An Efficient Multi Authority and Privacy of Data Access Control in the Cloud Storage Systems

Reddi Narendra Kumar[1], Behara Vineela [2]

Final M.Tech Student[1], Asst.professor[2]

[1,2]Dept of CSE, *Sarada Institute of Science, Technology and Management (SISTAM), Srikakulam, Andhra Pradesh*

Abstract: *Cloud Storage is an important service of cloud computing for storing data into cloud and retrieve data from the cloud computing. So that the data owners will allow to stored data into cloud and users to access data from the cloud. Data access control is an effective way to ensure that provide security of stored data in the cloud. However cloud service separates the roles of the data owner from the data service provider and the data owner does not interact with the users directly for providing data access service, which makes the data access control a challenging issue in cloud storage systems. Because the cloud server cannot be fully trusted by data owners, existing server-based access control methods are no longer applicable to cloud storage systems. To prevent the untrusted servers from accessing sensitive data, traditional methods usually encrypt the data and only users holding valid keys can access the data. These methods require complicated key management schemes and the data owners have to stay online all the time to deliver keys to new users in the system. Moreover, these methods incur high storage overhead on the server, because the server should store multiple encrypted copies of the same data for users with different keys. By overcome those problems we can implement the cipher text policy based key generation schema will be used for generation for of the encryption key. After generating key the data owner will encrypt the data using idea algorithm and stored the data into cloud storage. If any user retrieve the file it will authenticated by using one time password authentication schema. After completion of authentication schema each user will retrieve the file and decrypt it. By performing those functionalities we can improve the efficiency of the project and also provide more privacy of stored data into cloud.*

Keywords: *Data Access Control, Authentication, Signature, Cryptography, one time password.*

I. INTRODUCTION

Now a day's cloud computing is an intelligently developed technology to store data from number of client. Cloud computing allows users to remotely store their data over cloud. Remote backup system is the progressive technique which minimizes the cost of implementing more memory in an organization. It helps government agencies and enterprises to reduce financial overhead of data management. They can extract their data backups remotely to third party cloud storage providers than maintaining their own data centres. An individual or an organization does not require purchasing the storage devices. Instead they can store their data to the cloud and archive data to avoid information loss in case of system failure like hardware or software failures. Cloud storage is more flexible, but security and privacy are available for the outsourced data becomes a serious concern.

To achieve secure data transaction in cloud, suitable cryptography method is used. The data owner must after encryption of the file, store to the cloud. If a third person downloads the file, they can view the record if they had the key which is used to decrypt the encrypted file. To overcome the problem Cloud computing is one of the emerging technologies, which contains huge open distributed system. It is important to protect the data and privacy of user. Certificate authority could be an international trustworthy certificate authority within the system. It sets up the system and accepts the registration of all the users.

The owner sends the encrypted knowledge to the cloud server in conjunction with the cipher texts. they are doing not trust the server to try and do knowledge access management. But, the access management happens within the cryptography. That's only if the user's attributes satisfy the access policy outlined within the cipher text; the user is in a position to decode the cipher text. Thus, users with completely different attributes will decode different number of content keys and therefore get totally different granularities of information from a similar data.

II. RELATED WORK

Wei Li, et al. [1] in access control systems for public cloud storage, brings a single-point bottleneck on both security and performance against the single authority for any specific attribute. First design multi-authority access control architecture to deal with the problem. By introducing the combining of (t, n) threshold secret sharing and multi-authority CP-ABE scheme, then proposes and realizes a robust and verifiable multi-authority access control system in public cloud storage, in which multiple

authorities jointly manage a uniform attribute set. Further by efficiently combining the traditional multi-authority scheme with this scheme, construct a hybrid one, which can satisfy the scenario of attributes coming from different authorities as well as achieving security and system-level robustness.

Yang, et al. [2] proposed a revocable multi-authority CP-ABE scheme, where efficient and secures revocation method introduced to solve the attribute revocation problem in the system. Attribute revocation method is efficient in the sense that it incurs less communication cost and computation cost, and is secure in the sense that it can achieve both backward security and forward security. This scheme does not require the server to be fully trusted, because the key update is enforced by each attribute authority not the server. Even if the server is not semi-trusted in some scenarios, this scheme can still guarantee the backward security. Then, apply proposed revocable multi-authority CP-ABE scheme as the underlying techniques to construct the expressive and secure data access control scheme for multi-authority cloud storage systems.

Shamir [3] proposed the concept of identity-based cryptography and Boneh et al. [4] constructed the first practical system identity-based cryptography. Sahai et al. [5] presented a fuzzy identity-based encryption scheme which is the earliest prototype of attribute-based encryption (ABE). Goyal et al. [6] further clarified the concept of ABE and proposed two complimentary forms of ABE: key-policy ABE (KP-ABE) and ciphertext-policy ABE (CPABE). According to Goyal's KP-ABE scheme, Bethencourt et al. [7] proposed a CP-ABE scheme that was closer to real access control systems. CP-ABE relates the user's secret key with a set of attribute and associates the ciphertext with an access structure tree. If the attribute set satisfies the access structure tree, then the user has the ability to decrypt the data. As CP-ABE schemes [7]-[8] are more natural to accomplish access control, we focus on the CP-ABE to realize our scheme.

III. PROPOSED SYSTEM

In this paper we are proposed an efficient data access control mechanism and also provide security of stored data into cloud storage. The proposed system mainly contains four entities are certificate authority, cloud server, data owner and data consumers. Here the certificate authority is a global trusted over the system and the certificate authority will perform the authentication process of each data consumer in the cloud. Before performing the authentication process the data consumers will register into cloud and also give the username, password of each data consumers. By using those username and passwords each user or data consumer will enter authentication process and perform the verification process of each user. By completion of verification or authentication process of data consumer, the data owner will encrypt the file and stored into cloud server. After completion of encryption process each data consumer will choose the decryption process. Before perform the decryption process the system will generate one time password and send that password to respect mobile of data consumer. After successful verification of one time password, it will get decryption provision of file. By retrieve required file and perform the decryption process will get plain format of data. The implementation procedure of all those entities is as follows.

Signature Generation and Data Consumers Authentication Process:

In this module each data consumer or user communicates with the Certificate Authority. The communication process can be done by performing verification of users in the cloud computing. Before performing the authentication or verification process of users, each user will generate signature by random universal key signature generation schema. The implementation process of random universal key signature generation schema is as follows.

1. Each user or data consumer will randomly generate two prime numbers P and Q.

2. By using those prime value user will calculate public key and private key is as follows.

n= P* Q

Private Key= (P, Q)

3. After generating public key and private key each user will randomly choose universal key (U_i).

4. By using those values each user will generate signature by using following code.

Xor= username^ U_i

Hash code (h1) =Hash (xor)

sig1= h1% n;

S_i=sqrt (sig1)

5. After generating signature S_i value send to certificate authority. Before sending Signature each user also sends universal key and public key to certificate authority.

By using those values the certificate authority generate signature and compare the both signature are equals or not. The implementation procedure of verification process is as follows.

1. The certificate authority will retrieve universal key, public key and signature from the data consumers.

2. By using those values the certificate authority again generate signature by using following code. The certificate authority will retrieve each username and perform xor operation with universal key.

Xor=U_i ^ username
Hash code= hash (Xor)
Modval= hashcode% public key
Sig= sqrt (Modval)

3. After generating sig value the certificate authority will compare those values to user signature value. If the both values are equal users are authenticates users or else not authenticated.

After completion of authentication process the certificate authority will send that status to each data consumer or user. Each user will retrieve the authentication status and status will contains authenticated user, then the user will get provision for decryption process. Before performing the decryption process each user also again verified by system for processing one time password verification. Before performing those operations the data owner will encrypt the data and stored into cloud.

Cipher Text Policy based Key Generation Schema and Encryption Process

In this module the data owner will encrypt the stored data and stored into cloud storage. Before performing the encryption process the data owner will choose stored file and retrieve the name of file. In the encryption process the key will be used as name of file. Before using the file name as key the data owner will encrypt that file name and use that cipher format data as key of the encryption process. The generation of cipher formatted key by using cipher text policy based key generation schema. The implementation procedure of cipher text policy based key generation schema is as follows.

1. The sender enter plain format data contain character A-M will be transformed into plain text ascii code value pulse 45.

2. The character of plain text contains N- Z will be transposed into plain text ascii code value pulse 19.

3. The plain text range between a-m will be transposed into plain text ascii code value minus 19.

4.The plain text range between n-z will be transpose into plain text ascci code value minus 45.
5. In the second classification process the plain text character range between 0-4 the cipher text is equal to multiplied by 2 plus one.

6. The plain text character range between 5-9 the cipher text is equal to plain text multiplied by 2 minus 10.

7. In the third classification process of plain text character contains special character, the cipher text values is also same as the plain text character.

8. After completion of step 7 result will be taking and convert those characters values into ascii code.

The data owner will take those ascii values as key and perform the encryption process. In this paper we are using idea algorithm for encrypt the data and stored into cloud.

One Time Password Generation and Decryption Process:

In this module the data consumer or user will perform the decryption process and get the original plain format file. Before performing the decryption process the data consumer again verified by system using the one time password verification process. The generation of one time password is as follows.

1. during the registration of user will enter password contains numbers from 1 to 9 and get that password.

2. By using that password the system will generate one time password.

3. Before generating one time password the system will generate 9 * 9 format grid contains data of a-z, A-Z, 0-9 and special characters. The grid formation is as follows.

a	s	d	f	g	h	j	K	!
q	w	l	e	r	t	y	U	%
z	x	c	v	i	o	p	B	^
6	n	8	m	A	Q	Z	S	&
1	W	X	2	E	D	3	C	*
R	4	F	V	5	G	T	B	>
7	Y	H	N	9	U	J	M	<
I	L	K	P	O	@	#	$	?

4. After generating grid the system will take password and retrieve each two value from that password.

5. Take two values and first value will be searching in the row and second value will be searching the column. Here we are maintaining grid position from column wise and row wise. So that take those values of two and will find out position of grid row and column and get coordinate value as result. Here we

take the example of first two character from the password is 38 and the generate value is as follows.

A	s	d	f	g	h	j	K	!
q	w	l	e	r	t	y	U	%
z	x	c	v	i	o	p	B	^
6	n	8	m	A	Q	Z	S	&
1	W	X	2	E	D	3	C	*
R	4	F	V	5	G	T	B	>
7	Y	H	N	9	U	J	M	<
I	L	K	P	O	@	#	$	?
1	2	3	4	5	6	7	8	9

1 2 3 4 5 6 7 8 9

6. So that take those values and repeat this process until the length of password is completed.

7. The result one time password will send to respect mobile number of the data consumer.

8. The data consumer will enter one time password and verify that passwords are equal then the decryption provision will be displayed.

9. If the passwords not equal it will not get decryption provision.

After completion of verification process the data consumer will retrieve the required file name and perform the cipher text policy based key generation schema. By performing that process the data consumer will retrieve the cipher format key and using that it will decrypt the file. By performing the decryption process the data consumer will use idea decryption technique. So that by implementing those processes we can perform the multi authentication process of data consumers and also provide more security of shared files.

IV. CONCLUSIONS

As the number of users in cloud computing increasing security issues are also increasing accordingly. The main security issue can be how to control the unauthorized data access in cloud. In this paper we proposed an efficient data access control scheme with improved security. Our scheme not only restricts the unauthorized access but also ensures secure access by the authorized users. So that to provide security of data and also improve the accessing permission to each data consumer. By performing those operations in this paper we are proposed random universal key signature schema for authentication and key generation for encrypting data. By generation key we are using the cipher text policy based key generation schema and using that key we are encrypt the data. By performing the encryption process we are using idea algorithm and also perform one more verification process for generating one time password. By verifying the one time password it will get decryption provision and data consumer will choose required file for decryption process. To perform the decryption process the data consumer will use idea algorithm decryption process. so that by implementing those concepts we can improve data accessing provision and also improve security of stored data in the cloud.

REFERENCES

[1]. Wei Li, Kaiping Xue, Yingjie Xue, and Jianan Hong, "TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage", *IEEE Transactions on parallel and distributed systems, VOL.24, NO. 06, October 2015.*J.

[2]. Kan Yang and Xiaohua Jia, "Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage", *IEEE Transactions on parallel and distributed systems, VOL. 25, NO. 07, July 2014.*

[3]. A. Shamir, ―Identity-based cryptosystems and signature schemes,‖ in Proceedings of the 4st Annual International Cryptology Conference: Advances in Cryptology - CRYPTO'84. Springer, **(1984)**, pp. 47–53.

[4] D. Boneh and M. K. Franklin, ―Identity-based encryption from the weil pairing,‖ in Proceedings of the 21st Annual International Cryptology Conference: Advances in Cryptology - CRYPTO'01. Springer, **(2001)**, pp. 213–229.

[5]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, ―Attribute-based encryption for fine-grained access control of encrypted data,‖ in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS'06). ACM, **(2006)**, pp. 89–98.

[6]. A. Sahai and B. Waters, ―Fuzzy identity-based encryption,‖ in Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology - EUROCRYPT'05. Springer, **(2005)**, pp. 457–473.

[7] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Security and Privacy, 2007. SP'07. IEEE Symposium on, **(2007)**, pp. 321-334.

[8]. Z. Liu, Z. Cao, and D. S. Wong, "Blackbox traceable CP-ABE: how to catch people leaking their keys by selling decryption devices on ebay," in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, **(2013)**, pp. 475-486.

[9]. K. Yang, X. Jia, and K. Ren, "DAC-MACS: Effective data access control for multi authority cloud storage systems," *IEEE Trans. Information Forensics and Security*, vol. 8, no. 11, pp. 1790-1801, Nov. 2013.

[10]. M. Chase and S. S. M. Chow, "Improving privacy and security in multi authority attribute-based encryption," *Proc. CCS'09*, pp.121-130, 2009.

BIOGRAPHIES:

Reddi Narendra Kumar is student in M.tech (CSE) in Sarada Institute of Science Technology and Management, Srikakulam. He has received his B.tech (CSIT) from Sarada Institute of Science Technology and Management, Ampolu Road, Srikakulum. His interesting areas are data mining, network security and cloud computing

Behara Vineela is working as Asst.professor in Sarada Institute of Science, Technology and Management, Srikakulam, Andhra Pradesh. He received his M.Tech (CSE) from AITAM, Tekkali, Srikakulam, and Andhra Pradesh. JNTU Kakinada Andhra Pradesh. Her research areas include Network Security