SECURE ACCESS CONTROL WITH MULTIPLE KEY VERIFICATION FOR CLOUD STORAGE

[1]Mr S Aravinda Krishnan, [2]Vijayalakshmi T, [3]Yashaswini T A, [4]S Sahithya

[1]Assistant Professor,Department of Computer Science and Engineering,SRM Institute of Science and Technology,Chennai,India. Email: [1]aravindakrishnan.s@vdp.srmuniv.ac.in

[2,3,4] Student,Department of Computer Science and Engineering,SRM Institute of Science and Technology,Chennai,India

ABSTRACT

Cloud brokers implemented an additional layer for enhanced security purpose for the data consumers, a dishonest broker can easily take advantage of the clients. So a secure system has been proposed in order to provide more security for the data that is stored in cloud. This system allows the trusted authority to securely store their data and share it to the data receivers. Using KP-ABE encryption algorithm, the data which has been uploaded by the data owners are encrypted and stored in cloud. We also propose a hybrid model by combining RSA and AES to provide multi key verification system in order to achieve more security. When the data receiver wants to download the file, a request is sent to the data owner seeking permission for downloading the key and also to ensure that the data receiver is an authorized user for accessing the data. After the request has been accepted by the data owner the data receiver can download the file(data) using the secret keys through which the data is decrypted. This method ensures more privacy to the data and provides security.

Keywords: *Cloudcomputing, KP-ABE, Hybrid model, DataProtection.*

1. INTRODUCTION

In cloud computing, there are chances for the data to get leaked through any third party entry or usage, Hence the data is vulnerable, therefore users need to encrypt the data before they are being shared. Access control prevents the data from unauthorized usage of the shared data. Attribute-based encryption keeps the data secured and provides data privacy from one-to-one and one-to-many data receivers. In Cipher text policy attribute based encryption(CP-ABE)[1]there are chances for data leakage because the central authority has the control over the secret keys which is used for decrypting the files stored in cloud.

Key policy attribute based encryption(KP-ABE) is much more flexible and can be used in general applications.. The encrypted file is uploaded to the Cloud Service Provider(CSP)[1] by the data owners. The data owner usually stores the shared files in hierarchical structure, by dividing the shared files in many subgroups located at different access levels. This integrated access structure saves storage cost and time cost. In this model , the data owner holds the authority of allowing who can view the data or file shared. The entire cloud sharing takes between data owner and data receiver. The data receiver sends the request for the file which he wants to download and data owner checks of he is an authorized user or not and once verified, the owner shares the key. The data receiver downloads the key to access the decrypted file. The cipher text is decrypted only if the matching set of attributes is uploaded. The key work creation distribution is achieved on multiple authorization domains and the burden of key authority center is made easy.

2. RELATED WORK

Data access control is a troubled issue in public cloud storage. CP-ABE[1] based encryption proves to be flexible, fine-grained, and secure data access for cloud storage servers. However in the existing CP-ABE scheme, the single attribute authority is time consuming and secret key distribution is not achieved easily. Hence it results in single point performance also there might be a loss in the private key, loss in the private means the receiver may not receive the decrypted messages. In the attribute based access in cloud-assisted content sharing networks, it combines a novel Multi-message cipher-text Policy attribute[3] based encryption technique and this design is used to access the control scheme for sharing scalable media data. In this technique, the decryption is slow for low-end devices because a modular exponentiation operation will be required. In the enabled personalized search for the encrypted outsourced data, the personalized multi-keyword ranked search over encrypted data(PRSE)[2] in cloud computing for privacy preservation, with the help of Wordnet, the user creates an interest model to track the history of the users to express user interest efficiently. The main disadvantage of this model is that there is no user privacy and the data are not secured but monitored which makes creates data vulnerability. Also in the Improving privacy and security in the multi-authority attribute-based encryption, it determines decryption ability based on a user's attributes. In this attribute methodology, the user obtain the keys for appropriate decryption by a trusted central authority(CA)[2] and global identifiers(GID). The CA has the power to decrypt every cipher text. The use of consistent GID allows the authorities to combine the information to build a full profile of all the user's attributes which is again a threat to the user's privacy. In order to provide more privacy to the data, a new method of eliminating the central authority(CA) has been introduced and implemented.

3. PROPOSED APPROACH

We propose a secured data cloud storage system, which allows the authorized data owners to securely upload their confidential data on the cloud. The data which has been stored in the cloud is of encrypted form so that the data stored is protected and can be selectively shared to the data receivers by decrypting the cipher text. Different from other encryption policies which uses a central authority as a mediator between data owners and receivers to share the secret keys for downloading the files, we use KP-ABE method. Data owners upload their files in the cloud storage. The uploaded files get stored only when the data owners has space allocated to them, i.e. only authorized person can store their files in cloud. The uploaded files are encrypted using KP-ABE Encryptions scheme. We also propose a hybrid model by combining RSA and AES algorithms for multi key verification. Using this hybrid model we can generate three keys to secure the data. This hybrid model provides more security to the data uploaded by the trusted authority. The uploaded cipher text is further spilt based on its size and stored in six data centers such that the original file is not got until correct keys are uploaded to download the file. The data owner has the access for the file he has uploaded. When the data receiver wants to download the file, a request is sent to the data owner seeking permission for downloading the key and also to ensure that the data receiver is an authorized user for accessing the data. After the request has been accepted by the data owner the data receiver can download the file(data) using the secret keys through which the data is decrypted. Attributes have been set in order to provide additional security to reach the download page. The original file is got only when all the keys are uploaded correctly until then decryption will not occur. This hybrid models generates multiple keys which are needed to integrate the cipher texts which is stored in multiple locations. This eliminates unauthorized access of the cipher text. Performance measurements indicate that the proposed system is efficient in securing the data by restricting unauthorized access and has a low computation time.

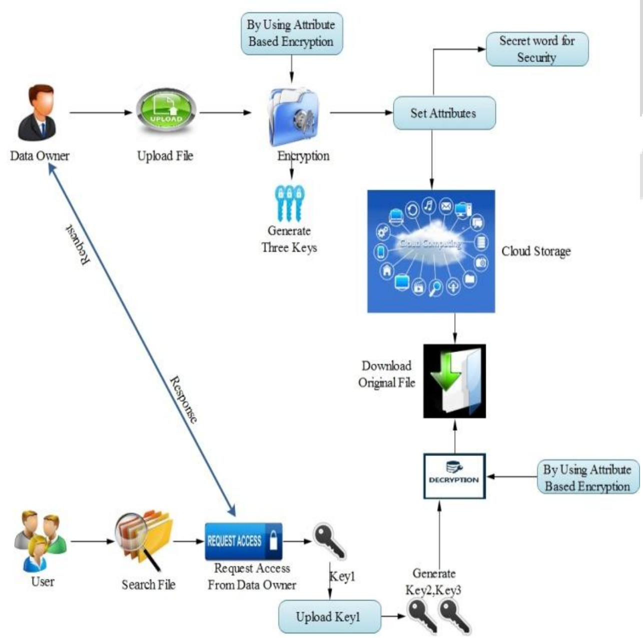

Fig-1 System Architecture

4. ALGORITHM

KP-ABE(Key Policy Attribute based Encryption) is used for encrypting the data which is been stored in the cloud in order to provide secure storage. The files that are uploaded by the data owners are encrypted using KP-ABE. In order to provide more secure access to the data we propose a hybrid model by combining RSA and AES for multi key verification system. Using this hybrid model we generate three keys for secure access. Unless until the data receivers upload the correct keys, decryption will not occur and thus the original file cannot be downloaded.

4.1 Encryption of file

The file is encrypted by the procedure Encryption (b) where the key is initialized and takes the whole file as a message using the new fileoutputstream(out) where byte is stored as the new byte. Inorder to read the files, initialization is done to read the file. While i! = -1 do ,inorder to write the we use fos.write (b, 0, i); i=cis.read (b); -p to read the files. The file encrypted is stopped using the end while.

4.2 Key generation

The key generation is achieved using the Procedure Summation Keygen ( ) masking public key & byte format and for each i=0 upto i<byptes12.lenght and for initialization, int j=bytes12 [i]; Inorder to convert the string to binary we use, String s3=Integer.toBinaryString (j); String temp= temp + Integer.parseInt (s3); S3=toBinaryString (temp); when the key is generated we end the program by using the end for ; end Procedure.

4.3 Decryption of file

The encrypted file is decrypted using the procedure Decryption (b) where the file that has to be encrypted. nit (cipher.DecryptMode, Secret key); cis=new fileOutputStream (fis, encrypt); fos=new fileOutputStream (dec);byte [ ] b=new byte [8]; to read the file we use inti=cis.read (b); while i! =-1 do; fos.write (b, 0, i); i=cis.read (b); the decryption of file is completed using the end while; end Procedure

5. CONCLUSION

A cloud based secure data system is proposed that allows the authorized data owners to securely upload their confidential data on the cloud service providers. This service provider shares the data between the data owner and data receiver without any untrusted or unauthorized users to access the files. Data owners can encrypt their files using the KP-ABE encryption scheme. A hybrid model of RSA and AES is used to provide more security to the data. The security and efficiency analysis shows the hybrid model is not only efficient but also practical. The hierarchical structure of storing files in multiple parts enables scalability and flexibility, reducing any threat to the shared data. This prevents from any illegal or unauthorized access to the data. When the owner uploads the files, the receiver can request for the desired file and when the request is accepted by the owner of the data, the data receiver will be able to download the file. Hence more privacy is provided and time complexity and space complexity is eliminated making this model more efficient and trusted cloud service provider.

REFERENCES

[1]. Seunghwan Park, Kwangsu Lee, and Dong Hoon Lee ,"New Constructions of Revocable Identity-Based Encryption From Multilinear Maps", 1556-6013 © 2015 IEEE

[2]. U Tejaswi , V P S Vinay Kumar," Identity-based Encryption with Outsourced Revocation in Cloud Computing" IJAEM 040107 Copyright @ 2015 SRC. All rights reserved.

[3]. Alexandra Boldyreva,Vipul Goyal, Virendra Kumar , "Identity-based Encryption with Efficient Revocation", 14th ACM Conference on Computer and Communications Security, CCS 2008, ACM Press, 2008.

[4]. Dan Boneh and Matt Franklin,"Identity-Based Encryption from the Weil Pairing", CRYPTO 2001, LNCS 2139, pp.213-229, 2001.

[5]. Benoit Libert and Damien Vergnaud "Adaptive-ID Secure Revocable Identity-Based Encryption", ICT-2007-216646 ECRYPT II

[6]. Amit Sahai and Brent Waters,"Fuzzy Identity-Based Encryption",R. Cramer (Ed.): EUROCRYPT 2005, LNCS 3494, pp. 457–473, 2005.

[7]. Eiichiro Fujisaki ,Tatsuaki Okamoto, “How to Enhance the Security of Public-Key Encryption at Minimum Cost”, E-83A(1):24{32, Jan.2000.
[8]. Benoit Libert , JeanJacques Quisquater “ Efficient revocation and threshold pairing based cryptosystems” PODC '03 Boston, Massachusetts USA Copyright 2001 ACM 089791886/97/05 ...$5.00.
[9]. Jae Hong Seo and Keita Emura ,“Revocable Hierarchical Identity-Based
Encryption: History-Free Update, Security Against Insiders, and Short Cipher texts”, K. Nyberg (ed.): CT-RSA 2015, LNCS 9048, pp. 106–123, 2015.
[10]. Jae Hong Seo and Keita Emura ,“ Revocable Identity-Based Encryption Revisited: Security Model and Construction”, January 10, 2013
[11] P.-W. Chi and C.-L. Lei, ”Audit-free cloud Storage via deniable attribute-based encryption,” IEEE Transactions on Cloud Computing, article in press (DOI: 10.1109/TCC.2015.2424882), 2015.
[12] J. Li, Y. Shi, and Y. Zhang, ”Searchable ciphertext-policy attributebased encryption with revocation in cloud storage,” International Journal of Communication Systems, article in press (DOI: 10.1002/dac.2942), 2015.
[13] H. Qian, J. Li, Y. Zhang, and J. Han, ”Privacy preserving personal health record using multi-authority attribute-based encryption with revocation,” International Journal of Information Security, vol. 14, no. 6, pp. 487-497, 2015.
[14] A. Fiat and A. Shamir, “How to prove yourself: practical solutions to identification and signature Problems,” Proc. Crypto’ 86, LNCS, vol. 263, pp. 186-194, 1987.
[15] K. Kurosawa and S. Heng, “From digital signature to ID-based identification/signature,” Proc. PKC’04, LNCS, vol. 2947, pp 248-
261, 2004.
[16] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, “Strong authentication for RFID systems using the AES algorithm,” Proc. CHES’04, LNCS, vol. 3156, pp. 357-370, 2004.
[17] Y.-M. Tseng, T.-Y.Wu, and J.-D.Wu, “A pairing-based user authentication scheme for wireless clients with smart cards,” Informatica, vol. 19, no. 2, pp. 285-302, 2008.
[18] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, and T. Kivinen, “Internet key exchange protocol version 2 (IKEv2) ,” IETF, RFC 7296, 2014.
[19] A. Freier, P. Karlton, and P. Kocher, “The secure sockets layer (SSL) protocol version 3.0,” IETF, RFC 6101, 2011.

.