ISSN: 2096-3246
Volume 55, Issue 02, April, 2023

https://doi.org/10.5281/zenodo.12707458

# Effective File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing

**EDIGA KISHORE KUMAR GOWD,VIJAYA BHASKAR MADGULA,KUMMARA RANGA SWAMY**

**Assistant Professor[1,2,3],**

KISHORE_EDIGA@GMAIL.COM, vijaya.bhaskar2010@gmail.com, rangaswamy.kumara@gmail.com

department of CSE, Sri Venkateswara Institute of Technology,

N.H 44, Hampapuram, Rapthadu, Anantapuramu, Andhra Pradesh 515722

**Keywords:**

**ABSTRACT**

To manage the exponential growth of shared data, cloud computing has emerged as a top contender among application platforms. Users should encrypt their data before sharing it in order to keep it safe on the cloud. By using the cloud, customers with limited computer capabilities may access massive amounts of processing power, bandwidth, storage, and even relevant software that can be shared on an as-needed basis, all while paying for what they really need. As the first barrier against unauthorised access to shared information, access management is of the utmost importance. On the one hand, sensitive data includes outsourced computation tasks, which may contain things like business financial records, private research data, and personally identifiable health information. Encrypting sensitive data before outsourcing it is essential for preventing illicit data leaks and assuring end-to-end security. guarantee the security of data stored online and elsewhere. Important exposure that was present in earlier studies but went overlooked poses a risk to clients. Additionally, the enormous client decryption cost severely restricts ABE's practical adoption. The proposed Cooperation Mechanism not only fixes the key exposure problem, but it also handles the key escrow issue. Meanwhile, it greatly decreases the overhead associated with client decryption. Computation on encrypted data is made more difficult by the fact that cloud cannot execute any meaningful operations on the underlying cypher text-policy using ordinary data encryption techniques. The proposed method not only accomplishes scalability, but also has a hierarchical structure

ISSN: 2096-3246
Volume 55, Issue 02, April, 2023
https://doi.org/10.5281/zenodo.12707458

# Introduction

Cloud computing, which is a kind of web-based service-oriented computing, offers a platform for the distribution of data and applications via the Internet. administration in a manner that was previously only accessible in product form. An interconnected system of computers, sometimes referred to as the "cloud," makes these services accessible via portable electronic devices like laptops.

**Overview Cloud**

Computing is use of hardware and software to deliver service over network (typically the Internet). An example of Cloud Computing provider is Google's Gmail. Gmail users can access files and applications hosted by Google via the internet from any device. Cloud Computing is to protect data from leaking, users need to encrypt their data before shared. Cloud computing poses privacy concerns because service provider can access the data that is in the cloud at any time. It could accidentally or deliberately alter or even delete information. Many cloud providers can share information with third parties if necessary for purposes of law and order even without warrant. That is permitted in their privacy policies, which users must agree to before they start using cloud services. Solutions to privacy include policy and legislation as well as end users' choices for how data is stored. Users can encrypt data that is processed or stored within cloud to prevent unauthorized access[1]. Role based authentication isintegration of public key cryptography with symmetric key cryptography, whereby data, public key, group key, and policy are required for each encryption operation. The term "policy" refers to a set of rules that can be specified in a variety of ways, including as a chain. For instance, in a hospital setting, the policy could be written as "{doctor, patient}", meaning that anyone from the group of doctors or patients could decrypt the document at the same time.In such circumstances, patients cannot access the encrypted document until their physicians have done so. In a business environment, where various departments and employees need varying degrees of access control and privacy settings, policy-based encryption is quickly gaining popularity. Our proposed system will provide various levels of encryption, decryption, authentication, authorization, and privacy settings for doctors, administrators, and patients in an enterprise hospital context deployed in a local cloud with a fog computing architecture.In order to identify anomalies in medical images, we suggest using a system based on machine learning. Here, we show how to employ CP-ABE in a machine learning framework and with human beings. the whole task showcase all of medical scanning in an enterprise hospital application both plain record encryption and image encryption with the help of CP-ABE..

## **1.** LITERATURE SURVEY

The literature survey that containing study of different schemes available in Attribute Based encryption(ABE). An efficient file hierarchy attribute-based encryption scheme (FH-CP-ABE) is proposed by Shulan Wang, JunweiZhou, Joseph K. Liu, Jianping Yu, Jianyong Chen and WeixinXie. The layered

ISSN: 2096-3246
Volume 55, Issue 02, April, 2023
https://doi.org/10.5281/zenodo.12707458

access structures are integrated into 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 costs of encryption are saved. Moreover, the proposed scheme is proved to be secure under the standard assumption. 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 CPABE with a hierarchical structure of access policy, so as to achieve simple, flexible and fine-grained access control.

### 1.1 Attribute Based Encryption

Introduced in 2005 by Sahai and Waters, this attribute-based encryption technique aims to offer security and access management. Users may encrypt and decrypt data based on user characteristics using attribute-based encryption (ABE), which is public key based one-to-many encryption. Where factors (such as the user's country of residence or the kind of subscription she has) determine the cypher text that is used as a secret key. In this kind of system, decryption of cypher text is contingent upon the user key matching the cypher text's properties. Number matching must be at least the threshold value d in order for decryption to be feasible. One of the most important security features of Attribute-Based Encryption is its resilience to collusion [3]-[5]. Even if an enemy has several keys, data should remain inaccessible until at least one of those keys gives access. One issue with attribute based encryption (ABE) schemes is that data owners are required to encrypt data using the public keys of all authorised users. Since this technique controls user access to the system by using monotonic features, its practical usefulness is limited.2.2 Major Guideline Encryption Based on Attributes

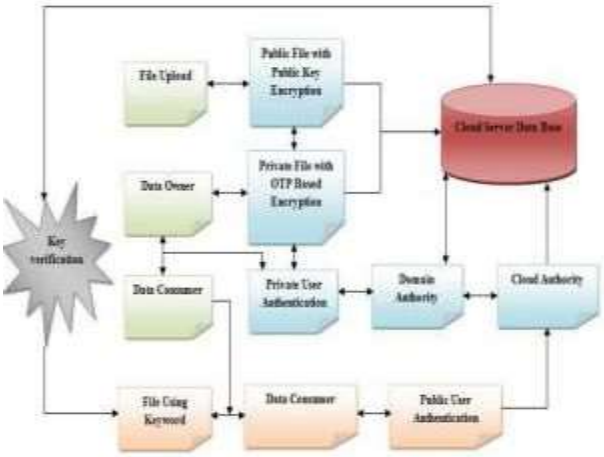
The traditional model of ABE has been changed in this way. An access tree structure is used to grant users permissions on data properties. The cutoff In an access tree, gates serve as nodes. Leaf nodes link the qualities. The specified user secret key reflects the access tree structure. A user's ability to decode certain cypher texts is controlled by their private key and the monotonic access structures that are attached with the cypher texts' labels. The KP-ABE scheme[6] is specifically tailored for one-to-many communications.

SCOPE

We provide privacy secure in public social cloud computing. In our project we implement hierarchical attribute base security hierarchy are Cloud authority, Domain authority and users. Cloud authority can only have privilege to create or remove the domain(private cloud authority) in cloud and they can maintain all details in overall cloud Domain authority can create or remove users inside domain this users are called private users . Users are two types private cloud user public cloud user’s Private cloud users are depends domain Public users under cloud authority

SYSTEM ARCHITECTURE

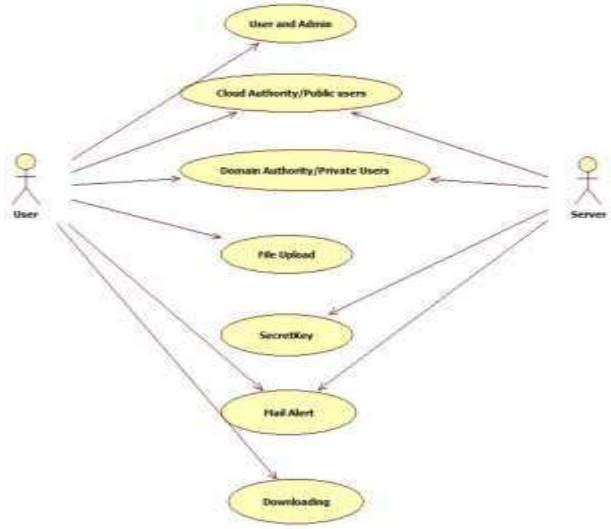
ISSN: 2096-3246
Volume 55, Issue 02, April, 2023
https://doi.org/10.5281/zenodo.12707458




## **4.1** UML DIAGRAM

### UML DIAGRAM USE CASE DIAGRAM

A use case illustrates unit of functionality provided by the system. The main purpose use-case diagram is to help development teams visualize functional requirements system, including relationship of "actors" (human beings who will interact with system) to essential processes, as well as relationships among different use cases. The use case has two actors: user and server. User gives image as input and server performs the operation



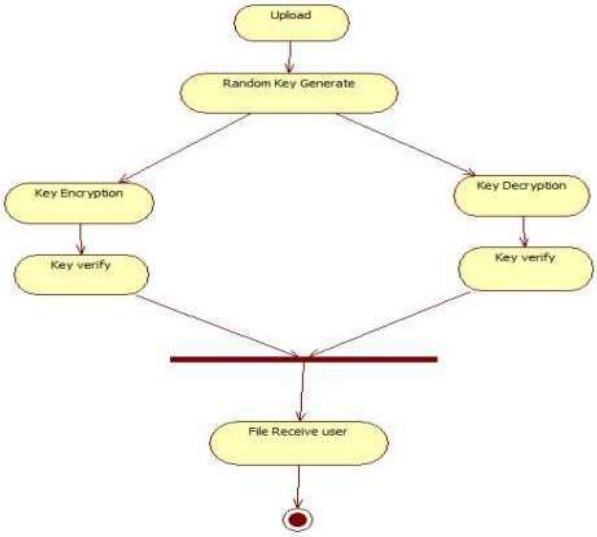

## **4.2** ACTIVITY DIAGRAM

Activity diagrams are graphical representations of workflows stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modelling Language, activity diagrams are intended

ISSN: 2096-3246
Volume 55, Issue 02, April, 2023
https://doi.org/10.5281/zenodo.12707458

to model both computational and organizational processes (i.e. workflows). Activity diagrams show the overall flow of control. Activity diagrams are constructed from limited number of shapes, connected with arrows. The most important shape types:

- Rounded rectangles represent actions
- Diamonds represent decisions;
- Bars represent start (split) or end (join) of concurrent activities;A black circle represents start (initial state) workflow; An encircled black circle represents end (final state)

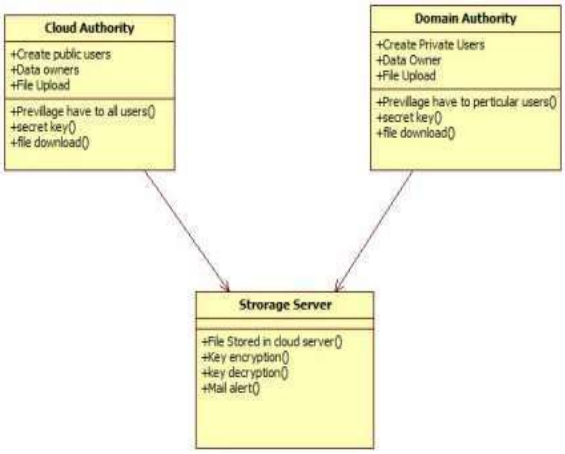



## **4.3** CLASS DIAGRAM

The class diagram shows how different entities (people, things, and data) relate to each other in other words, it shows static structures system. A class diagram can be used to display logical classes. Class diagrams can also be used to show implementation classes, which are the things that programmers typically deal with. A class is depicted on class diagram as rectangle with three horizontal sections, as shown in above figure. The upper section shows class's name; middle section contains class's attributes; and lower section contains class's operations (or "methods"). The

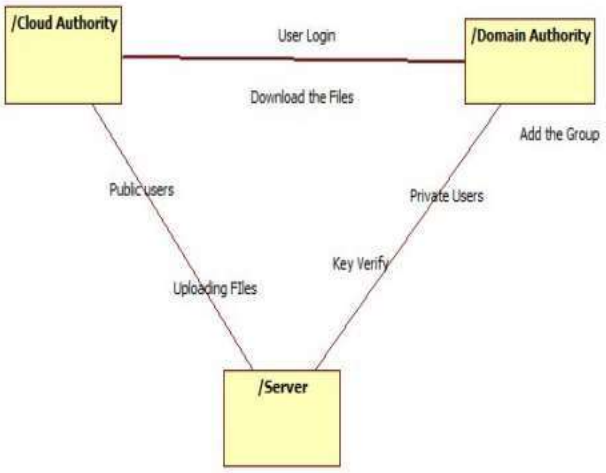
diagram has five main classes which give attributes and operations used in each class.

ISSN: 2096-3246
Volume 55, Issue 02, April, 2023
https://doi.org/10.5281/zenodo.12707458




## **4.4** COLLABORATION DIAGRAM

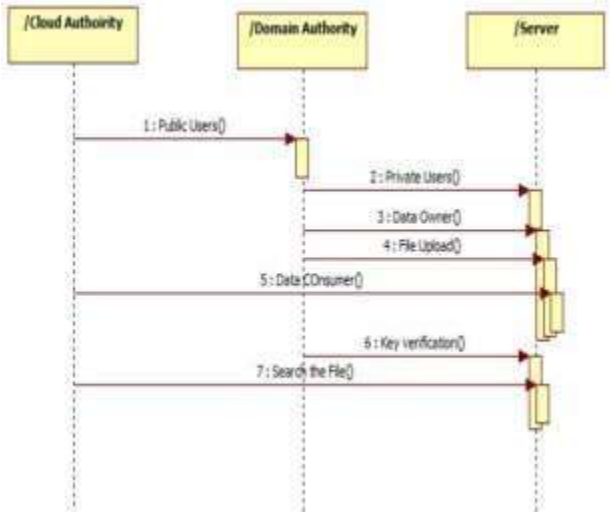
Collaboration diagrams are technique for defining external object behavior. They include same information as Sequence Diagrams (or message trace diagrams) but are better able to show asynchronous message passing. Collaboration diagrams show how objects collaborate by representing objects by icons and their message passing as labeled arrows.




## **4.5** SEQUENCE DIAGRAM

A sequence diagram is an interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. A sequence diagram shows object interactions arranged in time sequence. It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario. Sequence diagrams are typically associated with use case realizations in the Logical View of the system under development. Sequence diagrams are sometimes called event diagrams, event scenarios.

ISSN: 2096-3246
Volume 55, Issue 02, April, 2023
https://doi.org/10.5281/zenodo.12707458




## 5. DATA FLOW DIAGRAM

**Data Flow Diagram / Use Case Diagram / Flow Diagram:**

- The DFD is also called as bubble chart. Itϖ is simple graphical formalism that can be used to represent system in terms input data to system, various processing carried out on these data, and output data is generated by system
- The data flow diagram (DFD) is one most important modeling tools. It is used to model system components. These components are system process, data used by process, an external entity that interacts with system and information flows in system.
- DFD shows how information movesϖ through system and how itis modified by series transformations. It is graphical technique that depicts information flow and transformations that are applied as data moves from input to output.
- DFD is also known as bubble chart. A DFDϖ may be used to represent system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

**System Implementation Modules**

- Data Owner
- Data Consumer
- Domain level Security
- Attribute based security

ISSN: 2096-3246
Volume 55, Issue 02, April, 2023
https://doi.org/10.5281/zenodo.12707458

- Secret file accessing

## 6. MODULES DESCRIPTION

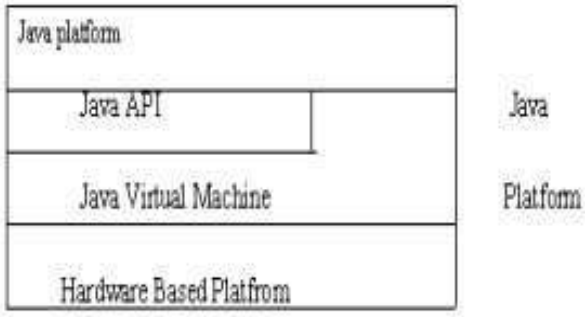
**Data Owner**

The data owner uploads their data to the cloud server in this module. The data owner encrypts the files before storing them in the cloud to ensure their protection. Data files may have their expiry times changed by the data owner. The owner of the data may be able to decrypt the file. The data owner has the power to grant or deny access to the file with encrypted contents. Data owner to use cloud servers for the majority of computing tasks. Elegantly granular access control is provided by KP-ABE. A public key that corresponds to a set of characteristics in KP-ABE is produced according to an access structure and then used to encrypt each file using a symmetric data encryption key (). A file containing encrypted data is kept.With the necessary characteristics and the encrypted. The user may decode the encrypted, which is used to decrypt the file, if the linked properties of a cloud-stored file match the access structure of their key. For the purpose of sharing it with data consumers, data owners encrypt their data files before storing them on the cloud. Data consumers must first decode the encrypted data files they want to access from the cloud before they can access the shared data. Domain authorities oversee the operations of each data owner and consumer. The parent domain authority, often known as the trusted authority, oversees a domain authority. A hierarchical structure is used to organise data owners, data consumers, domain authorities, and the trusted authority.

**Data Consumer:**

With the encrypted key, the user can only access the data file if they have the permission to do so. Domain authority is the only entity that may grant permissions at the user level, and only domain authority has access over datausers. Malicious users may conspire to gain sensitive files outside their rights, since users might attempt to access data files either inside or outside of their scope of access. Before storing their data files on the cloud, data owners encrypt them so that data consumers may access and use them. Data consumers access the shared data files by downloading encrypted files from the cloud and decrypting them. Domain authority oversees all data owners and consumers. The parent domain authority or trusted authority oversees a domain authority. Following a hierarchical structure, we have data consumers, domain authorities, trusted authority, and data owners. People who use data will be online at all times. Unlike the cloud provider, trusted authority, and domain authorities, who are constantly online, they come online only when absolutely essential. Presumably, there is a lot of space for data and processing power on the cloud. Furthermore, we assume that data consumers have read-only access to data files. Customers may access their data stored in the cloud and navigate its hierarchical structure by creating an account and logging in. APIs are structured like departmental libraries, with relevant components packaged together. A Java programme, such an applet or application, is shown in the accompanying figure. Figure: Java programme is protected from hardware requirements by Java API and Virtual Machine.

ISSN: 2096-3246
Volume 55, Issue 02, April, 2023
https://doi.org/10.5281/zenodo.12707458




**JAVA Platform**

As platform-independent environment, Java can be bit slower than native code. However, smart compliers, wheel-tuned interpreters, and just in time byte compilers can bring Java's performance close to that of native code without threatening portability.

## **6.** CONCLUSION

Two schemes, Anony Control (which is semi-anonymous) and Anony Control-F (which is totally anonymous), are available to deal with the issue of user privacy on cloud storage servers. Our suggested systems provide both fine-grained privilege management and identity anonymity in the context of cloud computing by using numerous authorities to regulate access depending on users' identity information. Especially in a cloud computing environment that relies on the Internet, our system's ability to withstand up to N − 2 authority breach is very desirable.

## FUTURE ENHANCEMENTS

Future enhancement this project is following schemes. A unified scheme for resource protection in automated trust negotiation. Automated trust negotiation using cryptographic credentials

## **7.** REFERENCES

[1]In "A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing," published in the October 2014 issue of the IEEE Transactions on Information Forensics and Security, the authors are K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, T. V. X. Phuong, and Q. Xie. This sentence is paraphrased from an article published in the September 2015 issue of the IEEE Transactions on Computers, which is titled "ktimes attribute based anonymous access control for cloud computing." The authors of the article are T. H. Yuen, J. K. Liu, M. H. Au, X. Huang, W. Susilo, and J. Zhou.

The paper "CP-ABE with constant-size keys for light weight devices" was published in May 2014 in the IEEE Transactions on Information Forensics and Security and was co-authored by F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan.

In August 2014, C. Fan, S. Huang, and H. Rung published an article titled "Arbitrary state attribute based encryption with dynamic membership" in the IEEE Transactions on Computers, volume 63, issue 8, pages 1951–1961.

ISSN: 2096-3246
Volume 55, Issue 02, April, 2023
https://doi.org/10.5281/zenodo.12707458

In "Privacy Preserving Cloud Data Access with Multi Authorities," published in the 2013 IEEE INFOCOM proceedings, T. Jung, X. Mao, X.-Y. Li, S.-J. Tang, W. Gong, and L. Zhang discuss methods for protecting sensitive data in the cloud. An article published in 2011 by J. Hur and D. K. Noh titled "Attribute based access control with efficient revocation in data outsourcing systems" was published in the IEEE Trans. on Parallel Distributed Systems. In the 2016 Proc. ICCCN, N. Oualha and K. T. Nguyen presented "Light weight attribute based encryption for the Internet of Things," which can be found on pages 1-6. 8. "An effective key management system for personal health data in Easwarmoorthy, Sophia, and Karrothu's work:

cloud, for the 2016 Proc. WiSPNET, pages 1651–1657. The authors of the paper "Secure distributed key generation in attribute based encryption systems" (D. Pletea, S. Sedghi, M. Veeningen, and M. Petkovic, 2015, pp. 103-107), authored the paper. 10 "An attribute based encryption scheme secure against malicious KGC" (G. Zhang, L. Liu, and Y. Liu, 2012, pp. 1376–1380) in Proc. TRUSTCOM.