**An Efficient File Hierarchy Attribute-BasedEncryption Scheme in Cloud Computing**

**ABSTRACT:**

Ciphertext-policy attribute-based encryption(CP-ABE) has been a preferred encryption technology tosolve the challenging problem of secure data sharing incloud computing. The shared data files generally have thecharacteristic of multilevel hierarchy, particularly in the area ofhealthcare and the military. However, the hierarchy structureof shared files has not been explored in CP-ABE. In this paper,an efficient file hierarchy attribute-based encryption schemeis proposed in cloud computing. The layered access structuresare integrated into a single access structure, and then, thehierarchical files are encrypted with the integrated accessstructure. The ciphertext components related to attributes couldbe shared by the files. Therefore, both ciphertext storage andtime cost of encryption are saved. Moreover, the proposedscheme is proved to be secure under the standard assumption.Experimental simulation shows that the proposed scheme ishighly efficient in terms of encryption and decryption. With thenumber of the files increasing, the advantages of our schemebecome more and more conspicuous.

**EXISTING SYSTEM:**

* Sahai and Waters proposed fuzzy Identity-BasedEncryption (IBE) in 2005, which was the prototype ofABE. Latterly, a variant of ABE named CP-ABEwas proposed.
* Since Gentry and Silverberg proposed the firstnotion of hierarchical encryption scheme, many hierarchicalCP-ABE schemes have been proposed. For example,Wang *et al.* proposed a hierarchical ABE scheme by combiningthe hierarchical IBE and CP-ABE.
* Wan *et al.* proposed hierarchical ABE scheme. Later, Zou gave ahierarchical ABE scheme, while the length of secret keyis linear with the order of the attribute set. A ciphertextpolicyhierarchical ABE scheme with short ciphertext is also studied.
* In these schemes, the parent authorizationdomain governs its child authorization domains and a top-levelauthorization domain creates secret key of the next-leveldomain. The work of key creation is distributed on multipleauthorization domains and the burden of key authority centeris 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.

**PROPOSED SYSTEM:**

* In this study, an efficient encryption scheme based onlayered model of the access structure is proposed in cloudcomputing, which is named file hierarchy CP-ABEscheme(or FH-CP-ABE, for short). FH-CP-ABE extends typicalCP-ABEwith a hierarchical structure of access policy, soas 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 structureto solve the problem of multiple hierarchical files sharing.The files are encrypted with one integrated accessstructure.
* Secondly, we also formally prove the security ofFH-CP-ABE scheme that can successfully resist chosenplaintext attacks (CPA) under the Decisional BilinearDiffie-Hellman (DBDH) assumption.
* Thirdly, we conduct and implement comprehensive experimentfor FH-CP-ABE scheme, and the simulation results show that FH-CP-ABE has low storage cost and computationcomplexity 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 storageand time cost of encryption are saved.
* The proposed schemehas an advantage that users can decrypt all authorizationfiles by computing secret key once. Thus, the time cost ofdecryption is also saved if the user needs to decrypt multiplefiles.
* The computation cost of decryption can also be reduced ifusers need to decrypt multiple files at the same time.

**SYSTEM ARCHITECTURE:**



**MODULES:**

* Data owner Module
* User and Physician Module
* Cloud Service Provider (CSP)
* Authority Module
* File hierarchy System

**MODULES DESCRIPTION:**

**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 medicalInformation 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 PhysicianModule:**

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 idand he/she will request admintoaccess 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 andSecret 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

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium Dual Core.
* Hard Disk : 120 GB.
* Monitor : 15’’LED
* Input Devices : Keyboard, Mouse
* Ram : 1GB.

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows 7.
* Coding Language : JAVA/J2EE
* Tool : Netbeans 7.2.1
* Database : MYSQL

**REFERENCE:**

Shulan Wang, Junwei Zhou, *Member, IEEE*, Joseph K. Liu, *Member, IEEE*,Jianping Yu, Jianyong Chen, and WeixinXie, “An Efficient File Hierarchy Attribute-BasedEncryption Scheme in Cloud Computing”, **IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 6, JUNE 2016.**