A Secure Encryption Scheme for Data Sharing in unreliable cloud Environment

Bhushan Patil, Gajanan Kuntewad, Imran Shaikh, Siddesh Rane, Prof. R. S. Gute
Sinhgad Technical Education Society Skn Sinhgad Institute Of Technology & Science

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.

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 it 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 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 efcient and ne-grained big data access control scheme with privacy-preserving policy. Specically, 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 les are not available for user to In improved Cipher text policy attribute base encryption scheme, as our scheme is an efficient encryption scheme and also file is upload on cloud with its attribute access policy and encrypted file upload on cloud. Our scheme also hide whole attribute of file and upload encrypted attributed on cloud so safety of file store on cloud are ensure. Attribute authority in our scheme generate public key while uploading file on cloud and also provides secret key of file for downloading file from cloud. Our scheme also provide multi keyword rank search, in this scheme while uploading file on cloud user enter multiple keyword while uploading file so that when consumer want search file then result is exact matching to consumers keyword. Also while uploading file time server in our scheme assign time duration with file so that file is accessible to user only for that particular time period after time expire files are not display to user or not accessible. Data consumer of cloud enter keyword and attribute of file to search require file on cloud and consumer get to rank file and after entering secret key of file user can download that file and decrypt file In scheme overview, we get the proper system for storing and accessing. Data owner of cloud store their files in cloud and generate access policy of files according to attribute and then upload file on cloud after receiving keys from Attribute authority. User want to download file from cloud then attribute bloom filter first match attributes of users with files attribute and also check user according to access policy. Data file on cloud are uploaded with access policy and time specified with that file for proper search and access also for providing an efficient results to user.

2. Proposed System:

In improved Cipher text policy attribute base encryption scheme, as our scheme is an efficient encryption scheme and also file is upload on cloud with its attribute access policy and encrypted file upload on cloud. Our scheme also hide whole attribute of file and upload encrypted attributed on cloud so safety of file store on cloud are ensure. Attribute authority in our scheme generate public key while uploading file on cloud and also provides secret key of file for downloading file from cloud. Our scheme also provide multi keyword rank search, in this scheme while uploading file on cloud user enter multiple keyword while uploading file so that when consumer want search file then result is exact matching to consumers keyword. Also while uploading file time server in our scheme assign time duration with file so that file is accessible to user only for that particular time period after time expire les are not display to user or not accessible

3. Motivation of the Project:

We are motivated from the drawbacks of existing system. The existing techniques on is only encrypt file and upload that file on 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 cause some security issues and also some of storage issues.

4. Literature Survey:

1. Paper Name: Efficient and Fine-grained Big Data Access Control Scheme with Privacy-preserving Policy

Author Name: K. Yang and X. Jia, Expressive,

The 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. To assist data decryption, and 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[1]. An expressive, efficient and revocable data access control scheme for multi-authority cloud storage systems, where there are multiple authorities co-exist and each authority is able to issue attributes independently. Specifically, and also a revocable multi-authority CP-ABE scheme, and apply it as the underlying techniques to design the data access control scheme. And also attribute revocation method can efficiently achieve both forward security and backward security. The analysis and simulation results demonstrate the data access control scheme is secure in the random oracle model and is more efficient than previous works[2].

2. Paper Name: Time-domain attribute-based access control for cloud-based video content sharing: A cryptographic approach,

Author Name: K. Yang, Z. Liu, X. Jia, and X. S. Shen,

How to securely share text contents to a certain group of people during a particular time period in cloud-based web application, and propose a cryptographic approach, a provably secure time domain attribute-based access control (TAAC) scheme, to secure the cloud-based text content sharing. Specifically, firstly proposed a provably secure time-domain attribute-based encryption scheme by embedding the time into both the ciphertexts and the keys, such that only users who hold sufficient attributes in a specific time slot can decrypt the text file contents, and also propose an efficient attribute updating method to achieve the dynamic change of users attributes, including granting new attributes, revoking previous attributes, and regranting previously revoked attributes. And how to control those text file contents that can be commonly accessed in multiple time slots and how to make special queries on text file contents generated in previous time slots. The security analysis and performance evaluation show that TAAC is provably secure in generic group model and efficient in practice[3].

3. Paper Name: Enabling negrained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data

Author Name: H. Li, Y. Yang, T. Luan, X. Liang, L. Zhou, and X. Shen,

Developing the fine-grained multi-keyword search schemes over encrypted cloud data are three-fold. First, the relevance scores and preference factors upon keywords which enable the precise keyword search and personalized user experience. Second, a practical and very efficient multi-keyword search scheme. The proposed scheme can support complicated logic search the mixed AND, OR and NO operations of keywords. Third, the classified sub-dictionaries technique to achieve better efficiency on index building, trapdoor generating and query. Lastly, we analyze the security of the proposed schemes in terms of confidentiality of documents, privacy protection of index and trapdoor, and unlinkability of trapdoor. Through extensive experiments using the real-world dataset, we validate the performance of the proposed schemes. Both the security analysis and experimental results demonstrate that the proposed schemes can achieve the same security level comparing to the existing ones and better performance in terms of functionality, query complexity and efficiency [4].

4. Paper Name: Attribute-based access control with hidden policies and hidden credentials,

Author Name: K. Frikken, M. Atallah, and J. Li,

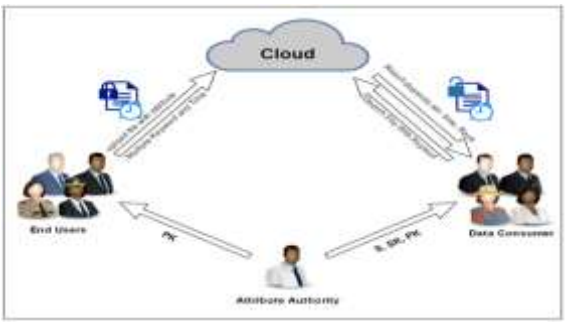
Attribute-Based Access Control with Hidden Policies and Hidden Credentials, present protocols that protect both sensitive credentials and sensitive policies. That is, Alice gets the resource only if she satisfies the policy, Bob does not learn anything about Alices credentials (not even whether Alice got access), and Alice learns neither Bobs policy structure nor which credentials caused her to gain access. And the protocols are efficient in terms of communication and in rounds of interaction [5].

5. Paper Name: Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,

Author Name: B. Waters,

Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization, create a method for directly embedding any LSSS structure M* into the public parameters in our reduction. In the proofs of this system a simulator can program" the LSSS matrix M* of the challenge ciphertext (in the selective model of security) [6].

5. Architecture Diagram:



6. Mathematical Model:

1. Let S be a system. S=I,O,P,F,s,Ic

2. Identify set of input as I

Let I =Set of outsourced data sets by corresponding data user

3. Identify set of output as O

Let O=Securely data sharing with group participant and remove malicious user

from group through Attribute Authority

4. Identify the set of processes as P

P=AA,B,V,K, S, SK, PK,S

AA=Attribute Authority

B=Set of Files.

V=No of Data Consumer.

K=.Key Agreement.

SK- Secrete Key

PK = Public Key

5. Identify failure cases as F

F=share data to malicious user in group.

6. Identify success as s.

s=share data in group and give private key to all Data consumer

7. Algorithm:

AES steps of encryption for a 128-bit block:

1. Derive the set of round keys from the cipher key.

2. Initialize the state array with the block data (plaintext).

3. Add the initial round key to the starting state array.

4. Perform nine rounds of state manipulation.

5. Perform the tenth and final round of state manipulation.

6. Copy the final state array out as the encrypted data (ciphertext).

MD5 Algorithm

Step 1. Append Padding Bits

Step 2. Append Length

Step 3. Initialize MD Buffer

Step 4. Process Message in 16-Word Blocks

8. Conclusion:

In this paper 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.

References:

[1] Kan Yang, Qi Han, Hui Li, Kan Zheng, Zhou Su, Xuemin (Sherman) Shen An Efficient and Fine-grained Big Data Access Control Scheme with Privacy-preserving Policy, DOI 0.1109/JIOT.2016.2571718, IEEE Internet of Things Journal.

[2] 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. 17351744, July 2014.

[3] 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.

[4] H. Li, Y. Yang, T. Luan, X. Liang, L. Zhou, and X. Shen, Enabling ne grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data, IEEE Trans. on Dependable and seecure Computing [DOI:10.1109/TDSC.2015.2406704], 2015.

[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. 12591270, 2006.

[6] B. Waters, Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization, in Proc. of PKC11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 5370.

[7] ArtiMohanpurkar, Madhuri Joshi Fingerprinting Numeric Databases with Information Preservation and Collusion Avoidance Volume 130 No.5, November2015