International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 9 • Number 45 • 2016

Cloud Data Sec – Secure Data Sharing on the Cloud

Prakash Kumar[a] and Punit Gupta[b]

[a]*Department of Computer Science Engineering & IT, JIIT, Noida, India*

E-mail: aaritprakash@gmail.com

[b]*Department of Computer Science Engineering & IT, JUIT, Solan, Himachal pradesh, India*

E-mail: punitg07@gmail.com

Abstract: Data protection and Data security in cloud is one of the major concerns shown by most the organizational heads before the adoption of the cloud environments, and that too in an un-trusted cloud environment, where most of the data needs to be shared either to the public, or to a particular community. Sometimes the data is required to be shared even in a private manner, where only an organization's limited authorities are entitled to access and share it. To overcome the above mentioned challenges, Cloud Data Sec technique is being proposed and the same is implemented for sharing the data safely and securely via the un-trusted public cloud. The proposed Cloud Data Sec technique is implemented and compared with various existing and currently used crypto graphic algorithms. The proposed technique is a client side encryption technique that exploits the AES algorithm features that highly protects and secures the data in cloud environments. Through evaluations and comparisons, the efficiency and scalability of the Cloud Data Sec has been proven.

Keywords: *Secure Data Sharing, Encryption, Decryption, Data Confidentiality, Cloud.*

1. INTRODUCTION

The sixth annual study of IDC(International data Corporation) proclaims that the investment will increase by 40% on the "infrastructure" of the digital universe and telecommunications till 2020. As a result, the investment on storage space will decrease by $1. 80. Decrease in investment per gigabyte(GB) will increase investment in the area of cloud computing[1].

With the venture in the field of cloud computing, wherein helping us to store our data in large amount and thus reducing our hardware cost, but on the other hand, it also poses a threat, a risk of DATA confidentiality. To prevent the unauthorized access to the data,encrypting the data file is required before uploading it onto the cloud[2-4]. To avoid data problems, one of the best known alternatives is client side encryption[5,6]. The key required to encrypt the file should be kept out of the reach of the cloud Service Provider. The secret key is updated without revocation of the user key of all the remaining users and that too while keeping the key management complexity as low as possible, is a great challenge. Access control policies should be flexible among users. One user can share their data with another [7-10].

In this paper, Data is being encrypted before uploading the file. The key used is also being encrypted further using Public key to ensure data confidentiality. Access control[11] and user revocation are the key aspects of this paper. This is in reference to an organization wherein there is a manager, who is the trusted person. The manager is responsible entirely for the user registration and user revocation [12]. At the time of registration, manager sends a secret key to that particular user with which the user encrypts the file. User can encrypt the file using this secret key and encrypt the secret key using the public key. User is able to share data directly with another user [13].

2. PROBLEM STATEMENT

Data confidentiality is very challenging due to the fact that today users outsource their work on the servers, which is under control of un-trusted cloud service providers(CSPs). Thus Cryptography causes secured file uploading and sharing. Files are further subdivided into filegroupswhere each file group has its own encrypting file group key and these keys are further encrypted using public key which is distributed among all the users. Though, this distribution brings about large overhead particularly in case of large file sharing. But in case of user revocation these filegroup key is not required to be updated. Thus security is achieved by keeping the keys out of the reach of the malicious CSP.

Secured policies include two main steps- firstly, any user before getting registered should not be able to access any data, secondly, any user, after being revoked should also have no access to any kind of data. It is required to keep in mind that Confidentiality of the data should not be hindered by any malicious user. The data should not be known. Access Control is achieved by re-encryptingthe each filegroup key with the public key of the known user. This encryption is done using AES encryption Algorithm. User Revocation is a critical aspect in this paper which is taken care of well. User being revoked can't access any data in any manner, and there is no need of updating any of the keys. Low storage cost at the client side is good to achieve.

3. SYSTEM MODEL AND DESIGN GOALS

The project architecture is an example of a company uses cloud storage system[14] to give access to its employee to share files in encrypted form. The project model consists of four different types of entities:The cloud storage,a companymanager and a large number of staffs. The cloud storage is provided by CSPs. The cloud storage is very unsecure because CSPs are very likely to be outside of company. The application services are host on virtual infrastructure provided by CSPs. A company manager:Assuming that managers are the trusted players of project model. The manager has been given the charge of user registration, user revocation, provide secret key to the new user. The staffs: They are registered by the manager. They can share files on the cloud in encrypted form and can download files shared by other staffs on the cloud.

3.1. Design Goal

Cloud Data Sec include access control, data confidentiality,anonymity and traceability and efficiency.

Access control: User can access the cloud data for data uses. Unauthorized users cannot access the cloud data and users revoked by the manager cannot access cloud again.

Data confidentiality: Unauthorized user and CSPs are not able to access data stored on the cloud. The challenge for data confidentiality is to available data for dynamic user.

Anonymity and traceability: Anonymity means that user can access data without revealing their identity.

Efficiency: Users can efficiently share the data with other clouds and store the data too onto the other clouds. User revoked by the manager without updating the key of rest of the users. New user can explore the stored data before its own participation on the cloud.

4. CRYPTOGRAPHIC TECHNIQUE

4.1. Existing Algorithms

Cipher algorithms consist of asymmetric and symmetric key algorithm [6]. In asymmetric two keys are required for encryption and decryption. In symmetric algorithm, only single key is used for both. Symmetric encryption algorithm is faster with respect to asymmetric encryption algorithm. As shown in table 1.

Table 1
Encryption Algorithms with used in specific network structures with key Size details

Algorithm Name	*Structure*	*Cipher Type*	*Rounds*	*Key Size (In bits)*
AES	Substitution-permutation network	Block	10, 12, 14	128, 192, 256
DES	Balanced Feistel network	Block	16	56
Triple DES	Feistel network	Block	48	112, 168
RC2	Source-heavy Feistel network	Block	18	40 to 1024
Blowfish	Feistel network	Block	16	32 to 448
Skipjack	Unbalanced Feistel network	Block	32	80

4.2. Comparative Analysis

Various symmetric encryption algorithms have been analyzedbased on key size, throughput, CPU memory utilization, energy consumption, attacks, encryption time, and decryption time. Table 2 shows encryption times for AIFF and AVI file types with 50 MB and 100 MB file sizes using different Encryption Algorithms. Table 3 shows encryption Time and Encryption Rate of various Algorithms for Sparse and Dense AIFF file. Figure 1 displays the performance of various encryption Algorithms and their encryption time for different file types, with different data type of size 50MB Figure 2 shows encryption algorithm and their encryption times with varied key sizes.

Table 2
Encryption times for AIFF and AVI file types with 50 MB and 100 MB file sizes using different Encryption Algorithms

		Encryption Time in Millisecond					
File Type	*Size (In MB)*	*AES*	*DES*	*3-DES*	*RC2*	*Blowfish*	*Skipjack*
		128	*56*	*112*	*40*	*32*	*80*
AIFF	50	455	1253	3804	1095	614	1729
	100	909	2595	7628	2189	1223	3505
AVI	50	456	1268	3810	1112	629	1731
	100	918	2586	7631	2224	1267	3515

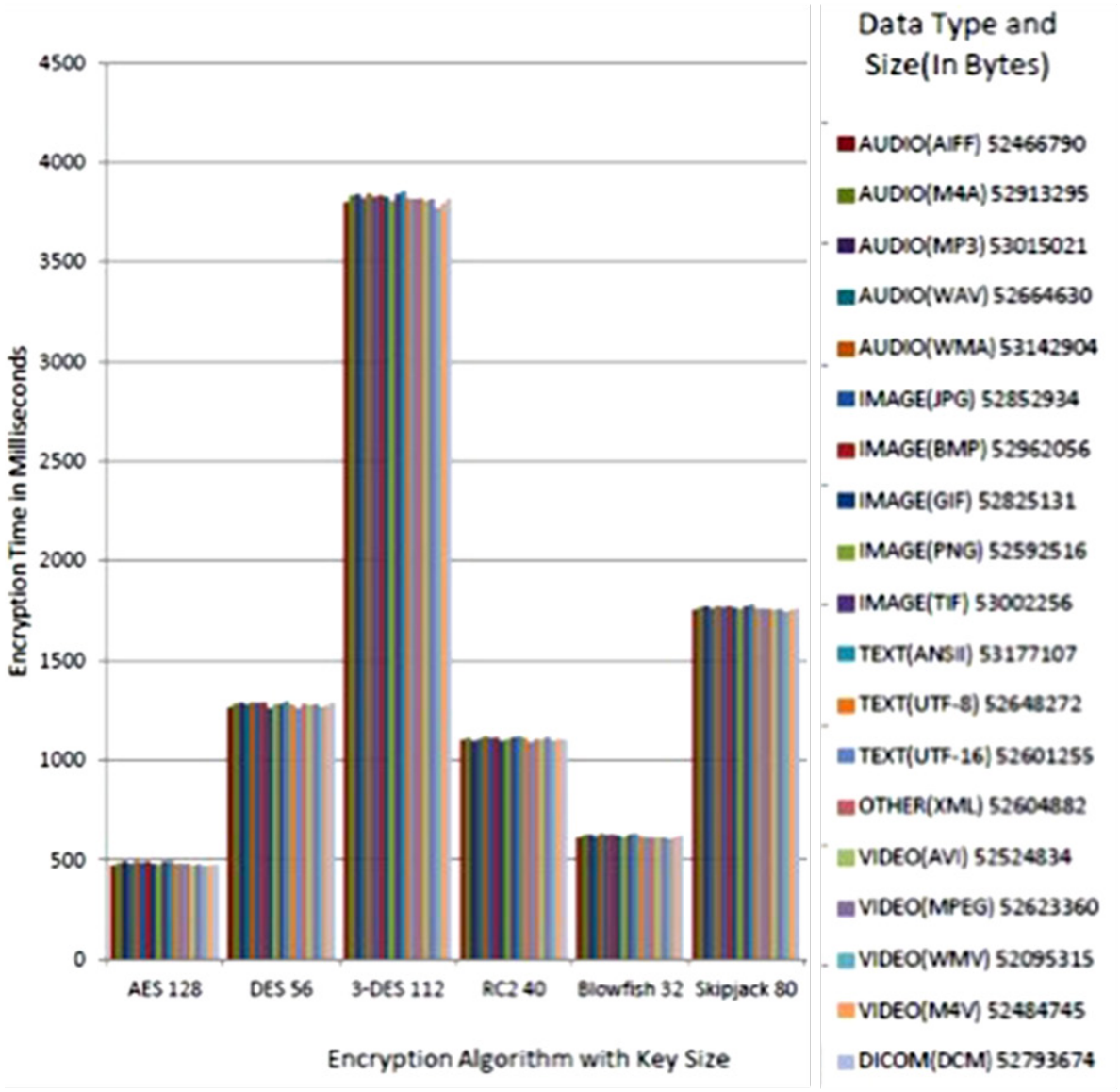

Figure 1: Encryption Algorithms and their Encryption time for different file types. For files of different data type of size 50MB

Table 3
Encryption Time and Encryption Rate of various Algorithms for Sparse and Dense AIFF file

Algorithm Name	*Sparse (72000118 Bytes) AIFF file*		*Dense (61392454 Bytes) AIFF file*	
	Encrypt Time(ms)	*Encryption Rate(MB/s)*	*Encrypt Time(ms)*	*Encryption Rate(MB/s)*
AES 128	634	108.28	540	108.40
DES 56	1801	38.11	1537	38.08
3-DES 112	5076	13.52	4365	13.41
RC2 128	1520	45.16	1285	45.55
Blowfish 128	854	80.38	723	80.96
Skipjack 128	2386	28.77	2042	28.66

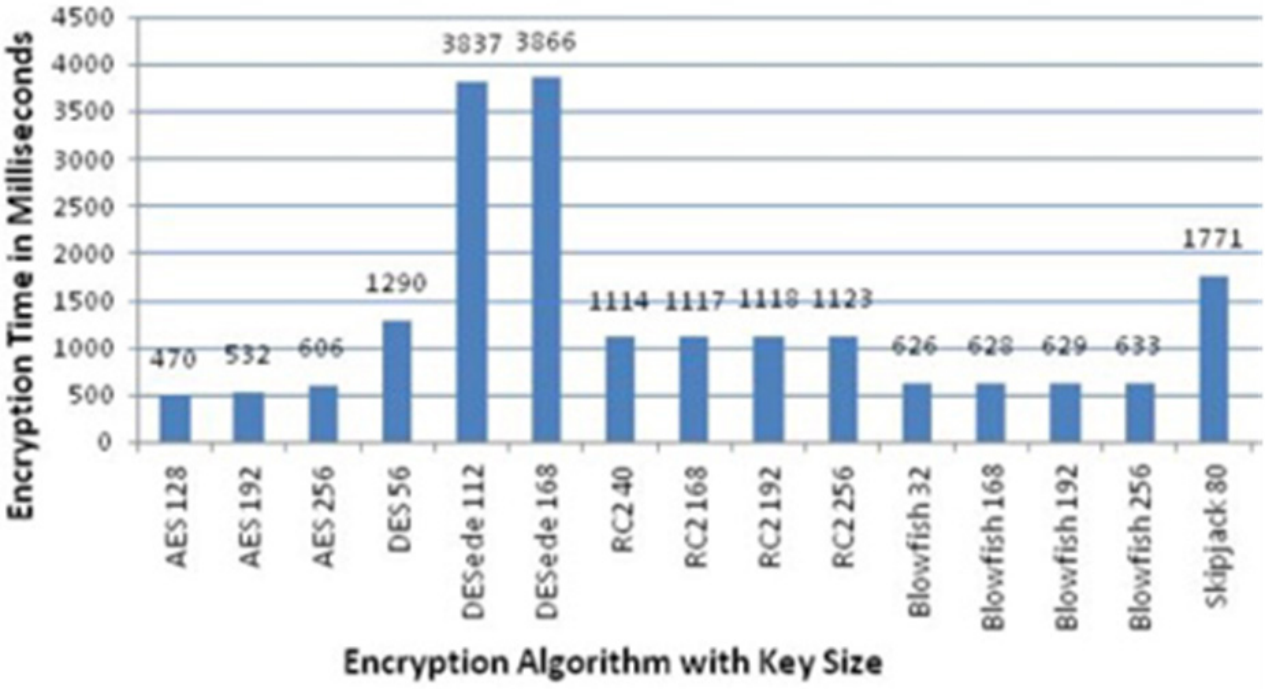

Figure 2: Encryption Algorithm and their Encryption times with varied key sizes

4.3. Proposed Algorithm

AES is the most widely used symmetric algorithm. It consists of three block ciphers, AES- 128, 192, 256 respectively which are sufficient enough to securely protect government top secret level data which requires either 192 or 256 key length [17].

In CloudDataSec, we have used AES-128 for encryption, and in the above comparative analysis it can be seen clearly that AES- 128 encryption performance is the best among all.

4.3.1. Cryptographic assumption of AES

AES has two heuristic assumptions [18-19] that needed to make our cryptanalysis work. The first one is the nonlinearities in S-boxes of AES seems like independent random bits. The second one is the "codes of the code" for AES seems like independently selected random binary linear codes.

The two heuristic assumptions about AES needed to make our cryptanalysis work are

1. The nonlinearities inside AES's S-boxes behave enough like independent random bits.
2. The "codes of the code" for AES (these are certain binary linear error correcting codes that may be associated with secret-key cryptosystems, §10) behave enough like independently selected random binary linear codes.

4.3. 2AES-128 Encryption Algorithm [6]

It uses 5*5 matrix to copied 200 bits input. Initially, the data bytes are filled in the columns and after that they are filled in the rows. Once the data is filled, round key addition is performed, followed by ten iterative rounds of encryption. Encryptions performed in first nine rounds are the same whereas there is a minor difference in the tenth round[6].

4.3.2.1. Sub Bytes Transformation

The Sub Byte transformation technique adopts the following criteria. Substitution Box (S-Box) technique adopted, where each and every byteof the state matricesare replaced with the other byte(Substitution Box method).

4.3.2.2. Shift Rows Transformation

The Shift Rows transformation technique is as follows: First row bytes of the State Matrixremains the same and is copied as it is without making any shift in the byte. Whereas the second, third, fourth and fifth rows are shifted in a cyclic manner to the left by one byte, two bytes, three bytes and four bytes respectively.

4.3.2.3. Mix Columns Transformation

The Mix Columns Transformation operation performed as follows: Bytes of each column are mixed up to the fixed polynomial matrix by a certain multiplication factor[2]. It completely changes the scenario of the cipher even if the all bytes look very similar. The Inverse Polynomial Matrix does exist in order to reverse the mix column transformation.

4.3.2.4. Add Round Key Transformation

In this method, bitwise Exclusive-OR operation is performed by adding a roundkey to the State.

4.3.3. AES Decryption Algorithm

Decryption is the process of extracting the plaintext from cipher text. Various transformations are used for the encryption, viz. Inverted SubBytes transformation, Inverted ShiftRows transformations,Inverted Mixed Columns transformations and AddRoundKey transformations.

4.3.3.1. Inverted SubBytes Transformation

Inverted Sub Bytes is the transformation performed by inversing the Sub Bytes, i.e.,the inverse Substitution Box technique is performed to the individual bytes in the State. The inverse of the Substitution Box is constructed by first performing the inverse to the affine transformation in [1] and then performing the computation for the multiplicative inverse in GF(2^8).

4.3.3.2. Inverted Shift Rows Transformation

Inverted ShiftRows transformation is computing the inverse of the ShiftRowsi.e. the bytes in the first row of the State is not changed, whereas, the second, third, and fourth and fifth rows are shifted in a cyclic manner by one byte, two bytes, three bytes and four bytes to the right respectively.

4.3.3.3. Inversed Mixed Columns Transformation

Inversed Mixed Columns transformation is computing the inverse transformation of the MixColumns. It is a complex procedure as it involves severely the byte multiplication under GF (2^8).

5. THE PROPOSED SCHEME: CLOUDDATASEC

5.1. Overview

Secured sharing is achieved as we encrypt it twice *i.e*. Double encryption is applied. Thus ensuring that only and only the registered non-malicious users can have access to it. Additionally this makes the new users to use the data in an easy and convenient way.

Each user is simply required to login, and if the user is not the authenticated registered user or even if the user has been revoked, then in such cased the users won't be able to access it, thus protecting the confidentiality. To make things easier,it is assured that the manager is entitled wholly and solely, *i.e*. the manager is the most authenticated person to keep a check on the revoked users thereby reducing overhead.

5.2. Scheme Description

Now, detailed description of the CloudDataSec is done which includes user revocation, file generation, file encryption, file decryption and file access.

5.2.1. User Registration

User is registered by the manager, where user receives its private key to be used by him later on. For accessing the files, or when encrypting or decrypting them. User registration is very important as it provides the authenticity to the user and the right to access the cloud.

5.2.2. User Revocation

It is also done by the manager by simply removing the user data or the user data folder from the cloud which results in complete privacy of the data from that user and now this user cannot access any kind of data. He is being denied of all the privileges. Even after user revocation, no updating to the keys is required, thus saving cost.

5.2.3. File Generation

File is generated simply first by encrypting the file, saving it onto desktop, then uploading that encrypted file onto the cloud by the respective user. This is done using AES algorithm.

5.2.4. File Deletion

File on the cloud is deleted by the user himself by simply clicking on a button and choosing the file to be deleted.

5.2.5. File Access

File is accessed as the user login into his valid account; he is entitled to view the files available on the cloud. But the files are in encrypted form, so in order to read the data or the information the user is required to decrypt the file using the key and that key is also in the encrypted form. So the user is first required to decrypt the key using his public key. Then on getting access to the key, he decrypts the fileand thus he gains access to the file.

5.2.6. Traceability

The malicious user can be traced easily by the manager as he has all the information and data of all the users. Every user has to use his private key to encrypt any file before uploading and he can upload and download the files only through his account, so whenever he tries to perform any malicious activity he can easily be caught.

6. PERFORMANCE EVALUATION

6.1. Storage

The CloudDataSec is implemented in Django (Python Framework). So in Django a folder is created which worked as cloud. Any registered users and manager can access shared data (encrypted form) and share data on cloud. Every user has their own drive where user can save their important files.

There is no restriction on the size of the file *i.e.* file of any size can be shared on the cloud or one user to another user.

Manager: In Cloud Data sec, private key of individual user is send by manager to the user email id. The registration of user, reserves space for that user in cloud *i.e*., it makes their drive and store all detail in the database. So manager has list of all users.

User: When data is shared among the users then the user sharing the data or the information, can share it in raw form *i.e*. as it is or in encrypted form. Because in the Cloud Data Sec client side encryption /decryption are used whereby the key used to encrypt the file is also shared in the encrypted form.

6.2. Simulation

The Cloud Data Sec consists of three components client, manager and Cloudstorage. Django(Python Framework) is used to implement the CloudDataSec. MVC Design of MVT Framework provide model to implement Database of the CloudDataSec and Template represents the user interface of the CloudDataSec.

All processes are implemented on laptop with Ubuntu 10. 04 LTS, AMD Athlon 64*2 CPU, clock speed 1.9GH, 1G RAM, 500Gb HDD 7000 RPM. The cloud data storage is conducted on laptop with intel i7, 6Gb Ram, GTX 480, Eizo CG 24inch screen, 128GB SSD for Linux, 2x 2TB, HD for Data.

6.2.1. Client Computation Cost

In Cloud Data Sec, client computation cost is almost negligible as Django (python Framework) uses only our system's memory thus no worry about the memory space. User Revocation is simply done by deleting that user's folder, thus denying all access rights to that user which involves no cost. Also, however large the file size may be, speed of sharing the file is not affected. Encryption has been done client side and not the server side, thus time is saved, cost is saved.

6.2.2. Cloud Computation Cost

In Cloud Data Sec, the files stored on the cloud cause zero cloud computation cost. As whenever we access the file, it can be accessed easily and directly if we are an authenticated and registered user involving no cost. Similarly before uploading the file the user can encrypt the file client side only, thus saving time and cost. Decrypting the file on downloading is also done at client side. Overall cloud computation cost is nil and accuracy and efficiency is maintained.

7. CONCLUSION

In Cloud Data Sec, the user shares data to another user directly or on the cloud without the fear of their privacy being hindered. In case of malicious acts, the disclosure of the identity lies with the manager. This proposed scheme also enables user revocation being done efficiently. User Registration is also done by the manager. New user gets the privilege of decrypting the files and getting the access to the files updated before their arrival. Client side encryption/decryption makes the whole process even faster. Thus data is shared efficiently in an un-trusted environment in a secured manner. Proposed algorithms proves to performs better and insures to be more secure then existing algorithm.

REFERENCES

[1] Gantz J, Reinsel D. The Digital Universe in 2020: Big Data, Bigger Digital Shadows and Biggest Growth, in The Far East, December 2012, Sponsored by EMC Corporation.

[2] Arya P K, Kanimozhi S K. An Authentication Approach for Data Sharing in Cloud Environment for Dynamic Group, International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014, pp 262-267.

[3] NesrineK,Maryline L, Barbori ME. CloudaSec: A Novel Public-key based Framework to Handle Data Sharing Security in Clouds, SECRYPT 2014, pp. 5-18.

[4] Yu S,WangC,Ren K, Lou W. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing, in Proceedings of the IEEE INFOCOM 2010, March 2010, pp.1-9.

[5] Liu X, Zhang Y, Wang B, Yan J. Mona: secure multi-owner data sharing for dynamic groups in the cloud, in IEEE Transactions on Parallel and Distributed Systems, vol:24, Issue: 6, Dec 2012, pp. 1183-1191.

[6] Pahal R, Kumar V. Efficient Implementation of AES, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013.

[7] Gayathri P S, Jennifa, J A S, Revathi T. Enhancing Security of Dynamic Data for Storage Services In Cloud Computing, International Journal of Innovative Research in Science, Engineering and Technology, Vol. 3, Issue 3, March 2014, pp. 2037-2143.

[8] Wang B, Li H, Li M. Privacy-preserving public auditing for shared cloud data supporting group dynamics. , IEEE International Conference on Communications (ICC), June 2013,pp. 1946-1950.

[9] Rewadkar D N, Ghatage S Y. Cloud storage system enabling secure privacy preserving third party audit, in International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), July 2012, pp.695-699.

[10] Kallahalla M, Riedel E, Swaminathan R, Wang Q, and Fu K. Plutus: Scalable Secure File Sharing on Untrusted Storage,Proceedings of the second USENIX Conference on File and Storage Technologies, FAST '03, 2003, pp. 29-42.

[11] Ruj S, Stojmenovic M, Nayak A. Privacy preserving access control with authentication for securing data in clouds, 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), May 2012, pp. 556-563.

[12] Varalakshmi P, Shajina A R, Soniya V S. SMOADS-Secured Multi-Owner Attribute-based Data Sharing in cloud computing, in Fifth International Conference on Advanced Computing (ICoAC), December 2013, pp. 318-324.

[13] Goh E, Shacham H, Modadugu N, Boneh D. Sirius: Securing Remote Untrusted Storage, Proceedings of the Network and Distributed Systems Security Symposium (NDSS), 2003, pp. 131-145.

[14] Xue K, Hong P, A Dynamic Secure Group Sharing Framework in Public Cloud Computing, in IEEE Transactions on cloud computing, Vol. 2, Issue: 4, October 2014, pp. 459-470.

[15] Chase M, Chow S S, Improving privacy and security in multi-authority attribute-based encryption, in Sixteenth ACM conference on Computer and communications security, 2013, pp. 121-130.

[16] Manjusha R. ,Ramachandran R. , Comparative study of attribute based encryption techniques in cloud computing, in International Conference on Embedded Systems (ICES),July 2014, pp. 116-120.

[17] Lian Y, Xu, L, Huang X, Attribute-Based Signatures with Efficient Revocation, Fifth International Conference on Intelligent Networking and Collaborative Systems (INCoS), September 2013, pp. 573-577.

[18] Arora I, Gupta A, Cloud Databases: A Paradigm Shift in Databases, in International Journal of Computer Science Issues (IJCSI), 2012, pp. 77-83.

[19] Warren D, Smith W. AES seems weak,Linear time secure cryptography, International Association for Cryptologic Research, June 2007, pp. 1-24.