An Efficient & Fine-grained Big Data Access Control Scheme with Privacy-Preserving Policy

Sushma J. Hiwrale[1] Prof. D.R. Deshmukh[2]
[1,2]Department of Computer Science & Engineering
[1,2]MIT Aurangabad, India

Abstract— In accessing of huge data continue cloud major issue inflicting loss of data in cloud and facing a retardant in authority and privacy of users. Cipher text-Policy Attribute based writing (CP-ABE) is also a promising writing technique permits} end-users to cipher their data to a lower place the access policies made public over some attributes {of data information of information} of information} shoppers and alone permits data shoppers whose attributes satisfy the access policies to decrypt the information. In CP-ABE, the access policy is connected to the cipher text in plaintext kind, which might jointly leak some personal knowledge regarding end-users. Existing ways that alone half hide the attribute values at intervals the access policies, whereas the attribute names unit of measurement still unprotected. Wherever as uploading a file time server is said to file to provide access to file for restricted time alone. Attribute authority in our theme assign personal key to user whereas uploading files on cloud and jointly files secret key and private key to data shopper whereas uploading. Once coming back into keyword user shopper will get prime rank result depends upon attribute and time.

Key words: Big Data Access Control Scheme

I. Introduction

In the era of large info, a vast amount of data is generated quickly from various sources (e.g., sensible phones, sensors, machines, social networks, etc.). Towards these large info, normal computer systems do not appear to be competent to store and methodology these info. Because of the versatile and elastic computing resources, cloud computing may 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 exclusively share end-users' info to commissioned users, it is necessary 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 applied, the cloud server becomes the attempt 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 modification end-users to manage the access of their own info, some attribute-based access management schemes unit 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. Exclusively the users whose attributes can satisfy the access policy unit eligible to decipher the information.

In associate degree efficient and fine-grained large info access management theme with privacy-preserving policy. Specifically, we have a tendency to tend to cover the overall attribute (rather than exclusively its values) inside the access policies. However, once the attributes unit hidden, not exclusively the unauthorized users but in addition the commissioned users cannot grasp that attributes unit involved inside the access policy, that produces the key writing a tough draw back. to assist info secret writing, we have a tendency to tend to in addition vogue a very distinctive Attribute Bloom Filter to determine whether or not or not associate degree attribute is inside the access policy and notice the precise position inside the access policy if it's inside the access policy[5]. Security analysis and performance analysis show that our theme can preserve the privacy from any LSSS access policy whereas not mistreatment pr overhead.

We introduce a time server in our theme to assign express time with each file that's uploading on cloud [6]. So whereas user uploads file on cloud express time is expounded to that. So this file is accessible to info shopper only for that specific amount 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 huge information access management theme with time server. This technique implements model of activity whole attribute in its access policy instead of activity solely its price. Therefore users cannot recognize attributes of files.

III. Literature survey

A. A Robust, Distortion Minimization Fingerprinting Technique for Relational Database

- Authors: Namrata Gursale, Arti Mohanpurkar
- Description

During 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 administrative body is in charge for prohibited distribution of data set. A logical extension of this analysis is to extend the technique on non-numeric strings data.

1) 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.

B. Fingerprinting Numeric Databases with Information Preservation & Collusion Avoidance

- Authors: Arti Mohanpurkar, Madhuri Joshi
- Description

The method technique facilitates with security against the possession law-breaking and a provision for traitor tracing (if any unauthorized copy is found). The insertion of fingerprint bits in numeric data bases would possibly modification the numeric information to some extent. A loss {of knowledge of information of information} of may even be discovered due to these changes in numeric data. Here add is extended by finding a novel methodology for inserting a fingerprint at intervals the information in conjunction with the peace of mind of knowledge preservation. The info preservation is shown in terms of result on mean, variance and variance once method, that's found to be minuscule.

1) Disadvantages

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

C. Applying Watermarking For Copyright Protection, Traitor Identification and Joint Ownership: A Review

- Authors: A. A. Mohanpurkar, M. S. Joshi
- Description

During 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 algorithm and detection algorithm unit projected. Thus, the watermark signal throughout this technique is expected to be extra purposeful and has closely related to the copyright holder.

1) Disadvantage

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

D. Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage

- Authors: T. Venkateswara Rao, V Pradeep
- Description

In this paper, we have a tendency to tend to projected avoidable multi-authority CPABE theme which will support economical attribute revocation. Then, we have a tendency to tend to create a decent information access management theme for multi-authority cloud storage systems. we have a tendency to tend to boot proven that our theme was demonstrable secure at intervals the random oracle model. The voidable multi-authority CPABE is also a way, which can be applied in any remote storage systems and on-line social networks etc.

1) Disadvantages

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

E. 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've a bent to plan a fine-grained access management theme (FAC) with economical attribute revocation and about-face in smart grid. The planned FAC could be a heap of applicable for smart access management issues since it supports dynamic operations. Moreover, we've a bent to give thorough security analysis and unarguable that the FAC area unit ready to do high level security guarantees. To boot, performance analysis and analysis show that the FAC could be a heap of economical compared with the prevailing schemes through comprehensive experiments. For the long-term work, we would explore privacy-preserving data aggregation draw back in smart grid.

1) Disadvantages

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

F. 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 cryptographic approach, TAAC, to achieve time-domain attribute-based access management for cloud-based video content sharing. Specifically, we've projected a provably secure time-domain attribute-based cryptography theme by embedding the time into every the cipher texts and thus the keys, such only users World Health Organization hold ample attributes terribly} very specific amount can rewrite the data. to achieve the dynamic modification of users' attributes, we've collectively projected a cheap attribute amendment 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 some way to achieve access management of video contents that are ordinarily accessed in multiple time slots and therefore 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.

1) 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 merely cipher file and transfer that file on cloud. Several file are store in cloud. There's no such access policy for file that specific documented users will solely access that file. Conjointly therein system whole attribute isn't hidden solely name of attributes are hidden. This causes some security problems and conjointly a number of storage problems.

In associate economical huge knowledge access theme, knowledge owner transfers encrypted move into cloud at time of uploading it request to attribute generator for public key so upload move into cloud. Whereas uploading a file there's associate 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 wish to go looking that file Attribute bloom filter checks user matching access policy of that file and conjointly checks keyword of trapdoor looking out, if attribute of user is matched with access policy and time then Rank search result's planning to the user then user transfer solely resulted file mistreatment secret key obtaining from attribute Authority.

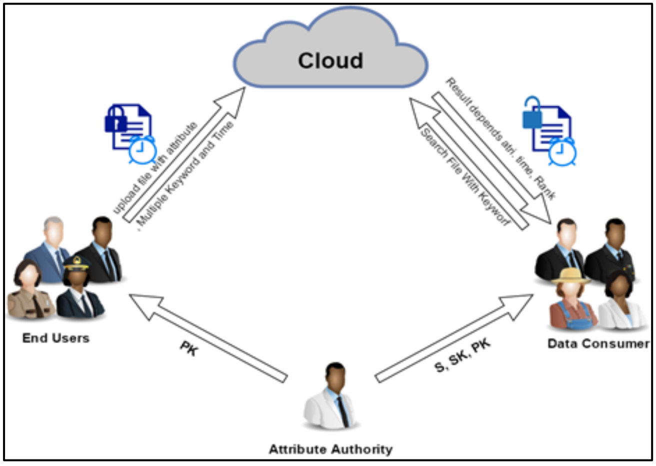
Cloud
upload file with attribute
, Multiple Keyword and Time
Result depends atri, time, Rank
Search File With Keywor
End Users
Data Consumer
PK
S, SK, PK
Attribute Authority

Fig. 1: System Architecture

A. *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,

1) Step 1: Setup (PK,MSK): The setup algorithm takes as input a security parameter l. It outputs the public key and master secret key.
2) Step 2: Key Generation (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.
3) Step 3: Encrypt(PK,m, (M,p))->(CTABF):The data encryption algorithms contains: data encryption subroutine Enc and Attribute Bloom Filter building subroutine ABFBuild

   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 ciphertext CT.

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

V. RESULTS

Fig. 2: Home

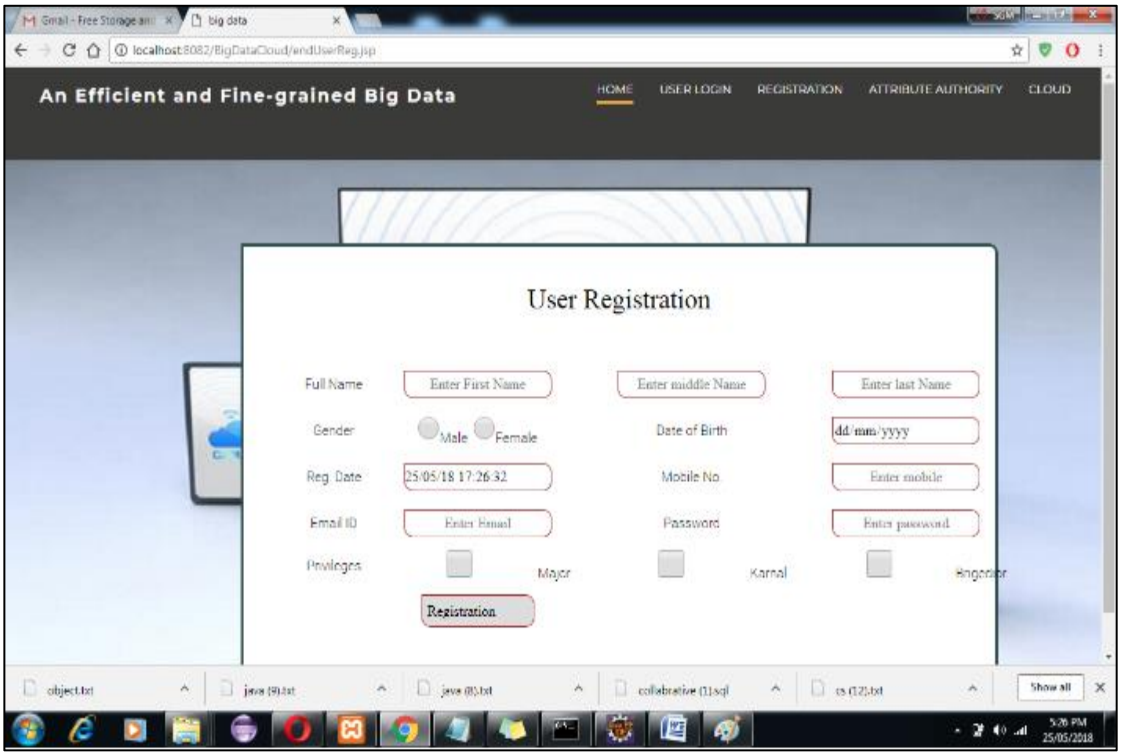

Fig. 3: User Register

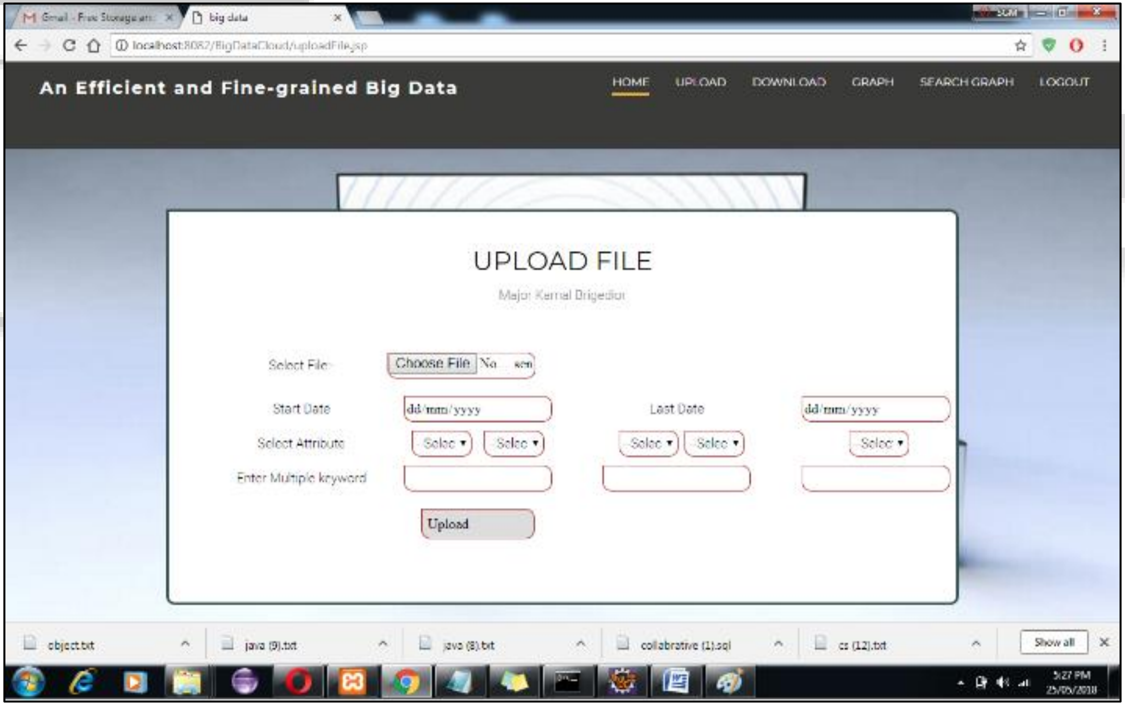

Fig. 4: File Upload

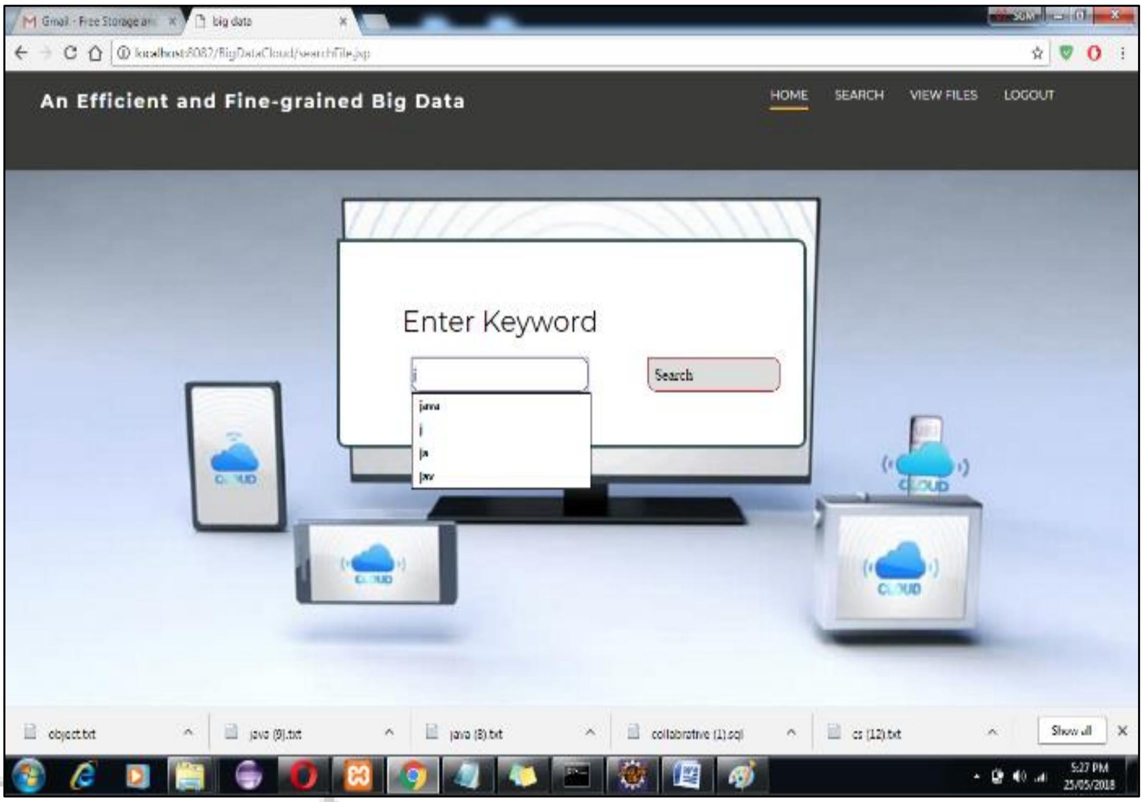

Fig. 5:

VI. Conclusion

We have projected associate economical and fine-grained knowledge access management theme for giant knowledge, wherever the access policy won't leak any privacy info. In our technique, it will hide the complete attribute (rather than solely its values) within the access policies. This could lead authentication drawback whereas user would like to transfer file. We have conjointly designed associate attribute localization rule to gauge whether or not associate attribute is within the access policy. So as to boost the potency, a completely unique Attribute Bloom Filter has been designed to find the precise row numbers of attributes within the

Access matrix. We've conjointly incontestable that our theme is by selection secure against chosen plaintext attacks. Moreover, we've enforced the ABF by victimization Murmur Hash and also the access management theme to indicate that our theme will preserve the privacy from any LSSS access policy while not using a lot of overhead. In our future work, we'll specialize in a way to wear down the offline attribute guesswork attack that check the guesswork "attribute strings" by regularly querying the ABF.

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.

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] 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.