International Journal of Current Trends in Engineering & Technology
Received 1 May 2018, Received in revised form, 15 May 2018, Accepted 23 June 2018, Available online 30 June 2018
www.ijctet.org, ISSN: 2395-3152
Volume: 04, Issue: 03 (May- June, 2018)

PROFICIENT AND FINE-GRAINED HUGE DATA ACCESS MANAGE SYSTEM WITH PRIVACY- PRESERVING POLICY

P. Rohini
M. Phil Scholar, Department of computer science
Raja Doraisingam Government Arts College Sivaganga, Tamilnadu, India, rohini17.m@gmail.com;
A. Prema
Assistant professor, Department of computer science
Raja Doraisingam Government Arts College, Sivaganga, Tamilnadu, India, latharaman2012jr@mail.com;

Abstract: **-** Ciphertext Policy Attribute Based Encryption (CP-ABE) has been desired encryption knowledge to solve the stimulating difficult of secure data sharing in cloud computing. Ciphertext-Policy Attribute based Encryption (CP-ABE) is a hopeful encryption technique that enables end-users to encrypt their data under the access policies well-defined over some attributes of data consumers and only allows data customers whose attributes satisfy the access policies to decrypt the data. In CP-ABE, the arrival policy is devoted to the ciphertext in plaintext method, which may also disclosure some reserved data about users. Existing methods partially hide the attribute values in the access policies, while the attribute names are still unprotected. In this paper, we propose an efficient and fine-grained big data access control scheme with privacy-preserving policy. Specifically, we fur the entire attribute (rather than only its values) in the access policies. To contribution data decryption, we also proposal a novel Attribute Bloom Filter to assess whether an attribute is in the access policy and locate the exact location in the access policy if it is in the access policy.

Keywords: Big data, Ciphertext-Policy Attribute based Encryption (CP-ABE), cloud Server.

I. INTRODUCTION

"Big data" is a term used to describe a collection of data sets with the following three characteristics: Volume- Large amounts of data generated. Velocity- Occurrence and rapidity, of which data are generated, captured and shared. Variety-Diversity of data types and formats from various sources. (19)

The size and complexity of big data makes it difficult to use traditional database management and data processing tools. Data is being created in much shorter cycles from hours to milliseconds. There is also a trend underway to create larger databases by combining smaller data sets so that data correlations can be discovered.

It has driven the requirement for technological organization and tools that can internment, collection, analyses and imagine vast amounts of disparate structured and unstructured data (25). These data are being generated at increasing volumes from data intensive technologies including, but not limited to, the use of the Internet for activities such as accesses to information, social networking, mobile computing and commerce. Corporations and governments have begun to recognize that there are unexploited opportunities to improve their enterprises that can be discovered from these data.

Cloud computing is rising computing technology that uses Internet. It consists of the use of computing resources that are delivered as a service over a network. In cloud computing model users have to give access to their data for storing and performing the desired business operations. Hence cloud service provider must provide the trust and security (23), as there is valuable and sensitive data in huge amount stored on the clouds. There are concerns about flexible, scalable and fine grained access control in the cloud computing. Generally, among the various requirements, today's access control schemes should at least meet the following ones: 1) fine-grained access policy, 2) protection of user privacy Recently, the notion of ABE [20], has attracted much attention in the research community to design flexible and scalable access control systems. For the first time, ABE enables public key based one-to-many encryption. Therefore, it is envisioned as a highly hopeful public key primitive for realizing scalable and fine grained access control systems, where deferential yet flexible access rights can be assigned to individual users. To address composite and common access policy, two kinds of ABE have been proposed: key-policy ABE (KP-ABE) and cipher text-policy ABE (CP-ABE). In KP-ABE, access policy is assigned in attribute private key, whereas, in CP-ABE, the access policy is specified in the cipher text.

II. CIPHER TEXT POLICY ATTRIBUTE BASED ENCRYPTION

Introduced the thought of another changed form of ABE called CP-ABE that is Cipher text Policy Attribute Based Encryption. In CP-ABE scheme (22), attribute policies are related with data and attributes are associated with keys and only those keys that the associated attributes satisfy the policy associated with the data are able to decrypt the data. CP-ABE works in the reverse way of KP-ABE. In CP-ABE the cipher text is associated with an access tree structure and each user secret key is embedded with a set of attributes (3). In ABE, including KP-ABE and CP-ABE, the ability runs the algorithm Setup and Key Generation to produce system MK, PK, and user secret keys. Only accredited users (i.e., users with intended access arrangements) are able to decrypt by calling the algorithm Decryption (7). In CP-ABE, each user is associated with a set of attributes. His secret key is created based on his attributes. While encrypting a message, the encrypted

International Journal of Current Trends in Engineering & Technology
Received 1 May 2018, Received in revised form, 15 May 2018, Accepted 23 June 2018, Available online 30 June 2018
www.ijctet.org, ISSN: 2395-3152
Volume: 04, Issue: 03 (May- June, 2018)

or specifies the edge access structure for his interested attributes. This message is then encrypted based on this access arrangement such that only those whose attributes satisfy the access arrangement can decrypt it.

With CP-ABE technique, encrypted data can be kept confidential and secure against collusion attacks CP -ABE scheme consists of following algorithms: (9)

- **Setup** → (PK, MSK). The setup algorithm precedes as input a safety restriction λ, its outputs the public key and master secret key.
- **KeyGen** (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.
- **Encrypt** (PK, m, (M, ρ)) → (CT, ABF). The data encryption algorithms contains: Data encryption subroutine Enc and Attribute Bloom Filter building subroutine ABFBuild.
  - ❖ **Enc** (PK, m, (M, ρ)) →CT. The data encryption Subroutine takes as inputs the public key PK, the dispatch m and entrance structure (M, ρ). It outputs a ciphertext CT.
  - ❖ **ABFBuild** (M, ρ) → ABF. The ABF structure subroutine takes as input the entrance policy (M, ρ). It outputs the Attribute Bloom Filter ABF.
- **Decrypt** (M, ABF, PK, SK, CT) → m.The decryption algorithm contains of two subroutines: ABFQuery and Dec.
  - ❖ **ABFQuery**(S, ABF, PK) → ρ0. 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 ρ0 = {(rownum, att)} S, which shows the corresponding row number in the access matrix M for all the attributes att ∈ S.
  - ❖ **Dec** (SK, CT, (M, ρ0)) → m or ⊥. The statistics decryption algorithm takes as inputs the secret key SK, the ciphertext CT as well as the entrance matrix M and the restored attribute mapping ρ0. If the attributes can satisfy the access policy, it outputs the message m. Otherwise, it outputs ⊥.

III. MOVING BIG DATA INTO CLOUD

Big Data is a data exploration methodology enabled by modern improvements in technologies and architecture. However, massive data entails a massive commitment of hardware and processing properties, making reception costs of massive data technology prohibitive to small and medium sized businesses (21). Cloud computing offers the assurance of huge data implementation to small and medium sized businesses.

Big Data processing is performed through a programming paradigm known as Map Reduce. Typically, implementation of the Map Reduce paradigm requires networked attached storage and similar processing (17). The computing requirements of Map Reduce programming are often outside what small and medium sized business are able to commit.

The defector approach of hard drive shipping is not flexible or secure. This effort reviews suitable, cost-decreasing upload of huge, dynamically generated, geo dispersed data into the cloud, for processing using a Map Reduce-like framework(4). Difficult at a cloud with different statistics centres, we classical a cost-minimizing data association problem, and propose two online algorithms: an online lazy migration (OLM) algorithm and a randomized fixed horizon control (RFHC) algorithm, for enhancing at any given time the choice of the data centre for statistics aggregation and processing, as well as the routes for transmitting data there. Careful appraisals among these connected and disconnected algorithms in accurate sets are accompanied through extensive experiments, which demonstrate close-to-offline-optimum performance of the online algorithms.

TABLE-I Difference between security and privacy (8)

S. No	Security	Privacy
1.	It is the "confidentiality, integrity and availability" of data	It is the appropriate use of user's information
2.	It may provide for confidentiality or to protect an enterprise	It concerns with consumer's right to safeguard their information from any other parties
3.	Various techniques like Encryption, Firewall etc. are used in order to inhibit data concession from technology or liabilities in the network of an organization	The organization can't sell its customer/user's information to a third party without prior consent of user
4.	It offers the ability to be confident that decisions are respected	It is the ability to decide what information of an individual goes

IV.PROPOSED SYSTEM

The aim of this paper is to hide the whole attribute instead of only partially hiding the attribute values. Moreover, we do not restrict our method to some specific access structures. The basic idea is to express the access policy in LSSS access structure.

- Without the attribute matching function r, it is necessary to design an attribute localization algorithm to evaluate whether an attribute is in the

International Journal of Current Trends in Engineering & Technology
Received 1 May 2018, Received in revised form, 15 May 2018, Accepted 23 June 2018, Available online 30 June 2018
www.ijctet.org, ISSN: 2395-3152
Volume: 04, Issue: 03 (May- June, 2018)

access policy and if so find the correct position in the access policy.

- To this end, we promote build a novel Attribute Bloom Filter to locate the attributes to the anonymous access policy, which can save a lot of storage overhead and computation cost especially for large attribute universe.

This following picture shows the structural design for proposed work

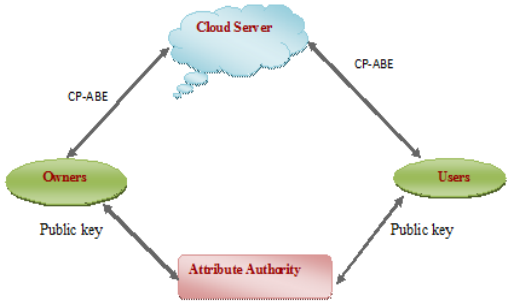

Figure 1- Methodology for proposed work

Definition of System Model

We consider the big data access control system, as shown in Fig. 1. The system consists of five entities, namely Cloud Servers, Attribute Authority, End-users, and Data Consumers.

Cloud Servers Cloud Servers are employed to store, share and process big data in the system. The cloud servers are managed by cloud service providers, who are not in the same trust domain as end-users. Thus, cloud servers cannot be trusted by end-users to enforce the access policy and make access decisions. We also assume that the cloud server cannot collude with any End-users or Data Consumers.

Attribute Authority The attribute authority manages all the attributes in the system and assigns attributes chosen from the attribute space to end-users. It is also a key generation centre, where the public parameters are generated. It also grants different access privileges to end-users by issuing secret keys according to their attributes. The attribute authority is assumed to be fully trusted in the system.

User, they are the data owners/producers who outsource their data into the cloud. They also would like to mechanism the entrance of their data by encrypting the data with CP-ABE. End-users are assumed to be honest in the system.

Owner request the data from cloud servers. Only when their aspects can satisfy the access policies of the data, data consumers can decrypt the data. However, data consumers may try to conspire together to access some data that are not manageable individually.

V. LITERATURE SURVEY

R. Lu, H. Zhu, X. Liu, J. K. Liu, and J. Shao in **Toward efficient and privacy-preserving computing in big data era** (16) Big data, because it can mine new knowledge for economic growth and technical innovation, has recently received considerable attention, and many research efforts have been directed to big data processing due to its high volume, velocity, and variety (referred to as "3V") challenges. In addition to the 3V challenges, the successful of big data also hinges on fully understanding and managing recently arise security and privacy challenges. If data are not authentic, new mined knowledge will be unimpressive; while if privacy is not well addressed, people may be reluctant to share their data. Because security has been investigate as a new dimension, "veracity," in huge data, in this article, we aim to exploit new challenges of big data in terms of privacy, and assign our attention toward efficient and privacy-preserving compute in the big data era. Specifically, we first make official the common architecture of big data analytics, identify the corresponding privacy requirements, and introduce an efficient and privacy-preserving cosine similarity computing protocol as an example in response to data mining's efficiency and privacy necessities in the big data era.

Brent Waters presented **Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization** (20) we present a new method for realize Ciphertext-Policy Attribute Encryption (CPABE) under concrete and non interactive cryptographic assumption in the standard model. Our solutions allow any encryption to identify access control in terms of any access formula over the attribute in the system. In our most capable system, ciphertext size, encryption, and decryption time scales linearly with the complication of the access formula. The only previous work to achieve this parameter was limited to a proof in the generic group model. We present three constructions within our framework. Our initial system is verified selectively secure below an assumption that we call the decisional Parallel Bilinear Diffie-Hellman Exponent (PBDHE) assumption which can be viewed as a generalization of the BDHE assumption. Our then two constructions present performance tradeoffs to reach provable security respectively under the (weaker) decisional Bilinear-Diffie-Hellman Exponent and decisional Bilinear Diffie-Hellman assumptions.

H. Lin, Z. Cao, X. Liang, and J. Shao **Secure Threshold Multi Authority Attribute Based Encryption without a Central Authority**(15) An attribute based encryption scheme (ABE) is a cryptographic primitive in which every user is identified by a set of attributes, and some function of these attributes is used to determine the ability to decrypt each ciphertext. Chase planned the first multi authority ABE scheme in TCC 2007 as an answer to an open difficulty on hand by Sahai and Waters in EUROCRYPT 2005. However, her scheme needs a fully trust essential authority which can decrypt every

International Journal of Current Trends in Engineering & Technology
Received 1 May 2018, Received in revised form, 15 May 2018, Accepted 23 June 2018, Available online 30 June 2018
www.ijctet.org, ISSN: 2395-3152
Volume: 04, Issue: 03 (May- June, 2018)

ciphertext in the system. This central authority would endanger the whole system if it's tainted. This paper presents a threshold multi authority fuzzy identity based encryption (MA-FIBE) scheme without a central authority for the first time. An encrypter can encrypt a message such that a user could only decrypt if he has at least dk of the given attributes about the message for at least $t+1$, $t \leq n/2$ honest authorities of all the n attribute authorities in the proposed scheme (17). The security proof is based on the secrecy of the underlying joint random secret sharing protocol and joint zero secret sharing protocol and the standard decisional bilinear Diffie-Hellman assumption. The proposed MA-FIBE could be extended to the threshold multi authority attribute based encryption (MA-ABE) scheme and be further extended to a proactive MA-ABE scheme.

T. Nishide, K. Yoneyama, and K. Ohta **Attribute-Based Encryption with Partially Hidden Encryptor-Specified Access Structures** (18) we propose attribute-based encryption schemes where encryptor-specified access structures (also called ciphertext policies) are hidden. By using our schemes, an encryptor can encrypt data with a hidden access structure. A decryptor obtains her secret key associated with her attributes from a trusted authority in advance and if the attributes associated with the decryptor's secret key do not satisfy the access structure associated with the encrypted data, the decryptor cannot decrypt the data or guess even what access structure was specified by the encryptor. We prove security of our construction based on the Decisional Bilinear Diffie-Hellman assumption and the Decision Linear assumption. In our security notion, even the legitimate decryptor cannot obtain the information about the access structure associated with the encrypted data more than the fact that she can decrypt the data.

J. Li, K. Ren, B. Zhu, and Z. Wan **Privacy-aware attribute-based encryption with user accountability** (12) a new public key primitive, attribute-based encryption (ABE) is envisioned to be a promising tool for implementing fine-grained access control. To further address the concern of user access privacy, privacy-aware ABE schemes are being developed to achieve hidden access policy recently. For the purpose of secure access control, there is, however, still critical functionality missing in the existing ABE schemes, which is user accountability. Currently, no ABE scheme can completely prevent the problem of illegal key sharing among users. In this paper, we tackle this problem by firstly proposing the notion of accountable, anonymous, and ciphertext-policy ABE (CP-A3BE, in short) and then giving out a concrete construction. We start by improving the state-of-the-art of anonymous CP-ABE to obtain shorter public parameters and ciphertext length. In the proposed CP-A3BE construction, user accountability can be achieved in black-box model by embedding additional user-specific information into the attribute private key issued to that user, while still maintaining hidden access policy. The proposed constructions are provably secure.

VI. IMPLEMENTATION

The picture represents Encrypt and Decrypt of Existing work

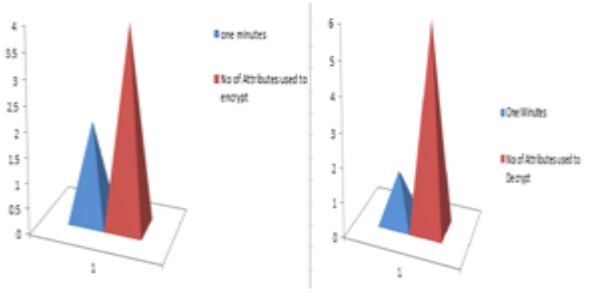

Fig-2 CP-ABE Encrypt and Decrypt of existing work (8)

Table-2 Upload Files

ID	FILE NAME	DESCRIPTION	DATE&TIME	ACCESS POLICY	GRAPH
1	Java	This file based on java language	2017.08.29 12:20:02:0	Software Developer	View
2	Java script	This file based on java script	2017.08.29 12:21:06:0	Software Developer	View
3	PHP	This files contains the basics of PHP	2017.08.29 12:21:44:0	Software Developer	View
4	Tablets Details	This is about the tablets name and uses	2017.08.29 12:24:45:0	Doctor	View
5	Students Mentality	This files explains about students mentality	2017.08.29 12:26:32:0	Professor	View

Based on the diagram time taken for encrypt and decrypt process of proposed is less than existing system

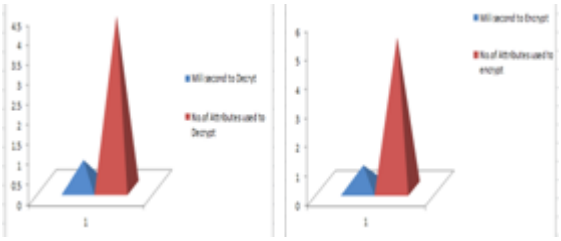

Figure-3 CP-ABE Encrypt and Decrypt of proposed work

CONCLUSION

In this paper, 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. Different from the existing methods which only partially hide the attribute values in the access policies, our method can hide the whole attribute (rather than only its values) in the access policies. However, this may lead to great challenges and difficulties for legal data consumers to decrypt data. To manage with this problem, we have also intended an attribute localization algorithm to appraise 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 confirmed that our scheme is selectively safe against chosen plaintext outbreaks. 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 disconnected attribute estimating attack that check the guessing "attribute strings" by constantly querying the ABF.

REFERENCE

[1]. A. Beimel, "Secure schemes for secret sharing and key Technion Haifa, Israel, 1996.
[2]. B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," Communications of the ACM, vol. 13, no. 7, pp. 422–426, 1970.
[3]. D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Theory of cryptography. Springer, 2007, pp.535– 554.
[4]. C. Dong, L. Chen, and Z. Wen, "When private set intersection meets big data: an efficient and scalable protocol," in Proc. of CCS'13. ACM, 2013, pp. 789– 800.
[5]. K. Frikken, M. Atallah, and J. Li, "Attribute-based access control with hidden policies and hidden credentials," IEEE Trans. On Computers, vol. 55, no. 10, pp. 1259–1270, 2006.
[6]. J. Hur, "Attribute-based secure data sharing with hidden policies in smart grid," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 11, pp.2171–2180, 2013.
[7]. J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in Advances in Cryptology EUROCRYPT'08. Springer, 2008, pp. 146–162.
[8]. J. Lai, R. H. Deng, and Y. Li, "Expressive cp-abe with partially hidden access structures," in Proc. of ASIACCS'12. ACM, 2012, pp.18–19.
[9]. J. Lai, R. H. Deng, and Y. Li, "Fully secure cipertext-policy hiding cpabe," in Information Security Practice and Experience. Springer, 2011, pp. 24–39.
[10]. L. Lei, Z. Zhong, K. Zheng, J. Chen, and H. Meng, "Challenges on wireless heterogeneous networks for mobile cloud computing," IEEE Wireless Communications, vol. 20, no. 3, pp. 34–44, 2013.
[11]. 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.
[12]. J. Li, K. Ren, B. Zhu, and Z. Wan, "Privacy-aware attribute-based encryption with user accountability," in Information Security. Springer, 2009, pp. 347– 362.
[13]. H. Li, D. Liu, Y. Dai, and T. H. Luan, "Engineering searchable encryption of mobile cloud networks: when qoe meets qop," IEEE Wireless Communications, vol. 22, no. 4, pp. 74–80, 2015.
[14]. H. Li, Y. Yang, T. Luan, X. Liang, L. Zhou, and X. Shen, "Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data," IEEE Trans. on Dependable and Secure Computing [DOI: 10.1109/TDSC.2015.2406704], 2015.
[15]. H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," in Proc. of INDOCRYPT, 2008. Springer, 2008, pp. 426–436.
[16]. R. Lu, H. Zhu, X. Liu, J. K. Liu, and J. Shao, "Toward efficient and privacy-preserving computing in big data era," IEEE Network, vol. 28, no. 4, pp. 46– 50, 2014.
[17]. P. Mell and T. Grance, "The NIST definition of cloud computing," [Recommendations of the National Institute of Standards and Technology Special Publication 800-145], 2011.
[18]. T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," in applied cryptography and network security. Springer, 2008, pp. 111–129.
[19]. Z. Su, Q. Xu, and Q. Qi, "Big data in mobile social networks: a qoeoriented framework," IEEE Network, vol. 30, no. 1, pp. 52–57, 2016.
[20]. B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. of PKC'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 53–70.
[21]. K. Yang, X. Jia, and K. Ren, "Secure and verifiable policy update outsourcing for big data access control in the cloud," IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 12, pp. 3461–3470, Dec 2015.
[22]. 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.
[23]. 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.
[24]. S. Yu, K. Ren, and W. Lou, "Attribute-based content distribution with hidden policy," in Secure Network Protocols (NPSec'08 Workshop).IEEE, 2008, pp. 39–44.
[25]. K. Zheng, Z. Yang, K. Zhang, P. Chatzimisios, K. Yang, and W. Xiang, "Big data-driven optimization for mobile networks toward 5g," IEEE Network, vol. 30, no. 1, pp. 44–51, 2016.