelligent gain admission to power. Ciphertext-coverage attribute primarily based encryption (CP-ABE) is certainly one of possible schemes which has plenty more flexibility and is extra appropriate for preferred packages.

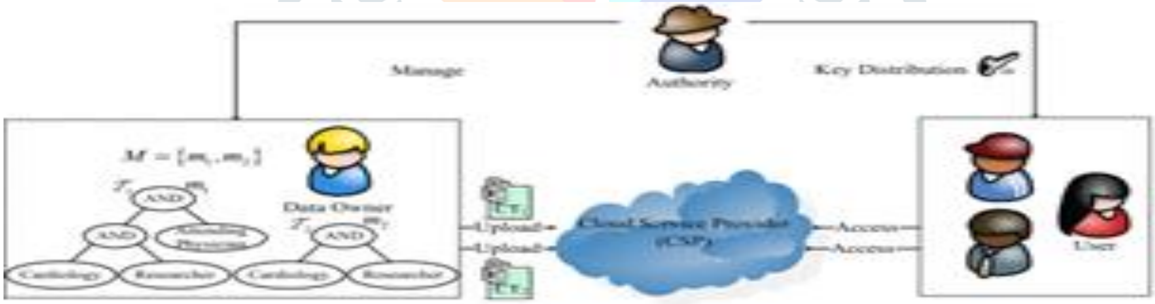


Fig.1: The data sharing in the cloud computing.

CP-ABE [1] scheme to encrypt the records m1 and m2 via different get right of entry to rules based on the actual want. For instance, an attending physician wishes to get right of entry to each the affected person's call and his medical document in order to make a diagnosis, and clinical researcher simplest needs to get right of entry to some clinical take a look at consequences for educational motive.

II. RELATED WORK

C. Gentry and A. Silverberg [2] proposed the principle thought of various leveled encryption plot, numerous progressive CP-ABE plans have been proposed. For instance, Wang et al. proposed a various leveled ABE conspire by joining the progressive IBE and CP-ABE. X. Xie, H.Ma, J. Li [2] and B. Waters [3,4,5] proposed various leveled CP-ABE. Afterward, Zou gave a progressive ABE plot, while the length of input is straight with the request of the characteristic set. At introduce, there are three sorts of access structures AND door, get to tree, and Linear Secret Sharing Scheme (LSSS) utilized as a part of existing CP-ABE plans. Cheung and Newport initially utilized AND door get to structure to accomplish CP-ABE plan. Then, there are CP-ABE plans in view of access tree that help AND, OR, and edge, and in linear secret sharing scheme (LSSS) where and are the ordinary plans of access tree and LSSS. Other CP-ABE plans with specific highlights had been given For instance, J.Hur [6] proposed a certainties sharing plan to clear up the issue of key escrow by method for the utilization of an escrow loosened key issuing convention between the key age focus and the measurements putting away focus. Green et al[7] further, Lai et al. Proposed CP-ABE plans with outsourced unscrambling to lessen the workload of the decoding individual and C-I Fan[8] Proposed an arbitrary-kingdom ABE scheme to remedy the trouble of the dynamic association control. In addition, Guoet al proposed a novel steady-size decryption key CP-ABE scheme for storage-limited devices. Rosenberger and Waters proposed a web/offline ABE scheme to enhance the velocity of key generation and encryption, where each computation paintings in the processes is cut up into two phases offline section and online section.

III. FRAMEWORK

The device version in cloud computing is given, which incorporates 4 one-of-a-type entities: authority, CSP, information proprietor and user. Among those entity, we assume that information proprietor has good enough documents with ok get admission to degrees and M = m_1, . . . , m_k is shared in cloud computing. Here, m_1 is the highest hierarchy and m_k is the lowest hierarchy. If a person can decrypt m1, the person also can decrypt m_2, . . . , M_k. Authority: It is a totally relied on entity and accepts the client enrollment in cloud and it may additionally execute Setup and key generation operations. Cloud Service Provider (CSP): It is a semi-trusted Entity in cloud services.

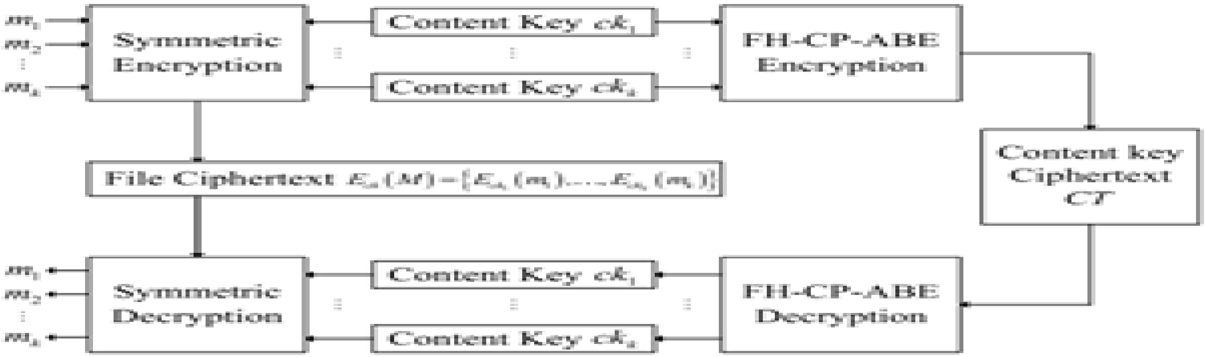


Fig2: The framework of FH-CP-ABE scheme.

There is no doubt it can perform the assigned duties and return correct consequences. However, it would really like to find out as a first-rate deal touchy contents as feasible. It affords ciphertext storage and transmission services. Data Owner: It has big data to be saved and shared in cloud tool. The entity is in price of defining get admission to structure and executing encrypt operation and it uploads ciphertext to CSP. User: It desires to access a big range of data in cloud machine. The entity first downloads the corresponding ciphertext then it executes Decrypt operation will be performed. In Fig 2, a records proprietor procedures the documents as follows: Firstly, the records proprietor chooses k content fabric keys ck_1, . . ck_k, and encrypts documents M1, . . . , MK with the content material fabric keys via the use of symmetric encryption algorithm (i.e., DES, AES). The cipher texts are denoted as Eck(M) = Eck_1(m1),...,Eck_k(MK). Then, the data owner encrypts ck_1, . . ck_k. The use of FH-CP-ABE encryption algorithm and obtains an protected ciphertext of content keys(CT). The policy of decryption are defined as underneath. Firstly the man or woman decrypts ciphertext(CT) and obtains content material fabric key with the aid of the use of FH-CP-ABE decryption operation. Then, the man or woman can reap file by way of the use of using symmetric decryption set of policies with the content material key. Definition 2: The FH-CP-ABE scheme consists of four operations: Setup, KeyGen, Encrypt and Decrypt. It is defined as follows : *Cloud Service Provider (CSP):* It is a semi-trusted in entity in cloud framework. It can sincerely perform assignments and return remedy comes about CSP. In any case, it might want to discover however much delicate substance as could reasonably be expected. In the proposed framework, it gives ciphertext capacity and transmission administrations. Data Owner: It has large information should have been put away and shared in cloud framework. In our plan, the substance is responsible for characterizing access structure and executing Encrypt task. Also, it transfers ciphertext to CSP. User: It needs to get to a large number of data in cloud framework. The entity initially downloads the relating ciphertext at that point it executes Decrypts task of the proposed scheme.

Ring Signature:

Signature Generation:

Generating a signature involves six steps. The plaintext is signify by m, the ring keys by p1, p2,…, pn.

1.Calculate the key k=H(m)

2. Pick up a random value v.

3.Pick random x_i for all ring members and calculate $y_i = g_i(x_i)$

4. Slove ring equation for $y_{s.}$

5. Signer private key $x_s = g^{-1}_{s}(y_s).$

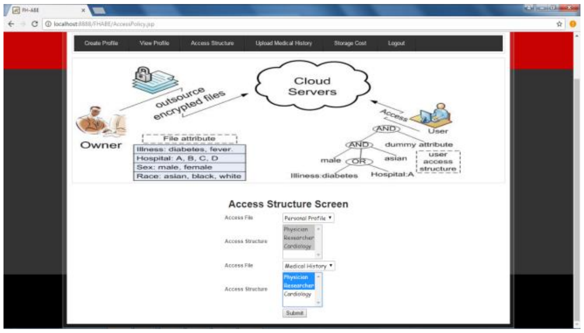
6. The ring signature now is the (2n+1) tuple (p1, p2, p3…pn;v;x1,x2…..,xn).

Signature verification:

1. Apply for all public keys Xi : yi = gi(xi).
2. Calculate the symmetric key k=H(m).
3. Ring equation verify holds $c_{k,v}(y_1,y_2,\dots y_n)=v$.

IV. EXPERIMENTAL RESULT

In this System, proposes to Cloud storage for storing data from users as well as data owner. Ciphertext Policy-Attribute Based Encryption (CP-ABE) has been preferred encryption technology to clear up the challenging trouble of comfortable statistics sharing in cloud computing.



Access Structure Screen

Access File: Personal Profile

Access Structure: Physician, Researcher, Cardiology

Access File: Medical History

Access Structure: Physician, Researcher, Cardiology

The shared information documents commonly have the characteristic of multilevel hierarchy, especially within the region of healthcare and the navy. However, the hierarchy structure of shared files has now not been explored in CP-ABE. The graph is represented that CP-ABE and FH-CP_ABE encryption techniques throughputs. As well as Storage cost is less compared to CP-ABE. To facilitate the presentation in the below,

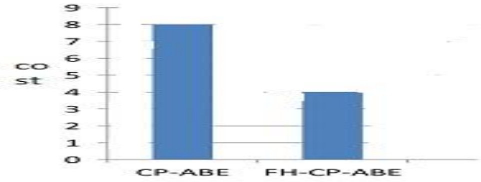


Fig: The storage cost of ciphertext of CP-ABE and FH-CP-ABE.

The encryption process modifying the Basic of FH-CP-ABE scheme in order to reduce computational complexity. In ciphertext (CT) Computation Cost on Data Owner. The layered model of the access structure is provided to share multiple hierarchical files. Some nodes can be removed from CT unless the information node, no-leaf node, level node, or any information about the level node indicating the transport node in the hierarchical access tree. Files are encrypted with an integrated access structure. So, data owner can encrypt the different levels of the files and generate an integrated ciphertext only executing the encryption algorithm one time. Especially, some common attributes should be computed only once instead of many times since each common attribute is appeared in the integrated access structure one time, where the common attribute denotes that it is appeared in multiple access sub-trees associated with k hierarchical files. That is, these delivery nodes are eliminated from CT in the event that they do no longer directly or circuitously contain stage node. More precisely, we improve the element Cˆ (x, y), j approximately transport node in CT. All other operations execute exactly as in Basic FH-CP-ABE. In order to make a clear description, we use an example to similarly illustrate the improved encryption procedure in the step of Cˆ (x, y), j of ciphertext. Security: report ciphertext confidentiality and content key ciphertext confidentiality. We assume that the hierarchical documents are adequately encrypted via the use of symmetric encryption set of rules (i.e., DES, AES). Therefore best the safety proof of FH-CP-ABE need to be provided. In this phase, the security activity of the proposed scheme is given first of all. Then a formal safety proof is furnished primarily based on the outcomes of the literatures.

V.*CONCLUSIONS AND FUTUREWORK*

The proposed scheme is a variant of CP-ABE to properly share hierarchical documents in cloud computing. Hierarchical documents are encrypted with the right to admission to the format and the cipher components associated with features are shared using the documents. Therefore, the cost of both the cipher text storage and the encryption time will be saved. In cryptography, a ring signature is a form of digital signature that can be achieved by subscribers in the collection of clients that each have keys. Therefore, a message signed with a Ring signature is recommended by a person in a selected organization of people. Finally, conclude that one of the protection residences of a Ring signature is that it wants to be computationally infeasible to determine which of the organization individuals' keys turned into used to supply the signature.

VI. REFERENCES

[1] J. Liu, X. Huang, and J. K. Liu, “Secure sharing of personal health records in cloud computing: Ciphertext-policy attribute-based signcryption,” *Future Generat. Comput. Syst.*, vol. 52, pp. 67–76, Nov. 2015.

[2].C. Gentry and A. Silverberg, “Hierarchical ID-based cryptography,” in *Advances in Cryptology*. Berlin, Germany: Springer, Dec. 2002,pp.548-566.

[3]. X. Xie, H. Ma, J. Li, and X. Chen, “An efficient ciphertext-policy attribute-based access control towards revocation in cloud computing,” *J. Universal Comput. Sci.*, vol. 19, no. 16, pp. 2349–2367, Oct. 2013.

[4]. J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” in *Proc. IEEE Symp. Secur. Privacy*, May 2007,pp.321-334.

[5].B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in *Proc. 14th Int. Conf. Pract. Theory Public Key Cryptogr. (PKC)*, vol. 6571. Mar. 2011, pp. 53–70.

[6]. J. Hur, “Improving security and efficiency in attribute-based data sharing,”
IEEE Trans. Knowl. Data Eng., vol. 25, no. 10, pp. 2271–2282,
Oct. 2013

[7]. M. Green, S. Hohenberger, and B. Waters, “Outsourcing the decryption of ABE ciphertexts,” in *Proc. 20th USENIX Conf. Secur.*, Aug. 2011,pp.1-16.

[8]. C.-I. Fan, V. S.-M. Huang, and H.-M. Ruan, “Arbitrary-state attribute-based encryption with dynamic membership,” *IEEE Trans. Comput.*,vol.63,no.8,pp.1951 –1961,Aug.2014.