Elysium Journal
Engineering Research & Management

P-ISSN: 2347-4408
E-ISSN: 2347-4734

AN EFFICIENT AND SECURE POLICY UPDATE OUTSOURCING SCHEME FOR BIG DATA STORAGE IN CLOUD

MBC AshaVani[1] and TR Vithya[2]

[1]*M Phil, Department of Computer Science, Selvam Arts and science college (Autonomous), Namakkal-637 003, Tamil Nadu, India.*
[2]*Assistant Professor, Department of Computer Science, Selvam Arts and Science College (Autonomous), Namakkal-637 003, Tamil Nadu, India.*

Abstract**: Store the big data in cloud is a best and an effective option due to its high volume and velocity. Generally, the cloud has the capability to store the big data and to process the high volume of user access requests. In cloud environment, the Attribute Based Encryption (ABE) technique ensures the end-to-end security of big data. But, the policy updating is a challenging issue, when the ABE is used to construct an access control schemes. With the help of trivial implementation, a data owners retrieve the data and re-encrypt it under new access policy, then send it back to the cloud. However, this approach sustains high communication overhead and heavy computational burden. Thus, this paper proposes a novel scheme to enable an efficient access control with dynamic policy updating for storing the big data in cloud. In this paper, an outsourced policy updating method is developed for designing the ABE systems that avoids the transmission of encrypted data and reduces the computation work of data owners. To check whether the cloud server has updated the cipher-texts correctly, an efficient and secure method was also proposed in this work. Finally, the experimental analysis demonstrates that the proposed system is correct, secure, efficient and complete.

Keywords—Attribute Based Encryption (ABE), Big Data, Cipher-Texts, Cloud.

1. INTRODUCTION

Big data has the high volume, high velocity, or high variety information assets, which requires new forms of processing and is shown in Fig 1. It enables the improved decision making, optimization of processes, and the discovery of insight. The existing data base tools used are difficult to process the big data since, it has a large volume of data and high complexity in processing the data. The possible solution is to store the big data in the cloud, which has the space for storing the big data and processing them efficiently. During the hosting process, the security of the cloud becomes a major concern because the servers cannot be fully trusted by the data owners.

Fig 1. Environment of Big Data

Attribute Based Encryption (ABE) [1] is an emerging and a promising technique for ensuring the end-to-end security of the data in the cloud storage system. The ABE allows the data owners to define the access policies and encrypts the data under such policies. The users, who satisfies the access policies alone can decrypt the data from the cloud. When there are more organizations in the cloud and outsourced data is large then the policy updating becomes an important issue. Hence, to overcome the problems faced by the outsourcing of data, the policies must be changed dynamically and frequently by the data owners.

The updating of policy is a challenging issue in Big data since, it contains large amount of data and it burdened the owners of the data to update the policy dynamically. To update the policy, the data owners have to retrieve the data from the cloud, updates the data and then, again sends the data to the cloud in the existing Attribute Based Access Control (ABAC) scheme. Hence, it creates the overheads at the data owners. In order to reduce the transmission delay and the computation overhead between the data owners and the cloud, a novel method Attribute Based Encryption (ABE) is implemented for updating the policy. In the proposed ABE scheme, the data owners instead of retrieving the data from the cloud it creates the new policies and sends the policy alone to the cloud. The cloud just updates the policies of the data without decrypting the data. Hence, the proposed ABE scheme have the advantages, which is listed as below:

- Less Computation overhead

P-ISSN: 2347-4408
E-ISSN: 2347-4734

- Minimizes the transmission delay

There are several challenges of outsourcing the policy to the cloud server and guaranteed the following requirements such as:

- Correctness
- Completeness
- Security

Correctness: The users having the sufficient attributes be able to decrypt the data under the new access policy by running the decryption algorithm.
Completeness: The updating of policies method should be able to update any type of access policies.
Security: The updating of policies should not break the security of the access control system or introduce the new security problems.

In this paper, our main aim is to solve the policy updating problem in ABE systems and we propose a novel efficient and secure policy update outsourcing method. The data owners send the policy updating queries to the cloud servers instead of retrieving and re-encrypting the data. The cloud server updates the policies of the encrypted data, which does not decrypt the data during the policy updating process.

The main contributions of this paper includes the following,

- A novel method for outsourcing the policy to the cloud server and formulated the policy updating problem in ABE.
- An efficient policy updating scheme is also proposed.
- A policy updating algorithms is designed for different access types. The different access policies includes,
    - Boolean formulas
    - LSSS Structure
    - Access Tree, etc.
- An efficient and secure policy for checking, whether the cipher texts are updated correctly by the cloud server are also proposed.

The remainder of the paper is systematized as follows, Section II describes the literature review related to the data encryption and decryption mechanisms for storing the data in the cloud. Section III illustrates the proposed ABE scheme with dynamic updating policy for big data. Section IV illustrates the conclusion of this paper.

2. RELATED WORK

This section illustrates the literature review related to the data encryption and decryption mechanisms for storing the data in the cloud. *Li, et al* [1]proposed a new patient-centric framework and the suitable mechanisms for accessing the data from the cloud server. The ABE scheme was used for encrypting the patient's record. This scheme enabled the dynamic modification of access policies or the attributes of the files. *Parno, et, al*[2]established the connection between the verifiable computation and the ABE. The definition of Verifiable Computation (VC) was also extended in two different ways such as (1) Public Delegation and the (2) Public verifiability. *Yang, et, al*[3]proposed an efficient attribute based revocation method for CP-ABE system, which greatly reduced attribute revocation cost. The proposed scheme was an efficient and provably secure in the random model. The designed access control framework in cloud storage was based on the cipher text policy ABE.

Lewko and Waters[4]developed a new methodology for utilizing the techniques for proving the selective security encryption schemes. They also presented the Cipher text policy Attribute based encryption scheme. *Yang, et al*[5]proposed DAC-MACS for effective controlling of data access for multi authority cloud storage systems. Data access control was an effective way for ensuring the security of the data in the cloud. The challenges faced by the cloud servers were:

- Data outsourcing
- Untrusted cloud servers
- Data access control

Cipher text-Policy Attribute-based Encryption (CP-ABE) was a promising technique for access control of encrypted data. It required the trusted authority and managed the attributes and distributes the keys in the system. *Yang, et, al*[6]designed an expressive, effective and revocable data access control scheme for multi-authority cloud storage systems. Data access control was an effective way to ensuring the security of the data in the cloud. CP-ABE was one of the most suitable technologies for accessing the data from the cloud.

Thatikayala, et al[7] proposed a new patient-centric framework and suitable mechanisms for accessing the data access control to PHRs stored in semi-trusted servers. The proposed method was used to achieve a fine grained and scalable data access control using the ABE, which encrypts the patient's record. *Lee, et al*[8]surveyed various ABE schemes and the two access structures were analyzed for the cloud environments. In the cloud environments the ABE played an important role. The access policy was named either as key-policy and the cipher text policy. The ABE had the advantages such as: to reduce the communication overhead of the internet and to provide the fine-grained access control.

Li, et al [9]presented a generic and efficient solution for implementing the ABE based on the access control system. They also introduced the secure outsourcing techniques and formulized the Outsourced ABE (OABE). Since, the cloud computing became relevant, more and more sensitive data was centralized into the cloud for sharing the information. *Chen and Zhao*[10] provided the concise analysis of the data security and the protection of privacy issues in the cloud

P-ISSN: 2347-4408
E-ISSN: 2347-4734

computing environment. It also discussed some current solutions for the problems faced by the cloud computing environment. The cloud computing has many potential advantages and the data were migrated to the public as well as the hybrid cloud. *Mishra, et al*[11]discussed the security issues in cloud computing. There were two technologies in the cloud, such as:

- Multi-tenancy
- Virtualization

These two technologies provided the security in the cloud. *Sahai, et al*[12]motivated the access control in cloud storage and considered the problem using the ABE, where the texts were stored by the third party. A comprehensive solution was also discussed in this work. The main contributions of this paper were:

- Revocable storage
- Protecting the newly encrypted data

AlZain, et al [13] surveyed recent research related to the single and the multi-cloud security and addressed the possible solutions. The used of cloud computing was increased rapidly in many organizations. Ensuring the security of the cloud was a major factor in the cloud computing environment. *Tebaa, et al*[14]proposed an application to execute any operations on the encrypted data. The main aim in the cloud computing environment was to consider the security issues. *Yang, et al*[15] designed an access control framework for the multi-authority access control scheme in the cloud storage. CP-ABE was regarded as one of the suitable technologies for accessing the data in the cloud storage.

3. PROPOSED METHOD

The proposed ABE method is divided into the following stages such as,

- Data creation by the data owners
- System Initialization
- Key generation
- Data encryption
- Data decryption
- Dynamic policy updation
- Check Policy Update

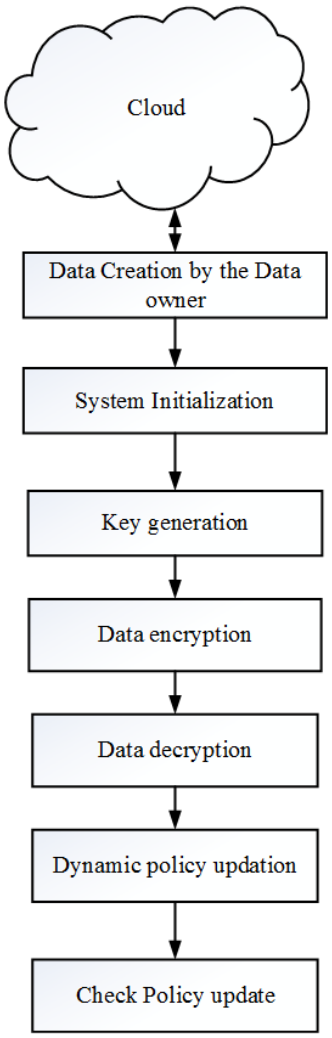

Fig 2. Overall Flow Diagram of the proposed ABE scheme for updating the policies dynamically

3.1 Data creation by the data owners

The data owners creates the data and stores them in the cloud. The cloud storage system is considered with the multiple authorities in Fig 3. The system model of the cloud has the following entities, which includes,

- Authorities (AA)
- Cloud Server (Server)
- Data owners (Owners)
- Data Consumers (Users)

3.1.1 Authority

The authority is independent with each other and it is responsible for managing the attributes of users in its own domain. The secret key and the public key pair is generated in each attribute in the domain and the key, which is secret is used according to his or her own attributes.

Server

The cloud server is responsible for storing the data owner's data. The cipher texts are updated at the server side and the new access policies are generated from the old policies.

P-ISSN: 2347-4408
E-ISSN: 2347-4734

3.1.2 Owner

The owner are responsible for defining the access policies and for encrypting the data under the required policies. They also ask the server to update the access policies of the encrypted data, which is stored in the cloud. The owners also check the updated policies by the cloud.

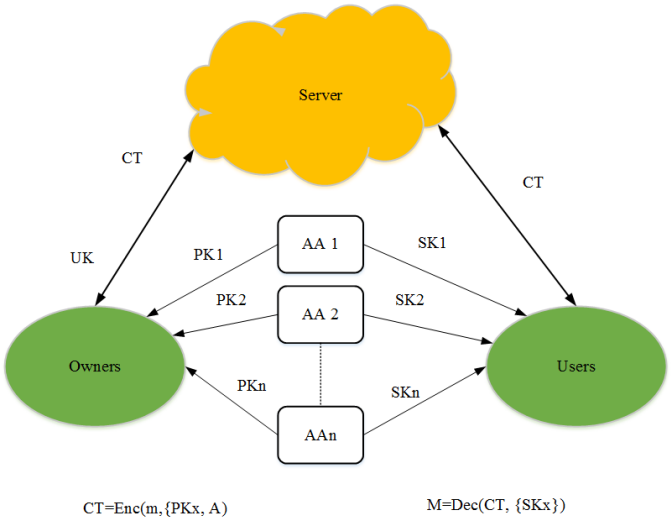

Fig 3. System Model with dynamic updating policy

3.1.3 User

Each and every user is assigned with the identity of the global user and gets the cipher texts free of cost from the cloud server. The user decrypts the data, only when the user has the respective attributes, which satisfies the access policies defined in the cipher texts.

Framework

For updating the policy in the cloud all the security requirements are met, and the dynamic policy access control scheme is the collection of the following algorithms.

- Global setup
- Authority Setup
- SKey Gen (Secret Key Generation algorithm)
- Encrypt
- Decrypt
- UKey Gen(Update Key Generation algorithm)
- CTUpdate (CipherText Updating algorithm)

3.2 System Initialization

The dynamic-policy access control scheme is based on an ABE method. Two phases are included in the system initialization phase, which includes,

- Setup
- Authority Setup

Setup

In the global setup, the two multiplicative groups are chosen with same order and the bilinear map is defined between them. The global parameter is also assigned in the global setup phase.

Authority Setup

Each authority runs the Authority Setup algorithm for generating the secret key and the public key pair. Let the S_{AID} denotes the Set of All Attributes managed by the authority AID. The authority chooses the random numbers and publishes the public keys to the user.

3.3 Key generation

The authority assigns the set of attributes for each and every user. Then, the secret keys are generated using the Secret Key Generation algorithm.

3.4 Data Encryption

The owner of the data encrypts the user's data by running the Encrypt algorithm. The data encryption algorithm takes the set of inputssuch as the public keys (PK)for relevant authorities. It chooses the random encryption exponent and a random vector. For each and every message the algorithm computes the cipher text. The data containsall the random numbers in an encrypted format.

3.5 Data Decryption

The data is decrypted by obtaining the random number and is done by the data owner. If the user has the secret key for the subset of rows of the data then, the data is decrypted using the secret keys of the user.

3.5.1 Policy Updating

The access policy of the encrypted data are updated using the policy updating procedure. The updation of the ciphertexts are delegated from the data owner causes heavy communication overhead of the data. The owner of the data updates the cipher texts from the previous access policy to the new access policy. The update key is first generated by running the update key generation algorithm, which sends the update key to the cloud server. After receiving the key, the cloud server runs the cipher text updating algorithm for updating the cipher text from previous access policy to the new access policy.

3.6 Dynamic Policy Updation

The access policy is expressed by either the LSSS structure or access tree structure. In this proposed scheme, only the monotonic structures are considered. The monotonic structures is similarly achieved by taking the NOT operation as another attribute.

First the policy updating scheme for monotonic Boolean formulas are designed. Then, the algorithms for updating the threshold tree access structures are designed. The general algorithm is designed for updating the threshold gate.

3.6.1 Updating a Boolean Formula

Access policies with Boolean formulas are represented using the simplest threshold access trees, where the leaf nodes in the tree represents the attributes and the non-leaf nodes represent the AND, and the OR gates. The Boolean

P-ISSN: 2347-4408
E-ISSN: 2347-4734

formulas is easily converted to the LSSS matrix form. There are four basic operations, which includes,

- Attr2OR
- Attr2AND
- AttrRmOR
- AttrRmAND

3.6.2 Updating a LSSS structure

The access policies in LSSS structure is expressed in the access control scheme. The data owner are enabled to re-randomize the encryption of the secret key. The owner of the data runs the Update Key Generation algorithm for constructing the update keys and sends the updated key to the cloud server.

3.6.3 Update Key Generation

The update key generation algorithm takes the public keys, encryption information of data, and the previous access policy, the new access policies as inputs. The update generation key first calls the Policy Generation algorithm for comparing the new access policies with the old access policies.

3.6.4 Cipher Text Update

The cloud server receives the update key from the data owner and the cloud sever runs the Cipher Text updating algorithm for computing the cipher text component. In our method all the pairing computations are moved to the cloud server, while the owner of the data does the minimum computation.

3.6.5 Updating a Threshold

There is a problem in changing from the old threshold gate to the new threshold gate. The existing methods introduces the security problem in the new threshold gate. To solve the problems faced by the existing methods, the value of the threshold data share is re-randomized. For converting the threshold gate to LSSS structure, the algorithm first converts the threshold gate into Boolean formulas, which in turn converts into the LSSS structure by calling the respective algorithm. The LSSS algorithm is the combination of two structures namely,

- DNF2SSS
- SSS2MSP

DNF2SSS: The algorithm DNF2SSS and is used to construct the Secret Sharing Scheme from the monotone DNF Boolean Formula.

SSS3MSP: This algorithm is adapted and the used to convert the secret sharing scheme into monotone span program.

3.7 Checking Policy Update

After the policy updating algorithm is run, the cloud sever and the data owner waits for the cloud server for finishing the updating operation of all the relevant cipher texts. Then, the owner of the data checks the cloud server, whether it has done any updations. The cloud server sends back the Checking Proof to the data owner. After receiving the proof, the data owner of verifies the correctness of the proof from the cloud server. If the proof is correct or wrong.

4. CONCLUSION

In this paper, the policy updating problem in big data access control systems are discussed and formulated, which satisfies the challenging security requirements. We have proposed a novel method for efficient and secure policy updating scheme in big data, which satisfies all the security requirements stated above. The drawback of the existing ABAC scheme is overwhelmed by the proposed ABE with dynamic policy updating scheme, which reduced the computation overhead at the data owner. The correctness of the proof is also verified by the proposed ABE method. The policy updating schemes is based onLewko and the waters [4] scheme, which is used for updating the policy schemes dynamically and is applied to other ABE systems also.

REFERENCES

[1] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, pp. 131-143, 2013.

[2] B. Parno, M. Raykova, and V. Vaikuntanathan, "How to delegate and verify in public: Verifiable computation from attribute-based encryption," in *Theory of Cryptography*, ed: Springer, 2012, pp. 422-439.

[3] K. Yang, X. Jia, and K. Ren, "Attribute-based fine-grained access control with efficient revocation in cloud storage systems," in *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security*, 2013, pp. 523-528.

[4] A. Lewko and B. Waters, "New proof methods for attribute-based encryption: Achieving full security through selective techniques," in *Advances in Cryptology–CRYPTO 2012*, ed: Springer, 2012, pp. 180-198.

[5] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, "Dac-macs: Effective data access control for multiauthority cloud storage systems," *Information Forensics and Security, IEEE Transactions on*, vol. 8, pp. 1790-1801, 2013.

[6] K. Yang and X. Jia, "Expressive, efficient, and revocable data access control for multi-authority cloud storage," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, pp. 1735-1744, 2014.

[7] S. THATIKAYALA and J. SRAVANTHI, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-Based Encryption," *International Journal of Scientific and Engineering and Technology Research*, vol. 3, pp. 4912-4917, 2014.

[8] C.-C. Lee, P.-S. Chung, and M.-S. Hwang, "A Survey on Attribute-based Encryption Schemes of

P-ISSN: 2347-4408
E-ISSN: 2347-4734

Access Control in Cloud Environments," *International Journal of Network Security*, vol. 15, pp. 231-240, 2013.

[9] J. Li, X. Chen, J. Li, C. Jia, J. Ma, and W. Lou, "Fine-grained access control system based on outsourced attribute-based encryption," in *Computer Security–ESORICS 2013*, ed: Springer, 2013, pp. 592-609.

[10] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in *2012 International Conference on Computer Science and Electronics Engineering (ICCSEE)*, 2012, pp. 647-651.

[11] A. Mishra, R. Mathur, S. Jain, and J. S. Rathore, "Cloud computing security," *International Journal on Recent and Innovation Trends in Computing and*

[12] A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for attribute-based encryption," in *Advances in Cryptology–CRYPTO 2012*, ed: Springer, 2012, pp. 199-217.

[13] M. AlZain, E. Pardede, B. Soh, and J. Thom, "Cloud computing security: from single to multi-clouds," in*45th Hawaii International Conference on System Science (HICSS), 2012*, 2012, pp. 5490-5499.

[14] M. Tebaa, S. El Hajji, and A. El Ghazi, "Homomorphic encryption applied to the cloud computing security," in *Proceedings of the World Congress on Engineering*, 2012, pp. 4-6.

[15] K. Yang and X. Jia, "Attributed-based access control for multi-authority systems in cloud storage," in *2012 IEEE 32nd International Conference on Distributed Computing Systems (ICDCS)*, 2012, pp. 536-545.