ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 5, Issue 3, March 2018

Secure and verifiable policy update Outsourcing big data in cloud computing

[1] T.Divya, [2] M.Thenmozhi,[3] A.Vidhya,[4] M.Karthikeyan
[1][2][3] Final Year Student, [4] Assistant Professor
[1][2][3][4]Department of Cse, Sengunthar College of Engineering, Tiruchengode

***Abstract* – Due to the high volume and velocity of big data, it is an effective option to store big data in the cloud, as the cloud has capabilities of storing big data and processing high volume of user access requests. Attribute-Based Encryption (ABE) is a promising technique to ensure the end-to-end security of big data in the cloud. However, the policy updating has always been a challenging issue when ABE is used to construct access control schemes. A trivial implementation is to let data owners retrieve the data and re-encrypt it under the new access policy, and then send it back to the cloud. This method, however, incurs a high communication overhead and heavy computation burden on data owners. In this paper, we propose a novel scheme that enabling efficient access control with dynamic policy updating for big data in the cloud. We focus on developing an outsourced policy updating method for ABE systems. Our method 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. Moreover, we also propose policy updating algorithms for different types of access policies. Finally, we propose an efficient and secure method 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.**

1. INTRODUCTION

This section discusses about the problem of existing research work that is still left unsolved. The survey analysis of recent works and some good study for BD privacy and security suggests than the issue is very critical and it needs a proper solution in real time applications scenario. An exhaustive study towards all the recently explored research contribution shows that they provide an efficient technique to solve certain security problems over big data approach in cloud. However, the area of big data is such a vast that it will be quite early to conclude effectiveness of any existing study as robust and resilient towards potential security threats. The problems that are left unsolved are as briefed below:

1. Less emphasis on authentication mechanism: There is a less number of improvement being carried out towards ensure a robust and fault-free authentication policy for big data users. Although, there are various novel ideas towards authentication system in cloud but they were never testified for their applicability over big data analytic-based application.

2. Few studies focusing on privacy: At present majority of the studies towards big data security have addressed the problem of data security and access control mainly. There is a very less emphasis on the design security that is mainly due to massive data size.

3. Less focus towards data brokers: At present, many of the cloud service providers are using multitenancy. They also have a practice of sharing certain segment of the data to the third party that tremendously increases potential risk. Privacy is the first thing to get compromised. The existing solution doesn't address such problems.

4. Storage insecurity in big data: It is well known fact that NoSQL database is still evolving and quite problematic to retain optimal security as per the demands. Normally, the big data are stored in multiple tiers where existing system doesn't really focus on how such existing encryption strategy is compliant of tier-based storage strategy.

II 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.

However, these methods cannot satisfy the completeness requirement, because they can only delegate key/ciphertext with a new access policy that should be more restrictive than the previous policy.

- 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.

- The policy updating problem has been discussed in key policy structure and ciphertext-policy structure

From the perspective of data security, which has always been an important aspect of quality of service, Cloud Computing inevitably poses new challenging security threats for number of reasons.

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.

Considering various kinds of data for each user stored in the cloud and the demand of long term continuous assurance of their data safety, the problem of verifying correctness of data storage in the cloud becomes even more challenging.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.

DRAWBACK

- 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.

- As an complementary approach, researchers have also proposed distributed protocols for ensuring storage correctness across multiple servers or peers. Again, none of these distributed schemes is aware of dynamic data operations. As a result, their applicability in cloud data storage can be drastically limited

- Due to its high volume and complexity, it becomes difficult to process big data using on-hand database management tools.

- 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 ciphertext-policy structure cannot satisfy the completeness requirement, because they can only delegate key/ciphertext with a new access policy that should be more restrictive than the previous policy.

- Furthermore, they cannot satisfy the security requirement either.

IIIPROPOSED 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:

• We formulate the policy updating problem in ABE systems and develop a new method to outsource the policy updating to the server.
• We propose an expressive and efficient data access control scheme for big data, which enables efficient dynamic policy updating.
• We design policy updating algorithms for different types of access policies, e.g., Boolean Formulas, LSSS Structure and Access Tree.
• 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.
• To formulate the policy updating problem in ABE systems and develop a new method to outsource the policy updating to the server.
• To propose an expressive and efficient data access control scheme for big data, which enables efficient dynamic policy updating?
• To design policy updating algorithms for different types of access policies, e.g., Boolean Formulas, LSSS Structure and Access Tree.
• To propose an efficient and secure policy checking method that enables data owners to check whether the ciphertexts have been updated correctly by cloud server.

ADVANTAGES

The Attribute based access control has a rich set of features. It includes;
• Policy checking entity free
• Storage Efficiency
• Dynamic policies but same keys
• Efficient and secure policy checking
• 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.
• More performance evaluation on policy updating algorithms and the policy checking method.
• 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.
• This method does not require any help of data users, and data owners can check the correctness of the ciphertext updating by their own secret keys and checking keys issued by each authority.

IV 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.

V 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.
• The coordinator is responsible for search the query into the database and retrieves the relevant information.)
In this module, the co-coordinator performs the global service between the two end users. Initially the Data Owner needs to submit the details of the patient in the server. Data Users needs to search the data which is stored the servers and they give request for the data and the Co-Ordinator sends the key to the Data users and the Data will be passed by the broker Way.

VI 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. The data will be passed from the co-coordinator and thus it will be submitted to the End Users (Data Users). (The broker module acts the role between the coordinator and the data users. The broker is the main responsible for user's authentication and the query forwarding .The brokers forward the query to the co-Ordinator and returns the required information to the user.

VII 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. During the encryption time the secret key for the file to decrypt the file is produced.

The owner has to keep the secret key. When they are retrieving the data from the cloud service providers the data will be in encrypted form. So this module plays an important role in our project.

VIII 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. It is also used when the local computer has a slow connection to the remote systems, but they have a fast connection between them. Without remote uploading functionality, the data would have to first be download to local host and then uploaded to the remote file hosting server, both times over slow connections.

IX CLOUD STORAGE SERVER (CSS):

An entity, which is managed by Cloud Service Provider (CSP), has significant storage space and computation resource to maintain the client's data.

X THIRD PARTY AUDITOR:

An entity, which has expertise and capabilities that clients do not have, is trusted to assess and expose risk of cloud storage services on behalf of the clients upon request.

XII MOBILE ALERT

An entity, which produces an alert to the cloud storage service provide or administrator who manages the cloud storage server.

XIII 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.

- 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] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine grained access control of encrypted data," in CCS'06. ACM, 2006, pp. 89–98.

[2] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in S&P'07. IEEE, 2007, pp. 321–334.

[3] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in PKC'11. Springer, 2011,pp. 53–70.

[4] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption Attribute-based encryption and (hierarchical) inner product encryption," in EUROCRYPT'10. Springer, 2010, pp. 62–91534–542.

[5] E. Damiani et al. 2010.New Paradigm for Access Control in Open Environment. Proceeding of 5th IEEE International Symposium on Signal Processing and Information.

[6] P. Bonatti and P. Samarati. 2012. A unified framework for regulating access and information release on the web. Journal of computer Security. 10(3): 241-272.

[7] L. Wang, D. Wijesekera and S. Jajodia. 2014. A logic based framework for attribute based access control. Proceeding of ACM workshop on formal methods in Security Engineering. pp. 45-55, ACM press.