International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)
ISSN: 2456-236X
Vol. **06** Special Issue **01** | **2021**

Secure Data Transmission: A Review

[1]Prof. Y. B Jadhao, [2]Prof. Anand A. Maha
[1,2] Assistant Professor, Department of Computer Science & Engineering,
Padm. Dr.V.B.K.C.O.E.Malkapur, Maharashtra, India

ABSTRACT

Now a day's large numbers of user uses cloud environment to store and retrieve their large amount of data over cloud so that they can access it from anywhere. As cloud is an open environment these users face lots of issue regarding their data like loss of data, privacy of users, authority of users etc. To overcome from these issues an 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

Keyword : - Big Data; Access Control; Privacy-preserving Policy; Attribute Bloom Filter; LSSS Access Structure

1. INTRODUCTION

In the era of big data, a huge amount of data can be generated quickly from various sources (e.g., smart phones, sensors, machines, social networks, etc.). Towards these big data, conventional computer systems are not competent to store and process these data. Due to the flexible and elastic computing resources, cloud computing is a natural fit for storing and processing big data. With cloud computing, end- users store their data into the cloud, and rely on the cloud server to share their data to other users (data consumers). In order to only share end-users' data to authorized users, it is necessary to design access control mechanisms according to the requirements of end-users. When outsourcing data into the cloud, end-users lose the physical control of their data. Moreover, cloud service providers are not fully-trusted by end-users, which make the access control more challenging. For example, if the traditional access control mechanisms (e.g., Access Control Lists) are applied, the cloud server becomes the judge to evaluate the access policy and make access decision. Thus, end-users may worry that the cloud server may make wrong access decision intentionally or 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 user 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. unintentionally, and disclose their data to some unauthorized users. In order to enable end-users to control the access of their own data, some attribute-based access control schemes are proposed by leveraging attribute-based encryption. In attribute-based access control, end-users first define access policies for their data and encrypt the data under these access policies. Only the users whose attributes can satisfy the access policy are eligible to decrypt the data.

In an efficient and fine-grained big data access control scheme with privacy-preserving policy. Specifically, we hide the whole attribute (rather than only its values) in the access policies. However, when the attributes are hidden, not only the unauthorized users but also the authorized users cannot know which attributes are involved in the access policy, which makes the decryption a challenging problem. To assist data decryption, we also design a novel Attribute Bloom Filter to evaluate whether an attribute is in the access policy and locate the exact position in the access policy if it is in the access policy. Security analysis and performance evaluation show that our scheme can preserve the privacy from any LSSS access policy without employing much overhead. We introduce a time server in our scheme to assign particular time with each file which is uploading on cloud. So while user uploads file on cloud particular time is associated with it.so this file is accessible to data consumer only for that specific time period then after that time files are not available for user to access.

2. LITERATURE REVIEW

A Robust, Distortion Minimization Fingerprinting Technique for Relational Database fingerprinting technique inserts the fingerprint bits subject to usability constraints. And results, minimum distortion in original data set as well as finds the guilty user who is responsible for illegal redistribution of data set. A logical extension of this research is to extend the technique on non-numeric strings data. [1]

Fingerprinting Numeric Databases with Information Preservation and Collusion Avoidance The fingerprinting technique facilitates with security against the ownership theft and a provision for traitor tracing (if any unauthorized copy is found). The insertion of fingerprint bits in numeric databases may change the numeric data to some extent. A loss of knowledge may be observed due to these changes in numeric data. Here the work in is extended by finding a novel way for inserting a fingerprint in the database along with the assurance of information preservation. The information preservation is shown in terms of effect on mean, variance and standard deviation after fingerprinting, which is found to be minuscule. [2].

Applying Watermarking For Copyright Protection, Traitor Identification and Joint Ownership: A Review scheme of watermarking relational databases for copyright protection is found. Speech signal is embedded as watermark into the relations; associated novel watermark insertion algorithm and detection algorithm are proposed. Thus, the watermark signal in this method is expected to be more meaningful and has closely related to the copyright holder. [3].

Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage
a revocable multi-authority CPABE scheme that can support efficient attribute revocation. Then, we constructed an effective data access control scheme for multi-authority cloud storage systems. We also proved that our scheme was demonstrable secure in the random oracle model. The revocable multi-authority CPABE is a technique, which can be applied in any remote storage systems and online social networks etc.[4].

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

Time-domain Attribute-based Access Control for Cloud-based Video Content Sharing: A Cryptographic Approach a cryptographic approach, TAAC, to achieve time-domain attribute-based access control for cloud-based video content sharing. Specifically, we have proposed a provably secure time-domain attribute-based encryption scheme by embedding the time into both the cipher texts and the keys, such that only users who hold sufficient attributes in a specific time period can decrypt the data. To achieve the dynamic change of users' attributes, we have also proposed an efficient attribute updating method which enables attribute authorities to grant new attributes, revoke previous attributes and re-grant previously revoked attributes to users at the beginning of each time slot. We have further discussed on how to achieve access control of video contents that are commonly accessed in multiple time slots and how to make special queries on video contents generated in previous time slots. We have provided the security proof for the proposed TAAC scheme in generic bilinear group model and random Oracle model. [6].

3. EXISTING SYSTEM

In Existing attribute-based access control schemes can deal with the attribute revocation problem, they all suffer from one problem: the access policy may leak privacy. This is because the access policy is associated with the encrypted data in plaintext form. From the plaintext of access policy, the adversaries may obtain some privacy information about the end-user. Hiding the values of attributes can somehow protect user privacy, but the attribute name may also leak private information. Moreover, most of these partially hidden policy schemes only support specific policy structures (e.g., AND- gates on multi-valued attributes).

4. PROPOSED SYSTEM

We propose an effective and big data access control scheme with privacy-preserving policy, where the whole attributes are hidden in the access policy rather than only the values of the attributes Cloud Servers Cloud Servers are employed to store, share and process big data in the system with time server. Attribute Authority: Assign attribute, and its key generation, and also grant different access privileges to End-users. End-user: End-users are the data owners/producers who outsource their data in encrypted with CP-ABE, time and with keyword store on cloud securely. Data Consumers: Data consumers request the data from cloud servers. data consumers decrypt the data.

5. SYSTEM ARCHITECTURE

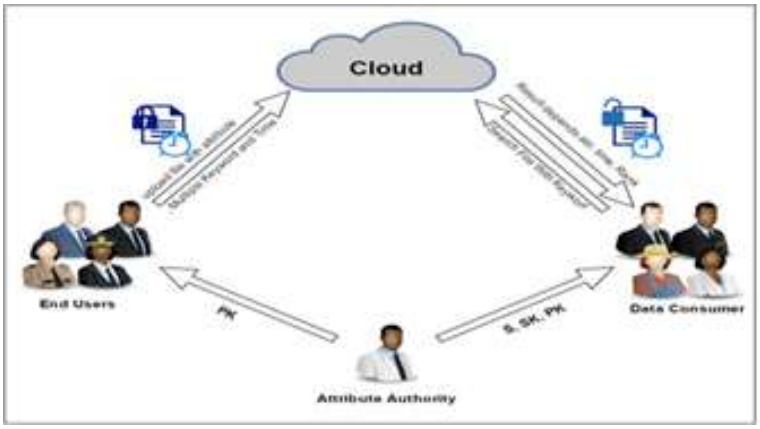

Fig -1 SYSTEM ARCHITECTURE

6. METHADOLOGY & ALGORITHMS

- We used the AES Algorithm for the Encryption format for the storing the data on cloud.
- We also used for Data sharing OTP for unauthorized access of the users.

A. AES Algorithm

- AES steps of encryption for a 128-bit block:
- Derive the set of round keys from the cipher key.
- Initialize the state array with the block data (plaintext).
- Add the initial round key to the starting state array.
- Perform nine rounds of state manipulation.
- Perform the tenth and _nal round of state manipulation.
- Copy the final state array out as the encrypted data (cipher text).

B. MD5 Algorithm

- MD5 Algorithm
- Step 1. Append Padding Bits Step 2. Append Length
- Step 3. Initialize MD Buffer
- Step 4. Process Message in 16-Word Blocks

7. 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 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.

8. REFERENCES

[1] M.Armbrust, A.Fox, R.Griffith, A.D.Joseph, R.Katz, A.Konwinski, G. Lee, D.Patterson, A.Rabkin, I.Stoica, andM.Zaharia. "A View of Cloud Computing,"Comm. ACM, vol. 53, no. 4, pp.50-58, Apr.2010.
[2] S.Kamara and K.Lauter, "Cryptographic Cloud Storage," Proc.Int'l Conf. Financial Cryptography and Data Security (FC), pp.136-149, Jan. 2010.
[3] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K.Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc.USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.
[4] E.Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.
[5] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc.
[6] Shucheng Yu, Cong Wang, Kui Ren, and Weijing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.
[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute- Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006[8] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282- 292, 2010.
[9] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008
[10] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yang, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191, June 2013