Preserving Privacy for Access Policies for Secure Data Storage in Clouds

K.Rohini
M.Tech Student, Department of CSE
JNTUA College of Engineering Ananthapuramu
Andhra Pradesh, India
E-mail: rohini.tdpr@gmail.com

Dr.K.Madhavi
Assistant Professor, Department of CSE
JNTUA College of Engineering Ananthapuramu
Andhra Pradesh, India
E-mail: kasamadhavi@yahoo.com

Abstract: **Cloud computing is well known for its ubiquitous behavior, as the users can store and avail the data from cloud at any point of time irrespective of the location through internet. In the current era, cloud computing is receiving lots of attention from the researchers to enhance the access control policies of the user in retrieving confidential data stored in the cloud. This paper addresses the problem of securing the highly sensitive data stored in the clouds. As the cloud server is aware of accessibility policy of each record stored in it, a novel and enhanced privacy preserving framework is proposed based on cipher-text policy attribute based encryption mechanism. In this case, the user can assign a security policy based on the attributes and restrict the unauthorized and anonymous users accessing the confidential data. In general, during cipher-text policy attributes based encryption cipher-texts are allied with access policies as well as the keys are allied attribute set. The proposed schema specifies that, it is not necessary to associate the access policy along with the cipher text such that the user privacy is guaranteed. For this purpose, Paillier algorithm is used for hiding user access policies.**

Keywords—Access Control; Authentication; Cloud storage; Access policy; Attributes

I. INTRODUCTION

Now a days cloud computing is a rationally developed technology to store data from more than one client. Cloud computing is an environment that enables data independence and location transparency. Remote backup system is the advanced concept which reduces the cost for implementing more memory in an organization. It helps enterprises and government agencies reduce their financial overhead of data management. They can archive their data backups remotely to third party cloud storage providers rather than maintain data centers on their own. An individual or an organization may not require purchasing the needed storage devices. Instead they can store their data backups to the cloud and archive their data to avoid any information loss in case of hardware / software failures. Even cloud storage is more flexible, how the security and privacy are available for the outsourced data becomes a serious concern. There are three objectives to be main issue

Confidentiality – preventing sensitive information from unauthorized persons. The main threat accomplished when storing the data with the cloud.

Integrity – the assurance that information can only be accessed or modified by authorized one’s.

Availability – is a guarantee of reliable access to the information by authorized people.

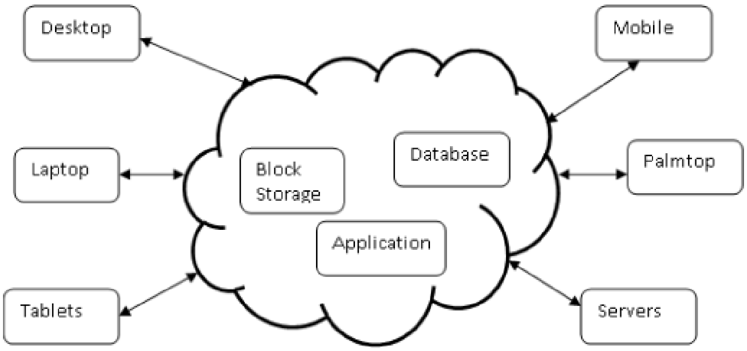

Fig1: Example diagram for data sharing with cloud storage

To achieve secure data transaction in cloud, suitable cryptography method is used. The data owner must encrypt the file and then store the file to the cloud. To overcome the problem with hackers there are lot of techniques introduced to make secure transaction and secure storage.

The notion of ABE, which was presented by Sahai and Waters [1], has attracted abundant attention from diverse academicians to construct a versatile and scalable access management system as ABE allows public key based on one-to-many coding. The encryption standards used for transmit the file securely. The encryption technique was implemented with set of key operations to maintain the secrecy. Recently, addressed Anonymous Authentication for data storing to clouds. Anonymous authentication is the process of validating the user without the details or attributes of the user. An anonymous ABE was introduced in [2, 3] and it is improved by [4]. Anonymous Attribute Based Encryption has a broad range of applications for instance, in some military circumstances So the cloud server doesn’t know the details or identity of the user, which provides privacy to the users to hide their details from other users of that cloud. Security and privacy protection in clouds are examined and experimented by many researchers[9][15]. Using homomorphic encryption[10][11], the cloud receives cipher text and performs operations on cipher text only. The cloud does not know on what data it has operated on, but the result can be decoded by the user.

II. RELATED WORK

A. Attribute-based Encryption (ABE) Scheme:

In [5][13] Waters and Sahai presented an attribute based encryption scheme which consists of an administrator, sender and a receiver. The role of the administrator is to generate predefined keys based on the attributes of the master key and a public key. Initially, if a new user is to be included into the system and he holds attributes of his own the administrator will redefine the attributes to generate master and public key for that particular user. While transmitting the data it is the responsibility of the sender to encrypt the data with a set of descriptive attributes and a public key. The main role of the receiver decrypts the encrypted data using the private key obtained from the administrator.

B. Key-Policy ABE Scheme:

KP-ABE (Key-Policy Attribute Based Encryption) scheme was presented in [6][14]. KP-ABE initially builds an access policy in the user's private key based on the set of attributes that describes the encrypted data.

C. Cipher-text-Policy (CP) ABE scheme:

Bethencourt et al in [7][12] presented Cipher-text-Policy ABE scheme, in which the access policy is designed based on the encrypted data instead of a user's private key as specified KP-ABE. During CP-ABE, the access policy is designed with the encrypted data and a set of the attributes are allied with the user's private key. The receiver can decrypt the data only If the attributes in user's private key persuade the access structure of the encrypted data, else the message cannot be obtained.

D. Decentralized Access Control with Anonymous Authentication:

Sushmita Ruj [8] presented a technique which provides authentication for anonymous users, which facilitates user revocation and replay attacks. By using this only valid users can decrypt the data based an access policies but the Cloud knows the access policies of every file is the problem.

III. PROPOSED SCHEME

Decentralized access control for the confidential data in the cloud could be achieved only if the authoritative users with legitimate attributes can access them. On using the proposed scheme, the user identity is confined form the cloud servers during authentication.

The architecture explains about the following:

- Cloud storage server : It can be used to store the data and to access the data.
- Decentralized Key Generator : It generates keys for both encryption/decryption and signing.
- Trustee : A trustee can be an individual or organization which holds or manages social insurance numbers.
- Creator : The message MSG is encrypted under access policy and it decides who can access the data.
- User : When a user wants to read, the cloud sends Cipher text. The user decrypts the cipher text into plain text only when the user has the matching attributes.

During the process of key generation the access policy is designed for each user depending on the token Υ issued by the trustee which is considered as a central administrator. Once if the creator receives a token, then it is forwarded to the DKG where the private key is generated based on the access policy and attribute set.

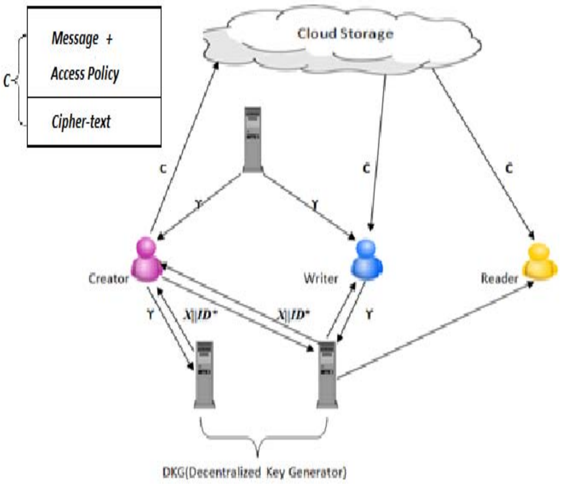

Fig2: Cloud Server Architecture

The process of key generation is accomplished based on the paillier algorithm, an asymmetric probabilistic algorithm for public and private key cryptography.

The steps involved for keygen is as follows:

Step 1***:*** Select two distinct large prime attributes 'm' and 'n' with equal length in such a way that

$\gcd(mn,(m-1)(n-1)) = 1$.

Step 2 ***:***Calculate $P = mn$ and $\alpha = \mathrm{lcm}(m-1,n-1)$.

Step 3: Choose random integer ***i*** such that $i \in X^*_{p2}$

Step 4: Make sure that the value of P is divisible with the order of ***i*** using modular multiplicative inverse such that

$\boldsymbol{\mu} = (K(i^{\lambda} \bmod p^2)) \bmod p$ where 'K' is defined as $K(b) = \frac{b-1}{i}$.

Encryption In the process of encryption ,

Step 1***:*** Let us consider M_{sg} be the message to be encrypted where $M_{sg} \in X_p$

Step 2***:*** choose a random attribute r where $r \in X_p{}^*$

Step 3: determine ***cipher text*** as $C = i^{Msg} . r^P \bmod P^2$

Decryption During the process of decryption,

Step 1***:*** Let us consider C as the ciphertext to be decypted where $C \in X^*_{p2}$

Step 2: Determine the plain text as $M_{sg} = K(C^{\lambda} \bmod p^2)\, \boldsymbol{\mu} \bmod P$

In the process of decrypting the ciphertext under the ciphertext policy 'X' such that the DKG extracts the attribute set from the corresponding message such that the attribute set is defined as $\boldsymbol{A_L}$=(φ1, φ2, φ3.... φn) out of X. Finally, with the help of the Decentralized key generator the reader could be able to decrypt the message.

IV. DESIGN

In this section, we present the design of our proposed work. First, we present the File uploading process as well as File downloading process.

A. File Upload

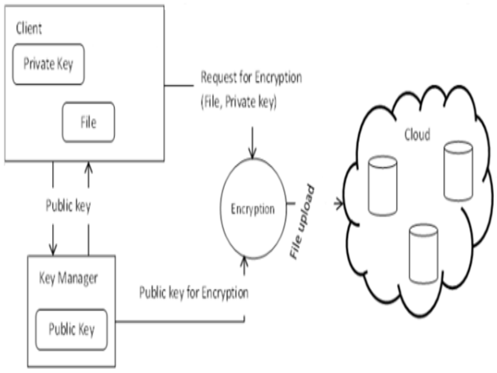

Fig3: File uploading process.

The client made request to the key manager for the public key, which will be generated according to the policy associated with the file. Based on access policies, public key also differs. But for same public key for same policy will be generated. Then the client generates a private key by combining the username, password and security credentials.

Then the file is encrypted with the public key and private key and forwarded to the cloud.

B. File Download

The client can download the file after completion of the authentication process. As the public key maintained by the key manager, the client request the key manager for public key. The authenticated client can get the public key. Then the client can decrypt the file with the public key and the private key. The users credentials were stored in the client itself. During the file download the cloud will authenticate the user whether the user is valid to download the file. But the cloud doesn't have any attributes or the details of the user.

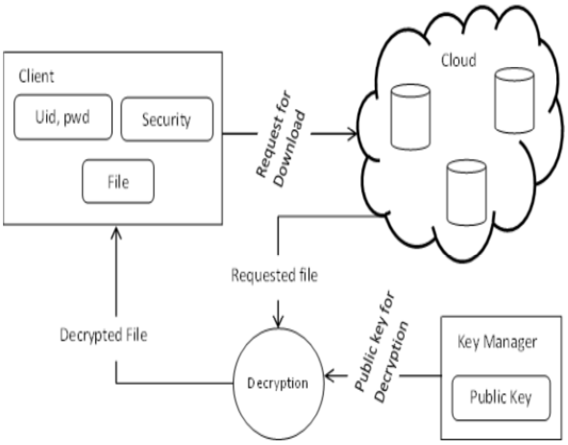

Fig4: File downloading process

V. COMPARISON OF OUR SCHEME WITH EXISTING ACCESS CONTROL SCHEME

Below is the table1 that compares our scheme with other existing schemes like secure efficient access to outsourced data, Effective Data Access Control for Multi-authority attribute based encryption and others.

1-W-M-R means One Writer & Many Readers, M-W-M-R means Many Writers & Many Readers. Some of the schemes supports only 1-W-M-R but out scheme supports M-W-M-R. All other schemes do not support all the features that specified in the above table, but our scheme is decentralized and it provides privacy preserving authentication.

Table1:Comparison with other schemes

Schemes	**Centralized/ Decentralized**	**Write/Read Access**	**Privacy Preserving Authentication**	**Preserving Privacy for Access Policies**
Secure and efficient access to outsourced data	Centralized	1-W-M-R	No Authentication	No
Effective Data Access Control for Multi-authority attribute based encryption	Decentralized	1-W-M-R	Not privacy preserving Authentication	No
Access control to outsourced data with attribute based cryptosystems	Decentralized	M-W-M-R	Authentication	No
Preserving Privacy for Access Policies For more secure data storage	**Decentralized**	**M-W-M-R**	**Authentication**	**Yes**

It also has the added feature of preserving privacy for access policies of the users, but other schemes do not have this feature.

V. CONCLUSION

In this paper, we presented a secure cloud storage utilizing decentralized access control together with anonymous authentication. Eventually, on using this technique the cloud will not be able to know the user details, but it still verifies the authentication details of the user. As the cloud is aware of the access policies for each record, Paillier cryptosystem is used to hide the access policies of the user for more secure data storage. The particular files tend to be related to file access policies, in which utilized to access the particular files positioned on the cloud. Uploading as well as downloading of an file with a cloud together with standard Encryption / Decryption is actually more secure.

REFERENCES

[1] Amit Sahai and BrentWaters. Fuzzy Identity-Based Encryption. EUROCRYPT'05, LNCS 3494, pp. 457-473, Springer, 2005.

[2] Apu Kapadia, Patrick P. Tsang, and Sean W. Smith. Attribute-based Publishing with Hidden Credentials and Hidden Policies. In Proc. of Network and Distributed System Security Symposium (NDSS), pp. 179-192, 2007.

[3] Shucheng Yu, Kui Ren, and Wenjing Lou. Attribute-Based Content Distribution with Hidden Policy. NPSEC'08, pp. 39-44, 2008.

[4] Takashi Nishide, Kazuki Yoneyama, and Kazuo Ohta. ABE with Partially Hidden Encryptor-Specified Access Structure. ACNS'08, LNCS 5037, pp. 111-129, Springer, 2008.

[5] Sahai and B.Waters. Fuzzy identity based encryption. In EUROCRYPT, pages 457–473, 2005

[6] Shucheng Yu, Kui Ren, Wenjing Lou, and Jin Li. Defending Against Key Abuse Attacks in KP-ABE Enabled Broadcast Systems. Accepted by SECURECOMM'09. Also available at http://eprint.iacr.org/2009/295.

[7] J. Bettencourt, A. Sahai, and B.Waters"Ciphertext-policy attribute based encryption "in Proceedings of IEEE Symposium on Security and Privacy, pp. 321V334, 2007

[8] S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds," Proc.IEEE/ACM Int'l Symp. Cluster, Cloud and Grid Computing, pp. 556-563, 2012.

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

[10] C. Gentry, "A Fully Homomorphic Encryption Scheme," PhD dissertation, Stanford Univ., http://www.crypto.stanford.edu/ craig, 2009.

[11] A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-Based Cloud Computing," Proc. Third Int'l Conf. Trust and Trustworthy Computing (TRUST), pp. 417-429, 2010.

[12] X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp 343-352, 2009.

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

[14] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure Threshold Multi- Authority Attribute Based Encryption without a Central Authority," Proc. Progress in Cryptology Conf. (INDOCRYPT), pp. 426-436, 2008.

[15] M. Chase and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. ACM Conf. Computer and Comm. Security, pp. 121-130, 2009.

BIOGRAPHIES

K.Rohini received B.Tech degree in Information Technology from Rajeev Gandhi Memorial College of Engineering and Technology Nandyal, affiliated to JNTUA College of Engineering, Ananthapuramu, A.P, India, during 2009 to2013. Currently pursuing M.Tech in Software Engineering at JNTUA College of Engineering, Ananthapuramu, A.P, India, during 2013 to 2015.Her area of interest is Cloud Computing.

Dr. K. Madhavi is an Assistant Professor of Computer Science and Engineering at Jawaharlal Nehru Technological University College of Engineering, Ananthapuramu. She obtained her Bachelor degree in Electronics and Communication Engineering, Master of Technology in Computer Science from Jawaharlal Nehru Technological University Ananthapuramu and Ph.D. in Computer Science and Engineering from Jawaharlal Nehru Technological University Ananthapuramu. She has published several Research papers in National \ International Conferences and Journals. Her research interests includes Computer Networks and Wireless Networks.