International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Updating Policy with Access Control Using Multi Authority in the Cloud

V.Kalpana[1], J. Daphney Joann[2]

[1]ME-CSE, Kingston Engineering College, Vellore, India

[2]Assistant Professor, Department of CSE, Kingston Engineering College, Vellore, India

Abstract: ***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. A policy updating algorithm called LSSS is used for efficient and secure method allows data owner to check whether the cloud server has updated the cipher texts correctly.***

Keywords: Access Control, Policy Updating, Attribute based Encryption, Encryption-Decryption, Attribute Based Access control.

1. Introduction

Cloud computing is internet based computing, whereby shared resources, software and information are provided to computers and other devices on demand. Cloud provides many advantages as storing information on the cloud gives almost unlimited storage capacity, easy access to information gives access permission to data stored on cloud from anywhere if user is registered to it. 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.

2. Objective and Scope of the Paper

Policy updating issue has not been considered in existing traditional attribute-based access control Schemes. We also update the access policy of the encrypted data in the cloud. Heavy communication overhead of the data retrieval can be eliminated and the computation cost on data owners can also be reduced.

3. Existing System

Attribute-Based Encryption is used to ensure end-to-end security of big data in the cloud. Policy updating has always been a challenging issue when ABE is used to construct access control schemes. Policy updating becomes a significant issue as data access policies may be changed dynamically and frequently by data owners.

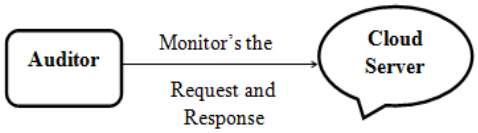
4. Problem Characterization

The policy updating problem in ABE systems and develop a new method to outsource the policy updating to the server. An expressive and efficient data access control scheme for big data enables efficient dynamic policy updating. To update the access policy of the encrypted data we use the cloud. Heavy communication overhead of the data retrieval can be eliminated and the computation cost on data owners can also be reduced.

5. Features of Sane

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

1) Policy checking entity free
2) Storage Efficiency
3) Dynamic policies but same keys



6. Literature Survey

A body of literature has been conducted by several authors and a list of them is given below;

1. 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.

2. 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.

3. Effective Data Access Control for Multiauthority 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.

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

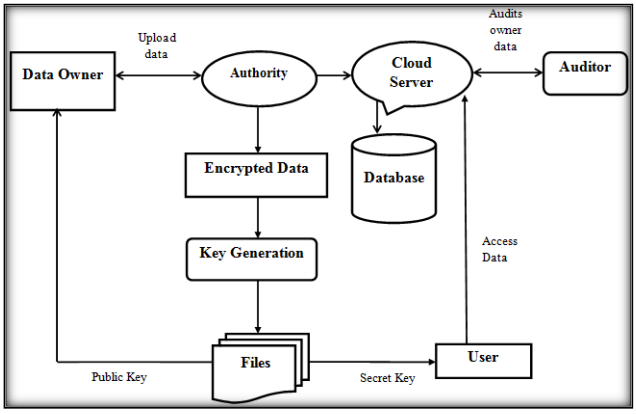
All existing CP-ABE schemes, it is assumed that there is only one authority in the system responsible for issuing attributes to the users. There are multiple authorities co-exist in a system and each authority is able to issue attributes independently. First design an efficient multi-authority CP-ABE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

5. 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.

7. Architecture Diagram

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.



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.

8. Modules

Data Owner

Data Owner achieves public key from any one of the authorities, and he uses the public key to encrypt the data file before outsourcing with third party it to the Cloud Servers.

Authority

The authority generates the key so that owner can encrypt the data and user can decrypt the data. It checks the data is safe also provide protection to the data. Each user data is assigned with a global user identity and can freely get the cipher texts from the Authority.

Key Generation

Here Keys are generating for every unique files. At the time of user retrieving any file key is essential for access the file. In a linear scheme, the secret is viewed as an element of a finite field, and the shares are obtained by applying a linear mapping to the secret and several independent random elements. Following is the LSSS algorithm used;

Input : $\{\vec{V}_i\}$ set of piece vectors for each attribute $Attr_i$
Input : S the secret to be shared
Output: M Monotone Span Program
Let $\vec{Z}$ be a vector and set $\vec{Z}$ (0) = S;
Let M be a matrix;
Let ρ be a labeling function;
  For all $Attr_i$ do
    For each piece vector $\vec{Z}_i$ for $Attr_i$; do
    Append each random value in $\vec{Z}_i$ to Z;
    Construct the position vector $\vec{Z}_i$ for $Attr_i$;
    Append $\vec{Z}_i$ to M;
    Let ρ (M, $\vec{Z}_i$) to $Attr_i$;
    end for

end for
Pad M with the same row size;
Return ($\vec{Z}$, M, ρ);

Cloud User
This module is used to help the user to search the file using the multiple key words concept and get the accurate result list based on the user query. The user is going to select the required file and register the user details. After entering the key User can download the file which is an encrypted data.

Auditing
Auditor monitors the user request and response provided by the cloud server. Auditors enumerate, evaluate, and test systems, practices, and operations to determine whether the systems safeguard the information assets, maintain data integrity, and operate effectively to achieve goals or objectives.

9. Results and Discussions

The data owner only needs to send the update keys to the cloud server, instead of the whole encrypted big data. Therefore, ABAC method can significantly reduce the communication cost during the policy updating. The scheme makes full use of the previous cipher texts encrypted under the old access structure. That is if an attribute in the new access policy has ever appeared in the previous access policy, the new cipher text component of this attribute can be derived from the previous cipher text component with the update key. The data owner only needs to compute cipher text components for new attributes. Delegate all the pairing operations to the server, such that the workload of the data owner can be further reduced.

Fig.1(a) compares the computation time between generating an update key (e.g., User Attributes, Resource Attributes and Environment Attributes in the scheme) versus generating a cipher text component (if the owner choose to re-encrypt the cipher text using a new secret) corresponding to an attribute. It is more efficient for data owners to only generate an update key than generate a cipher text component for each attribute.

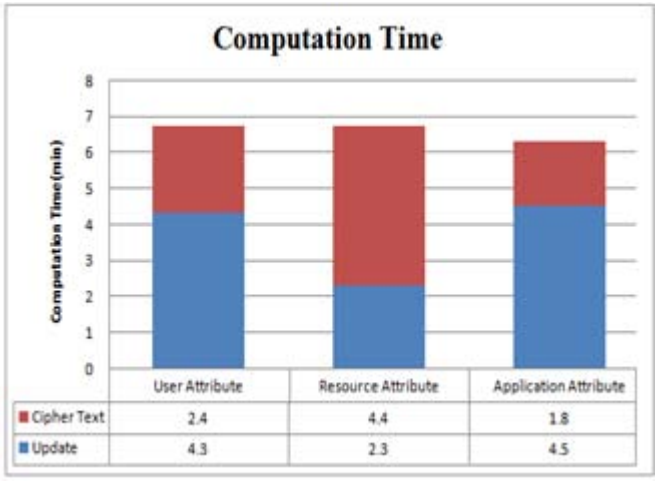


Figure 1(a): Computation time between Update keys and new cipher text components

Fig.1 (b) illustrates the computation time of each phase during the correctness checking of the policy updating. We can see the verification is much more time consuming than the challenge and the proof. However, it can avoid the heavy communication overhead when it copes with big data.

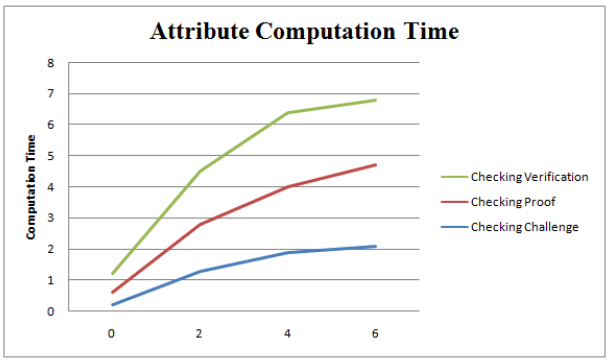


Figure 1 (b): Computation evaluation of policy checking

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. However, the policy updating becomes a difficult issue when applying ABE methods to construct access control schemes, because once data owner outsource the data into cloud, they won't store in local systems.

To change the access policies of encrypted data in the cloud, a trivial method 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 server. But this method will incur a high communication overhead and heavy computation burden on data owners.

10. Conclusion and Future Enhancement

The proposed scheme guarantees that the actual data owner could pass the cloud server's authentication and legally update the cipher text corresponding to the owner's data. Also designed policy updating algorithms with authentication for access policy expressed and also given the analysis of the scheme on the security, authentication and performance. Since the cloud will learn nothing of the data owner except that the owner could open the commitment, the scheme supports anonymous authentication. The access control scheme is constructed on prime order groups, because the group operations on prime order groups are much faster than the ones on Composite order groups. A dynamic policy access control scheme is secure in the generic bilinear group model. Public key encryption also called as asymmetric encryption involves a pair of keys, public key and private key associates with an entity. Ensure the data confidentiality in the cloud.

11. Acknowledgement

I would like to take this opportunity to express my profound gratitude and deep regard to my guide, *Ms.J.Daphney Joann*

M.E, CSE, Kingston Engineering College, for her exemplary guidance, valuable feedback and constant encouragement in completing this paper. Her valuable suggestions were of immense help in getting this work done. Working under her, was an extremely knowledgeable experience. Also, I would like to extend my sincere gratitude to my husband and my parents for their constant support and encouragement in completing this paper.

References

[1] X. Jia and K.Yang (2014) "Expressive, efficient and revocable data access control for multi-authority cloud storage", IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 7, pp. 1735–1744.
[2] Hulawale Kalyani, Paikrao Rahul and Pawar Ambika (2014) "Achieve Fine Grained Data Access Control in Cloud computing using KP-ABE along-with Lazy and Proxy Re-encryption", vol. 12, no. 3, pp. 135–174.
[3] T. Jung, X.-Y. Li, Z. Wan, and M. Wan (2013) "Privacy preserving cloud data access with multi-authorities," in INFOCOM'13. IEEE, vol. 6, no. 27, pp. 2625–2633.
[4] X. Jia, K. Ren, R. Xie, K. Yang and B. Zhang (2013) "DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems," IEEETrans. Info. Forensics Security, vol. 8, no. 11, pp. 1790–1801.
[5] Luan Ibraimi, Pieter Hartel, Qiang Tang and Willem Jonker (2012) "Efficient and Provable Secure Cipher text-Policy Attribute-Based Encryption", vol. 10, no. 18, pp. 790–180.
[6] X. Jia and K.Yang, "Attributed-based access control for multi-authority systems in cloud storage," in ICDCS'12. IEEE, 2012, vol. 18, no. 5,pp. 1–10.
[7] W. Lou ,K. Ren,C. Wang and S. Yu (2010) "Achieving secure, scalable, and fine-grained data access control in cloud computing," in INFOCOM'10, IEEE, vol. 4, no. 9, pp. 534–542.
[8] Guojun Wang, Jie Wu and Qin Liu (2010) "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services'', vol. 11, no. 6,pp. 113–156.
[9] Shashank Agrawal, Shweta Agrawal, Saikrishna Badrinarayanan(2009) "On the Practical Security of Inner Product Functional Encryption", vol. 14, no. 9, pp. 241–310.
[10] Amit Sahai ,Allison Lewko and Tatsuaki Okamoto (2009) "Fully Secure Functional Encryption: Attribute-Based Encryption and Hierarchical Inner Product Encryption", vol. 8, no. 21,pp. 564–642.
[11] A. Beimel(2009) "Secure schemes for secret sharing and key distribution" DSc dissertation, vol. 16, no. 21,pp. 794–948.
[12] Ferraiolo DF and Kuhun DR. 1992. Role Based Access Control. Proceeding of 15th National Computer Security Conference, Baltimore MD. pp. 554-563.
[13] R. Lehtinen, D. Russell and G. Gangemi Sr. 2006. Computer Security Basics. O Reilly publications, 2nd edition.
[14] M. Blaze and J Feigenbaum *et al*. The Keynote trust management system. Version 2, IETF RFC 270.
[15] A. Pimlott and O. Kiselyov. 2006. SOUTEI, A Logic Based Trust Management System. Proceeding of 8th international symposium on Functional and Logic Programming, Springer, Japan. pp. 130-144.
[16] E. Damiani *et al*. 2005. New Paradigm for Access Control in Open Environment. Proceeding of 5th IEEE International Symposium on Signal Processing and Information.
[17] P. Bonatti and P. Samarati. 2002. A unified framework for regulating access and information release on the web. Journal of computer Security. 10(3): 241-272.
[18] L. Wang, D. Wijesekera and S. Jajodia. 2004. A logic based framework for attribute based access control. Proceeding of ACM workshop on formal methods in Security Engineering. pp. 45-55, ACM press.

Author Profile

V. Kalpana is a Post-graduate student in Computer Science Department, Kingston Engineering College, Vellore, India. She received B.E degree in 2008 from Priyadarshini engineering college, Vaniyambadi, India. Her research interests are Cloud Computing, data mining and data structure.

J. Daphney Joann Assistant Professor ,Currently working in the Department of Computer Science , Kingston Engineering College. She received her B.E degree Specialization in Computer Science and Engineering from C.S.I Institute of Technology, Anna University in April 2006. She then completed M.E CSE from Adhiyamaan College of Engineering , Anna University with First class and Distinction in June 2008. Her research interests are in the areas of Wireless Networks, Web Technology & Network Security.