# Data Extraction using Classified property based encipher procedure

**D.Saravanan**
Faculty of Operations & ITICFAI Business School (IBS), Hyderabad,
The ICFAI Foundation for Higher Education (IFHE)(Deemed to be university u/s 3 of the UGC Act 1956)Hyderabad-India.

**ABSTRACT**
Cloud computing has become one of the most emerging field in the technology park. Schemes such as attribute-based encryption technique are used for the access control of the third-party data. For protecting the data from hacker various secured data transaction are used. In the proposed work Cipher texts are encrypted to one particular user as well as to multiple users due to its hierarchical structure. It controls the access of complex structured data in a flexible and secured manner. The cipher-text policy enhances the flexible performance for the third-party data

**Keywords**
Access control, cloud computing, Distributed Environment, Cryptography, Encryption, Decryption.
*Article Received: 18 October 2020, Revised: 3 November 2020, Accepted: 24 December 2020*

## Introduction

Due to its various benefits, cloud computing has become the most beneficial pattern in the IT industry. Cloud computing reduces costs and capital expenditures, increases operational efficiencies, scalability, flexibility and immediate market growth. Commercial cloud computing has been built such as Google App Engine, Sales' Customer Relation Management.

One of the vital security concerns are privacy preserving and data security in cloud computing. In this techniques used cloud platform to perform and store their data sets. But increasing the demand of storage and vast usage of internet storing the data in cloud platform is not so safe. So the confidential data are not to be disclosed to the business organization otherwise enterprise users will face serious outcomes. Henceforth the data security is at the prioriesrequirement. Fine-grained access control and flexible access is desired in the service-oriented architecture. For instance, the health-care system requires restricted access of medical records whichshould be displayed only to the eligible data sets, similarly, other application in cloud allows only the authorized user or authorized senior people in the respective company can only access those data sets. Such sensitive records either required by the legislation or by company regulations.

In this paper, first the hierarchical attribute set based encryption method is shown in extension with the algorithm with a hierarchical architecture to show flexible and scalable access of data. Next this scheme enhances user grant, file creation, user revocation, file access and file deletion based on Hierarchical attributed set based encryption. Thirdly it analyzes its performance by enhancing CP-ABE technique. Lastly, hierarchical attributed set based encryption technique is implemented to experiment performance evaluation.

## Problem Definition

### Existing System

In the existing technique any information are stored in the cloud storage information are converted into unreadable format then it is stored in the cloud platform. The techniques or the procedure used for converting the information into unreadable format are kept secretly. Only the authorized users who involved the transaction only can view the secrete clue. But this technique creates a lot of complexity whenever the number of users get increased. It is very difficult to store all user's information in a single location. Second there is separate mechanism is required to manage this clue process it creates the additional burden to the user's community. Third problem after generating the clue if the user forgot the clue it is very difficult to complete the transaction. Suppose the legal user want to extract information even the user forgot the key then there is a separate procedure need to develop for find the clue for accessing the original data sets. **Disadvantage**

- Cipher texts are encrypted to multiple user.
- No administrator is there to maintain security.
- Complex to store data since ABE scheme is not flexible.
- User revocation is difficult in CP-ABE scheme.

## Suggested design

Any cloud platform contains five basic elements. One the service given to the client based on their request, data proprietor who use the cloud service,

stored data accessed by the user community, each cloud platform created for specific province, the owner of the province, user used the service through proper legalization. This five groups are arranged in order to access the specified information's. The cloud service provider manages a cloud to provide data storage service. The data files are encrypted by the data owners. Data owners store the encrypted files in the cloud for sharing it with the data consumers.Data are stored in the cloud are kept in unreadable format. So that any legitimate user wants to read the particular data set from the cloud they download the un readable format information after using the proper mechanism convert the unreadable information's into readable format. Each of this data sets are monitored by owner of the cloud province. Each this cloud province is monitored and controlled by the head cloud province authority.

**Advantages:**

- Cipher texts are encrypted to one particular user as well as to multiple users.
- Domain authority performs the administrator process for security.
- Proposed system are easy to access and easy to maintain because information's are stored in a classified order.
- Efficient user revocation is followed.

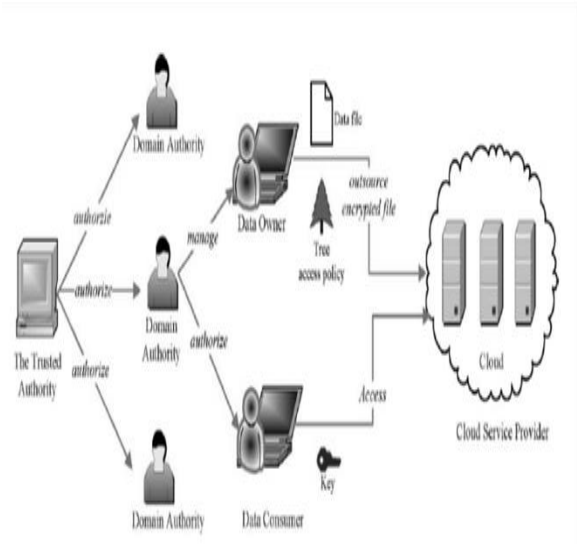



**Figure 1.**Classified property based System Model

The data proprietoracquires the public key from domain authority provided by the trusted authority. The data owner encrypts the data file with the help of the key provided. The domain authority is the chief administrator who manages the data owner as well as the data consumer. After receiving the clue, the cloud province authority circulates the clue to the respective client and proprietor. In this clue circulation the clue was generated by the focal expert and confidential expert. The cloud province authority stores this clue in the unreadable format in the cloud platform for easy communication and transformation. Data consumer gets the encrypted file from the cloud and then decrypts it with the help of private key provided by the trusted authority.

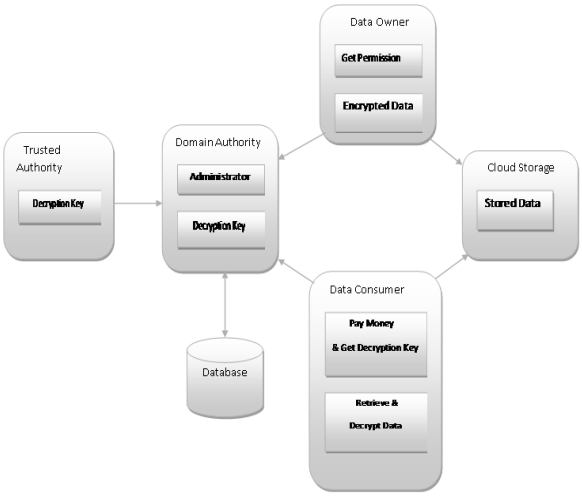



**Figure 2.** Encrypted system model.

## Experimental setup

First, the classified property based ASBE extends the ASBE algorithm improves flexibility and security in gets all the necessary process of getting the expected output. A full-fledged access control scheme based on hierarchical attribute set based encryption scheme is used. The scheme supports authority grant, user grant, creation/deletion of file. In cloud system One the service given to the client based on their request, data proprietor who use the cloud service, stored data accessed by the user community, each cloud platform created for specific province, the owner of the province, user used the service through proper legalization. In this components the confidential expert produces the clue for the transaction and necessary supporting parameters and properties for the operation Each and every transaction the cloud province expert circulate the clue and supporting information to the sub cloud province.

**Algorithm: Classified property based encipher procedure**

Step1: Initially set secluded and open variable for the transaction.
Set w: As work constraint for the transaction
Set O: As Open constraint for the transaction
Set P: As principal key and kept in confidently for the transaction
Step2: Generate clue (W, O, P)
In the clue generation p declared and kept as the confidently for any client c and the p as the product output.
Step3: Encipher (P,C, O)
Here in step 3 the principal key p and the input text IT and the classified property C and the product output Cipher product CP.
Step4: Decipher (CP, CKu)
It will collect the input information from the CP and confidential key CKu and produce the product output as a message.
Step 5: In the step4 the clue and the input text follows the classified procedure connected with the cipher product CP, then m is the initial message.
Step6: If the initial message m otherwise return null.

This algorithm helps encrypt the given data's. In step 1 initial declaration are done. In step 2 user declare the input key and output generated key information based on the initial declaration. In step 3 the input public key and message are converted into cipher text form. In step 4 the selected input from step 3 is decrypted based on the key structured associated secret key.

## Experimental Result

This output show that the data owner send request to the domain authority and receives request by the trusted authority.

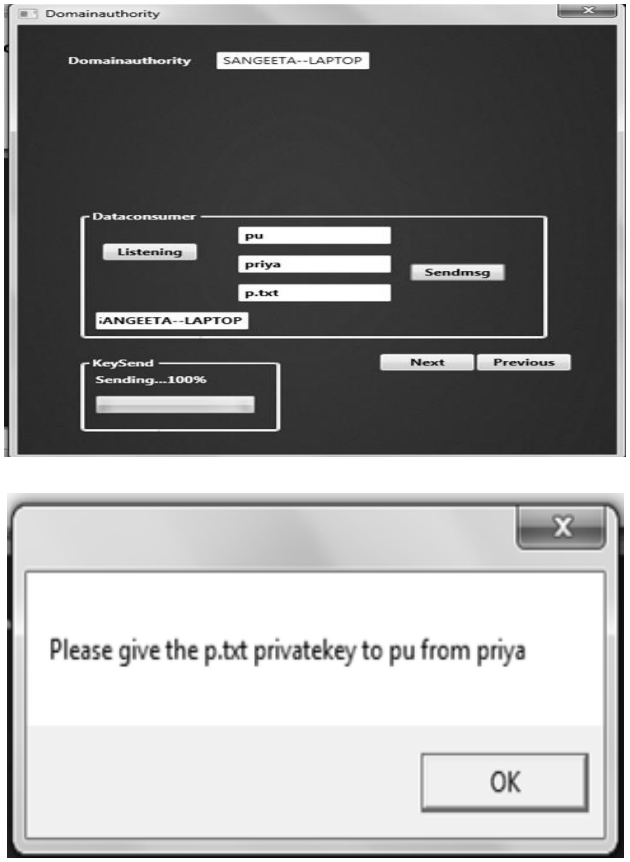



**Figure 3.** Domain authority receives request from dataconsumer and send it to the trusted authority

This output shows that the trusted authority sends public key to the domain authority.

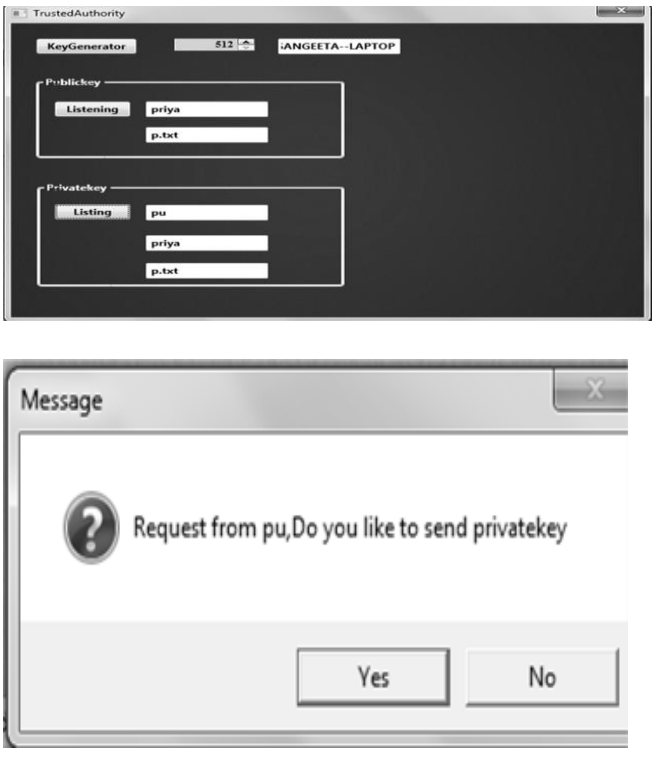



**Figure 4.**Trusted authority sends the privatekey to the domain authority.

This output shows that the domain sends the private key to the data consumer.

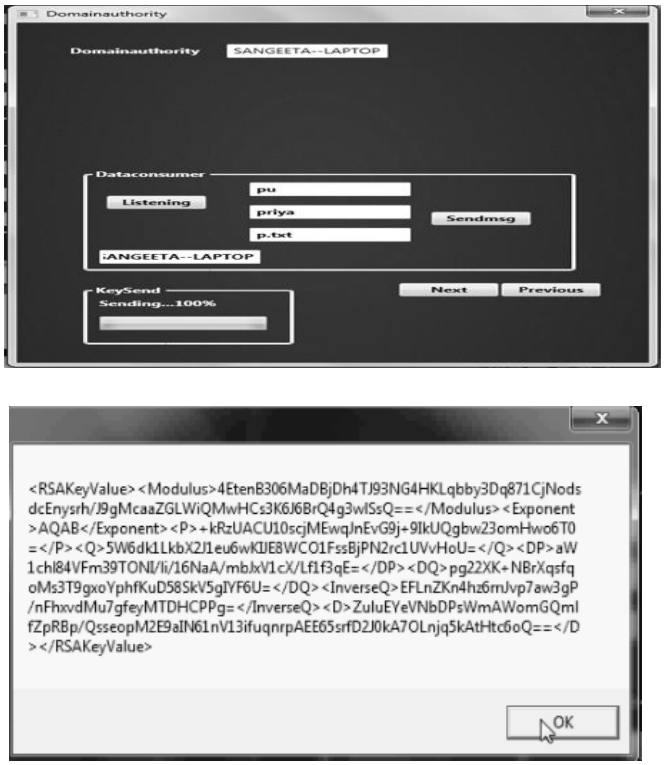
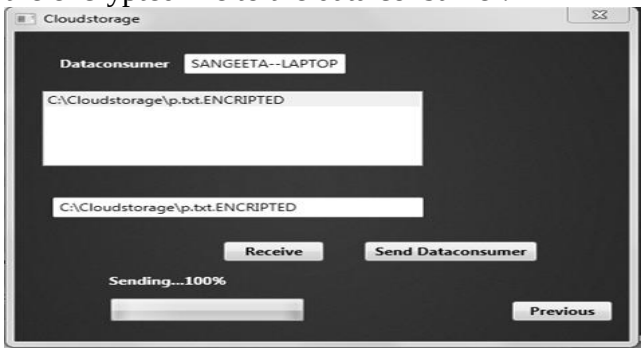



**Figure 5.** Domain authority sends the privatekey to the dataconsumer.

This output shows that the cloud storage sends the encrypted file to the data consumer.



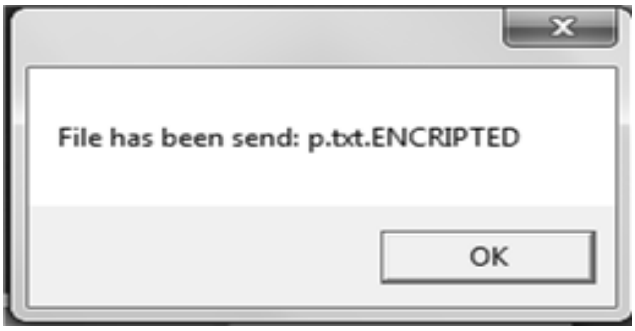




**Figure 6.** Cloud storage sends the encrypted file to the dataconsumer

This page shows that the data consumer receives the encrypted file and then decrypts it with the help of private key.

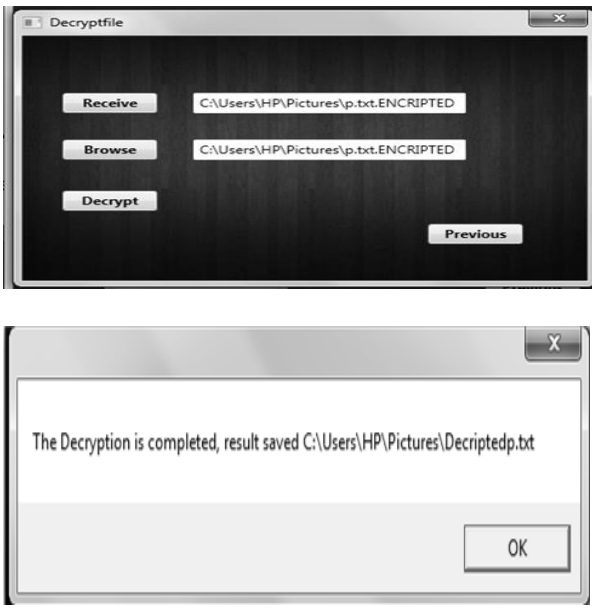



**Figure 7**. Data consumer decrypt the encrypted file

## Conclusion and Future work

The classified based property technique performs its operations separately or the process combined with the other methods such as property based encipher technique. In the proposed technique user get the clue from the confidential experts so that information is get more safely. Experimental outcome proofs that the proposed classified based property technique works high powerfully compare with the current systems. The experimental outcome also verifies that proposed system works more securely than any current security techniques. Our current system works

well in message type of input datasets, it future extended for image data sets.

## References


[1] S. Yu, C. Wang, K. Ren, and W. Lou, "Achiving secure, scalable, and fine-grained data access control in cloud computing," in Proc. IEEE INFOCOM 2010, 2010, pp. 534–542.

[2] D.Saravanan, Dr.S.Srinivasan, " A proposed New Algorithm for Hierarchical Clustering suitable for Video Data mining.", International journal of Data Mining and Knowledge Engineering", Volume 3, Number 9, July2011.Pages 569-572

[3] D.Saravanan, "Clustering the irregularity events in intelligence surrounding systems" Int. Journal of pure and applied mathematics, Vol. 119, No.12(2018), Pages 15025-15035, May-2018 (Special Issues), ISSN:1311-8080.

[4] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in Proc. ESORICS, Saint Malo, France, 2009.

[5] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE Symp. Security and Privacy, Oakland, CA, 2007.

[6] A. Sahai and B. Waters, "Fuzzy identity based encryption," in Proc. Acvances in Cryptology—Eurocrypt, 2005, vol. 3494, LNCS, pp. 457–473.

[7] G.Wang, Q. Liu, and J.Wu, "Hierachical attibute-based encryption for fine-grained access control in cloud storage services," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Chicago, IL, 2010.

[8] D.Saravanan, "Video data image retrieval using – BRICH", World journal of Engineering, Vol.14, Issuu 4, Pages 318-323, Aug 2017.

[9] D.Saravanan, Dr.S.Srinivasan, "Video Image Retrieval Using Data Mining Techniques "Journal of Computer pplications, Volume V, Issue No.1. Jan-Mar 2012. Pages39-42. ISSN: 0974-1925

[101V. Goyal, O. Pandey, A. Sahai, and B.Waters, "Attibute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Alexandria, VA, 2006.

[11]H. Harney, A. Colgrove, and P. D. McDaniel, "Principles of policy in secure groups," in Proc. NDSS, San Diego, CA, 2001.

[12] P. D. McDaniel and A. Prakash, "Methods and limitations of security policy reconciliation," in Proc. IEEE Symp. Security and Privacy, Berkeley, CA, 2002.

[13] T. Yu and M. Winslett, "A unified scheme for resource protection in automated trust negotiation," in Proc. IEEE Symp. Security and Privacy, Berkel ey, CA, 2003.

[14] A.M. Barani, R.Latha, R.Manikandan, "Implementation of Artificial Fish Swarm Optimization for Cardiovascular Heart Disease" International Journal of Recent Technology and Engineering (IJRTE), Vol. 08, No. 4S5, 134-136, 2019.

[15] Manikandan, R and Dr.R.Latha (2017). "A literature survey of existing map matching algorithm for navigation technology. International journal of engineering sciences & research technology", 6(9), 326-331.Retrieved September 15, 2017.

[16] R. Sathish, R. Manikandan, S. Silvia Priscila, B. V. Sara and R. Mahaveerakannan, "A Report on the Impact of Information Technology and Social Media on Covid–19," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, 2020, pp. 224-230, doi: 10.1109/ICISS49785.2020.9316046