International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Email:editorijoer@gmail.com http://www.ijoer.in

Vol.4., Issue.4., 2016
(July-August)

RESEARCH ARTICLE

ISSN: 2321-7758

SIGNATURE BASED DATA SHARING OVER PUBLIC CLOUDS USING ELLIPTIC CURVES

SAURABH SINGH[1], Prof. SHATENDRA DUBEY[2]

[1,2]Department of Computer Science & Engineering, NRI Institute of Science & Technology
Bhopal, India

ABSTRACT

Cloud computing enables sharing of Data and resources over internet. During Sharing of data over cloud environment security is an important concern, hence various security algorithms are implemented to provide security from various attacks. Here in this paper an efficient Data Sharing using Hard Logarithmic based Signcryption and Unsigncrption is implemented which provides security from various attacks and also provides low computational cost and time.

Key Words —Cloud Computing, Signcryption, Unsigncryption, Signatures, Hard Logarithmic Problem, Elliptic Curves

INTRODUCTION

Cloud Computing considered as the expectations IT design and still undertakes to give unrestricted and expandable storage resource and other computing resources as an examination to cloud users in a very commercial approach [1] as services to cloud users. Now a day's cloud computing is a developed technology to store information from more than one client. Cloud computing is a situation that allows users to store the information. Cloud computing is a situation that allows clients to remotely store their information. Remote backup system is the difficult idea which decreases the charge for applying more memory in an association. It facilitates activities and government agencies decrease their financial transparency of data management. They can store their information backups remotely to third party cloud storage providers before sustain data centers on their individual. An individual or an organization may not need purchasing the required storage devices. As an alternative they can store their information backups to the cloud and documentation their information to stay away from any data loss in case of hardware / software failures.

Much of the information stored in clouds is highly susceptible such as, medical records and social networks. Even cloud storage is more elastic how the safety measures and confidentiality are accessible for the outsourced information becomes a serious apprehension. As they offer, the client should confirm itself before commencing any contract and alternatively, it must be guaranteed that the cloud does not alter with the information that is outsourced. User privacy is also need so that the cloud or other clients do not know the distinctiveness of the client. To right of entry a protected data transaction in the cloud the appropriate cryptographic technique is utilized. The owner must encrypt the file and then store the file in the cloud. If a third person downloads the file, clients may scrutiny the record if the client had the key which is utilized to decrypt the encrypted file. Occasionally, this may be a not a success due to the technology expansion and the hackers. The cloud can grasp the client responsible for the information it outsources and equally, the cloud is itself accountable for the services it make available. The legitimacy of the client who stores the information is also confirmed. With the purpose of guarantee privacy of susceptible information stored in public clouds a commonly approved approach is to encrypt the data before uploading it to the cloud. Since the cloud does not know the keys utilized to encrypt the data, the privacy of the information from the cloud is promised a representative approach used to support fine-grained encryption based right to use organize is to encrypt different sets of data items to which the same access control policy be appropriating with different symmetric keys and give clients also the relevant keys [2] or the capability to develop the keys [3], [4].

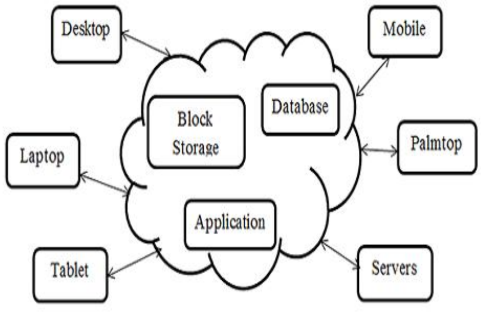

Figure-1: Cloud Data Storage

To avoiding the cloud from concerning in ranking and entrusting all the effort to the client is a usual approach to keep away from data leakage. On the other hand, the restricted computational control on the client side and the high computational operating cost prevents data security. The problem of protected multi-keyword top-k retrieval over encrypted cloud data consequently is: How to make the cloud does more work for the duration of the development of recovery without data leakage. As consider a cloud computing system hosting data service, as demonstrated in Figure 2, in which three different entities are concerned: cloud server, data owner, and data user. The cloud server hosts third-party data storage and retrieve services. Since information may contain responsive data, the cloud servers cannot be fully entrusted in protecting data [6]. For this motivation, outsourced files must be encrypted. Any type of data leakage that would influence data privacy is considered as undesirable.

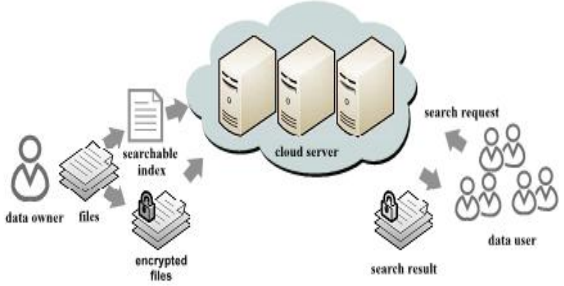

Figure-2: Scenario of retrieval of encrypted cloud data [6].

In Cloud Computing cloud users and cloud service providers are approximately certain to be from deferent trust domains. It turns out that on individual hand susceptible data should be encrypted before uploading to cloud servers; however, a protected client put into effect data access control method must be presented before cloud users have the freedom to outsource susceptible data to the cloud for storage. Comparable to any untrusted storage case, here they can determine the problem using a cryptographic-based data access control method. User revocation is a challenging problem because each attribute is feasibly distributed by multiple clients. Revocation of any particular client would concern others who distribute the similar characteristics. Here they mainly focus on realistic application circumstances for example data storage and sharing as shown by Figure.3, in which proxy servers are always accessible for providing different kinds of data services.

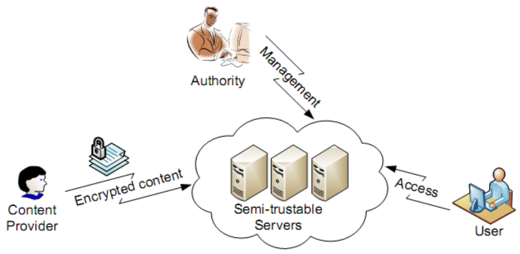

Figure 3: An example application scenario of data sharing.

Similar to previous work [5], these servers are imagined to be interested but straightforward as an alternative of being entirely untrusted. Specifically, they will directly execute the jobs allocated by genuine parties in the scheme. On the other hand, they have the encouragement to become skilled at the substances of encrypted data as much as feasible. The authority to allocate most expanded jobs of client revocation to proxy servers without revealing any secret data to them. On each revocation occurrence, the ability just produces numerous proxy re-encryption keys and broadcasts them to proxy servers. Proxy servers will keep informed secret keys for all clients but the one to be revoked. In this mode their construction puts minimal load on the ability upon each revocation occurrence.

Literature Survey

In this method author has [7] using Secure Hash algorithm for authentication reason, Secure Hash algorithm is the one of numerous cryptographic hash functions, most frequently used to authenticate that a file has been unchanged. The Paillier cryptosystem is a probabilistic asymmetric algorithm for public key cryptography. Revoked clients cannot right to use data after they have been revoked. The proposed method is elastic to replay show aggressions. A writer whose characteristics and keys have been revoked cannot write back decayed data. The protocol sustains multiple read and writes on the data stored in the cloud. The expenditures are similar to the subsisting concentrated approaches and the luxurious procedures are more often than not completed by the cloud. Proposing privacy preserving confirmed access control method. According to our method a client can generate a file and store it steadily in the cloud. This method consists of utilize of the two protocols ABE and ABS. The cloud verifies the authenticity of the user without knowing the user's identity before storing data. The system also has the additional characteristic of access control in which only legitimate clients are capable to decrypt the stored data. The cloud does not know the characteristics of the client who stores data, but only confirm the user's documentations. Key distribution is done in a decentralized method and also conceals the attributes and access policy of a client. One drawback is that the cloud be familiar with the access policy for each confirmation stored in the cloud. The method avoids replay attacks and sustains conception, alteration and reading data stored in the cloud.

Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters [8] initiated the idea of Attribute-Based Encryption for Fine Grained Access Control of Encrypted Data . He begins the new idea of cryptosystem for fine grained sharing of encrypted data i.e. call Key-Policy Attribute-Based Encryption (KPABE). In cryptosystem, ciphertexts are tagged with sets of attributes and private keys are connected with access arrangements that manage which ciphertexts a client is capable to decrypt. Fine-grained access control systems make possible granting differential access rights to a set of consumers and permit elasticity in identifying the access rights of entity clients. Numerous methods are known for applying fine grained access control. Secret-sharing schemes (SSS) are used to divide a secret among a number of parties.

In this paper author complete utilize of CP-ABE in the context of enterprise applications and also extended a revocation method that concurrently permits high flexibility, fine-grained access control and revocation. The section allocates clients a set of attributes within their secret key and distributes the secret key to the individual clients. Any client that assures the access control policy described from the data associate can right to use the data. When a client is revoked access rights the data is re-encrypted in the Cloud representation the revoked user's key useless. The method is established to be semantically protected against chosen cipher text attacks against the CP-ABE model. On the other hand, the method is not well-designed in the case of client revocation since the inform of cipher texts after user revocation places serious calculation in the clouds even if the load is relocated to the Cloud [9].

Lei et al. [10] then proposed the CL-PRE (Certificateless Proxy Re-Encryption) method for secure data sharing in public cloud backgrounds. Even though their method is based on CL-PKC to explain the key escrow difficulty and certificate management, it relies on pairing process. Even though modern progress in implementation methods, the computational expenditures need for pairing are still significantly high evaluated to the costs of normal operations such as modular exponentiation in restricted fields. Additionally, their method only accomplishes Chosen Plaintext Attack (CPA) security CPA security is frequently not adequate to assurance security in common protocol settings. Such as, CPA is not adequate for many applications such as encrypted email forwarding and protected data sharing that require security against Chosen Ciphertext Attack (CCA).

In this paper [11], here author has concentrate on the inadequacies of such earlier approaches and recommend a new mediated Certificate less Public Key Encryption (mCL-PKE) method that does not use pairing procedures. Since most CL-PKC methods are based on bilinear pairings, they are computationally costly. Our method reduces the computational in the clouds by using a pairing-free approach. Additional, the computation costs for decryption at the users are decreased as a semi-trusted security mediator incompletely decrypts the encrypted data before the clients decrypt. The protection mediator acts as a guiding principle enforcement point as well and sustains immediate revocation of cooperation or malicious clients. Based on our mCL-PKE method, they propose a new approach to promise the privacy of data stored in public clouds while enforcing access control conditions. There are five entities in our scheme: the data owner, users, the Security Mediator (SEM), the Key Generation Center (KGC), and the storage service.

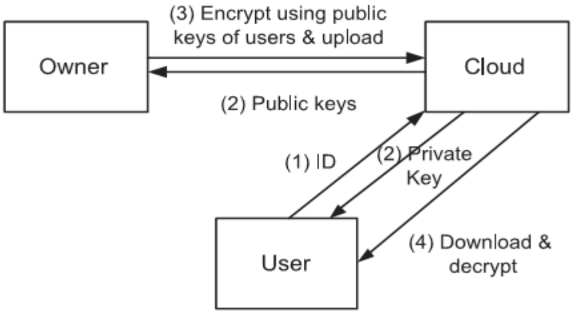

Figure-4: CL-PKE based fine-grained encryption [11].

The SEM, KGC, and the storage service are semi-trusted and be located in a public cloud. Even though they are not trusted for the privacy of the data and the keys, they are trusted for accomplish the protocols appropriately. According to the access control procedure the data owner encrypts a symmetric data encryption key using mCL-PKE method and encrypts the data items using symmetric encryption algorithm. Subsequently, data owner uploads encrypted data items and the encrypted data encryption key to the cloud. To become aware of that a most important benefit of our approach evaluated to traditional approaches is that the KGC, which is the thing in charge of generating the keys, exist in a public cloud.

Here author has proposes the merging of Attribute-Based Encryption (ABE) with proxy re-encryption in a cloud computing function permitting fine-grained access control of resources while attempt to offload re-encryption action to the cloud provider [12]. This method has many discrepancies to the cloud-based re-encryption method that will be anticipated; these differences demonstrate to be inconvenient in a mobile-based environment. The data owner, or designer, is engaged in generating a key for each novel client that joins leaves the method, rather than delegating this job to a trusted key authority below the client's manage. This is not only a excessive charge for a mobile client, but also unfeasible due to the user's mobility and consequently infrequent unavailability. Another difference is that a secret key must be renewed and re-distributed for each client in idle approach, whenever you like client revocation happens, to a certain extent than permitting clients to improve a widespread partition key based on public parameters which would decrease communication and consequence in higher competence. Also, the data re-encryption activity is combined in idle style, while in this suggestion, re-encryption occurs enthusiastically on an as-required starting point to a great extent falling server workload for data mainly right to use by just about the same set of users over time. The re-encryption occurs due to attribute re-definition, unlike the proposal. There is also no facility for exchanging key material in peer-to-peer fashion, which would be useful among mobile users utilizing cheap local wireless links such as Bluetooth. Finally, the scheme is based on KP-ABE (Key-Policy Attribute-Based Encryption), not CP-ABE.

Proposed Methodology

The methodology implemented here for providing Dynamic Data at Data centers with Multi Receiver Identity based Signcryption. The proposed methodology implemented will consists of following phases:

1. First of all create a cloud Environment.
2. The cloud Environment Setup consists of 'N' number of Cloudlets 'Ci', Data Centers 'DCi', Virtual Machines 'VMi', Brokers 'Bi'.
3. Now the user of the cloud starts sharing of data to other users of the cloud.
4. During the sharing of data over cloud environment four steps are performed initialized with Setup Phase and Key Generation Phase and Encryption Phase and Decryption and Verification Phase.

Cloud Environment Setup

Here the cloud environment is setup and simulate using Cloud Simulator in which first of all Cloudlets and Data Centers and Virtual Machines and Brokers are created.

a) If 'N' be the number of Requests to be send from Cloudlets 'Ci' to the Data Centers 'DCi' through Brokers 'Bi'.
b) Let us suppose 'Ri' number of resources to use during the sharing of data from Cloudlets 'Ci' to Data Centers 'DCi'.

Ci → Bi → DCi

c) For each of the Resource to be shared to data Centers

Ri → DCi

d) End

Security Algorithm

The technique implemented for the Secure Data Sharing uses Multi Receiver Identity Based Signcryption using Elliptic Curves which consists of Following Phases:

Setup

During the setup phase of the Signcryption methodology implemented here for data security. Here in the setup phase Elliptic Curves are created using the equation:

$$y^2 = ax^3 + bx + c$$

Where,

$$4a^3 + 27b^2 \neq 0$$

Elliptic Curve Cryptography contains the following Parameters over the finite field F^p.

Table 1. Various Notations Used

Symbol	**Description**
Q	The prime number of the order of p
a,b	The curve coefficient
B	is the base point or the common point (B_x, B_y)
N	Is the order of the base point B.
H	$\frac{E(F_q)}{n}$
Sk1	The secrete key of first user with (X, Y) Co-ordinates.
Sk2	The secrete key of other user with (X, Y) Co-ordinates.
P1	Is the generated public key of first user.
P2	Is the generated public key of other user.
*	Is the point multiplication

Key Generation

If User 'Ui' of the Cloudlet 'Ci' wants to share data with other users of the Cloud then during the setup of the elliptic curves both the users of the cloud shared a Common Base Point of the elliptic Curve 'B'. Now one User chooses a random point over the elliptic curve that would be the secret key of the first user as 'Sk1'. The Chosen Secrete Key is the combination of 'X' and 'Y' axis parameters as Sk1(X, Y). Similarly other user of the cloud also shares random point over the elliptic Curve of another secrete key as Sk2. The Chosen Secrete Key is the combination of 'X' and 'Y' axis parameters as Sk2(X, Y). With the help of the Secrete Key Public Key Parameters are generated using.

$$P1(X,Y) = Sk1(X,Y) * B(X,Y)$$
$$P2(X,Y) = Sk2(X,Y) * B(X,Y)$$

Here Point Multiplication '*' used here is the combination of point addition and point doubling.

Point Addition is the addition of two point $L = J + K$

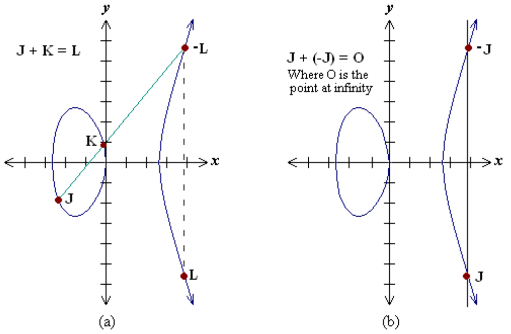

Figure 5. Point Addition used in Elliptic Curves

Point Doubling is the addition of point J to itself to obtain another point $L = 2 * J$.

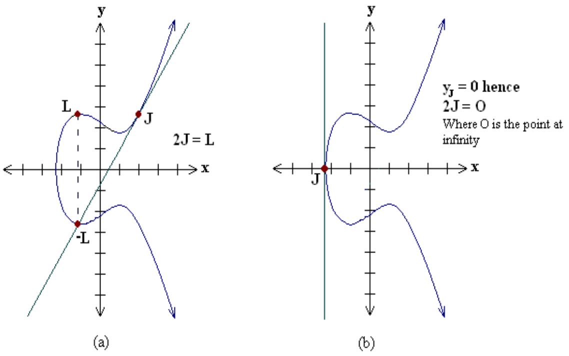

Figure 6. Point Multiplication used in Elliptic Curves

Signcryption Phase

The signcryption algorithm implemented here uses the Identity of the other users 'ID1'.

1. First of all select a random Integer 'r', $r \in R[1, n-1]$
2. Compute P ← [k] B
3. T ← [k] Sk1
4. Generate a set of keys from the key Derivation Function (k1||k2) ← KD(T,I)
5. Generate Cipher Text using the first Key c ← Ek1(m)
6. Generate Signature using the other key using Message Authentication Code

Sg← MACk2(c).

7. Sends the signcrypted text (P, C, Sg) to receiver.

Table 2. Various Annotations used for Parameters

Symbol	Description
r	Selected random integer.
R	Prime order number
P	Is the public key selected from the elliptic curve.
Sk1	Is the generated Secrete key of the first user
k	Generated private key of the user
KD	Is the Key Derivation Function.
B	Is the Common Base Point
E	Is the Encryption Algorithm
m	Message to be encrypted
k1	Key 1
k2	Key 2
c	Cipher text
Sg	Generated Signatures
MAC	Message Authentication Code Hash Function.

UnSigncryption Phase

As soon as the signcrypted message (P, C, Sg)is received to the Receiver with Identity 'IDi'.

a) Generate a message String T using T ← [x] P
b) Generate a set of Key pairs using Key Derivation Function

(k1||k2) ← KD(T,I)

c) Decrypt the message using Key k1, m ← Dk1(c).
d) Generate Signature using the other key using Message Authentication Code

Sg1← MACk2(m).

e) Now verify the message by checking if the generated signatures from the user

Sg == Sg1

f) If equal then message is verified message else invalid.

Result Analysis

The Table shown below is the analysis and comparison of various security attacks.

Table 3. Analysis of Security from various attacks

S. No.	Security Attacks	Existing Work	Proposed Work
1	Password Impersonation	No	Yes
2	Password Guessing Attack	Yes	Yes
3	Confidentiability	No	Yes
4	Public Verifiability	Yes	Yes
5	DoS Attack	Yes	Yes
6	Insider Attack	No	Yes
7	Denning Sacco Attack	Yes	Yes
8	DDoS Attack	No	Yes
9	Outsider Attack	Yes	Yes
10	Online Dictionary Attack	Yes	Yes
11	Offline Dictionary Attack	Yes	Yes
12	Server Masquerade Attack	Yes	Yes
13	Integrity	Yes	Yes
14	Unforgeability	Yes	Yes
15	Non-Repudiation	Yes	Yes
16	Forward Secrecy	Yes	Yes
17	Additional Authentication	No	Yes

The table shown below is the analysis and comparison of various phases and their respective hash values required.

Table 4. Analysis and comparison of total hash required

Scheme	Existing Work		Proposed Work	
	User	Server	User	Server
Registration	1xh	5h	1h	1h
Login	8h			
Authentication	3h	9h	1h	1h
Total	12h	14h	2h	2h

The figure shown below is the analysis and comparison of Signcryption and Un-Signcryption in Milli Second of the proposed methodology. The Signcryption time is computed for various bits on 112, 160, and 256 bits.

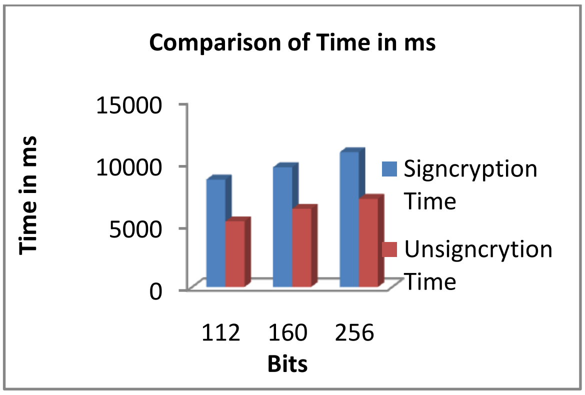

Figure 7. Comparison of Signcryption & UnSigncryption Time in ms

The figure shown below is the analysis and comparison of Storage Cost between Existing and proposed methodology. The proposed methodology implemented takes less Storage cost as compared to existing methodology implemented Mutual Authentication.

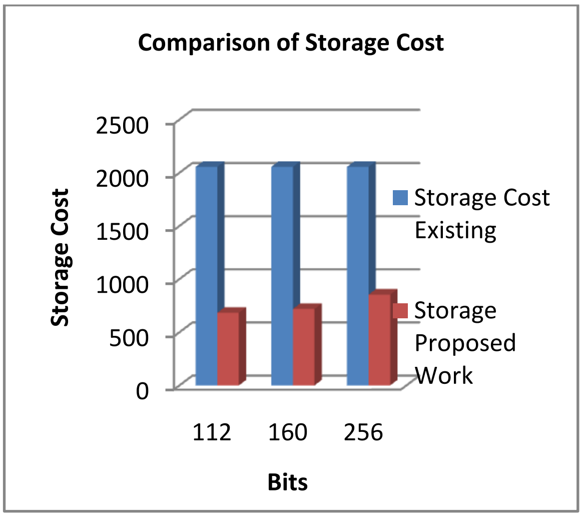

Figure 7 Comparison of Storage Cost

Conclusion

Data Sharing is a method of allocation data or resources on cloud so that the user can access the data in an easy manner. But During the sharing of data users needs to be authenticated, hence various techniques are implemented to ensure the accountability of shared data in the cloud. The proposed methodology implemented here for the sharing of data using Message Verification Code and Key Generation using Signcryption provides efficient results as related to the existing technique.

The projected methodology implemented here provides less computational time and security from various attacks as well as less power consumption and ability to balance load at the data centers and the virtual machines.

REFERENCES

[1]. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “Above the clouds: A berkeley view of cloud computing,” University of California, Berkeley, Tech. Rep. USB-EECS-2009-28, Feb 2009.

[2]. G. Miklau and D. Suciu, “Controlling access to published data using cryptography,” in Proc. 29th Int. Conf. VLDB, Berlin, Germany, 2003, pp. 898–909.

[3]. M. Nabeel, N. Shang, and E. Bertino, “Privacy preserving policy based content sharing in public clouds,” IEEE Trans. Knowl. Data Eng., vol. 25, no. 11, pp. 2602–2614, Sept. 2012.

[4]. N. Shang, M. Nabeel, F. Paci, and E. Bertino,“A privacy-preserving approach to policy-based content dissemination,” in Proc. 2010 IEEE 26th ICDE, Long Beach, CA, USA, pp. 944–955.

[5]. S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati. Over-encryption: Management of Access Control Evolution on Outsourced Data. In Proc. of VLDB’07, Vienna, Austria, 2007.

[6]. Jiadi Yu, Peng Lu, Yanmin Zhu, Guangtao Xue, “Toward Secure Multikeyword Top-k k Retrieval over Encrypted Cloud Data” IEEE Transactions On Dependable and Secure Computing, Vol. 10, No. 4, July/August 2013.

[7]. M. Suriyapriya, A. Joicy, “Attribute Based Encryption with Privacy Preserving In Clouds” International Journal on Recent and Innovation Trends in Computing and Communication Volume: 2 Issue: 2 February 2014.

[8]. 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

[9]. Tu S, Niu S, Li H, Xiao-ming Y, Li M, “Fine-grained access control and revocation for sharing data on clouds,” IEEE 26th international parallel and distributed processing symposium workshops and PhD forum (IPDPSW) 2012, pp 2146–2155.

[10]. X. W. Lei Xu and X. Zhang, “CL-PKE: A certificateless proxy re-encryption scheme for secure data sharing with public cloud,” in ACM Symp. Inform. Comput. Commun. Security, 2012

[11]. Seung-Hyun Seo and Xiaoyu Ding, “An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds”, IEEE Transactions On Knowledge And Data Engineering, Vol. 26, No. 9, September 2014.

[12]. S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proceedings of the 29th conference on Information communications, ser. INFOCOM'10. Piscataway, NJ, USA: IEEE Press, 2010, pp. 534-542.