Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 7, July 2015, pg.476 – 479

RESEARCH ARTICLE

Data Storage Using Decentralized Access Control With Multiple Authentication in Clouds

G.Divya[1], K.Kuppusamy[2]

[1]Research Scholar, Department of Computer Science & Engineering, Alagappa University, Karaikudi

[2]Professor, Department of Computer Science & Engineering, Alagappa University, Karaikudi

[1] divyagjk@gmail.com; [2] kkdiksamy@yahoo.com

Abstract - Cloud computing reaches enormous growth in an Internet-Based development and so privacy and security are the most important issues. In this paper, we propose a new decentralized access control scheme with multiple KDC's for securing data stored in cloud. In proposed scheme, the cloud provides the anonymous authenticity of the user through Third party auditor. Moreover, we implemented safe storage and access for creating a new file, modify the file and read the file in a cloud environment, a suitable encryption technique with key management is applied before outsourcing the data. We also secure access control by providing access to files with the policy-based access control using Attribute-Based Encryption (ABE) scheme. Multiple KDC's for key management is provided to achieve the decentralized architecture. Private Key is the combination of the user's credentials, so that high security will be achieved. The protocol supports multiple read and writes on the data stored in the cloud.

Keywords—Multiple KDC's, access control, decentralized, security, key management

I. INTRODUCTION

Cloud computing is a collection of scalable resources and computing infrastructure which provides services to users with the "pay only for use" strategy. 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 (also called clouds) using Internet[11]. This kind of technology helps users in handling resources effectively on-site. Though the advantages are clear, the critical factor in the present data outsourcing scenario is the enforcement of strong security mechanisms for data storage, transfer and processing in the cloud. The data that are stored in the cloud are often sensitive in nature. Remote backup system is the advanced concept which reduces the cost for implementing more memory in an organization[9]. For example, medical records and user-driven data generated in social networks are often stored in public or private clouds. Ensuring privacy and security of such data is important for users to trust the service providers. For achieving that, adequate authentication and access control techniques must be employed. A high level security system also ensures that only verified and valid services are provided to authorized users. Indeed, the process of authentication must be initiated for all valid transactions that are performed through the cloud. The first goal of our work is to implement anonymous authentication of users. The privacy settings of users must be followed in such a manner that the identity of the user should not become evident to either the cloud service providers or to other users. Thus, the anonymity of users is preserved. To provide secure data storage, the cloud data needs to be encrypted. The second goal of our work is to ensure data privacy and security. Many homomorphic techniques have been discussed. This kind of encryption ensures during the time that computations are performed on the data by a cloud's computing resources, they are not able to read the data. For this, the data must be suitably encoded before being encrypted. a decentralized architecture is proposed with several KDCs for key management. The main aim of paper is to design a scheme for distributed access control of data stored in cloud so that only authorized users with valid attributes can access them.

II. RELATED WORK

V. Goyal, et.al.,[2], worked on "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data ".In this paper, the sender has an authorization to encrypt information. A revoked attributes and keys of users cannot write again to stale information. The attribute authority receives attributes and secret keys from the receiver and he/she is able to decrypt information if it has matching attributes. There is a Distribution of audit-log information and screen out encryption.

In [3],J. Bethencourt, et.al., described that "Cipher text-Policy Attribute-Based Encryption". By using this approach the receiver has the access policy in the form of a tree. The tree contain attributes as leaves and monotonic access structure with AND, OR and other threshold gates. The main advantage is Encrypted information can be kept confidential even if the storage server is untrusted; Secure against collusion attacks.

In [5] M. Green, S. Hohenberger, and B. Waters, focuses on "Outsourcing the Decryption of ABE Ciphertexts,". This paper subcontract the decryption task to a proxy Server, so that the user made computation on minimum resources like hand held devices. Advantage is the user significantly saves bandwidth, without raising the number of transmission.

In [7] H.K. Maji,et.al., propose "Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance". In this paper, to ensure anonymous user authentication ABSs were introduced. This was also a centralized approach. The advantages of this is user significantly saves decryption time, without raising the number of transmissions.

III. SYSTEM MODEL

Firstly, the user get authenticated by registering user details in trustee and the trustee provide the token to authorize the verified user. After registration, the user can perform file operations such as writing a file, modifying the file and reading the file in cloud depends on their access policies. The user can get the key for encryption and decryption of files for file upload and downloading from any one of the Key Distribution Centre (KDC), which is presented in decentralized way.

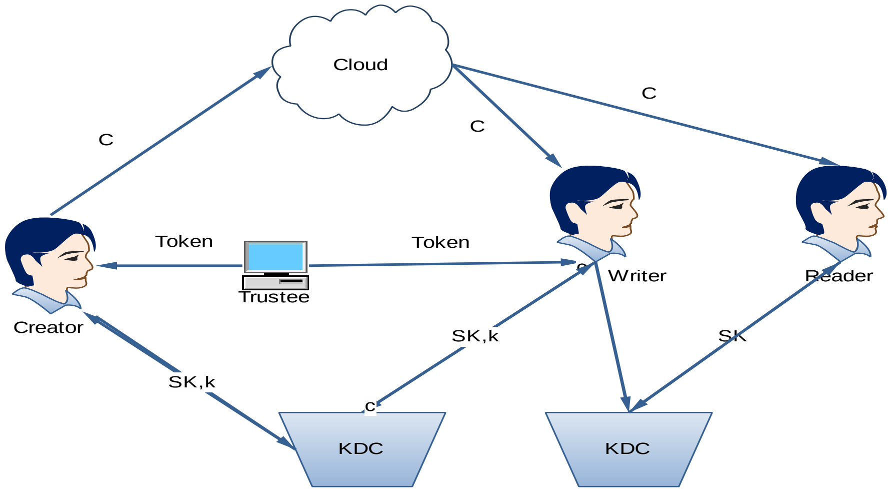

Fig. 1 Decentralized Access Mechanism

IV. PROPOSED WORK

A user gets authorisation by registering their details in cloud server and the trustee will generate token for authentication. By using the access control policy the user can perform specific operations. A user can upload a new file in cloud server, modify the file and read the file depends on their access rights. User files are stored in encrypted format using some encryption techniques with the help of Key Distribution Centre (KDC).
Steps involved in this system are described as follows:

A. User Registration

The users get registered to a particular KDCs by creating individual accounts by giving necessary details like user name, user id, password, email id and phone number. A successful registration is possible only if the details given by the user match with the KDC details.

B. Token Generation for anonymous authentication

All users initially register with their KDCs with their own unique identity UID. The KDC draws at random, key KBASE ∈ G, where a generator g generates random group of cyclic keys G. Now the token is generated typically as a combination of above parameters i.e. the user's UID, key and user's signature. The output token is γ = (UID, KBASE, K0, ρ), where ρ is the signature of the token generated using the authentication algorithm Digital Signature Standards with Secure Hash Algorithm (SHA-1). Hence the user details are hidden from cloud. In this way, an anonymous authentication is achieved.

C. Trustee and User Accessibility

After the registration process, users can log into their individual accounts with their credentials. Once the user logs in, specific operations such as file upload, file download, listing of files, revocation list and key details associated with that user can be performed. Third party authentication is done by a trustee where the user needs to get a token from the trustee for carrying out further operations. The contents of the token are again a typical combinations of user's user id, key and user signature. The hash function used for generating the user signature is Secure Hash Algorithm (SHA-1). Digital signatures are of great use in identifying the users uniquely and for checking the integrity of the content in case of tampering. In the proposed system, the signature is generated by taking the user's UID as input and finally the signature is obtained in a condensed format called message digest. This is obtained as a result of applying the hash function, and is computationally difficult to interpret at any point of time.

D. File Encryption and Upload

After the trustee's issuance of tokens to users, the users send their tokens to their respective KDC's for getting the keys for encryption and decryption of the files. The Paillier cryptosystem is implemented for generating keys. The users now encrypt their files with the received keys. They also set their own access policies, i.e. privileges to the file. The access policies set by individual users for their files that are hidden from other users by implementing a query driven approach. The user details are stored in encrypted format; therefore the attributes and privileges of users are hidden from the cloud.

E. File Decryption and Download

In this phase, the users can download the files from the cloud according to the access policies defined by the owners of the concerned files. The users satisfying access policy conditions can download a file and decrypt it using his private keys obtained from the corresponding KDC. This process is similar to file encryption and upload.

V. RESULTS AND DISCUSSION

The proposed scheme in the system uses strong authentication mechanism, where the users claim is validated at three levels. Initially, the users need to get themselves authenticated with KDC. For keys generation, a trusted third party verifies the user's credentials and gives back the secure token. Finally a message digest of the UID is generated using SHA-1 and the file to be uploaded is encrypted using Paillier cryptosystem. In this manner, a three way authentication is achieved. In this paper made key distribution is done in a decentralized way and verifies the trusted authority gives original token to user. The file access policy can be implemented with Multi Authority based Attribute based Encryption. This decentralized scheme provides user revocation and prevents replay attacks. Even though the cloud does not know the identity of the user who stores information, but it verifies the user's credentials. Using the technique we can avoid the number of wrong hits during authentication. Create a random delay for authentication, so the hacker can confuse to identify the algorithm.

VI. CONCLUSION

In this paper, we addressed the security and storage issues simultaneously based on the type of architecture, access control methods and the authentication techniques. The key distribution is done in a distributed way by implementing multiple KDC structure. The users are anonymously authenticated and their attributes are hidden from the cloud by implementing digital signature algorithm. The access policies associated with individual files are hidden from other users by implementing a Query based approach. Further, storage related security issues are enhanced by implementing a Homomorphic encryption technique to encrypting the outsourced data. Also, the cloud servers are prone to various types of attacks that can cause data loss or leakage. This issue is addressed by implementing a string matching algorithm that detects deviations and automatically retrieves the lost data using backed-up data.

REFERENCES

[1] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 457-473, 2005.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.

[4] M. Chase, "Multi-Authority Attribute Based Encryption," Proc. Fourth Conf. Theory of Cryptography (TCC), pp. 515-534, 2007.

[5] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the Decryption of ABECiphertexts," Proc. USENIX Security Symp., 2011.

[6] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance," IACR Cryptology ePrint Archive, 2008.

[7] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," Topics in Cryptology - CT-RSA, vol. 6558, pp.376-392,2011.

[8] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," Topics in Cryptology - CT-RSA, vol. 6558, pp.376-392,2011.

[9] R.Ranjith, D.Kayathri Devi "Secure Cloud Storage using Decentralized Access Control with Anonymous Authentication", Vol. 2, Issue 11, November 2013, IJARCCE.

[10] SushmitaRuj ,MilosStojmenovic ,Amiya Nayak , "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds", Issue No.02 - Feb. (2014 vol.25)pp: 384-394, Published by the IEEE Computer Society

[11] R.Ranjith, S.Murugaanandam, "Privacy Preserving Authenticated Access Control with Decentralized Key Management in Clouds", 2014 IJEDR | Volume 2, Issue 1 | ISSN: 2321-9939.

[12] Hemalatha,Balaji.V,Nirupama.P, "Anonymous Authentication for Decentralized Access Control of Cloud data", ISSN: 232 7782Issue 11, November 2014.