Attributes based Encryption with Seclusion Preserving in Clouds

J.Lavanya[1] U.Hari Prakash[2]
[1]Assistant Professor
[1,2]Department of Computer Science
[1]Idhaya College for Women, Tamil Nadu, India [2]Rajalakshmi Engineering College, Chennai, India

Abstract— *Cloud computing is used for renting the services. Different types of services are provided by cloud computing systems .Highly sensitive storage of data in clouds is taking place, hence Security and Seclusion of data in cloud is an area of concern. User Seclusion is also required so that the cloud or other users do not know the identity of the user. The cloud can hold the user accountable for the data it outsources, and likewise, the cloud is itself accountable for the services it provides. The validity of the user who stores the data is also verified. Apart from the technical solutions to ensure security and Seclusion, there is also a need for law enforcement. We propose a new decentralized access control scheme for secure data storage in cloud, that supports anonymous authentication. In the proposed scheme, the cloud verifies the authenticity of the server without knowing the user's identity before storing data. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. We also address user revocation. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The communication, computation, and storage overheads are better compared to the centralized approaches of the existing system.*

Keywords— Attributes based Encryption, Seclusion Preserving in Clouds

I. Introduction

Our scheme also has added the feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data store in the cloud. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. A hierarchical structuring of relations may result in more classes and a more complicated structure to implement. Therefore it is advisable to transform the hierarchical relation structure to a simpler structure such as a classical flat one. It is rather straightforward to transform the developed hierarchical model into a bipartite, flat model, consisting of classes on the one hand and flat relations on the other. Flat relations are preferred at the design level for reasons of simplicity and implementation ease. There is no identity or functionality associated with a flat relation. A flat relation corresponds with the relation concept of entity-relationship modeling and many object oriented methods.

II. Proposed system

We propose a new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication. Our scheme also has added the feature of access control in which only valid users are able to decrypt the stored information.

III. Implementation

The requirements specification is a technical specification of requirements for the software products. It is the first step in the requirements analysis process it lists the requirements of a particular software system including functional, performance and security requirements. The requirements also provide usage scenarios from a user, an operational and an administrative perspective. The purpose of software requirements specification is to provide a detailed overview of the software project, its parameters and goals. This describes the project target audience and its user interface, hardware and software requirements.

IV. System architecture

Research in cloud computing is receiving a lot of attention from both academic and industrial worlds. In cloud computing, users can outsource their computation and storage to servers (clouds) using Internet. Clouds can provide several types of services like applications (e.g., Windows Apps), infrastructures (e.g., Amazon's EC2), and platforms to help developers write applications (e.g., Amazon's S3). Much of the data stored in clouds is highly sensitive, for example, medical records and social networks. Security and Seclusion are thus very important issues in cloud computing. In one hand, the user should authenticate itself before initiating any transaction, and on the other hand, it must be ensured that the cloud does not tamper with the data that is outsourced. User Seclusion is also required so that the cloud or other users do not know the identity of the user. The cloud can hold the user accountable for the data it outsources, and likewise, the cloud is itself accountable for the services it provides. The validity of the user who stores the data is also verified. Apart from the technical solutions to ensure security and Seclusion, there is also a need for law enforcement. We propose a new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication. In the proposed scheme, the cloud verifies the authenticity of the server without knowing the user's identity before storing data. Our scheme also has added the feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data store in the cloud. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized.

V. Structural design

The proposed system, say has three users- user X, user Y, user Z. It also has a Cloud Server, a Cloud-Backup server and Multiple KDC's. When User x is uploading a file, the user has to get a token from the trustee, which verifies the user details and grants them the token. This token is now sent to the KDC where the user details are not revealed, but using the token provided by the trustee, KDC provides the user X with a Private and a Public key. If the user has already requested the keys at some other instant, it verifies the given token whether the token is unique. User X has now received the keys, using which user X can upload the data in the cloud. User X can set the access controls for other users. The data that has been uploaded is stored in the cloud backup server as well. Say User X has set Access control for User Y as read and User Z as Read and write. Now if user Y has to read the files, User Y will request the KDC for keys, once provided, the keys are used to display the data content. Now if user Z has to write the files, User Z will request for the keys, once provided, the keys are used to decrypt and download the data. Now once the file is been downloaded the contents of the file are liable to modify as the user Z has Read and Write access control and then can upload the file. The corruption of the file can be found out by String-matching algorithm, which compares each and every single string in the file uploaded by the owner and the modified file, in case of a corrupt file, the backup server will provide the original file as created by the File owner. The users having read access control, cannot download or edit the file, they cannot modify the existing file and the owner can amend the revocation of users (access controls). The keys are generated by Secure Hash algorithm in Trustee, while Paillier encryption technique is used by Key Distribution Center. The user identity is hidden and is not revealed to the Key Distribution Center and the Cloud Server.

VI. Conclusion

Thus Once the files are being updated the files are used for File Download, File Delete and File read. The files uploaded are saved automatically in the back-up server. In this project, System architecture is a life cycle of the implementation. It will provide the various security aspects using incentive protocol. This protocol works between the source and destination node. Every node temporarily store the reports and evidences and submit it to Trusted Party to get the payment correctly.

References

[1] S. Ruj, M. Stojmenovic and A. Nayak, "Seclusion Preserving Access Control with authentication for Securing Data in Clouds", IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, pp. 556–563, 2012.

[2] C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing", IEEE T. Services Computing, vol. 5, no. 2, pp. 220–232, 2012.

[3] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in IEEE INFOCOM. , pp. 441–445, 2010.

[4] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Financial Cryptography Workshops, ser. Lecture Notes in Computer Science, vol. 6054. Springer, pp. 136–149, 2010.

[5] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-based authentication for cloud computing," in CloudCom, ser. Lecture Notes in Computer Science, vol. 5931. Springer, pp. 157–166, 2009.

[6] A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-based cloud computing," in TRUST, ser. Lecture Notes in Computer Science, vol. 6101. Springer, pp. 417–429, 2010.

[7] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," in ACM ASIACCS, pp. 282–292, 2010.