INTERNATIONAL JOURNAL · ENGINEERING RESEARCH

International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

IJIEMR Transactions, online available on 20th FEB 2019. Link :

http://www.ijiemr.org/main/index.php?vol=Volume-08&issue=ISSUE-02

Title: **PRIVACY PROTECTION BASED ACCESS CONTROL SCHEME IN CLOUD BASED SERVICES**

Volume 08, Issue 02, Pages: 45–50.

Paper Authors

T.USHA RANI, M.SATHYAM REDDY

Loyola Institute of technology and management, Dulipalla, satennapalli, Guntur, A.P, India

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

PRIVACY PROTECTION BASED ACCESS CONTROL SCHEME IN CLOUD BASED SERVICES

[1]T.USHA RANI, [2]M.SATHYAM REDDY

[1]M.Tech scholar, Dept of CSE, Loyola Institute of technology and management, Dulipalla, satennapalli, Guntur, A.P, India

[2]Assistant professor, Dept of CSE, Loyola Institute of technology and management, Dulipalla, satennapalli, Guntur, A.P, India

ABSTRACT: With the rapid development of computer technology, cloud-based services have become a hot topic. They not only provide users with convenience, but also bring many security issues, such as data sharing and privacy issue. In this paper, we present an access control system with privilege separation based on privacy protection. In the privacy protection scheme, we divide users into private domain and public domain logically. In private domain, to achieve read access permission and write access permission, we adopt the Key-Aggregate Encryption and the Improved Attribute-based Signature respectively. In PUD, we construct a new multi-authority cipher text policy attribute-based encryption scheme with efficient decryption to avoid the issues of single point of failure and complicated key distribution, and design an efficient attribute revocation method for it. The analysis and simulation result show that our scheme is feasible and superior to protect users' privacy in cloud-based services.

KEY WORDS: Access control, data sharing, privacy protection, cloud-based services.

I.INTRODUCTION

With the rapid development of cloud computing, big data and public cloud services have been widely used. Users can store their data in the cloud service and rely on the cloud service provider to give data access to other users. However, the cloud service provider can no longer be fully trusted. Because it may give data access to some illegal users or attackers for profit gain. For users, it is necessary to take full advantage of cloud storage service, and also to ensure data privacy. Therefore, the study of access control scheme to protect users' privacy in cloud environment is of great significance. Since traditional access control Strategy cannot effectively solve the security problems that exist in data sharing, various schemes to achieve encryption and decryption of data sharing have been proposed.The cloud storage services is a technology in cloud computing, which provides the flexible online data storage services for data owners over the Internet, such as online archiving, collaboration and social networking. These clouds allow users to abandon local storage and use online storage. The data owners not need to consider the underlying technical details of storage capacity, type of storage devices, data storage location and data protection. They only need to pay-as-you-use, and can get the storage space from the cloud servers. It can reduce the cost for data owners, and has been widely used. However, the cloud storage services, which make the data out of the data owners' control.The cloud storage access control is one of the important methods to access data legally and protected confidentiality data. The users submit access requests to the cloud servers through the interface of cloud servers. Once the cloud servers receives the users' access requests, identifying users' identity, and determining the users' access privileges. The users who have the legality privileges enable to access data. Otherwise, the cloud servers reject users' requests. But the data owners do not fully trust the cloud servers, so we can't implement access control in the cloud server-side. Cipher text access control technology is a scheme when access confidentiality data in the unlikelihood scenarios of the cloud server-side. The working principle is: the data owners encrypt the data files before storing data in the cloud server, the cloud server control the users' access permission for secret key to achieve the goal of security access control. Therefore, how to achieve efficient cipher text access control becomes the most important issue for the security cloud storage services.Some methods have been presented about cipher text access control scheme. These methods are better able to address data confidentiality issues, but the users' data secret key access permission managed by data owners. With the amount of data and user volume growth, the complexity of rights management will be improved significantly. It will become the bottleneck of the application because the load is increased in the data owner side. The cloud service provider consists of two parts: data storage server and data service management. Data storage server is responsible for storing confidential data files, and data service management is in charge of controlling external users' access to secret data and returning the corresponding cipher text. Users in private domain have special privileges, such as family, personal assistant, close friends and partners. This domain has a small number of users and small scale attributes, and the data owner knows users' identities, which is easy to manage. Data Owner can develop different access control strategies based on the characteristics of users in public and personal domain encrypt uploaded files using the corresponding encryption method and then send them to the cloud server.

II.RELATED WORK

In the practical cloud environment, there are a lot of authorities and each authority in their own field manages part of users' attributes. The attributes owned by the user are issued from different authorities. For example, a data owner may want to share his medical data with a user who owns the doctor attribute issued by medical institutions and the medical researcher attribute by the clinic practice management. Therefore, exploiting multi authority is more realistic in the practical scenarios. If there is only one authority, all the distribution of the keys are handed over by one trusted authority. The frequent interaction between the user and trust authority will not only bring bottlenecks for the system load capacity, but also increase the potential security risks.

Firstly the data owner uploads the attribute-based encrypted data files to the cloud server. When a user requests the encrypted data from the cloud server, the cloud server will first check his transformation key. Only if the corresponding attributes satisfy the access structure, will the cloud server output a partially decrypted cipher text and then sends it to the user. Finally, upon receiving the partially decrypted cipher text, the user can use his private key to recover the message. For the user, the public key and file class label are all known, he can use the algorithm to encrypt the files after he modified, and then upload them to the cloud. But whether the cloud server saves the modified file is decided by the write access control policy. On the one hand, in the complex cloud environment, if a user's modification operations are very frequent, maybe he is very important to the user, so that the user may be stricken from outside attacks. Therefore, the user worries the leak of identity after the signature. On the other hand, in the data sharing scheme, the separate access of read and write to the file is extremely important.When a user is revoked, his transformation keys will be deleted by the cloud server. Thus, he can no longer receive the partially decrypted cipher text and cannot recover the original message. On the other hand, when a new user joins to share the outsourced data, the cipher text will be re-encrypt by the cloud server so that he can also decrypt the cipher text. Therefore, the forward and backward security of the outsourced data can be guaranteed. For user revocation, we do not need to re-encrypt the cipher text and update all non-revoked users' private keys. Instead, we only need to delete the user's transformation keys. Without the transformation key, he can no longer decrypt the cipher text. On the other hand, when attribute revocation occurs, private keys of all non-revoked users will not be updated, only the transformation keys which are stored in the cloud server and the involved cipher text need to be updated. Thus, the efficiency of revocation can be greatly improved.The data owner defines access policies and encrypts the data files in accordance with this policy. Each user is distributed a key related to his attribute. As long as the user's attributes meet the access policy he can decrypt the file. However, if there is only one authority in the system and all public and private keys are issued by the authority. The frequent interaction between the user and trust authority will not only bring bottlenecks for the system load capacity, but also increase the potential security risks. When a user requests the encrypted data from the cloud server, the cloud server will first check his transformation key. Only if the corresponding attributes satisfy the access structure, will the cloud server output a partially decrypted cipher text and then sends it to the user. Finally, upon receiving the partially decrypted cipher text, the user can use his private key to recover the message.User must be able to execute the data owner's default re-encryption program faithfully. Secondly, the cloud servers may spy on data owner's data files, so we should not disclosed to the cloud server any data in plaintext information in the process of re-encryption. The cloud servers might collude with a small number of malicious users for the purpose of harvesting file contents when it is highly beneficial. Communication channel between the data owner/users and the cloud servers are assumed to be secured under existing security protocols. More specifically, we associate each data file with a set of attributes, and assign each user an expressive access structure which is defined over these attributes. Data confidentiality is also achieved since the cloud servers are not able to learn the plaintext of any data file in this construction.

III. PROPOSED MODEL

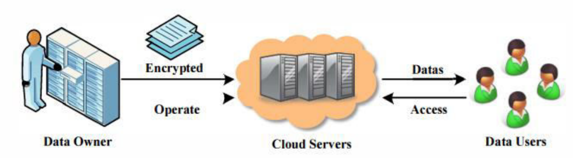

Fig. 1: STORAGE AND ACCESS PROCESS

The above figure (1) shows the block formation of storage & access process. The owner assigns a set of meaningful attributes which are necessary for access control for each data file. All data files can have a subset of attributes in common. Each attribute is associated with one attribute update. The access structure of each user is implemented through an access tree. In this access tree, interior nodes are threshold gates, and leaf nodes are the data file attributes. For the purpose of key management, we require the root node to be an AND gate with one child being the leaf node which is associated with the virtual attribute, and the other child node being any threshold gate. To do any operation in cloud, the user and the owner should register there. For registration the user and the owner will send a registration request to the corresponding domain authority. Then the domain authority verifies that is the new member accepting there terms and conditions. If they are ready to accept the terms and conditions, then the domain authority will forward that request to the trusted domain. Then the trusted authority will provide a permanent id to each of the owners and users. Then they can set a password for them.To upload a file, first the data owner will encrypt the file using his private key and send it to the next higher level. That is domain authority. Then the domain authority will check that the owner is a registered one or not. If he is a registered owner, then the domain authority will forward that encrypted file to the trusted authority. To download any file from the cloud, firstly the data user sends a request to his corresponding domain authority. Then the domain authority will verify the user. If it is a valid user, then it will forward that request to the trusted authority. Then the trusted authority will forward this request to the corresponding data owner. Then the owner will check the attribute set of that user. If the user have a valid attribute set, then the owner send a key to the user. When the owner send a key to the user then the clock will start counting. After a certain time period, that key becomes an invalid one. So the user should access the requested file within that time limit.Only the data owner can delete his file from the cloud. During the registration time of the data owner, the trusted authority will provide an id number to each of the data owners. These id numbers are permanent for them. Also each of them have a password, which is not permanent. To delete a file, the data owner firstly sends a request to his corresponding domain authority. This request contains the owner id and the file name. Then the domain authority will ask password to the owner. If the owner gives the correct password, then the domain authority will forward the deletion request to the trusted authority. After that the trusted authority will delete the file from cloud.Here the data owner can upload his file to the cloud. To make his file as more secured, firstly he will encrypt that file and then upload to the un trusted cloud. Only the data owner knows that the key to decrypt the files. So the uploaded files are safe in the un trusted cloud. When a data user wants to access any file from the cloud, then it send a request to the cloud. Then the cloud will forward that request to the owner. Then the owner will check the attribute set of that user. If the user have a valid attribute set, then the owner send a key to the user. When the owner send a key to the user then the clock will start counting. After a certain time period, that key becomes an invalid one. So the user should access the requested file within that time limit.

IV. RESULTS

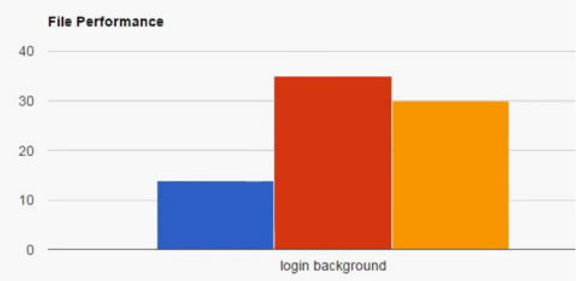

Fig. 2: performance comparison of logic background in access control scheme

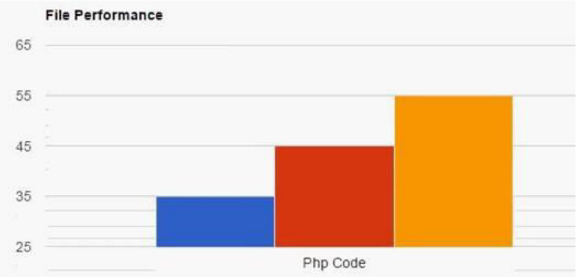

Fig. 3: performance comparison of pin code in access control scheme

IV. CONCLUSION

It is a highly efficient model for provide access control in cloud computing. It is in a hierarchical structure and it using a clock for providing decryption key based on time. This model ensure both security and access control in cloud computing. The main operations in this model are registration, file upload, file download and file deletion. When the user's permission is revoked, which greatly reduces the computation cost of data owners. Our scheme has prominent properties of user access permission confidentiality and user secret key accountability.

V. REFERENCES

[1] Y.G.Min, Y.H.Bang, "Cloud Computing Security Issues and Access Control Solutions", Journel of Security Engineering, vol.2, 2012.

[2] Z.Wan, J.Liu, R.H.Deng, "HASBE:A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing", IEEE Transactions on Forensics and Security, vol 7, no 2, APR 2012.

[3] P.Mell, "The NIST Definition of Cloud Computing." U.S. Department of Commerce:Special Publication 800-145.

[4] M.Li, S.Yu, Y.Zheng, K.Ren, 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, no 1, JAN 2013.

[5] Y.Tang, P.P.C.Lee, J.C.S.Lui, R.Perlman, "Secure Overlay Cloud Storage with Access Control and Assured Deletion," IEEE Transactions on Dependable and Secure Computing, vol 9, no 6 NOV/DEC 2012.

[6] Y.Zhu, Hu, D.Huang, S.Wang, "Towards Temporal Access Control in Cloud Computing," Arizona State University, U.S.A.

[7] A.R.Khan, "Access Control in Cloud Computing Environment," ARPN Journal of Engineering and Applied Sciences, vol 7, no 5, MAY 2012.

[8] B.Sosinsky, "Cloud Computing Bible," , Ed. United States of America: Wiley, 2011.

[9] M.Zhou, Y.Mu, W.Susilo, M.H.Au, "Privacy-Preserved Access Control for Cloud Computing," IEEE International Joint Conference, 2011.

[10] S.Yu, C.Wang, K.Ren, W.Lou, "Achieving Secure, Scalable, and Finegrained Data Access Control in Cloud Computing," Journel from Illinois Institute of Technology.