International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 08, August 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

A Dynamic File Ranking Attribute-Based Encryption System in Cloud Storage

Banda Raju[1], N.Raghu[2], M.Sarika[3]

[1]Pursuing M.Tech (CSE), [2]Working as an Assistant Professor, [3]Working as an Assistant Professor CSE,
[1,2,3]Kamala Institute of Technology and Science, Singapuram, Huzarabad, Karimnagar, Telangana 505468
Affiliated to JNTUH,(India)

ABSTRACT

Data Sharing in Cloud Computing securely has become a problem in challenging the encryption process. So here by we have proposed a Ciphertext-policy attribute-based encryption (CP-ABE) to solve the problems faced by encryption technology. In this we propose known different levels for shared data files especially towards healthcare and military. In this CP-ABE the exploration of this kind of hierarchy structure of shared files is not mentioned. In this paper, a modified file hierarchy attribute-based encryption scheme is proposed in cloud computing. The Different layered access structure is compressed and developed into one access structure and the previous hierarchical files are encrypted with that one access structure. The attributes of related cyphertext components can be shared by the files. By this the storage of cyphertext and time cum cost of encryption will be saved. Based on the standard assumption the proposed scheme is way more secure. The practical results show the better results by this in terms of encryption and decryption. The advantages of our scheme may be more conspicuous as the number of files are increasing.

Keywords—Cloud Computing, Data Sharing, File Hierarchy, Ciphertext-Policy, Attribute-Based Encryption

I.INTRODUCTION

With the thriving of system innovation and portable terminal, online information sharing has turned into another "pet", for example, Facebook, Myspace. Meanwhile, cloud computing [1]– [5] is a standout amongst the most encouraging application stages to understand the touchy growing of information sharing. In cloud computing, to shield information from leakage, clients need to encrypt their information before being shared. Access control [6], [7] is foremost as it is the primary line of safeguard that forestalls unapproved access to the common information. As of late, attribute based encryption (ABE) [8]–[10] has been pulled in much more considerations since it can keep data privacy and figure it out fine-grained, one-to-numerous, and non-intelligent get to control. Ciphertext-policy quality based encryption (CP-ABE) [11]– [21] is one of possible plans which has a great deal greater adaptability what's more, will be more appropriate for general applications [22], [23]. In cloud computing, as represented in Fig. 1, expert acknowledges the client enrolment and makes a few parameters. Cloud service provider (CSP) is the director of cloud servers and gives various administrations to customer. Information proprietor scrambles and transfers the created ciphertext to CSP. Client downloads and decrypts the interested ciphertext from CSP. The common records generally have various levelled structure. That is, a gathering of records are isolated into various progressive system subgroups situated at diverse get to levels. On

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

the off chance that the records in the same various levelled structure could be encoded by a coordinated get to structure, the capacity cost of ciphertext and time cost of encryption could be saved.

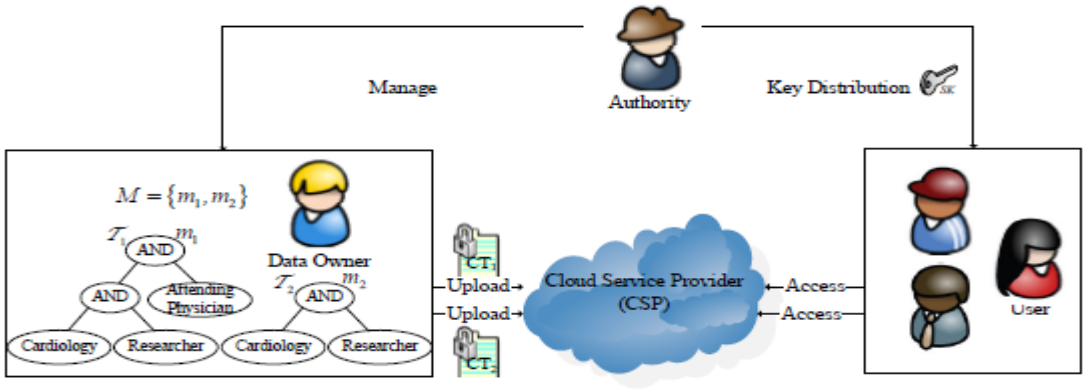


Fig. 1. An example of secure data sharing in cloud computing.

Organizations need to store enormous amount of data. Network storage providers are giving the resources for organizations on demand. The Cloud computing has emerged to provide many application services to fulfil the user's demand [1]. The user also be aware about hacking and leakage of information in the cloud. In the cloud data storage application, the cloud can store the user's data and share the data's because the cloud can provide the "pay as you go" environment [4]. The data owner needs to make a flexible and scalable access control policy to command users' access right, so that only the authorized users can access the cloud data [5, 6]. One of the most important security concerns in clouds is the data security and privacy, always the first requirement of every cloud user is to provide security along with data confidentiality and flexible access control.

The decryption keys are disclosed only to the authorized users. This method has some drawbacks. Efficient key method to issue the decryption keys is desired for this established method. This method does not support scalability and flexibility, because when the number of authorized users increase it is not efficient. So, to overcome these issues many schemes are introduced.

This project is including the modules that are uploading the files from the users also as well as they can download by using the secrete key. In existing system, there is no any restriction to users but this project. Retrieval result based on hierarchy by the cloud server according to some privileges criteria.

A. Problem Definition

To demonstrate the secured and efficient access to data from cloud by developing a web application. This application should allow the users to get registered with the cloud/service provider hosting the application. Usually Administrators and Data owners would have the privilege of storing/uploading data to the cloud. This application should provide privilege for a registered user to upload an encrypted file to the cloud. Users should also be able to download the files by using the secret key which is generated during the process of uploading the file.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

B. Scope and Objectives

1) **Scope**

The scope of the project is to develop the software for user who use cloud for storing data and retrieving the data. User should be able to store and retrieve the files (functionality for Uploading and Downloading). Establishing security of the shared files by using CP-ABE scheme with hierarchical
access and providing an efficient file sharing solution to the customers over the cloud.

2) Objectives

1. To provide secured way of storing data based on Ciphertext-Policy attribute-based encryption (CP-ABE) on the cloud server according to some privileges criteria having hierarchical access.
2. To give the result accurately and confidentially by using secret key while downloading the data from server.

II. LITERATURE SURVEY

In cloud computing, the data owner wants to share the data from the cloud in the sense owner encrypt the data then uploaded into the cloud storage. All the sensitive cloud data are encrypted to avoid the unauthorized user access of the cloud data. The different schemes exist that provide security, data confidentiality and access control. The encryption scheme provides security to the cloud data, and one of the schemes is attribute based encryption scheme. One of the encryption schemes is Attribute-Based Encryption (ABE) which is a new paradigm where such policies are specified and cryptographically enforced in the encryption algorithm itself. The existing ABE schemes are of two types. They are Key-Policy ABE (KP-ABE) scheme and Cipher Text-Policy ABE (CP-ABE) scheme. In KP-ABE scheme, attribute policies are associated with keys and data is associated with attributes. Only the keys associated with the policy that is satisfied by the attributes associating the data can decrypt the data. In CP-ABE schemes, attribute policies are associated with data and attributes are associated with keys and only those keys that the associated attributes satisfy the policy associated with the data are able to decrypt the data.

A. Attribute-based Encryption Scheme

Attribute-based encryption (ABE) is a vision of public key encryption that allows users to Encrypt and decrypt messages based on user attributes. Standard encryption is inefficient when selectively sharing data with many people, since the data needs to be encrypted using every User's public key. There are authority, sender and receiver in the ABE scheme, and authority's role is to generate keys for data sender and users to encrypt or decrypt data. In this scheme, the authority generates keys according to attributes; and these attributes of public key and master key, which are generated by the authority. All the attributes used in the potential and any data user who wants to add to this system, and owns to attributes don't include pre- defined attributes. The authorities will re-define attributes and generate a public key and master key again. Data sender's to encrypt data with a public key and a set of descriptive attributes. A data receiver to decrypt encrypted data with private key sent from the authority.

B. Key Policy Attribute Based Encryption

Key Policy Attribute Based Encryption scheme is a public key cryptography primitive that is for one-to-many communications. In this, data are associated with attributes for each of which a public key is defined. The one who encrypts the data, i.e., the encrypt associates the set of attributes to the data or message by encrypting it

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

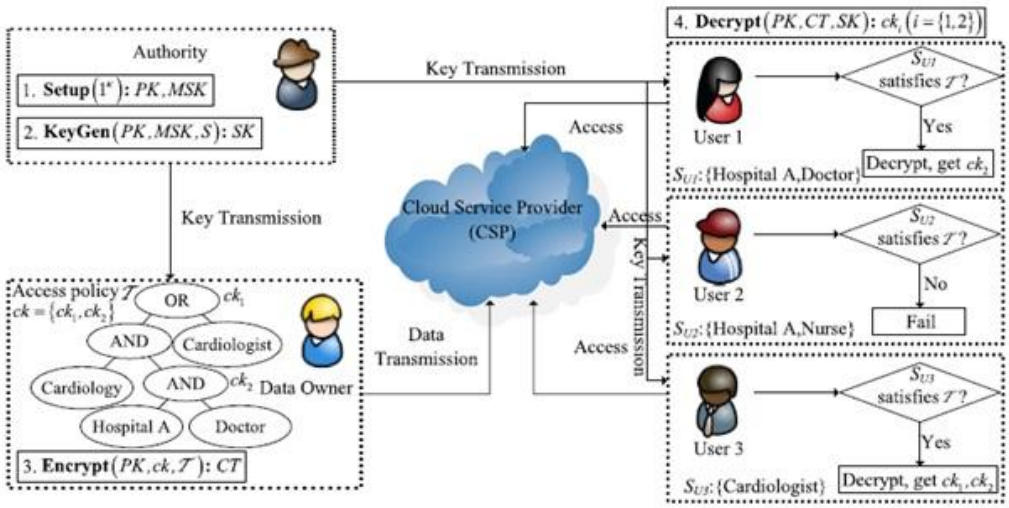
with a public key. Users are assigned with an access structure which is defined as an access tree over the data attributes. The nodes that are interior of the access tree [8].

Key-policy attribute-based encryption (KP-ABE) is an important class of ABE, where cipher texts are labelled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. KP-ABE has important applications in data sharing on un trusted cloud storage. However, the cipher text size grows linearly with the number of attributes embedded in cipher text in most existing KP-ABE schemes [24]. In cloud computing, an access control mechanism based on KP-ABE together with a re-encryption technique is used for efficient user revocation. This scheme enables a data owner to reduce most of the computational overhead to cloud servers. The use of this encryption scheme KP-ABE provides fine-grained access control. Each file or message is encrypted with a symmetric data encryption key (DEK), which is again encrypted by a public key corresponding to a set of attributes in KP-ABE, which is generated corresponding to an access structure.

D. Cipher Text Policy Attribute Based Encryption

Cipher text-policy attribute-based encryption can be viewed as a generalization of identity-based encryption. So as in identity-based encryption, there is a single public key, and there is a master private key that can be used to make more limited private keys. However, CP-ABE is much more flexible than plain identity-based encryption, in that it allows complex rules specifying which private keys can decrypt which cipher texts. in particular, the private keys are associated with sets of attributes or labels, and when we encrypt, we encrypt to an access policy which specifies which keys will be able to decrypt[10,11]. In cipher text-policy attribute-based encryption (CP-ABE), depends how attributes and policy are associated with cipher texts and users' decryption keys. In a CP-ABE scheme, a cipher text is associated with a monotonic tree access structure and a user's decryption key is associated with set of attributes. In this scheme, the roles of cipher texts and decryption keys are switched as that in KP-ABE) the cipher text is encrypted with a tree access policy chosen by an encryptor, while the decryption key is created with respect to a set of attribute. A highlight from this scheme is security to proven, including collusion resistance and generic group model. Implementation and performance made by Benchmarked on 64-bit AMD 3.7 GHZ workstation. Essentially on overhead beyond group operations in PBC library.

III. SYSTEM ARCHITECTURE



IV. EXISTING SYSTEM

Our existing solution applies cryptographic methods by disclosing data decryption keys only to authorize users. These solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine grained data access control is desired, and thus do not scale well.

V.DISADVANTAGES OF EXISTING SYSTEM

Software update/patches- could change security settings, assigning privileges too low, or even more alarmingly too high allowing access to your data by other parties.

Security concerns- Experts claim that their clouds are 100% secure - but it will not be their head on the block when things go awry. It's often stated that cloud computing security is better than most enterprises. Also, how do you decide which data to handle in the cloud and which to keep to internal systems once decided keeping it secure could well be a full-time task?

Control- Control of your data/system by third-party. Data - once in the cloudalways in the cloud! Can you be sure that once you delete data from your cloudaccount will it not exist any more... ...or will traces remain in the cloud

VI.PROPOSED SYSTEM

In order to achieve secure, scalable and fine-grained access control on outsourced data in the cloud, we utilize and uniquely combine the following three advanced cryptographic techniques:

- Key Policy Attribute-Based Encryption (KP-ABE).
- Proxy Re-Encryption (PRE)
- Lazy re-encryption

VII. ADVANTAGES OF PROPOSED SYSTEM

- Low initial capital investment
- Shorter start-up time for new services
- Lower maintenance and operation costs
- Higher utilization through virtualization
- Easier disaster recovery

More specifically, we associate each data file with a set of attributes, and assign each user an expressive access structure which is defined over these attributes. To enforce this kind of access control, we utilize KP-ABE to escort data encryption keys of data files. Such construction enables us to immediately enjoy fine-grainedness of access control. However, this construction, if deployed alone, would introduce heavy computation overhead and cumbersome online burden towards the data owner, as he is in charge of all the operations of data/user management. Specifically, such an issue is mainly caused by the operation of user revocation, which inevitably requires the data owner to re-encrypt all the data files accessible to the leaving user, or even needs the data owner to stay online to update secret keys for users. To resolve this challenging issue and make the construction

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

suitable for cloud computing, we uniquely combine PRE with KP-ABE and enable the data owner to delegate most of the computation intensive operations to Cloud Servers without disclosing the underlying file contents. Such a construction allows the data owner to control access of his data files with a minimal overhead in terms of computation effort and online time, and thus fits well into the cloud environment. Data confidentiality is also achieved since Cloud Servers are not able to learn the plaintext of any data file in our construction. For further reducing the computation overhead on Cloud Servers and thus saving the data owner's investment, we take advantage of the lazy re-encryption technique and allow Cloud Servers to "aggregate "computation tasks of multiple system operations. As we will discuss in section V-B, the computation complexity on Cloud Servers is either proportional to the number of system attributes, or linear to the size of the user access structure/tree, which is independent to the number of users in the system. Scalability is thus achieved. In addition, our construction also protects user access privilege information against Cloud Servers. Accountability of user secret key can also be achieved by using an enhanced scheme of KP-ABE.

VIII.CONCLUSION

In this paper, survey different attribute-based encryption schemes used in clouds. Many encryption schemes like KP-ABE, EKP-ABE, CP-ABE, ABE, ABE with NMAS, are discussed in which all the schemes are strong in efficient access control. Based on the discussion above, these schemes have properties: data are encrypted with its attributes and need to care about number of users. Each attribute has public key, secret key and random polynomial. Authorized attribute can access to decrypt the cloud data. These papers conclude a survey based on attribute based encryption schemes that provide security and performance changed at the maximum level.

REFERENCES

[1] M. Armbrust, A. Fox, R. Grith, A. D. Joseph,R. Katz, A. Konwinski, G. Lee, D. Patterson,A. Rabkin, I. Stoica,and M. Zaharia, "A view of cloud computing," Communications of the ACM,vol. 53, pp. 50-58, 2010.

[2] R.Ostrovsky, A. Sahai, and B.Waters, "Attribute-based encryption with non-monotonic access structures," in proccedings of the 14th ACM conference on computer and communications security, pp.195-203, 2007.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption,"in Proceedings of IEEE Symposium on Security and Privacy, pp. 321-334, 2007.

[4] M. D. Dikaiakos, D. Katsaros, P. Mehra, G. Pallis, and Athena Vakali,"Cloud computing: Distributed internet computing for it and scienti¯c research," IEEE Internet Computing, vol. 13, pp. 10-13, 2009.

[5] C. C. Chang, I. C. Lin, and C. T. Liao, "An access control system with time-constraint using support vector machines," International Journal of Network Security, vol. 2, no. 2, pp. 150-159, 2006.

[6] S.F.Tzeng, C.C.Lee, and T.C.Lin, "A novel key management scheme for dynamic access control in a hierarchy," international journal of Network security. Vol.12, no.3 pp.178-18-, 2011.

[7] A.Sahai and B.Waters, "Fuzzy identity based encryption," Advances in cryptology V EUROCRYPT, vol.3494 of LNCS, pp.457-473, 2005.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

[8] V. Goyal, O. Pandey, A. Sahai, and 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, pp. 89-98, 2006.

[9] R.Ostrovsky, A.Sahai, and B.Waters, "Attribute-based encryption with non-monotonic access structures," in procceding of the 14th ACM Conference on computer and communications security, pp.195-203, 2007.

[10] B.Waters,"Ciphertext-Policy attribute-based encryption" An expressive, efficient, and provably secure realization," public key cryptography V PKC, vol 6571 of LNCS, pp.53-70, 2011.

[11] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-policy attribute based encryption," *IEEE Symp. Security and Privacy*, Oakland, CA, 2007.

[12] M. Pirretti, P. Traynor, P. McDaniel and B. Waters, "Secure Atrribute-Based Systems", *ACM conference on Computer and Communications Security (ACM CCS),* 2006.

[13] A. Kapadia, P. Tsang and S. Smith, "Attribute-based publishing with hidden credentials and hidden policies", *NDSS*, 2007.

[14] Rakesh Bobba, Himanshu Khurana and Manoj Prabhakaran, "Attribute-Sets: A Practically Motivated Enhancement to Attribute-Based Encryption", July 27, 2009

[15] Nuttapong Attrapadung, Benoit Libert, and Elie de Panafieu, "Expressive Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts", *14th International Conference on Practice and Theory in Public Key Cryptogr hy,* Taormina, Italy, Marc

[16] M.S.Hwang and L.C.Lin, "Introduction to Information and Network security (4ed, in Chinese), " in Mc Graw Hill, in Taiwan, 2011.

[17] L.Ibraimi, M.Petkovic, S.Nikova, P.Hartel, and W.Jonker, "Mediated ciphertext-policy attribute based encryption and its application, "Information security Application, vol.5932 of LNCS, pp.309-323, 2009.

[18] S.Kamara and K.Lauter, "Cryptographic cloud storage," in proccedings of the 14th international conference of Financial cryptograpy and data security, pp.136-149,2010.

[19] Ramasamy S, Vahidhunnisha :" Survey on Multi Authority Attribute Based Encryption for Personal Health Record in Cloud Computing, ISSN: 2278-621X, November 2013.

[20] Q.Li, H.Xiong, F.Zhang and S.Zeng, "An expressive decentralizing KP-ABE scheme with content size cipher text," International journal of Network security, vol.15, no.3, pp.161-170, 2013.

Author Details

1. **BANDA RAJU** pursuing M.Tech(CSE)(15281D5807)(2015-2017)from Kamala Institute of Technology and Science, Singapuram, Huzarabad, Karimnagar, Telangana 505468, Affiliated to JNTUH, India.
2. **N.Raghu** working as Assistant Professor, Department of (CSE), from Kamala Institute of Technology and Science, Singapuram, Huzarabad, Karimnagar Telangana 505468, Affiliated to JNTUH, India.
3. **M.Sarika** working as Assistant Professor, Department of (CSE), from Kamala Institute of Technology and Science, Singapuram, Huzarabad, Karimnagar Telangana 505468, Affiliated to JNTUH, India.