Attribute-Based Encryption Scheme in Cloud Computing Using Efficient File Hierarchy

M. Spoorthika[1], B. Srinivasulu[2]
[1]*M.Tech(CSE),PG Scholar, Dept.of CSE, Gouthami Institute Of Technology & Management For Women,Peddasettipalli (V), Proddatur*
[2]*Assistant Professor, Dept.of CSE, Gouthami Institute Of Technology & Management For Women,Peddasettipalli (V), Proddatur*

***Abstract*- Cipher text-policy attribute-based encryption (CP-ABE) has been a preferred encryption technology to solve the challenging problem of secure data sharing in cloud computing. The shared data files generally have the characteristic of multilevel hierarchy, particularly in the area of healthcare and the military. However, the hierarchy structure of shared files has not been explored in CP-ABE. In this paper, an efficient file hierarchy attribute-based encryption scheme is proposed in cloud computing. The layered access structures are integrated into a single access structure, and then, the hierarchical files are encrypted with the integrated access Structure. The cipher text components related to attributes could be shared by the files. Therefore, both cipher text storage and time cost of encryption is saved. Moreover, the proposed scheme is proved to be secure under the standard assumption. Experimental simulation shows that the proposed scheme is highly efficient in terms of encryption and decryption. With the number of the files increasing, the advantages of our scheme become more and more conspicuous.**

***Index Terms*- Attribute-based encryption, cipher text policy, fine-grained access control, re-encryption**

I. INTRODUCTION

In cloud computing, to protect data from leaking, users need to encrypt their data before being shared. Access control [6], [7] is paramount as it is the first line of defense that prevents unauthorized access to the shared data. With the burgeoning of network technology and mobile terminal, online data sharing has become a new "pet", such as Facebook, MySpace, and Badoo. Meanwhile, cloud is one of the most promising application platforms to solve the explosive expanding of data sharing. In cloud computing, to protect data from leaking, users need to encrypt their data before being shared. Access control is paramount that prevents unauthorized access to the shared data. Recently, attribute-based encryption (ABE) has been attracted much more attentions since it can keep data privacy and realize fine-grained ,one-to-many n,and non interactive access control. Ciphertext-policy attribute based encryption (CPABE) is one of feasible schemes which has much more flexibility and is more suitable for general applications.

Cloud computing has rapidly become a widely adopted paradigm for delivering services over the internet. Therefore cloud service provider must provide the trust and security, as there is valuable and sensitive data in large amount stored on the clouds. For protecting the confidentiality of the stored data, the data must be encrypted before uploading to the cloud by using some cryptographic algorithms. In this paper we going to discuss about attribute based encryption scheme and its categories.

Sahai and Waters proposed Fuzzy Identity-Based Encryption [9] in 2005, and this paper proposed the first concept of the attribute-based encryption scheme through public key cryptography. Fuzzy Identity-Based Encryption in which identities as a set of descriptive attributes. Fuzzy IBE can be used for an application that we call attribute based encryption.In this scheme in which each user is identified by a set of attributes, and some function of this attributes is used to determine decryption ability for each ciphertext. M. Pirretti, P. Traynor, P. McDaniel, and B. Waters proposed Secure attribute-based systems [6]in2006. This paper gave an implementation of the ABE encryption system with more complex access policy with (AND, OR gate) based on [9]. This work also demonstrated different applications of attribute-

based encryption schemes and addressed several practical notions such as key-revocation and optimization. However, this work is dismissed after the proposal of KP- ABE and CP-ABE, which is more flexible and efficient. In 2006, Goyal et al. proposed an key-policy attribute-based encryption (KP-ABE) scheme [3]. Fine grained access control provided by KP-ABE as compared with classical model.In 2007 Bethencourt et al. proposed an ciphertext- policy attribute based (CP-ABE) scheme [1]. Data owner only trusts the key issuer as CP-ABE scheme addresses the problem of KP-ABE. Both KP-ABE and CP-ABE are able to enforce general access policies that can be described by a monotone access structure. Moreover, Muller proposed an distributedattribute-based encryption scheme in 2008; Yu e. proposed a finegrained data access control encryption scheme ; Tang proposed a Verifiable attribute based encryption scheme . Ostrovsky et al. proposed an enhanced ABE scheme which supports non-monotone access structures[8]. In 2008 Muller et al. proposed an distributed attribute-based encryption scheme [5] . Wang et al. pro- posed a hierarchical attribute-based encryption scheme(HABE) [10] in 2010. which integrates properties in both a HIBE (hierarchiel identity based encryption) model and a CP-ABE model. There after introduceMA-ABE(multi-authorities ABE)schemes [2] that use multiple parties to distribute attributes for users.Attribute-based encryptionschemes can be further categorized as either monotonic or non-monotonic besed on there type of acess structure.

II. LITERATURER SURVEY

1) A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing

AUTHORS: K. Liang et al

In this paper, for the first time, we define a general notion for proxy re-encryption (PRE), which we call deterministic finite automata-based functional PRE (DFA-based FPRE). Meanwhile, we propose the first and concrete DFA-based FPRE system, which adapts to our new notion. In our scheme, a message is encrypted in a ciphertext associated with an arbitrary length index string, and a decryptor is legitimate if and only if a DFA associated with his/her secret key accepts the string. Furthermore, the above encryption is allowed to be transformed to another ciphertext associated with a new string by a semitrusted proxy to whom a re-encryption key is given. Nevertheless, the proxy cannot gain access to the underlying plaintext. This new primitive can increase the flexibility of users to delegate their decryption rights to others. We also prove it as fully chosen-ciphertext secure in the stanard model.

2) Fine-grained twofactor access control for Web-based cloud computing services

AUTHORS: J. K. Liu, M. H. Au, X. Huang, R. Lu, and J. Li

In this paper, we introduce a new fine-grained two-factor authentication (2FA) access control system for web-based cloud computing services. Specifically, in our proposed 2FA access control system, an attribute-based access control mechanism is implemented with the necessity of both a user secret key and a lightweight security device. As a user cannot access the system if they do not hold both, the mechanism can enhance the security of the system, especially in those scenarios where many users share the same computer for web-based cloud services. In addition, attribute-based control in the system also enables the cloud server to restrict the access to those users with the same set of attributes while preserving user privacy, i.e., the cloud server only knows that the user fulfills the required predicate, but has no idea on the exact identity of the user. Finally, we also carry out a simulation to demonstrate the practicability of our proposed 2FA system.

3) Ciphertext-policy attributebased encryption

AUTHORS: J. Bethencourt, A. Sahai, and B. Waters

In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous AttributeBased

Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe auser's credentials, and a party encrypting data determinesa policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, we provide an implementation of our system and give performance measurements.

4) Arbitrary-state attributebased encryption with dynamic membership

AUTHORS: C.-I. Fan, V. S.-M. Huang, and H.-M. Ruan

Attribute-based encryption (ABE) is an advanced encryption technology where the privacy of receivers is protected by a set of attributes. An encryptor can ensure that only the receivers who match the restrictions on predefined attribute values associated with the ciphertext can decrypt the ciphertext. However, maintaining the correctness of all users' attributes will take huge cost because it is necessary to renew the users' private keys whenever a user joins, leaves the group, or updates the value of any of her/his attributes. Since user joining, leaving, and attribute updating may occur frequently in real situations, membership management will become a quite important issue in an ABE system. In this paper, we will present an ABE scheme which is the first ABE scheme that aims at dynamic membership management with arbitrary states, not binary states only, for every attribute. Our work also keeps high flexibility of the constraints on attributes and makes users be able to dynamically join, leave, and update their attributes. It is unnecessary for those users who do not change their attribute statuses to renew their private keys when some user updates the values of her/his attributes. Finally, we also formally prove the security of the proposed scheme without using random oracles.

5) HASBE: A hierarchical attributebased solution for flexible and scalable access control in cloud computing.

AUTHORS: Z. Wan, J. Liu, and R. H. Deng

Cloud computing has emerged as one of the most influential paradigms in the IT industry in recent years. Since this new computing technology requires users to entrust their valuable data to cloud providers, there have been increasing security and privacy concerns on outsourced data. Several schemes employing attribute-based encryption (ABE) have been proposed for access control of outsourced data in cloud computing; however, most of them suffer from inflexibility in implementing complex access control policies. In order to realize scalable, flexible, and fine-grained access control of outsourced data in cloud computing, in this paper, we propose hierarchical attribute-set-based encryption (HASBE) by extending ciphertext-policy attribute-set-based encryption (ASBE) with a hierarchical structure of users. The proposed scheme not only achieves scalability due to its hierarchical structure, but also inherits flexibility and fine-grained access control in supporting compound attributes of ASBE. In addition, HASBE employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes. We formally prove the security of HASBE based on security of the ciphertext-policy attribute-based encryption (CP-ABE) scheme by Bethencourt and analyze its performance and computational complexity. We implement our scheme and show that it is both efficient and flexible in dealing with access control for outsourced data in cloud computing with comprehensive experiments.

III. EXISTING SYSTEM

- Sahai and Waters proposed fuzzy Identity-Based Encryption (IBE) in 2005, which was the prototype of ABE. Latterly, a variant of ABE named CP-ABE was proposed.
- Since Gentry and Silverberg proposed the first notion of hierarchical encryption scheme, many hierarchical CP-ABE schemes have been proposed. For example, Wang et al. proposed a hierarchical ABE scheme by combining the hierarchical IBE and CP-ABE.
- Wan et al. proposed hierarchical ABE scheme. Later, Zou gave a hierarchical ABE scheme, while the length of secret key is linear with the order of the attribute set. A ciphertextpolicy hierarchical ABE scheme with short ciphertext is also studied.
- In these schemes, the parent authorization domain governs its child authorization domains and a top-level authorization domain creates secret key of the next-level domain. The work of

key creation is distributed on multiple authorization domains and the burden of key authority center is lightened.

DISADVANTAGES OF EXISTING SYSTEM:

- In Existing System time and cost for encryption is high.
- No any special multiple hierarchical files are used.
- Decryption system time and computation cost are very high.

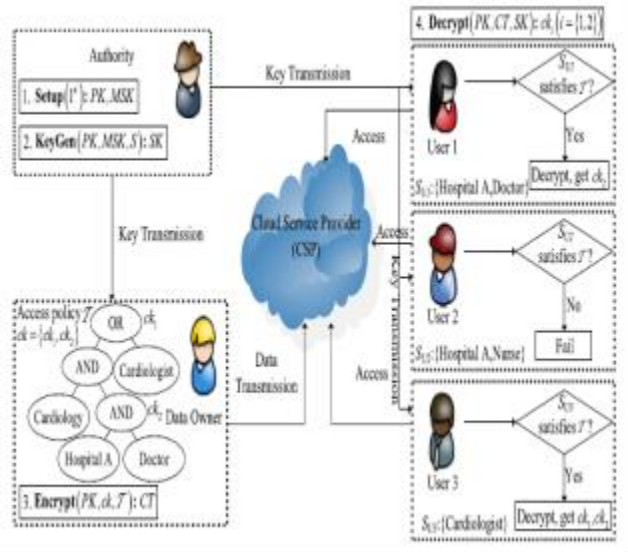
IV PROPOSED SYSTEM

Issues such as scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control.For improving the limitations of the above technique we propose a new sheme Categorical Heuristics on Attribute- based Encryption (CHAE). . Category based on heuristic scheme describes a message and a predicate over the universe of attributes. A attributes satisfy the predicate, endorsed the message.

- In this study, an efficient encryption scheme based on layered model of the access structure is proposed in cloud computing, which is named file hierarchy CP-ABE scheme (or FH-CP-ABE, for short). FH-CP-ABE extends typical CP-ABE with a hierarchical structure of access policy, so as to achieve simple, flexible and fine-grained access control.
- The contributions of our scheme are three aspects.
- Firstly, we propose the layered model of access structure to solve the problem of multiple hierarchical files sharing. The files are encrypted with one integrated access structure.
- Secondly, we also formally prove the security of FH-CP-ABE scheme that can successfully resist chosen plaintext attacks (CPA) under the Decisional Bilinear Diffie-Hellman (DBDH) assumption.
- Thirdly, we conduct and implement comprehensive experiment for FH-CP-ABE scheme, and the simulation results show that FH-CP-ABE has low storage cost and computation complexity in terms of encryption and decryption.

ADVANTAGES OF PROPOSED SYSTEM:

- CP-ABE feasible schemes which has much more flexibility and is more suitable for general applications
- Multiple hierarchical files sharing are resolved using layered model of access structure.
- In proposed system both ciphertext storage and time cost of encryption are saved.
- The proposed scheme has an advantage that users can decrypt all authorization files by computing secret key once. Thus, the time cost of decryption is also saved if the user needs to decrypt multiple files.
- The computation cost of decryption can also be reduced if users need to decrypt multiple files at the same time.



System Architecture

V. METHODOLOGY

Data owner Module:

In the first module, we develop the Data Owner Module. Owner Will Signup and Wait for the approval Key of admin. After Getting key Owner can login using the key, and upload any records related to users medical Information on the cloud.

In this module, data owner will check the progress status of the file upload by him/her. It has large data needed to be stored and shared in cloud system. In our scheme, the entity is in charge of defining access structure and executing Encrypt operation. And it

uploads ciphertext to CSP. After the completion, owner logout the session

User and Physician Module:
In this module, we develop the User Module. User Will registries and login on the user's page. We develop the module, such that, the User will search for his/her medical records by given user medical record id on the page. User will get search results of the medical records related to the id and he/she will request admin to access the document which is encrypted one by the admin. After Getting decrypt key from the admin, he/she can access to the medical records. User logouts the session. It wants to access a large number of data in cloud system. The entity first downloads the corresponding ciphertext. Then it executes Decrypt operation of the proposed scheme.

Cloud Service Provider (CSP)
It is a semi-trusted entity in cloud system. It can honestly perform the assigned tasks and return correct results. However, it would like to find out as much sensitive contents as possible. In the proposed system, it provides ciphertext storage and transmission services. In this module, we also develop admin module process. Admin Will Login on the admin's page. He/she will check the pending requests of any of the above person. After accepting the request from the above person, he/she will generate master key for encrypt and Secret key for decrypt.

Authority Module:
It is a completely trusted entity and accepts the user enrollment in cloud computing. And it can also execute Setup and KeyGen operations of the proposed scheme. The Researcher will registries and login on the researcher's page. Researcher will search for any medical records by the disease category (i.e Cancer, Hernia..etc..). Researcher will Request for decrypt key to the admin. After getting the key from admin, researcher will access to the medical records of patient without their personal details. After the process, Researcher logouts the session.

File hierarchy System:
The large number of classes in the Java IO package is overwhelming and annoying. However, if we use Java, we still need to understand those classes. In fact, the classes in Java IO package is not very complex, but we need a good way to learn those. There are two important factors for understanding the classes:
1). Java io class hierarchy diagram
2). Decorator pattern

VI.CONCLUSION

In this paper, we analyse different attribute-based encryption schemes: ABE, KP-ABE, CP-ABE, ABE with non-monotonic access structure, HABE and MA-ABE .The main access polices are KP-ABE and CP-ABE, further schemes are obtained based on these policies. Based on their type of access structure the schemes are categorized as either monotonic or non-monotonic. CHABE an adaptation of Attribute Based Encryption (ABE) for the purposes of providing guarantees towards the provenance the sensitive data, and moreover towards the anonymity of the data owner. Our scheme also enables dynamic modification of access policies o supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios.

REFERENCES

[1] J. Bettencourt, A. Sahai, and B.Waters"Ciphertext-policy attribute based encryption "in Proceedings of IEEE Symposium on Security and Privacy, pp. 321V334, 2007.
[2] V Bozovic, D Socek, R Steinwandt, and V. I. Vil-lanyi, "Multi- authority attribute-based encryption with honest-but-curious central authority" International Journal of Computer Mathematics, vol. 89,pp. 3, 2012.
[3] 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}
[4] Q. Liu, G. Wang, and J. Wu, "Time based proxy re-encryption scheme for secure data sharing in a cloud environment," Information Sciences .In Press, 2012.
[5] Muller, S. Katzenbeisser, and C.Eckert, "Distributed attribute-based encryption," in Proceedings of ICISC, pp. 20{36, 2008.

[6] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. “Secure attribute-based systems”. In Proceedings of the 13th ACM conference on Computer and communications security, pages 99{112. ACM Press New York, NY, USA, 2006.

[7] Rakesh Bobba, Himanshu Khurana and Manoj Prabhakaran, “AttributeSets: A Practically Motivated Enhancement to Attribute-Based Encryption”, July 27, 2009

[8] R. Ostrovsky and B. Waters. “Attribute based encryption with non- monotonic access structures”.In Proceedings of the 14th ACM conference on Computer and communications security, pages 195{203. ACM New York, NY, USA,2007.

[9] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” inProc.EUROCRYPT, 2005, pp. 457473

[10] G. Wang, Q. Liu, and J.Wu,”Hierachical attibute- based encryption for fine-grained access control in cloud storage services," in Proceedings of the 17th ACM conference on Computer and communications security.