Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 05, May -2018

PRIVACY-PRESERVING AND FINE GRAINED ACCESS SCHEME FOR BIG DATA DEDUPLICATION IN CLOUD

Vikash Kumar[1st], Ashish Jha[2nd], Rohit kumar Pandit[3rd], Kunal Roshan[4th], Aditya Kumar[5th]

[1,2,3,4,5] *D.Y.Patil Collage of Engineering Akurdi*

Abstract— *In cloud computing environment there are many users of cloud stores there data and accessing of large data stored on cloud. But these users face some of major issue causing loss of data in cloud and facing a problem in authority and privacy of users. Cipher text-Policy Attribute based Encryption (CP-ABE) is a promising encryption technique that enables end-users to encrypt their data under the access policies defined over some attributes of file and upload encrypted file with encrypted attribute with key provided by attribute authority. Cloud consumers want to download and only allow data consumers whose attributes satisfy the access policies to decrypt the data. In CP-ABE, the access policy is attached to the cipher text in plaintext form, which may also leak some private information about end-users. Existing methods only partially hide the attribute values in the access policies, while the attribute names are still unprotected, these issues are modify in our scheme to provide more security. While uploading a file time server is associated with file to provide access to file for limited time only after that time file is unavailable for consumers. Also attribute bloom filter generate attributes of file while uploading and this attributes are store with file. Attribute authority in our scheme assign public key to user while uploading files on cloud and also files secret key and private key to data consumer while uploading. After entering keyword consumer will get top rank result depends upon attribute and time and can download that file if consumer having key of that file and can decrypt file.*

I. INTRODUCTION

In the era of large info, a colossal amount of data is generated quickly from various sources (e.g., smart phones, sensors, machines, social networks, etc.). Towards these large info, customary computer systems do not appear to be competent to store and technique these info. Due to the versatile and elastic computing resources, cloud computing might be a natural appropriate storing and method large info. With cloud computing, end-users store their info into the cloud, and think about the cloud server to share their info to various users (data consumers). Thus on entirely share end-users' info to authorized users, it's a necessity to vogue access management mechanisms in step with the wants of end-users. Once outsourcing info into the cloud, end-users lose the physical management of their info. Moreover, cloud service suppliers do not appear to be fully-trusted by end-users that build the access management tougher. For example, if the quality access management mechanisms unit of measurement applied, the cloud server becomes the conceive to gauge the access policy and build access decision. Thus, end-users would possibly worry that the cloud server would possibly build wrong access appeal purpose or accidentally, and disclose their info to some unauthorized users. Thus on amendment end-users to manage the access of their own info, some attribute-based access management schemes unit of measurement projected by investment attribute-based cryptography. In attribute-based access management, end-users first define access policies for his or her info and code the data beneath these access policies. Entirely the users whose attributes can satisfy the access policy unit of measurement eligible to decrypt the information.

In Associate in Nursing efficient and fine-grained large info access management theme with privacy-preserving policy. Specifically, we tend to tend to cover the entire attribute (rather than entirely its values) inside the access policies. However, once the attributes unit of measurement hidden, not entirely the unauthorized users but to boot the authorized users cannot grasp that attributes unit of measurement involved inside the access policy, that produces the key writing a tough draw back. to assist info secret writing, we tend to tend to boot vogue a totally distinctive Attribute Bloom Filter to determine whether or not or not Associate in Nursing attribute is inside the access policy and realize the precise position inside the access policy if it's inside the access policy. Security analysis and performance analysis show that our theme can preserve the privacy from any LSSS access policy whereas not victimization ample overhead.

We introduce a time server in our theme to assign express time with each file that's uploading on cloud[6]. Therefore whereas user uploads file on cloud express time is expounded thereto. So this file is accessible to info consumer only for that specific measure then at the instant time files do not appear to be offered for user to access..

II. SCOPE

Scope of system is to produce services to cloud user by implementing associate degree economical fine grained massive knowledge access management theme with time server. This method implements model of activity whole attribute in its access policy instead of activity solely its price. Thus users can't grasp attributes of files.

III. LITRATURE SURVEY

1. A Robust, Distortion Minimization Fingerprinting Technique for Relational Database
Authors: Namrata Gursale, Arti Mohanpurkar
Description: In this paper, the projected method technique inserts the fingerprint bits subject to usability constraints. And results, minimum distortion in original data set still as finds the guilty user UN agency is answerable for prohibited distribution of information set. A logical extension of this analysis is to extend the technique on non-numeric strings data.
Disadvantages:
- This scheme does not provide efficient mining operation on numerical data generated from finger prints.
- It is difficult to access files from large size of data.

2. **Fingerprinting Numeric Databases with Information Preservation and Collusion Avoidance**
Authors: Arti Mohanpurkar, Madhuri Joshi
Description: The process technique facilitates with security against the possession crime and a provision for traitor tracing (if any unauthorized copy is found). The insertion of fingerprint bits in numeric information bases may modification the numeric information to some extent. A loss of knowledge of information of information of might even be discovered as a result of these changes in numeric data. Here the add is extended by finding a novel methodology for inserting a fingerprint inside the information in conjunction with the peace of mind of information preservation. the info preservation is shown in terms of result on mean, variance and variance once method, that's found to be minuscule

Disadvantages:
- It is difficult to process large and complex numerical data.
- While dealing with numerical data it requires distributed approach.

3. **Applying Watermarking For Copyright Protection, Traitor Identification and Joint Ownership: A Review**
Authors: A. A. Mohanpurkar, M. S. Joshi
Description: In this paper, a very distinctive theme of watermarking relative databases for copyright protection is found. Speech signal is embedded as watermark into the relations; associated novel watermark insertion formula and detection formula unit projected. Thus, the watermark signal throughout this system is foretold to be extra purposeful and has closely related to the copyright holder.

Disadvantage:
- Large scale of unauthorized copying and increase in violation of copyright and tampering with content may occur.

4. **Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage**
Authors: T. Venkateswara Rao, V Pradeep
Description: In this paper, we tend to tend to projected avoidable multi-authority CPABE theme which will support economical attribute revocation. Then, we tend to tend to create an honest data access management theme for multi-authority cloud storage systems. We tend to tend to in addition proved that our theme was demonstrable secure among the random oracle model. The voidable multi-authority CPABE could also be a method, which can be applied in any remote storage systems and on-line social networks etc.

Disadvantages:
- This scheme does not support user revocation.
- Attribute use in this system are light weighted i.e. this attributes are not completely hidden.

5. **Enabling Fine-grained Access Control with Efficient Attribute Revocation and Policy Updating in Smart Grid**

Authors: Hongwei Li , Dongxiao Liu , Khalid Alharbi, Shenmin Zhang , Xiaodong Lin
Description:
In this paper, we tend to plan a fine-grained access management theme (FAC) with economical attribute revocation and policy change in sensible grid. The planned FAC is additional appropriate for sensible access management problems since it supports dynamic operations. Moreover, we tend to gave thorough security analysis and incontestable that the FAC can do high level security guarantees. Additionally, performance analysis and analysis show that the FAC is additional economical compared with the present schemes through comprehensive experiments. For the longer term work, we'd explore privacy-preserving information aggregation drawback in sensible grid.

Disadvantages:
- This scheme does not verify integrity of user or verify user authentication.
- Difficulties may occur in accessing large data in grid.

6. Time-domain Attribute-based Access Control forCloud-based Video Content Sharing:A Cryptographic Approach

Authors: Kan Yang, Zhen Liu, Xiaohua Jia, Fellow, IEEE, and Xuemin (Sherman) Shen, Fellow, IEEE

Description: In this paper, we've projected a science approach, TAAC, to realize time-domain attribute-based access management for cloud-based video content sharing. Specifically, we've projected a provably secure time-domain attribute-based writing theme by embedding the time into every the cipher texts and so the keys, such exclusively users World Health Organization hold ample attributes during a} very specific amount can rewrite the information. To realize the dynamic change of users' attributes, we've jointly projected a cheap attribute modification methodology that allows attribute authorities to grant new attributes, revoke previous attributes and re-grant previously revoked attributes to users at the beginning of each interval. We've a lot of mentioned on how to realize access management of video contents that are commonly accessed in multiple time slots and also the thanks to kind special queries on video contents generated in previous time slots. We've provided the protection proof for the projected TAAC theme in generic linear cluster model and random Oracle model.

Disadvantage:

- If user require file after its time require then file is unavailable for user then problem may occur.
- Unauthorized user may access file or corrupt them.

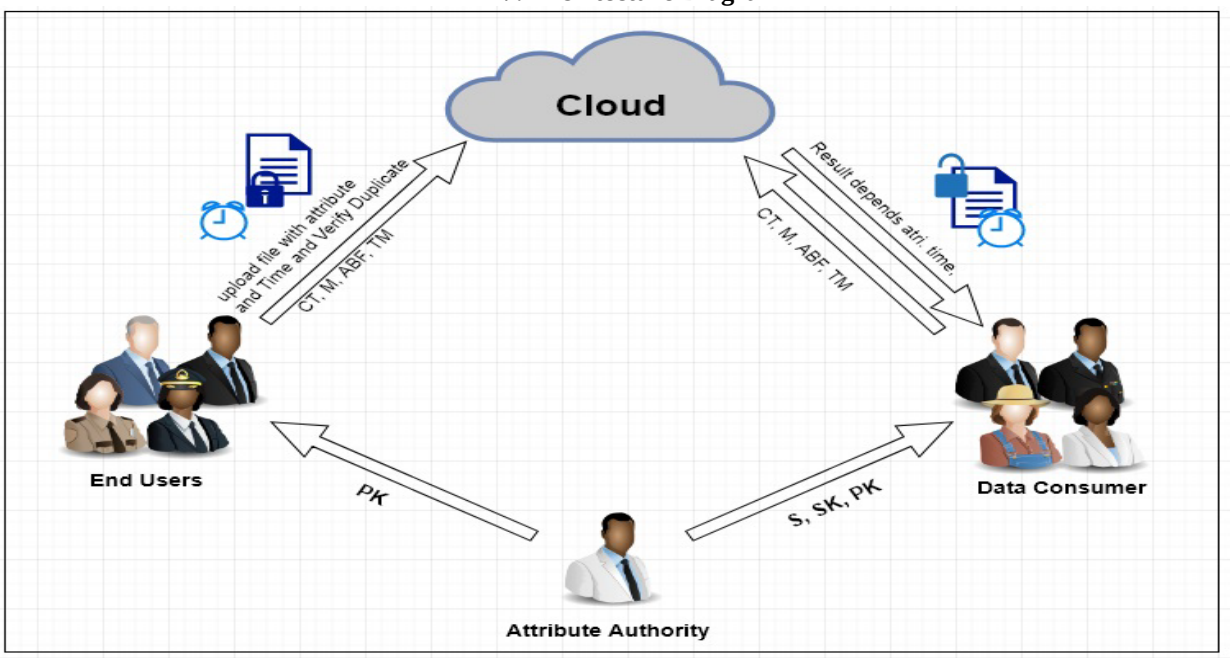
IV. PROPOSE SYSTEM

The existing techniques on is just write in code file and transfer that file on cloud. Several file square measure store in cloud. There's no such access policy for file that specific attested users will solely access that file. Additionally in this system whole attribute isn't hidden solely name of attributes square measure hidden. This causes some security problems and additionally a number of storage problems.

In Associate in nursing economical huge information access theme, information owner transfers encrypted come in cloud at time of uploading it request to attribute generator for public key then upload come in cloud. Whereas uploading a file there's Associate in nursing time related to it file in order that file remains for specific time solely and users will access that file for that point amount solely.

File is uploaded with attribute access policy for users with encrypted Index of that file. User need to go looking that file Attribute bloom filter checks user matching access policy of that file and additionally checks keyword of trapdoor looking, if attribute of user is matched with access policy and time then Rank search result's about to the user then user transfer solely resulted file victimization secret key obtaining from attribute Authority.

V. Architecture Diagram



Algorithm 1: AES Algorithm

Alogrithm Steps

Step 1: Start

Step 2: Derive the set of round keys from the cipher key.

Step 3: Initialize the state array with the block data (plaintext)

Step 4:Add the initial round key to the starting state array.

Step 5: Add the initial round key to the starting state array.

Step 6:Perform the tenth and final round of state manipulation.

Step 7: Copy the final state array out as the encrypted data (ciphertext).

MD5 algorithm description

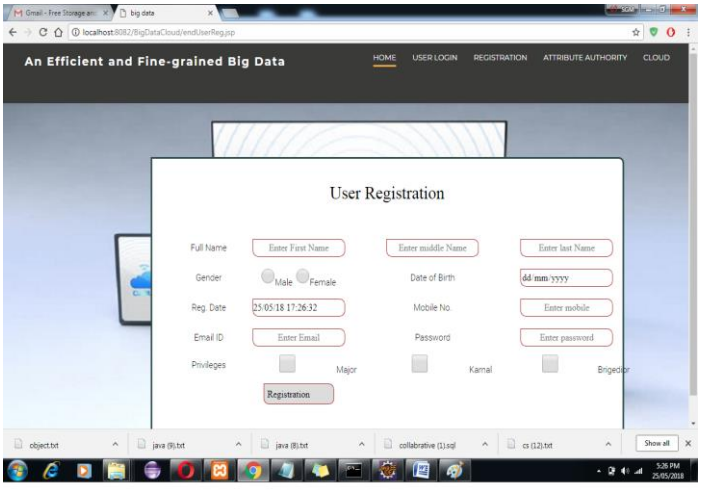
MD5 algorithm takes input message of arbitrary length and generates 128-bit long output hash. MD5 hash algorithm consist of 5 steps:

- Step 1. Append Padding Bits
- Step 2. Append Length
- Step 3. Initialize MD Buffer
- Step 4. Process Message in 16-Word Blocks
- Step 5. Output

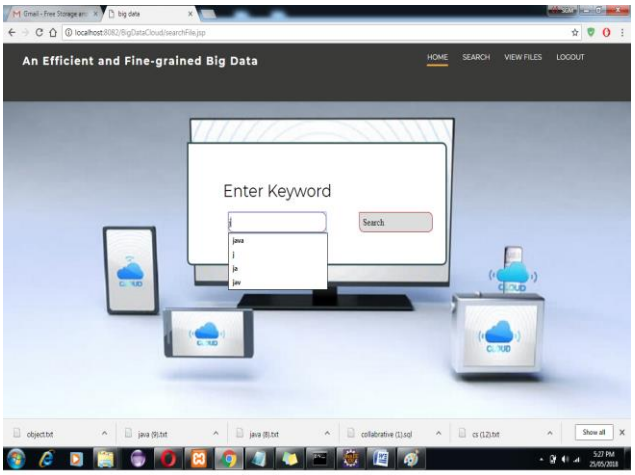
VII Results:

HOME PAGE

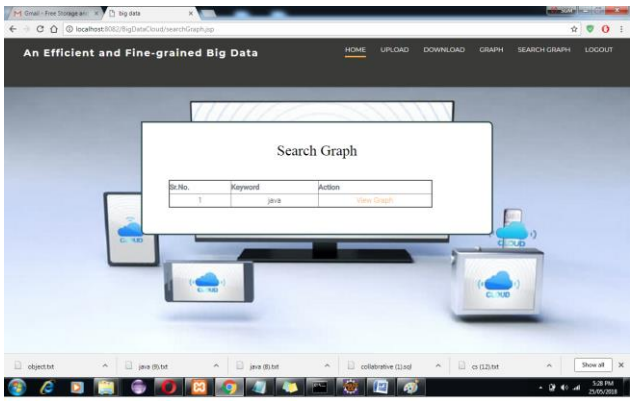
REGISTER



FILE UPLOAD



SEARCH FILE



SEARCH GRAPH

VIII. CONCLUSION

In this project propose a mechanism for cloud computing. In cloud users upload their files and also access files from cloud .So scheme provides an efficient encryption scheme for security of data stored on cloud and then efficient access policy on data files. While uploading files on cloud user request for key to attribute authority after receiving key user upload file with

specific time associated with it.While downloading file trapdoor is generated and multi-keyword search is perform on cloud data cloud gives top rank results and attribute authority gives keys for downloading files.

IX. ACKNOWLEDGMENT

We might want to thank the analysts and also distributers for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the school powers for giving the obliged base and backing.

X. REFERENCES

[1] Namrata Gursale, Arti Mohanpurkar,"A Robust, Distortion Minimization Fingerprinting Technique for Relational Database" Volume: 2 Issue: 6, June 2014.

[2]Ms. Arti Mohanpurkar, Ms. Madhuri Joshi, "Fingerprinting Numeric Databases with Information Preservation and Collusion Avoidance ", Volume 130 – No.5, November2015.

[3]A. A. Mohanpurkar, M. S. Joshi, "Applying Watermarking For Copyright Protection, Traitor Identification And Joint Ownership: A Review", 978-1-4673-0125-1 c 2011 IEEE.

[4] K. Yang and X. Jia, “Expressive, efficient, and revocable data access control for multi-authority cloud storage,” IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 7, pp. 1735–1744, July 2014.

[5] H. Li, D. Liu, K. Alharbi, S. Zhang, and X. Lin, “Enabling fine-grained access control with efficient attribute revocation and policy updating in smart grid,” KSII Transactions on Internet and Information Systems (TIIS), vol. 9, no. 4, pp. 1404–1423, 2015.

[6] K. Yang, Z. Liu, X. Jia, and X. S. Shen, “Time-domain attribute-based access control for cloud-based video content sharing: A cryptographic approach,” IEEE Trans. on Multimedia (to appear), February 2016.

