2020 6th International Conference on Advanced Computing & Communication Systems (ICACCS)

A Secure Data Dynamics and Public Auditing Scheme for Cloud Storage

Premlata Singh
Department of Computer Science & Engineering
Madan Mohan Malaviya University of Technology
Gorakhpur, India

Sushil Kr. Saroj
Department of Computer Science & Engineering
Madan Mohan Malaviya University of Technology
Gorakhpur, India

Abstract— **Cloud computing is an evolving technology that provides data storage and highly fast computing services at a very low cost. All data stored in the cloud is handled by their cloud service providers or the caretaker of the cloud. The data owner is concerned about the authenticity and reliability of the data stored in the cloud as the data owners. Data can be misappropriated or altered by any unauthorized user or person. This paper desire to suggest a secure public auditing scheme applying third party auditors to authenticate the privacy, reliability, and integrity of data stored in the cloud. This proposed auditing scheme composes the use of the AES-256 algorithm for encryption, SHA-512 for integrity check and RSA-15360 for public-key encryption. And perform data dynamics operation which deals with mostly insertion, deletion, and, modification.**

Keywords— Cloud Computing, Cloud Storage, Data Integrity, Security, Auditing

I. INTRODUCTION

According to the Forrester research says" The global cloud computing market is anticipated to rise from $272billion in 2018 to $624billion by 2023 at a compound annual growth rate of 18%, a report from research and markets showed[1].

Cloud computing is an advanced technology every person is used inner or outer in today's world [2]. The advance and rapidly expanding technology of cloud computing are used computation and storage. The very minimum cost is used storage and computation as a service in it. Service model provided three essential services in it: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service(SaaS)[3]. The NIST definition, "Cloud computing is a model permissive ubiquitous, convenient, on-demand network approach to a shared pool of configurable computing property(e.g. networks, servers, storage, applications, and services) that can be immediately provisioned and released with basic management effort or service provider interaction [4][6]. Cloud storage is a crucial service of cloud computing[5]. They involve data privacy, data protection, data availability, data location, and, secure transmission which is a crucial release in cloud security. The involved in cloud challenge security are threats, data loss, degradation, outside malicious attack and multi-tenancy [6].

The stored information of integrity is conserved for data integrity in the cloud system. The unauthorized users should not be accessed misappropriate or vary of data. Data integrity and reliability of data are faithful to preserve by the cloud computing provider. Data confidentiality is also a crucial way from a user's point of perspective therefore they store their private or confidential data in the cloud. Data confidentiality is taken to assure access control policies and authentication. The faith of cloud computing could be forward by rising cloud authenticate and data confidentiality. So the keep data on the cloud should be security, integrity, privacy, and confidentiality of crucial demands from the user perspective[7].

A secure data storage of cloud computing is presented of a data auditing scheme. Auditing is a refinement of checking the user data which can be done by the data owner or by a TPA[8]. The integrity of stored data on the cloud serves to maintain it. The TPA manage is split into two: one is private audibility, which allows the data owner can analyze the integrity of the data. No one has the authority to inquire about the server considering the data[8]. Though it attains to increases verification overhead of the user. Second is public audibility, the confidentiality of the data can check by only TPA. The behalf of the client can act TPA so TPA is an entity. The verification of integrity has handled to appropriate work that all essential expertise, capabilities, knowledge and professional skill and the position of the client is also reduced by it[8]. It should be crucial that TPA should efficiently or frequently audit the cloud data storage without requesting for the local copy of data[9]

The halt of a research paper is arranged to comply section1 is discuss the introduction and section 2 is discuss related work. The proposed method is discussed in section 3 and section4 is discussed in security analysis whereas the conclusion and future work in section 5.

II. RELATED WORK

Data stored in cloud computing are many difficulties in the integrity and privacy of users. So the approach needs some

978-1-7281-5197-7/20/$31.00 ©2020 IEEE

protection and adequates that data stored on the cloud can assure integrity and privacy.

Many strategies are suggested to meet these obligations.

Table 1:Notation summary of a cryptography operation

Symbol	Description
DO	Data Owner
CS	Cloud Server
TPA	Third Party Auditor
PuDO	Public key of Data Owner
PuCS	Public key of Cloud Server
PuTPA	Public key of Third Party Auditor
PrDO	Private key of Data Owner
PrCS	Private key of Cloud Server
PrTPA	Private key of Third Party Auditor
E	Encryption
D	Decryption
K	Symmetric key
DATA	Confidential data that we want to secure
DID	Data id
Ack	Acknowledgement
BA	Base Address
R	Receive
DID_N	New data id
DATA_N	New confidential data
RFD	Request for data
DEL	Delete
DATA^*	Modify/Append data
MD_R	Receive Meta data (Message digest)
MD_C	Comparing Meta data (Message digest)
M_{K_H}	Message digest

Wang et al. [10] have prospective a way of securing the cloud data. In their toward, HLA and random masking techniques are used in the proposed work. TPA cannot knowledge about data to store the cloud server. And this approach is used a multiuser setting and multiple auditing tasks on TPA. Batch auditing is supported better efficiency. In their approach lags of security concern. In their approach does not maintain confidentiality. It is not supporting data dynamic operation.

Mohta et al. [11] have prospective a way for cloud data are secure in public auditing schemes used in proposed work. In their approach, the RSA algorithm is used data confidentiality and data auditing is used TPA. They have used the SHA algorithm for generating the message digest.They have not mentioned which version of RSA (1024,2048,3072,15360). They also explained by data dynamic operation like insertion, deletion, and updation.

Meenakshi et al. [12] have prospective a way for auditing the TPA. In their approach, they have to use the Merkle hash tree for TPA audit the data. It supports data dynamic operation like insertion, deletion, and updation. They have maintained the integrity of data but in this approach, they have not maintained the confidentiality of data. Batch auditing is not supported.

Wang et al. [13] have prospective a way to support public auditing and privacy-preserving, in their approach, HLA and BLS signature along with MHT are used in this proposed work. In their approach support data dynamic by the Merkle hash tree. They have also maintained integrity. In their approach, confidentiality is not maintained and batch auditing is supported.

Morea et al. [6] have prospective a way for securing the cloud data. In their approach, they have used the AES for data confidentiality and TPA for data auditing. They have used the SHA-2 for generating the message digest. They have not mentioned which version of the AES(128,192,256)algorithm applied. They also not mentioned which version of SHA-2(224,256,512) applied. They did not mention how data are split and how these are encrypted due to there, we do not say their approach is secured.because all versions of AES and SHA that secure.

Yang et al. [14] have prospective a new security challenge that desires an autonomous auditing scheme to analyze the data integrity on the cloud server. In their approach, the random oracle model has been used to prove the security of cryptography. In the model maintain can the data integrity but cannot maintain the data confidentiality. The data dynamics operation and batch auditing are supported.

III. PROPOSED WORK

It requires to grow a robust auditing method and do data dynamics operation. It's no passed data on third-party auditor about auditing method. It performs a communication model.

It uses AES256, RSA-15360, and SHA512 algorithm. AES-256 is a standard and most acceptable algorithm for encryption and decryption processes. It works on the input block size of 128 bits having a key size of 256 bits[16]. Therefore, it has 2^{256} possible a key combination which is 78 digits number. It exponentially generates the number of astronomically in the observable universe. It is considered a strong algorithm among all. If a computer breaks 1 trillion decryption/seconds then it has taken 2^{57}year to break the AES-256[15]. It is more secure than RSA and ECC.

Table2: Required average time for exhaustive key search [15]

Symmetric Cipher	**Number of alternative keys[15]**	**Time required to break cipher if computer do 10^{12}decryption/s[15]**
DES-56	2^{56}	1hour
AES-128	2^{128}	$5.3\times10^{18\text{year}}$
Triple DES-168	2^{168}	$5.8\times10^{30\text{year}}$
AES-192	2^{192}	$9.8\times10^{37\text{year}}$
AES-256	2^{256}	$1.8\times10^{57\text{year}}$

Table3: Security comparison between symmetric and asymmetric cipher[16]

Symmetric Cipher	**Equivalent Asymmetric Cipher**	
	RSA	ECC
Skipjack-80	1024	160
Triple DES-112	2048	224
AES-128	3072	256
AES-192	7680	384
AES-256	15360	512

RSA-15360 algorithm is provided security equal to AES-256, therefore, it uses public-key encryption in the sending process[16].

SHA-512 algorithm was developed by NIST. It is a member of SHA-2 which is the latest version of the secure hash algorithm based on the Merkle-Damgard scheme. Ron Rivest has invented this algorithm that uses a one-way hash function. The previous algorithms SHA0, SHA1, SHA256 and SHA384 developed this algorithm. The SHA224, SHA256, SHA384, and, SHA512 are made by NIST of as the new standard hash function. SHA512 is a development of SHA1 which is an MD4 based improvement. The reliability of SHA512 is achieved by the ability to generate 512 bits hash value, This long hash value makes the SHA-512 more resistant to attack than any other hash function so sha512 is considered a powerful, robust and fast hash function ability to generate 512 bits hash value, which is the longest hash value that a hash function can generate[18]. This long hash value makes the SHA-512 more resistant to attack than any other hash function so SHA512 is considered a powerful, robust and fast hash function[17].

Table 4: :Difference each SHA algorithm variation[17]

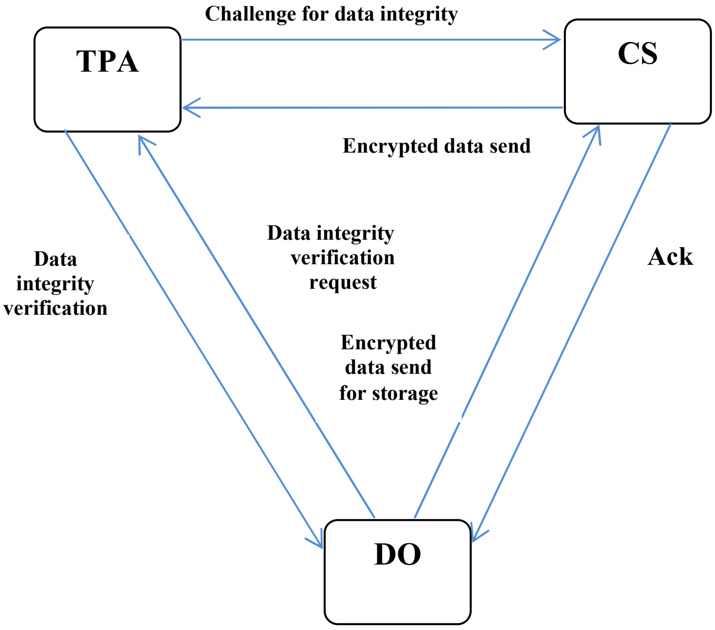
Algorithm	**Word**	**Message**	**Block**	**Digest**	**Security**
SHA-224	32	$<2^{64}$	512	224	112
SHA-256	32	$<2^{64}$	512	256	128
SHA-384	64	$<2^{128}$	1024	384	192
SHA-512	64	$<2^{128}$	1024	512	256

Table 5: Comparison of multiple Hash function[17]

Algorithm	**The size of message digest**	**Message block size**	**Collision**
MD2	128	128	Yes
MD4	128	512	Almost
MD5	128	512	Yes
RIPEMD	128	512	Yes
RIPEMD128/256	128/256	512	No
RIPEMD160/320	160/320	512	No
SHA-0	160	512	Yes
SHA-1	160	512	Theoretical attack(2^{61})
SHA-256/224	256/224	512	No
SHA-512/384	512/384	1024	No
WHIRPOOL	512	512	No

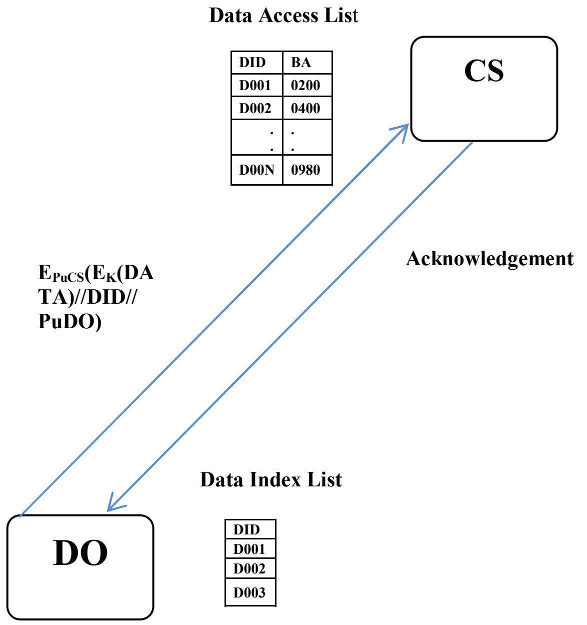
Communication model: The communication model consists of three entities: they are DO, CS, and TPA. It perform three operation: (i) Secure data storage (ii) TPA challenge (iii) Data dynamics.

Fig1.Communication Model in the Proposed Scheme


Challenge for data integrity
TPA
CS
Encrypted data send
Data integrity verification
Data integrity verification request
Ack
Encrypted data send for storage
DO

(i)Secure data storage (Data confidentiality and entity authentication):

Fig .2.Secure data storage



A. DO (Procedure to be followed by DO):

1. Select the data and encrypt it with symmetric key cryptography (i.e.AES-256 here).

   E_K (DATA)

2. Update the Data Index List

   Data Index List←Update (Data Index List, DID)

3. Append encrypted data, data id and its public key. Encrypt these with RSA algorithm and send to CS.

   CS ← $E_{PuCS}(E_K(\text{DATA})) \parallel \text{DID} \parallel \text{PuDO})$

B. CS (Procedure to be followed by CS):

1. It decrypts the received data from DO.

   $D_{PrCS} (E_{PuCS}(E_K(\text{DATA}) \parallel \text{DID}))$

2. It stores the encrypted data on its server and update its Data Access List.

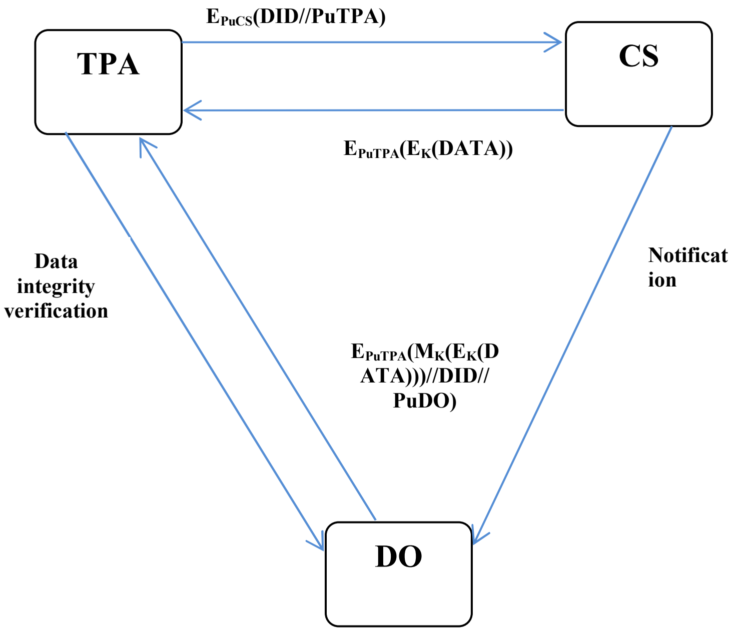
   Data Access List = Update (Data Access List, BA, DID).

3. Send the acknowledgement to DO.

   . Ack ←E_{PuDO} (R, DID).

(ii) TPA challenge (Data integrity):

Fig.3.TPA Challenge


TPA
CS
E_PuCS(DID//PuTPA)
E_PuTPA(E_K(DATA))
Data integrity verification
Notification
E_PuTPA(M_K(E_K(DATA))//DID//PuDO)
DO

A. DO (Procedure to be followed by DO):

1. It generates meta data of encrypted data using SHA-512 algorithm.

   $MD_R \leftarrow (M_{K_H}$ $(E_K(\text{DATA})))$

2. Append meta data of encrypted data, data id and its public key. Encrypt these with RSA algorithm and send to TPA.

   TPA ← E_{PuTPA} $(MD_R \parallel \text{DID} \parallel \text{PuDO})$

B. TPA (Procedure to be followed by TPA):

1. It decrypts the received challenge from DO.

   $D_{PrTPA} (E_{PuTPA}(MD_R \parallel \text{DID} \parallel \text{PuDO})$

2. Append data id and its public key. Encrypt these with RSA algorithm and send to TPA.

   CS←E_{PuCS}(DID || PuTPA)

3. It decrypts the information sent by CS and recover the encrypted data.

   $D_{PrTPA}(E_{PuTPA}(E_K(\text{DATA})) \parallel \text{DID} \parallel \text{PuCS}))$

4.Calculate the message digest on received encrypted data.

   $MD_C \leftarrow M_{K_H}$ $(E_K(\text{DATA}))$

5. Verify the data integrity by comparing calculated and received message digest.

IF

$MD_C == MD_R$

978-1-7281-5197-7/20/$31.00 ©2020 IEEE

```
THEN
    $E_K$(DATA) is not altered.
ELSE
    $E_K$(DATA) is altered.
```

6. TPA sends result to DO.

C. CS (Procedure to be followed by CS):

1. It decrypts the received challenge from TPA.

   $D_{PrCS}(E_{PuCS}(DID \parallel PuTPA))$

2. Append encrypted data, data id and its public key. Encrypt these with RSA algorithm and send to TPA.

   TPA $\leftarrow E_{PuTPA}((E_k(DATA) \parallel DID \parallel PuCS)$.

3. Send notification to DO.

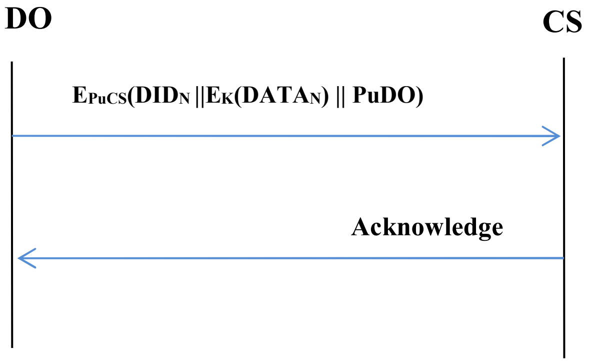
   DO $\leftarrow E_{PuDO}(PuTPA,DID)$.

(iii) Data Dynamic:

It consists of insertion, deletion and modification operation.

(a) Insertion:

Fig.4.Insertion in the Data Dynamics



A. **DO (Procedure to be followed by DO):**

1. For each new data generation DO creates data id of it.
2. Append encrypted new data, data id and its public key. Encrypt these with RSA algorithm and send to CS.

   CS$\leftarrow E_{PuCS}(DID_N \parallel E_k(DATA_N) \parallel PuDO)$

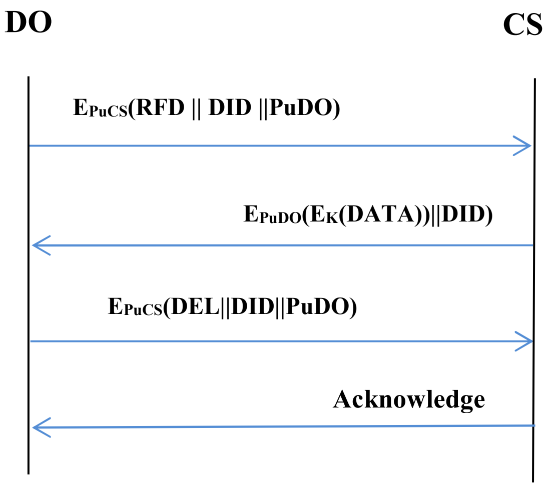
B. CS (Procedure to be followed by CS):

1. It receives the encrypted new data with its data id.
2. Store this new encrypted data on its server and updated the Data Access List.
3. Send the acknowledgement to DO.

   Ack $\leftarrow E_{PuDO}$ (R,DID)

(b) **Deletion:**

Fig.5.Deletion in the Data Dynamics


DO
CS
$E_{PuCS}(RFD \parallel DID \parallel PuDO)$
$E_{PuDO}(E_K(DATA))\parallel DID)$
$E_{PuCS}(DEL \parallel DID \parallel PuDO)$
Acknowledge

A.DO (Procedure to be followed by DO):

1. Append RFD, data id and it public key. Encrypt these with RSA algorithm and send to CS.

   CS $\leftarrow E_{PuCS}(RFD \parallel DID \parallel PuDO)$.

2. Append the data id of deleted data and is public key.Encrypt these with RSA algorithm and send to CS.

   CS$\leftarrow E_{PuCS}(DEL \parallel DID \parallel PuDO)$

B. CS (Procedure to be followed by CS):

1. It receive data request from DO.
2. Append encrypted data and data id. Encrypt these with RSA algorithm and send to DO.

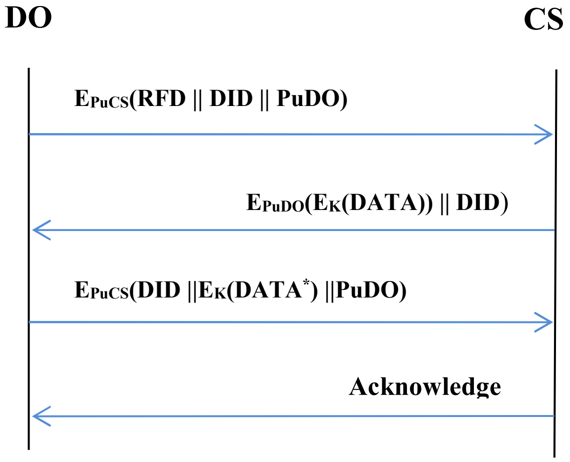
   DO$\leftarrow E_{PuDO}((E_k(DATA)) \parallel DID)$

3. After generating deletion request from DO.It delete the data and send acknowledgement to DO.

   Ack $\leftarrow E_{PuDO}$ (DEL$\parallel$ DID)

(c) Modification:

Fig.6.Modification in the Data Dynamics


DO
CS
$E_{PuCS}(RFD \parallel DID \parallel PuDO)$
$E_{PuDO}(E_K(DATA)) \parallel DID)$
$E_{PuCS}(DID \parallel E_K(DATA^*) \parallel PuDO)$
Acknowledge

A. DO (Procedure to be followed by DO):

1. After receiving the data from CS. It data required modification.
2. Append RFD, data id and it public key. Encrypt the with RSA algorithm and send to CS.

$$CS \leftarrow E_{PuCS}(RFD \,||\, DID \,||\, PuDO)$$

3.Append Data id, modified encrypted data and its public key. Encrypt these with RSA algorithm and send to CS.

$$CS \leftarrow E_{PuCS}(DID \,||\, E_k(DATA)^* \,||\, PuDO)$$

A. CS (Procedure to be followed by CS):

1 It receives data request from DO.

2. Append encrypted data and data id. Encrypt these with RSA algorithm and send to DO.

$$DO \leftarrow E_{PuDO}((E_k(DATA)) \,||\, DID)$$

IV. SECURITY ANALYSIS

In this part, The analyze security intensity and robustness is the approach by us.

1. **Data Confidentiality:** In this prospective method, DO encrypt the data and store CS. Although data is encrypted only by the symmetric key that DO can only see the data. CS can not knowledge about data. TPA requests for encrypted data to CS to check integrity. After that CS sends encrypted data to TPA. To protected data from an external attacker then CS has again encrypted the encrypted data to the public key. Because the key size is very increased then not affect the external attack.In this prospective method, No knowledge about the whole key. They know only about what they are authorized. Hence, the collision attack of CS and DO's is not possible[3].

2. **Data integrity**: The prospective method takes SHA-512 and compute the metadata (message digest) of data. DO encrypt data and metadata (message digest) of data. DO send metadata (message digest) to TPA, encrypt data sends to CS, TPA store the metadata (message digest) and request encrypted data to CS. CS send the encrypted data to TPA. Then TPA computes the metadata (message digest) to accept encrypted data. Data integrity is guaranteed the data is correct to compute the metadata (message digest)[3].

3. **Data Access Control:** The prospective method takes a data access list and data index list. The Data access-list essential contains the DID and BA. This list only CS is performing operation and data index list contains DID. Only DO has the right to perform any operation. This list TPA is not access data. CS can store the encrypted data for the robust data access list. CS can forward encrypted data to TPA what is in their access rights [3].

V. CONCLUSION AND FUTURE WORK

A secure auditing method is to store the data on the cloud in a secure manner. The prospective take the AES-256 algorithm, RSA-15360, and SHA-512 algorithm to assure that TPA cannot knowledge about data toward the robustness auditing scheme. We propose a data dynamics operation with mostly deal insertion, deletion and, modification. In the future, we would like to perform a batch auditing method of data.

REFERENCE

[1] The global cloud computing market report 2019.

[2] J Agarkhed, R Ashalatha-"An efficient auditing schheme for data storage security in cloud".2017[ICCPCT].

[3]. SK Saroj, G Noida,SK Chauhan, AK Sharma "Threshold cryptography based data security in cloud computing".S Vats-2015.

[4] Mell, Peter, and Tim Grance.The NIST definition of cloud computing(2011).

[5]]P.Mell and T.Grance,"The NIST definition of cloud computing",National Institute of Standards and Technology,Tech. Rep.,2009.

[6].Swapnali Morea, Sangita Chaudhari,"Third Party Public Auditing Scheme for Cloud Storage ",International Journal of Prpcedia Computer Science ,Volume 79,pp.69-76,2016.

[7] Zissis, Dimitrios, and Dimitrios Lekkas. Addressing cloud computing security issues. Future Generation computer systems 28.3(2012):583-592.

[8] B.L Adokshaja, and S.J.Saritha,"Third Party Public Auditing on Cloud Storage using the Cryptographic Algorithm"ICECDS-2017.

[9]Cong Wang, Sherman SM Chow, Qian Wang, Kui Ren, and Wenjing Lou."Privacy Preserving Public Auditing for Secure Cloud Storage. http://eprint.iacr.org/2009/579.pdf.

[10] Cong Wong, Sherman S M Chow, Qian Wang, Kui Ren, and Wen jing Lou. "Privacy Preserving Public Auditing for Secure Cloud Storage". IEEE Transactions on Computers, Volume 62, ISSUE 2, February 2013.

[11]Abhishek Mohta, Ravi Kant Sahu, Lalit Kumar. "Robust Data Security for Cloud while using Third Party Auditor". International journal of advanced research in CSE (IJARCSE), Volume 2, Issue 2, February 2012.

[12]IK Meenakshi and Sudha George. Cloud Server Storage Security using TPA.International Journal of Advanced Research in Computer Science and Technology (IJARCST) ISSN: 2347-9817, 2014.

[13] Qian Wang, Cong Wang, Kui Ren, and Wenjing Lou, and Jin Li. Enabling Public Auditability and Data Dynamics for Security in Cloud Computing. Parallel and Distributed Systems,IEEE Transactions on,22(5):847-859,2011.

[14] Kan Yang,Xiaohua Jia."An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing, IEEE Transaction on (1-10), 2012.

[15] W.Stalling,"Cryptography and network security,"LPE Sixth Edition,ISBN-978-013-335-4690.

[16] Kerry Maletsky,"RSA vs ECC comparison for embedded system"Atmel-8951.

[17] Meiliana Sumagita,Imam Riadi,"Analysis of secure hash algorithm(SHA) 512 for encryption process on web based application"IJCSDF-7(4):373-381.