# Fully Anonymous Attribute-Based Encryption for controlling Cloud Data

Prof.C.M.Jadhav[1] ,Ms.S.D.Shabade[2]

[1]*Head of Department, Department of Computer Science and Engineering,Bharat Ratana Indira Gandhi College Of Engineering, Kegaon, Solapur, Maharashtra, India*
[2]*P.G Student, Department of Computer Science and Engineering,Bharat Ratana Indira Gandhi College Of Engineering, Kegaon, Solapur, Maharashtra, India*

## Abstract

*Cloud computing is a innovatory computing paradigm, which enables flexible, on-demand, and low-cost usage of computing resources, but the data is outsourced to some cloud servers, and various privacy concerns emerge from it. Various schemes based on the attribute-based encryption have been projected to secure the cloud storage. However, most work focuses on the data contents privacy and the access control, while less interest is paid to the privilege control and the identity privacy. In this paper, we present a semi anonymous privilege control scheme Anony Control to address not only the data privacy, but also the user identity privacy in existing access control schemes. Anony Control decentralizes the central authority to limit the identity leakage and thus achieves semianonymity. Besides, it also generalizes the file access control to the privilege control, by which privileges of all operations on the cloud data can be managed in a fine-grained manner. Subsequently, we present the AnonyControl-F, which fully prevents the identity leakage and achieve the full anonymity. Our security analysis shows that both AnonyControl and Anony Control-F are secure under the decisional bilinear Diffie–Hellman assumption, and our performance evaluation exhibits the feasibility of our schemes.*

**Keywords**—*Anonymity, Multi-authority, Attribute-based Encryption*

## I.INTRODUCTION

Cloud computing is a completely new computing technique, by which computing resources are provided dynamically via Internet and the data storage is outsourced to someone or some party in a 'cloud'. It greatly attracts interest from both academic and industry world due to the profit-making, While outsourcing the data to the third party it should satisfy the two challenges. First of all, data confidentiality should be guaranteed. The data privacy is not only about the data contents. Since the most attractive part of the cloud computing is the outsourcing of computation, it is far beyond enough to just manage an access control. More likely, users want to control the right of data manipulation over other users or cloud servers.[1] [2] This isbecause when sensitive information or computation is outsourced to the cloud servers or user, which is out of users' control in most cases, privacy risks would raise constantly because the servers might illegally inspect users' data and access sensitive information, or other users might be able to infer careful information from the outsourced computation. Therefore, not only the access but also the operation should be managed. Secondly, personal information (defined by each user's attributes set) is at risk because user's identity is authenticated based on his information for the purpose of access control (or privilege control in this paper). As everyone is becoming more concerned about their identity privacy these days, the identity privacy also has to be protected before the cloud enters our life. Preferably, any authority or server alone should not know any client's personal data. Last but not least, the cloud computing system should be resilient in the case of security breach in which half part of the systemis compromised by attackers. [1]

## II.PROBLEM FORMULATION

In our framework, figure 1 there are five sorts of elements: N Attribute Powers (signified as A), central authority,Cloud Server, Data Owners and Data Consumers. A client can be a Data Owner and a Data Customer all the while. Authorities are assumed to have powerful computation abilities, and they are supervised by government offices because some attributes partially contain users‟ personally identifiable information. The entire attribute set is partitioned into N disjoint sets and controlled by every attribute authority, along these lines every attribute authority knows about just piece of information. Central authority is the trusted party where data owner and data consumer are communicated to attribute authority through central authority. A Data Owner is the entity who wishes to outsource encoded data file to the Cloud Servers. The Cloud Server, who is assumed to have adequate storage capacity, does nothing but store them. Recently joined Data Consumers ask for private keys from all of the Attribute authority , and they don't know which Attribute are controlled by which Attribute authority. At the point when the Data Consumers demand their private keys from the Attribute authority, Attribute authority together make relating private key and send it to them. All Data Consumers can download any of the encrypted information documents, however just those whose private keys fulfil the privilege tree Tp can execute the operation connected with benefit p. The server is designated to execute an operation p if and just if the client's accreditations are checked through the privilege tree Tp.

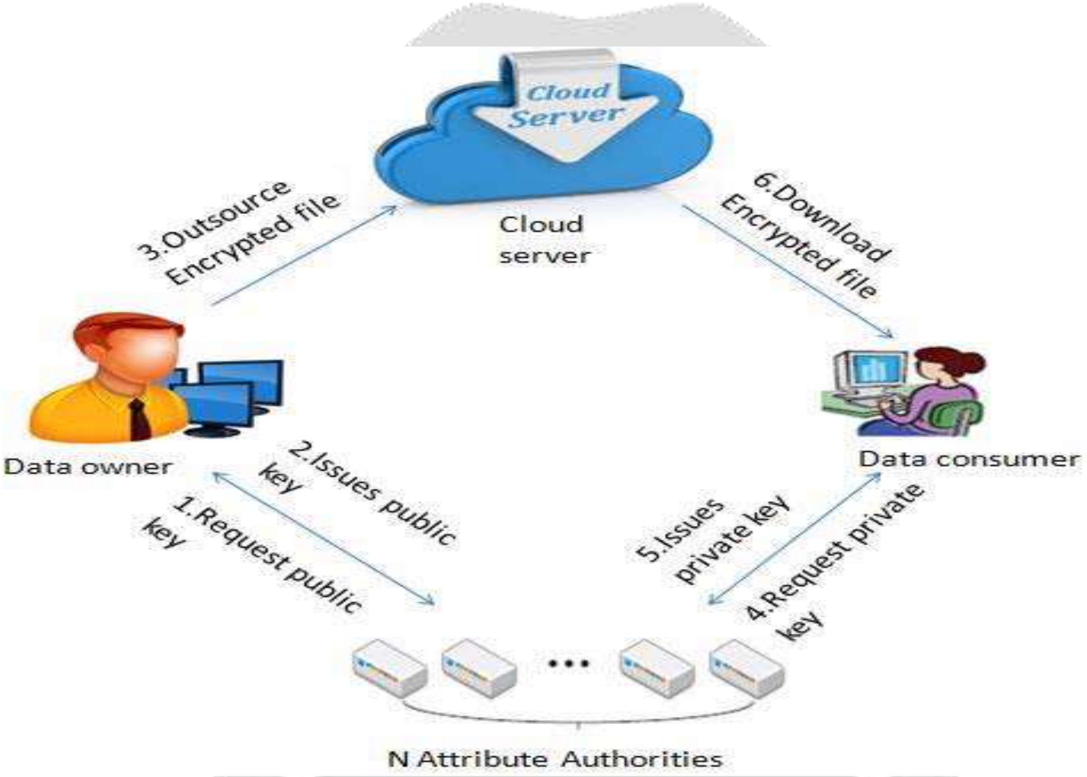

Figure 1: System Architecture

## III.IMPLEMENTATION

**MODULE DESCRIPTION**:

In our systemhaving the following modules:
1.Attribute Authorities
2.Data Consumers
3. Data Owners
4.Cloud Server

1.Attribute Authorities:

Attribute Authority & central authority together we called as attribute authorities .The module we have presented in which each user has an id and they can interact with each key generator (authority) using different pseudonyms. Our goal is to achieve a multi-authority CP-ABE which achieves the security that guarantees the confidentiality of Data Consumers identity information.

2.Data Consumers: A Data consumer is the entity who wishes to download/consume file from the Cloud Servers.

3.Data Owners:A Data Owner is the entity who wishes to outsource encoded data file to the Cloud Servers. The Cloud Server, who is assumed to have adequate storage capacity, does nothing but store them.

4.Cloud Server: The Cloud Server, who is assumed to have adequate storage capacity, does nothing but store them.

## IV.RESULTS

1.To upload and download files the data owner and consumer must be registered.

2.When their registration is completed then N-authorities will assign different attributes to user.

3.After this they have to request the authority for permission to perform operation on files.
4. N-Authorities provide public key, authority key for owner and private key, authority key for consumer to perform operations on files.
5. Using public key the data owner performs encryption and uploads files in to the cloud server.
6. Using private key the data consumer performs decryption and downloads files from the cloud server.
7. Attribute-based encryption module is using for each and every node encrypt data store. After encrypted data and again the re-encrypted the same data is using for fine-grain concept using user data uploaded. In such encryption scheme, an identity is viewed as a set of descriptive attributes, and decryption is possible if a decrypter’s identity has some overlaps with the one specified in the cipher text.
8. A multi-authority system is presented in which each user has an id and they can interact with each key generator (authority) using different pseudonyms. Our goal is to achieve a multi-authority CP-ABE which achieves the security defined above guarantees the confidentiality of Data Consumers’ identity information.
9. At the cloud server all the data is in encrypted form the cloud server is unable to see the details and data. By which we are providing not only providing data privacy but also user identity privacy by anonymity with fully anonymous attribute based encryption.

## V.CONCLUSION

This paper presents a semi-mysterious trait based benefit control plot AnonyControl and a fullyanonymous characteristic based benefit control plot AnonyControl-F to shows the client protection issue in a cloud storage server.By using the different specialists in the disseminated registering system, our proposed plans achieve fine-grained advantage control and in addition character mystery while controlling advantage control in perspective of customers' identityinformation. More altogether, our system can recognize up to N−2 master deal.We similarly facilitate clear security and execution examination which shows that AnonyControl both compelling and secure for conveyed stockpiling structure. The AnonyControl-F particularly gets the security of the AnonyControl and along these lines is similarly secure as it.
One of the best in class future works is to introduce the benefits to the customer framework on top of our Attribute Based Encryption. Supporting customer denial is an indispensable issue in the honest to goodness application, and this is an exceptional test in the use of ABE arrangements. [11]making our plans versatile with existing ABE plans bolster productive client refusal is one of our future works.

## VI. ACKNOWLEDGEMENT

I take this opportunity to express my gratitude to all respected who have rendered cooperation and guidance that supported me while developing this dissertation right from beginning.Primarily, I submit my gratitude and sincere thanks to my guide and Head of the department **Prof. C. M. Jadhav** for his constant motivation and support during the course of the work. I truly appreciate and value him esteemed guidance and encouragement from the beginning of this project. I would also like to thank our honorable Principal who encouraged us and created a healthy environment for all of us to learn in best possible way. I would like to thank all the staff members of our college for their help. Last but not the least, I would like to thank all my friends and family members who have always been there to support and helped me.

## VII.REFERENCES

[1]Taeho Jung, Xiang-Yang Li, Zhiguo Wan, Meng Wan," Cipher text-Policy Attribute-Based Encryption", T Jung - 2015.
[2]7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, February 9-11, 2010, Proceedings.
[3]White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Flexible Attributes Jianting Ning, Xiaolei Dong, Zhenfu Cao, Senior Member, IEEE, Lifei Wei, and Xiaodong Lin, Senior Member, IEEE
[4]20th European Symposium on Research in Computer Security, Vienna, Austria, September 21-25, 2015, Proceedings, Part 2.
[5]A. Shamir, "Identity-based cryptosystems and signature schemes," in CRYPTO. Springer, 1985, pp. 47–53.
[6]Frederic P.Miller,Agnes F.vandome,John McBrewster," Advanced Encryption Standard,2009,ISBN:6130268297 9786130268299.
[7]A. Sahai and B. Waters, "Fuzzyidentity-based encryption," in EUROCRYPT. Springer, 2005, pp. 457–473.
[8]"Decentralizing Attribute-Based Encryption" Allison Lewko, University of Texas at Austin lewko@cs.utexas.edu
[9]Vladimir Bozovic , Daniel Socek , Rainer Steinwandt , and Viktoria I. Villanyi. "Multi-authority attributes based encryption with honest-but-curious central authority".
[10]S. G. Akl and P. D. Taylor. Cryptographic Solution to a Multi Level Security Problem in Advances in Cryptology -- CRYPTO 1982.
[11]M.R.KAVITHA RANI,M.E, S.BRINDHA, M.E., "A Survey on Data Stored in Clouds" ISSN: 2350-0328 International Journal of Advanced Research in Science, Engineering and Technology Vol. 2, Issue 11 , November 2015