LARGE DATA ACCESS WITH EFFICIENT ATTRIBUTES ACCESS POLICY IN CLOUD COMPUTING.

Keertee Werulkar[1], Prof. S. T. Sawale[2], Akshay Kokane[3], Somesh Chunawale[4]
[1,3,4]Student, Final year, Information Technology, Anuradha Engineering College, Chikhli
[2]Asst. Prof., Information Technology, Anuradha Engineering College, Chikhli

Abstract

In accessing of enormous information keep on cloud major issue inflicting loss of information in cloud and facing a tangle in authority and privacy of users. Cipher text-Policy Attribute based mostly coding (CP-ABE) may be a promising coding technique permits} end-users to cipher their information beneath the access policies outlined over some attributes {of information of knowledge of information} shoppers and solely allows data shoppers whose attributes satisfy the access policies to decode the info. In CP-ABE, the access policy is connected to the cipher text in plaintext kind, which can conjointly leak some personal data concerning end-users. Existing ways solely part hide the attribute values within the access policies, whereas the attribute names area unit still unprotected. Whereas uploading a file time server is related to file to produce access to file for restricted time solely. Attribute authority in our theme assign personal key to user whereas uploading files on cloud and conjointly files secret key and personal key to information shopper whereas uploading. When coming into keyword user shopper can get prime rank result depends upon attribute and time.

Key words: Big Data, Access Control, Privacy-preserving Policy, Attribute Bloom Filter.

I. INTRODUCTION

In the era of massive information, an enormous quantity of information is generated quickly from numerous sources (e.g., good phones, sensors, machines, social networks, etc.). Towards these massive information, standard pc systems don't seem to be competent to store and method these information. Owing to the versatile and elastic computing resources, cloud computing could be a natural suitable storing and process massive information. With cloud computing, end-users store their information into the cloud, and consider the cloud server to share their information to alternative users (data consumers). So as to solely share end-users' information to licensed users, it's necessary to style access management mechanisms in step with the necessities of end-users. Once outsourcing information into the cloud, end-users lose the physical management of their information. Moreover, cloud service suppliers don't seem to be fully-trusted by end-users that build the access management tougher. For instance, if the standard access management mechanisms square measure applied, the cloud server becomes the decide to gauge the access policy and build access call. Thus, end-users might worry that the cloud server might build wrong access call on purpose or accidentally, and disclose their information to some unauthorized users. So as to change end-users to manage the access of their own information, some attribute-based access management schemes square measure projected by investment attribute-based encoding. In attribute-based access management, end-users 1st outline access policies for his or her information and code the information underneath these access policies. Solely the users whose attributes will satisfy the access policy square measure eligible to decode the information. In an efficient and fine-grained massive information access management theme with privacy-preserving policy. Specifically, we tend to hide the total attribute (rather than solely its values) within the access policies. However, once the attributes square measure hidden, not solely the unauthorized users however additionally the

licensed users cannot grasp that attributes square measure concerned within the access policy, that makes the secret writing a difficult downside. To help information secret writing, we tend to additionally style a completely unique Attribute Bloom Filter to gauge whether or not AN attribute is within the access policy and find the precise position within the access policy if it's within the access policy. Security analysis and performance analysis show that our theme will preserve the privacy from any LSSS access policy while not using abundant overhead.

We introduce a time server in our theme to assign explicit time with every file that is uploading on cloud. thus whereas user uploads file on cloud explicit time is related to it.so this file is accessible to information client just for that specific fundamental quantity then at the moment time files don't seem to be offered for user to access.

II. SCOPE

Scope of system is to provide services to cloud user by implementing an efficient fine grained big data access control scheme with time server. This system implements model of hiding whole attribute in its access policy rather than hiding only its value. So users can not know 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 process technique inserts the fingerprint bits subject to usability constraints. And results, minimum distortion in original knowledge set still as finds the guilty user UN agency is to blame for prohibited distribution of knowledge set. A logical extension of this analysis is to increase the technique on non-numeric strings knowledge.

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 felony and a provision for traitor tracing (if any unauthorized copy is found). The insertion of fingerprint bits in numeric knowledge bases might modification the numeric data to some extent. A loss of knowledge of could also be discovered because of these changes in numeric data. Here the add is extended by finding a unique method for inserting a fingerprint within the info in conjunction with the peace of mind of data preservation. the data preservation is shown in terms of result on mean, variance and variance when process, that is 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 completely unique theme of watermarking relative databases for copyright protection is found. Speech signal is embedded as watermark into the relations; associated novel watermark insertion algorithmic program and detection algorithmic program area unit projected. Thus, the watermark signal during this methodology is predicted to be additional purposeful and has closely associated with 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 projected a revokable multi-authority CPABE theme that may support economical attribute revocation. Then, we tend to created a good knowledge access management theme for multi-authority cloud storage systems. we tend to additionally proved that our theme was demonstrable secure within the random oracle model. The revokable multi-authority CPABE may be a technique, which may 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 proposed a fine-grained access control scheme (FAC) with efficient attribute revocation and policy updating in smart grid. The proposed FAC is more suitable for practical access control issues since it supports dynamic operations. Moreover, we gave thorough security analysis and demonstrated that the FAC can achieve high level security guarantees. In addition, performance evaluation and analysis show that the FAC is more efficient compared with the existing schemes through comprehensive experiments.

For the future work, we would explore privacy-preserving data aggregation problem in smart 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 for Cloud-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 cryptologic approach, TAAC, to attain time-domain attribute-based access management for cloud-based video content sharing. Specifically, we've projected a incontrovertibly secure time-domain attribute-based coding theme by embedding the time into each the cipher texts and therefore the keys, such solely users World Health Organization hold ample attributes in a very specific period will rewrite the info. to attain the dynamic amendment of users' attributes, we've conjointly projected AN economical attribute change methodology that permits attribute authorities to grant new attributes, revoke previous attributes and re-grant antecedently revoked attributes to users at the start of every interval. we've more mentioned on a way to attain access management of video contents that normally accessed in multiple time slots and the way to form 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 only encrypt file and upload that file on cloud. Many duplicate file are store in cloud. There is no such access policy for file that particular authenticated users can only access that file. Also in that system whole attribute is not hidden only name of attributes are hidden. This causes some security issues and also some of storage issues. In an efficient big data access scheme, Data owner uploads encrypted file in cloud at time of uploading it request to attribute generator for private key and then upload file in cloud. While uploading a file there is an time associated with it file so that file remains for specific time only and users can access that file for that time period only.

File is uploaded with attribute and access policy for users. User want to download that file Attribute bloom filter checks user matching access policy of that file and also checks attribute of user with attribute in access policy. If user is authenticated then allow that user to download that file.

V.ARCHITECTURE DIAGRAM

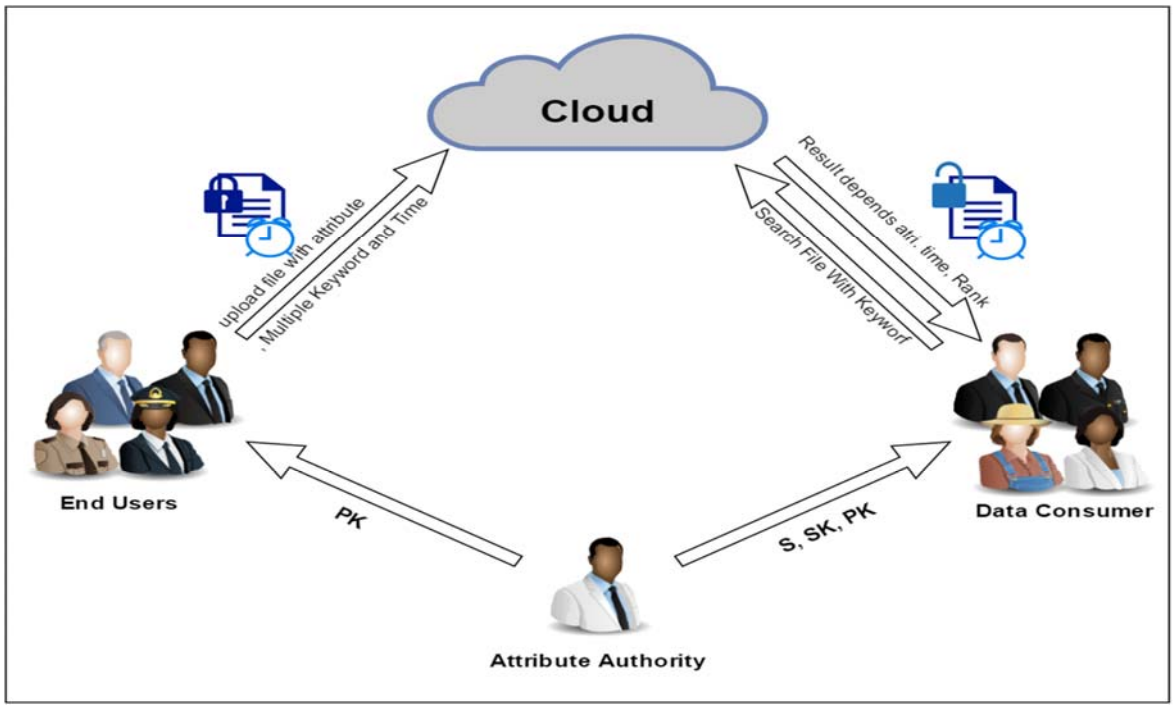

Figure. System Architecture

VI.MATHEMATICAL CALCULATION

Let S be the Whole system S= {I, P, O}
I-input
P-procedure
O-output

Input I-
F = {f1, f2, ….., fn}
Where,
F- Files
Procedure (P) = { Setetup , KeyGen, Encryption }

Now,
Step 1-Setup (PK,MSK): The setup algorithm takes as input a security parameter l. It outputs the public key and master secret key.

Step 2-KeyGeneration (PK,MSK,S) ->SK): The key generation algorithm takes as inputs the public key PK, the master key MSK and a set of attribute S. It outputs the corresponding secret key SK.

Step 3: Encrypt(PK,m, (M,p))->(CTABF):The data encryption algorithms contains: data encryption subroutine Enc and Attribute Bloom Filter building subroutine ABF Build

Enc(PK,m, (M,p))->CT:
The data encryption subroutine takes as inputs the public key PK, the message m and access structure (M,p). It outputs a cipher text CT.

ABFBuild (M,p) -> ABF. The ABF building subroutine takes as input the access policy (M,p). It outputs the Attribute Bloom Filter ABF.

Step 4: Decryption
Decrypt(M,ABF,PK,SK,CT) -> m
The decryption algorithm consists of two subroutines: ABFQuery and Decrypt.

ABFQuery(S,ABF,PK)-> p.
The ABF query algorithm takes as inputs the attribute set S, the Attribute
Bloom Filter ABF and the public key PK. It outputs a reconstructed attribute mapping r0 = f(rownum,att)gS, which shows the corresponding row number in the access matrix M for all the attributes all att €S.

Dec(SK,CT, (M,p)) -> m or β.
The data decryption algorithm takes as inputs the secret key SK, the cipher text CT as well as the access matrix M and the reconstructed attribute mapping. If the attributes can satisfy the access

policy, it outputs the message m. Otherwise, it outputs β.

Output (O) - Finally, the security and experimental analysis show that, compared with its relevant schemes our scheme is also secure and efficient

VII. CONCLUSION

We have proposed an efficient and fine-grained data access control scheme for big data, where the access policy will not leak any privacy information. In our method, It can hide the whole attribute (rather than only its values) in the access policies. This may lead authentication problem while user wish to download file. We have also designed an attribute localization algorithm to evaluate whether an attribute is in the access policy. In order to improve the efficiency, a novel Attribute Bloom Filter has been designed to locate the precise row numbers of attributes in the Access matrix. We have also demonstrated that our scheme is selectively secure against chosen plaintext attacks. Moreover, we have implemented the ABF by using Murmur Hash and the access control scheme to show that our scheme can preserve the privacy from any LSSS access policy without employing much overhead. In our future work, we will focus on how to deal with the offline attribute guessing attack that check the guessing "attribute strings" by continually querying the ABF.

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.

[7]. P. Mell and T. Grance, ''The NIST Definition of Cloud Computing,'' National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep., 2009.

[8]J. Bethencourt, A. Sahai, and B. Waters, ''Ciphertext-Policy Attribute-Based Encryption,'' in Proc. IEEE Symp. Security and privacy (S&P'07), 2007, pp. 321-334.

[9]B. Waters, ''Ciphertext-Policy Attribute Based Encryption: An Expressive Efficient, and Provably Secure Realization,'' in Proc. 4th Int'l Conf. Practice and Theory in Public Key Cryptography (PKC'11), 2011, pp. 5370.

[10]V. Goyal, A. Jain,O. Pandey, and A. Sahai, ''Bounded Ciphertext Policy Attribute Based Encryption,'' in Proc. 35th Int'l Colloquium on Automata, Languages, and Programming (ICALP'08), 2008, pp. 579-591.

[11]A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B.Waters, ''Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption,'' in Proc. Advances in Cryptology-EUROCRYPT'10, 2010, pp. 6291.

[12] S. Jahid, P. Mittal, and N. Borisov, ''Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation,'' in Proc. 6th ACM Symp. Information, Computer and Comm. Security (ASIACCS'11), 2011, pp. 411-415.

[13] S. Ruj, A. Nayak, and I. Stojmenovic, ''DACC: Distributed Access Control in Clouds,'' in Proc. 10th IEEE Int'l Conf. Trust Com, 2011, pp. 91-98.

[14] K. Yang and X. Jia, ''Attribute-Based Access Control for Multi-Authority Systems in Cloud Storage,'' in Proc. 32th IEEE Int'l Conf. Distributed Computing Systems (ICDCS'12), 2012, pp. 1-10.

[15] D. Boneh and M.K. Franklin, ''Identity Based Encryption from the Weil Pairing,'' in Proc. 21st Ann. Int'l Cryptology Conf.: Advances in Cryptology-CRYPTO '01, 2001, pp.213-22