PRIVACY-PRESERVING DATA ENCRYPTION STRATEGY FOR BIG DATA IN MOBILE CLOUD COMPUTING

[1] Ms. V.Kanmani , [2] Ms. K.P.Nandhini , [3] Ms. S.Swetha

1. Department of Computer Science and Engineering,

Vivekanandha College of Engineering for Women,
Tiruchengode - 637205.
bhavyasan44@gmail.com

2. Department of Computer Science and Engineering,

Vivekanandha College of Engineering for Women,
Tiruchengode - 637205.
nandhininishok@gmail.com

3. Department of Computer Science and Engineering,

Vivekanandha College of Engineering for Women,
Tiruchengode - 637205.
swethasanjay12@gmail.com

CORRESPONDING AUTHOR:
Mr.P.RAMESH, M.E.,(Ph.D)
Assistant Professor, Vivekanandha College of Engineering for Women,
Tiruchengode-637205
Email: pramesh.swami@gmail.com
Contact: 7708197090

ABSTRACT

Privacy has become a considerable issue when the applications of big data are dramatically growing in cloud computing. The benefits of the implementation for these emerging technologies have improved or changed service models and improve application performances in various perspectives. However, the remarkably growing volume of data sizes has also resulted in many challenges in practice. The execution time of the data encryption is one of the serious issues during the data processing and transmissions. Many current applications abandon data encryptions in order to reach an adoptive performance level companioning with privacy concerns. In this paper, we concentrate on privacy and propose a novel data encryption approach, which is called Dynamic Data Encryption Strategy (D2ES). Proposed approach aims to selectively encrypt data and use privacy classification methods under timing constraints. This approach is designed to maximize the privacy protection scope by using a selective encryption strategy within the required execution time requirements.

1. INTRODUCTION

Big data refers to high volume, high velocity, and/or high variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization. Due to its high volume and complexity, it becomes difficult to process big data using on-hand database management tools. An effective option is to store big data in the cloud, as the cloud has capabilities of storing big data and processing high volume user access requests in an efficient way. When hosting big data into the cloud, the data security becomes a major concern as cloud servers cannot be fully trusted by data owners. Attribute-Based Encryption (ABE) has emerged as a promising technique to ensure the end-to-end data security in cloud storage system.

It allows data owners to define access policies and encrypt the data under the policies, such that only users whose attributes satisfying these access policies can decrypt the data. When more and more organizations and enterprises outsource data into the cloud, the policy updating becomes a significant issue as data access policies may be changed dynamically and frequently by data owners. However, this policy updating issue has not been considered in existing attribute-based access control schemes to transfer the data back to the local site from the cloud, encrypt the data under the new access policy, and then move it back to the cloud server. By doing so, it incurs a high communication overhead and heavy computation burden on data owners. This motivates us to develop a new method to outsource the task of policy updating to cloud server.

The grand challenge outsourcing policy updating to the cloud is to guarantee the following requirements:

Correctness: Users who possess sufficient attributes should still be able to decrypt the data encrypted under new access policy by running the original decryption algorithm. Completeness: The policy updating method should be able to update any type of access policy.

Security: The policy updating should not break the security of the access control system or introduce any new security problems.

The policy updating problem has been discussed in key policy structure and cipher textpolicy structure Our scheme can not only satisfy all the above requirements, but also avoid the transfer of encrypted data back and forth and minimize the computation work of data owners by making full use of the previously encrypted data under old access policies in the cloud. The contributions of this paper include:

1. We formulate the policy updating problem in ABE systems and develop a new method to outsource the policy updating to the server.
2. We propose an expressive and efficient data access control scheme for big data, which enables efficient dynamic policy updating.
3. We design policy updating algorithms for different types of access policies, e.g., Boolean Formulas, LSSS Structure and Access Tree.

2. MODULES AND ITS DESCRIPTION

A) ADMIN MODULE

The admin module in our project manages the account information about the data owner. The admin only have the authorization to create new data owners.

B) CO-ORDINATOR MODULE

The process carried on this module is to provide a global service between the brokers and the database. The coordinator gets the query from the brokers in an encrypted manner.

C) BROKER MODULE

In this module, the broker performs the role who can act between the Co-coordinator and the data Users. The request which is all submitted from the data user will be verified and thus it will be passed to the co-coordinator.

D) ENCRYPTION MODULES

The first module in this project is file encryption module. This module is designed for encrypt the file before outsourcing the file into cloud service providers. The encryption process done by the dynamic data owner to prevent their data from the unauthorized users.

E) FILE UPLOAD MODULE

Transferring data from one remote system to another under the control of a local system is remote uploading. Remote uploading is used by some online file hosting services.

3. EXISTING SYSTEM

When hosting big data into the cloud, the data security becomes a major concern as cloud servers cannot be fully trusted by data owners. When more and more organizations and enterprises outsource data into the cloud, the policy updating becomes a significant issue as data access policies may be changed dynamically and frequently by data owners. However, this policy updating issue has not been considered in existing attribute-based access control schemes. The policy updating is a difficult issue in attribute-based access control systems, because once the data

owner outsourced data into the cloud, it would not keep a copy in local systems. When the data owner wants to change the access policy, it has to transfer the data back to the local site from the cloud, re encrypt the data under the new access policy, and then move it back to the cloud server. Attribute-Based Encryption (ABE) has emerged as a promising technique to ensure the end-to-end data security in cloud storage system. It allows data owners to define access policies and encrypt the data under the policies, such that only users whose attributes satisfying these access policies can decrypt the data. ii. The policy updating problem has been discussed in key policy structure and cipher text-policy structure. Firstly, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted due to the users' loss control of data under Cloud Computing. Therefore, verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data. Secondly, Cloud Computing is not just a third party data warehouse. The data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, reordering, etc. To ensure storage correctness under dynamic data update is hence of paramount importance.

3.1DRAWBACKS OF EXISTING SYSTEM

These techniques, while can be useful to ensure the storage correctness without having users possessing data, cannot address all the security threats in cloud data storage, since they are all focusing on single server scenario and most of them do not consider dynamic data operations. Incurs a high communication overhead and heavy computation burden on data owners. When more and more organizations and enterprises outsource data into the cloud, the policy updating becomes a significant issue as data access policies may be changed dynamically and frequently by data owners. However, this policy updating issue has not been considered in existing attribute-based access control schemes. Key policy structure and cipher text-policy structure cannot satisfy the completeness requirement, because they can only delegate key/cipher text with a new access policy that should be more restrictive than the previous policy. Furthermore, they cannot satisfy the security requirement either.

4. PROPOSED SYSTEM

Big data refers to high volume, high velocity, and/or high variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization. Attribute-Based Encryption (ABE) has emerged as a promising technique to ensure the end-to-end data security in cloud storage system. It allows data owners to define access policies and encrypt the data under the policies, such that only users whose attributes satisfying these access policies can decrypt the data. We focus on solving the policy updating problem in ABE systems, and propose a secure and verifiable policy updating outsourcing method. Instead of retrieving and re-encrypting the data, data owners only send policy updating queries to cloud server, and let cloud server update the policies of encrypted data directly, which means that cloud server does not need to decrypt the data before/during the policy updating. Our scheme can not only satisfy all the above requirements, but also avoid the transfer of encrypted data back and forth and minimize the computation work of data owners by making full use of the previously encrypted data under old access policies in the cloud. The contributions of this project include:

i. We formulate the policy updating problem in ABE systems and develop a new method to outsource the policy updating to the server.

ii. We propose an expressive and efficient data access control scheme for big data, which enables efficient dynamic policy updating.

iii. We design policy updating algorithms for different types of access policies, e.g., Boolean Formulas, LSSS Structure and Access Tree.

iv. To formulate the policy updating problem in ABE systems and develop a new method to outsource the policy updating to the server.

v. To propose an expressive and efficient data access control scheme for big data, which enables efficient dynamic policy updating?

vi. To design policy updating algorithms for different types of access policies, e.g., Boolean Formulas, LSSS Structure and Access Tree.

vii. To propose an efficient and secure policy checking method that enables data owners to check whether the cipher texts have been updated correctly by cloud server.

4.1 ADVANTAGES

The Attribute based access control has a rich set of features. It includes;

a. Policy checking entity free

b. Storage Efficiency

c. Dynamic policies but same keys

d. Efficient and secure policy checking

e. Cipher text updating by their own secret keys and checking keys issued by each authority. Our method can also guarantee data owners cannot use their secret keys to decrypt any cipher texts encrypted by other data owners, although their secret keys contain the components associated with all the attributes.

i. More performance evaluation on policy updating algorithms and the policy checking method.

ii. This scheme can not only satisfy all the above requirements, but also avoid the transfer of encrypted data back and forth and minimize the computation work of data owners by making full use of the previously encrypted data under old access policies in the cloud. iii. This method does not require any help of data users, and data owners can check the correctness of the cipher text updating by their own secret keys and checking keys issued by each authority.

This method can also guarantee data owners cannot use their secret keys to decrypt any cipher texts encrypted by other data owners.

5. ARCHITECTURE DIAGRAM

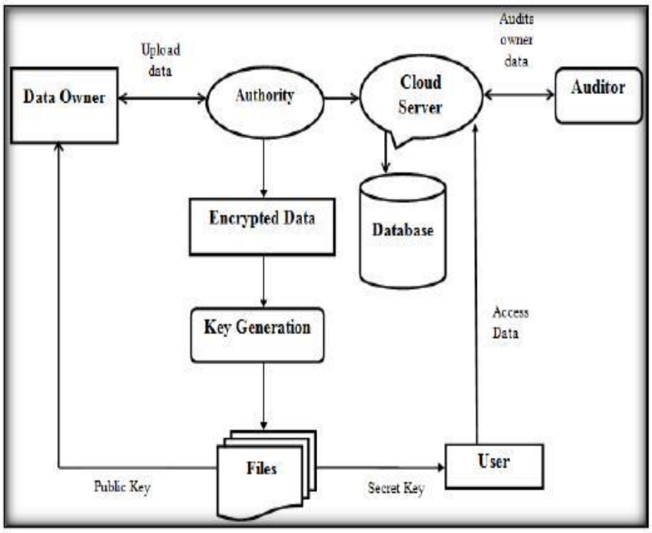

Figure 5.1: Encryption process

A policy updating algorithm for access policies known as LSSS that allows data owner to check whether the cloud server has updated the cipher texts correctly. The analysis shows that our policy updating outsourcing scheme is correct, complete, secure and efficient. The data owner sends a Checking Challenge to the cloud server. Then, the cloud server sends back a Checking Proof to the data owner. Upon receiving the proof, the data owner verifies the correctness of the proof from the cloud server. If the proof is correct, it means the cloud server has updated the cipher text correctly.

6.REVIEW'S OF PRIVACY PRESERVING FOR DATA ENCRYPTION.

Cloud got many issues regarding security especially on Data theft, Data loss and Privacy. Protecting cloud from unauthorized users and other threats is a very important task for security providers who are in charge of the cloud as secure cloud is always reliable source of information. Data owner uses cryptographic techniques to protect data from unauthorized access for providing protection to the privacy of their data and only those users can access data that have access permission. The policy updating has always been a challenging issue when ABE is used to construct access control schemes and develop a new method to outsource the policy updating to the server. Attribute Based Access Control method is used to avoid the transmission of encrypted data and minimize the computation work of data owners, by making use of the previously encrypted data with old access policies.

6.1Secure Cloud Storage Using Public Auditing

In this paper we are going to propose a public auditing scheme for the regenerating code based cloud storage. To obtain solution for regeneration problem of failed authenticators in the absence of data holders, we make a proxy, which is privileged to regenerate the authenticators, in the traditional public auditing system model. We also design a novel public verifiable authenticator, which is made by some keys. We also randomize the encode coefficients with a pseudorandom function to sure data privacy. Extensive security analysis shows this scheme is secure and provable under random oracle model. Experimental evaluation model indicates that this scheme is highly efficient and can be feasibly integrated regenerating cloud based storage.

6.2 Cloud Computing

National Institute of Standards and Technology (NIST) Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

6.3 Privacy Preservation in Cloud Computing

The main idea of this scheme can be summarized as follows: each participant first encrypts her/his private data with the system public key and then uploads the cipher texts to the cloud; cloud servers then execute most of the operations pertaining to the learning process over the cipher texts and return the encrypted results to the participants; the participants jointly decrypt the results with which they update their respective weights for the BPN network. For the duration of this process, cloud servers discover no privacy data of a participant even if they collude with all the rest participants. To sustain these functions over cipher texts, they adopt the BGN (Boneh, Goh and Nissim) doubly homomorphic encryption algorithm and tailor it to split the decryption capability among multiple participants for collusion-resistance decryption.

6.4 Expressive, efficient, and revocable data access control for multi-authority cloud storage

Cipher text-Policy Attribute-based Encryption CP-ABE is regarded as one of the most suitable technologies for data access control in cloud storage, because it gives data owners more direct control on access policies. It is difficult to directly apply existing CP-ABE schemes to data access control for cloud storage systems because of the attribute revocation problem. 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. Our attribute revocation method can efficiently achieve both forward security and backward security.

6.5 Privacy Preserving Cloud Data Access With Multi- Authorities

To deal with security problems, various schemes based on the Attribute-Based Encryption have been proposed recently. The privacy problem of cloud computing is yet to be solved. It presents an anonymous privilege control scheme Anony Control to address not only the data privacy problem in cloud storage, but also the user identity privacy issues in existing access control schemes. By using multiple authorities in cloud computing system, our proposed scheme achieves anonymous cloud data access and fine-grained privilege control.

6.6 Effective Data Access Control for Multi authority Cloud Storage Systems

Due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Existing access control schemes are no longer applicable to cloud storage systems, because they either produce multiple encrypted copies of the same data or require a fully trusted cloud server. Data access control for multi authority cloud storage (DAC-MACS), an effective and secure data access control scheme with efficient decryption and revocation.

6.7 Attributed-based access control for multi-authority systems in cloud storage

All existing CP-ABE schemes, it is assumed that there is only one authority in the system responsible for issuing attributes to the users. There are multiple authorities co-exist in a system and each authority is able to issue attributes independently. First design an efficient multi-authority CP-ABE scheme that does not require a global authority and can support any LSSS access structure. It proves its security in the random oracle model.

6.8 Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing

This paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. The problem of simultaneously achieving fine-grained, scalability, and data confidentiality of access control actually still remains unresolved. Defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents. We achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption.

A secure and verifiable policy updating outsourcing method called ABAC can avoid the transmission of encrypted data and minimize the computation work of data owners, by making use of the previously encrypted data with old access policies.

6.9 Attribute-based encryption (ABE)

ABE technique is regarded as one of the most suitable technologies for data access control in cloud storage systems.

There are two complementary forms of ABE

Key-Policy ABE (KP-ABE)

In KPABE, attributes are used to describe the encrypted data and access policies over these attributes are built into user's secret keys

Cipher text-Policy ABE (CP-ABE)

In CP-ABE, attributes are used to describe the user's attributes and the access policies over these attributes are attached to the encrypted data.

Recently, some attribute-based access control schemes were proposed to ensure the data confidentiality in the cloud. It allows data owners to define an access structure on attributes and encrypt the data under this access structure, such that data owners can define the attributes that the user needs to possess in order to decrypt the cipher text.

But this method will incur a high communication overhead and heavy computation burden on data owners.

6.10 Policy Attribute-Based Encryption

This method discussed on how to change the policies on keys. Authors also proposed a cipher text delegation method to update the policy of cipher text.

However, these methods cannot satisfy the completeness requirement, because they can only delegate key/cipher text with a new access policy which is more restrictive than the previous policy.

CONCLUSION:

A new outsourced ABE scheme is proposed that simultaneously supports outsourced key-issuing and decryption. With the aid of KGSP and DSP, this scheme achieves constant efficiency at both authority and user sides. Performance analysis shows that the proposed system i.e. outsourced ABE takes less encryption time and decryption time and the time increases as the file size increases. The time taken by the proposed scheme for encryption and decryption and key generation is in milliseconds. To sum up, this outsourced

ABE scheme achieves efficiency at both attribute authority and user sides during key-issuing and decryption without introducing significant overhead compared to the original approach.

Here, the data owner acts as the only authority in every cryptosystem. In large-scale systems, it is desirable to provide decentralized access control in the sense that the existence of multiple authorities in an application is allowed.

When encryption provides data confidentiality, it also greatly limits the flexibility of data operation. To address this issue, it is needed to combine ABE with cryptographic primitives such as searchable encryption, private information retrieval and homomorphic encryption to enable computations on encrypted data without decrypting.

REFERENCES :

[1] G. Ateniese et al., "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA, 2007, pp. 598–609.

[2] J. He, Y. Zhang, G. Huang, Y. Shi, and J. Cao, "Distributed data possession checking for securing multiple replicas in geographically dispersed clouds," J. Comput. Syst. Sci., vol. 78, no. 5, pp. 1345–1358, 2012.

[3] Batalla J Mastorakis, G., Mavromoustakis, C.X., Zurek, J. On cohabitating networking technologies with common wireless access for Home Automation Systems purposes. Special Issue on "Enabling Wireless Communication and Networking Technologies for the Internet of Things". IEEE Wirel. Commun. Mag. (2016)

[4] Batalla J Mavromoustakis, C.X., Mastorakis, G., Sienkiewicz, K.: On the track of 5G radio access network for IoT wireless spectrum sharing in device positioning applications. In: Internet of Things (IoT) in 5G Mobile Technologies, pp. 25–35. Springer International Publishing (2016)

[5] N.Nasurudeen Ahamed. March (2016) An Integrated Protection Scheme For Big Data And Cloud Services, International Journal of Advanced Research in Biology Engineering Science and Technology(IJARBEST), Vol. 2, Issue 10, March -2016

[6] Wang, Q., Wang, C., Ren, K., Lou, W., & Li, J. 2011. Enabling public auditability and data dynamics for storage security in cloud computing. Parallel and Distributed Systems, IEEE Trans. on, 22(5), 847-859.

[7] Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., Brandic, I.: Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Future Gener. Comput. Syst. **25**, 599–616 (2009).

[8]Verykios,V.S.Elmagarmid,A.K.Bertino,E.;Saygen,Y.Dasseni,E.Association rule hiding knowledge and data engineering. IEEE Transaction on Knowledge and Data Engineering, vol 16,issue 4th april 2004.pp.434-447.

[9]Kargupta,H.Datta,S.Wang,Q.Krishnamoorthy Sivakumar. On the privacy preserving properties of random data perturbation techniques .Third IEEE International Conference on Data Mining. ICDM 2003.19-22 nov.2003.pp.99-106.

LIST OF FIGURES