An Efficient Cloud Storage with Secure Dynamic Data Modification

K.HariPriya [#1] (Member – IEEE), P.Krishnamoorthy [*2]
[#]*M.E., Computer Science and Engineering*
V.S.B Engineering College
Karur, Tamilnadu,India.

[*]*Assistant Professor, Computer Science and Engineering*
V.S.B Engineering College
Karur, Tamilnadu,India.

Abstract- **Cloud computing is an on demand service where the user can obtain computer resources via the internet. Due to increase the advantages of cloud computing the individual users and organizations are store their data in cloud storage servers. But storing data in a third party cloud system is a serious issue. To avoid this issue the data's are encrypted before storing in storage server. The normal encryption system provides security but it does not support data integrity on the cloud storage server. To address this issue the research work proposed an Elliptic Curve Digital Signature algorithm, it provides data integrity and data origin authentication. To support a dynamic data modification the Merkle Hah Tree construction is also used. The User's data's are encrypted by using an efficient Elliptic Curve Digital Signature Algorithm (ECDSA). The encrypted data's are divided in to blocks by using Merkle hash tree, the authenticated user can perform all the operations like insert, delete and update at the particular block in storage server itself. To support the efficient handling of auditing tasks the third party auditor is used to verify the integrity of the dynamic data operations on the cloud storage server. Compare with existing system this research work provides a highly secure and efficient cloud storage server.**

Keywords: **- Cloud Computing, Merkle Hash Tree , Elliptic Curve Digital Signature Algorithm, Third Party Auditor**

I. INTRODUCTION

The internet is a most popular one in recent years. It provides many services to users. One of the important service is cloud computing. Cloud computing is an on demand computing technology that delivers the resources as a service to the users over the internet. The cloud service providers manage a pool of resources like operating system, storage space, machines, application programs and etc. Based on the cloud user's request the resources are provided to users. The important service provided by cloud computing is cloud storage. The local users can store their data in the remote cloud storage servers, from that the users can access the data from anywhere in the world. But storing data in a third party cloud system may affect the data confidentiality. For avoid this issue the data's are encrypted before storing in to storage server. In the general encryption system the data owner encrypts the data by using cryptographic methodology and stores the encrypted data at the cloud storage server. It provides data confidentiality but it does not provide high security and dynamic data modification. The unauthorized user may get the data while transfer from the data owner to the cloud server, or he can decrypt the data directly from the cloud server by getting cryptographic keys. Then the hacker may perform some modifications at the hacked data and again stored in to the storage server like a data owner. The cloud users and data owner can't identify the data hacking. The data displays like original data. The receiver thing like the data came from the data owner; it affects the data originality, data origin authentication, security and data integrity.

To avoid this issue the research work provides an Elliptic Curve Digital Signature Algorithm (ECDSA) for encrypt the data. The Elliptic Curve Digital Signature Algorithm (ECDSA) is the public key cryptography methodology. The data owner digitally signed the data when encryption and store on to the storage server. By identifying that digital signature the receiver can identify that the message was came from the original sender and it does not modify during transmission. By using this the proposed scheme provides data origin authentication, data integrity and security. For supporting dynamic data modification directly at the storage server the proposed scheme construct a Merkle Hash Tree. In the conventional storage server, if the data owner wants to modify the data stored at the storage server means first he should retrieve the data from the storage server then perform the operations like insert, delete, and update then again store the updated data in to storage server. It is a risky process. To avoid this issue the data's are encrypted by using ECDSA and divided in to blocks by using Merkle hash tree algorithm. The Merkle hash tree is a binary tree it divides the encrypted data in to equal eight blocks, and assigns the hash value for each block. The data owner can perform the operations like insert, delete, and update at the particular block directly at the storage server. Finally the cloud computing is a multi user environment. More users may access the cloud storage system at the same time. Each user performs some modification at cloud storage server. It may affect the data integrity. To verify the data integrity the data owner assigns an efficient Third Party Auditor (TPA). The TPA performs auditing at the cloud storage server and return the data integrity verification result to the user. From that the proposed scheme provides data integrity, data origin authentication, and high security to the cloud storage server.

II. RELATED WORKS

Recently the interest on signature verification is increasing highly. Aqeel Khalique et al.[1] and Don Johnson [7] proposed the implementation of elliptic curve cryptography signature algorithm for providing data integrity and data origin authentication .[12] propose a ECDSA implementation algorithm as approved on FIPS 186-3. Qian Wang et al[2] proposed the Merkle hash tree block tag authentication for dynamic modification of the data and Third party auditor mechanisms to support multiple auditing tasks. [13] Proposed a Merkle signature scheme and their cryptanalysis. The TPA verify the integrity of the data stored in the cloud[3]. Ateniese et al [4] describes about the public auditablity for the data stored in the untrusted storages. Erway et al. [8]was the first to explore constructions for dynamic provable data possession. They extend thePDP model in [4] to support provable updates to stored data files using rank-based authenticated skip lists. Afterwards Many improvements like security and scalability are described for untrusted storage [5]. Wang et al[6] describes about the public auditablity mechanisms for providing security to the data's.

III. PROBLEM STATEMENT

A. System Model

Fig 1 shows our system model. The following three entities are participated in the network architecture:

User: an entity going to store large volumes of data at storage server.

Cloud service provider: an entity maintain storage servers and key servers for store large volumes of user have encrypted data and cryptographic keys.

Third Party Auditor: an entity perform the business of auditing, is independent and reliable. Verify the integrity of the data by perform auditing for the user's.

The cloud system consists of storage servers and key servers. The storage servers store user's encrypted data and key servers maintain user's Cryptographic keys. By storing data in a third party cloud system the user can reduce the burden of maintaining all the data's in their own. The data owner or the user appoints the third party auditor to verify the integrity of the data stored in the storage server. The TPA get the privilege from user account and access the data from cloud storage server to verify the data integrity. The verification result will be send to the user.

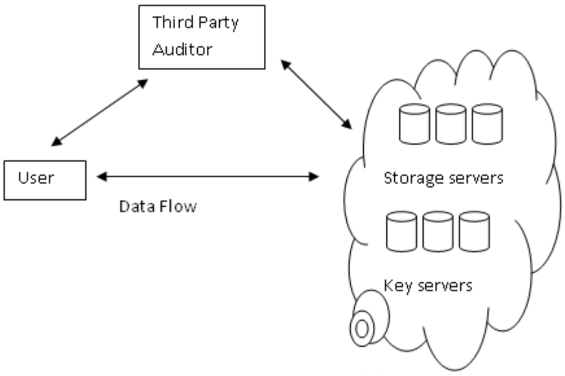


Fig1: System Model

IV. PROPOSED SYSTEM

The proposed system mainly consists of four phases: System setup, Data storage and retrieval, Dynamic data modification, Data integrity verification by TPA.

A. Elliptic Curve Digital Signature Algorithm

Elliptic Curve Cryptography is a public key cryptography algorithm. Elliptic curve cryptography provides efficient and secure solutions for the cloud storage servers. It requires fewer bits than the conventional encryption technologies for provides the similar amount of security. It provides data integrity data confidentiality and data origin authentication. Compare with existing cryptosystem it have a smaller key size, it leads to fast computation time ,reducing in processing power, saves the storage and bandwidth. The ECC signature algorithm mainly consists of three phases. These are key generation, signature generation and signature verification. The signature generation algorithm use the user's private key to generate the signature. The signature verification algorithm use the user's public key to verify the signature at server.

1) *Notation and Preliminaries:*

The ECDSA algorithm need the following domain parameters for perform signature generation and signature verification.

q	→ The size of the underlying field
FR	→ A field representation indicator
(a, b)	→ Elliptic curve parameters
G	→ (x_G, y_G) a point on the curve, known as the base point
n	→ The order of the base point G
h	→ The order of the Elliptic curve group divided by the Order n of g

The following are the ECC signature algorithm.

2) Elliptic Curve Digital Signature Algorithm Description:

KeyGen (): To generate the keys with the parameters (q, FR, a, b, G, n, h) the user should perform the following:
1. Select a random integer d € [1, n-1]
2. Compute Q = d * P
3. The Public and private keys are Q and d respectively

SigGen (): To sign a message M the user A with the parameters D=(q, FR, a, b, G, n, h) perform the following:
1. Select an integer k in the interval 1…n-1.
2. Calculate k * p= (x_1, y_1) and r=x_1 mod n (r=0 then go to step 1) where x is the range between 0…q-1
3. Compute k^{-1} mod n
4. Compute s= k^{-1}{h (m) + d. r} mod n (if s=0 then go to step 1) where h is the Secure Hash Algorithm (SHA)
5. The signature for a message M is the pair of integers (r, s)

SigVeri (): To verify the message M with respect to (r, s) user B gets an authenticated copy of A's parameters (q, FR, a, b, G, n, h) and the public key Q then do the following:
1. Verify that r and s are integers in the Interval [1, n-1]
2. Compute w=s^{-1} (mod n) and h(m)
3. Compute u_1=h(m).w (mod n) and u_2=r. w(mod n). Compute X=(x_2, y_2) = $u_1 * G + u_2 * Q$.
4. If X=0 then reject the signature. Otherwise compute v= x (mod n)
5. Accept the signature if and only if v=r.

B. Merkle hash tree

Fig 2 shows the Merkle hash tree (MHT). It is constructed as a binary tree. The MHT divides the parent node up to eight blocks. The hash value is associated with every non leaf node. It is an authenticated structure it is proved that the set of elements are unaltered and not damaged. The MHT is used in the proposed Scheme to divides the user's file in to blocks. When the user stores the file in to cloud storage server, it is divided in to eight blocks by using MHT and the hash value will be allocated to each block. The blocks are read from the left to right sequence. The storage server stores the block number, the content associated with that block, and its calculated hash value. The fig 3 shows the data stored in the server. It contains the file name, owner of the file, its associated block number, block size and the data associated with that block.

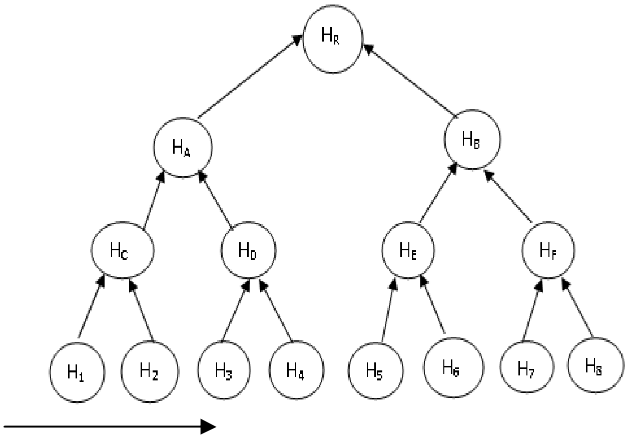


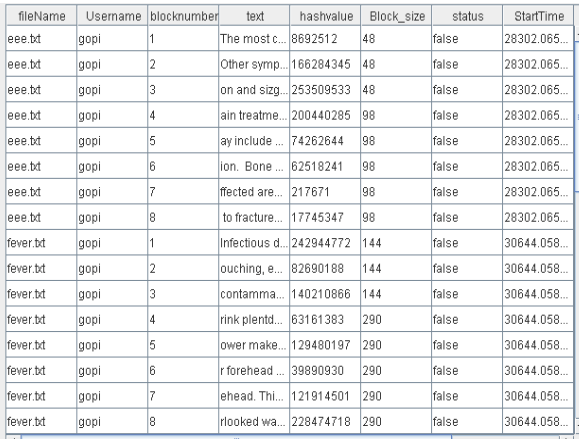
Fig 2: Merkle Hash Tree

C. System Setup Phase

In the system setup phase the system manager mainly choose the system parameters for a user. It allocates the public and secret keys for a particular user. The KEYGEN algorithm generates the public and secret keys for performing cryptographic function to a particular user. The keys are stored in to a separate key server. Because the key servers perform authentication when each user enter in to cloud based on his stored keys. If the hackers get the keys means he can easily decrypt the users data from the storage server, it affects the data integrity. So the keys should be kept as secret and protected from unauthorized users. The keygen algorithm gets the secret security parameter from the user for produce the public and private keys.

D. Data Storage and retrieval

The registered user can store their data in the cloud storage server. For providing confidentiality to the storage server the user's data's are signed before stored in to storage server. The proposed system mainly use an efficient Elliptic Curve Digital Signature Algorithm for signs the data. ECDSA algorithm signs the user's message with Respect of his private key. In the data retrieval phase the user wants to access the data from the storage server, sends the data retrieval request to the key server. The key Server Verifies the user authenticity, if the user is authenticated it sends the user's retrieval request with his identity to the storage server. The storage server retrieves the data based on user identity and return to the user in a readable form.



fileName	Username	blocknumber	text	hashvalue	Block_size	status	StartTime
eee.txt	gopi	1	The most c...	8692512	48	false	28302.065...
eee.txt	gopi	2	Other symp...	166284345	48	false	28302.065...
eee.txt	gopi	3	on and sizg...	253509533	48	false	28302.065...
eee.txt	gopi	4	ain treatme...	200440285	98	false	28302.065...
eee.txt	gopi	5	ay include ...	74262644	98	false	28302.065...
eee.txt	gopi	6	ion. Bone ...	62518241	98	false	28302.065...
eee.txt	gopi	7	ffected are...	217671	98	false	28302.065...
eee.txt	gopi	8	to fracture...	17745347	98	false	28302.065...
fever.txt	gopi	1	Infectious d...	242944772	144	false	30644.058...
fever.txt	gopi	2	ouching, e...	82690188	144	false	30644.058...
fever.txt	gopi	3	contamma...	140210866	144	false	30644.058...
fever.txt	gopi	4	rink plentd...	63161383	290	false	30644.058...
fever.txt	gopi	5	ower make...	129480197	290	false	30644.058...
fever.txt	gopi	6	r forehead ...	39890930	290	false	30644.058...
fever.txt	gopi	7	ehead. Thi...	121914501	290	false	30644.058...
fever.txt	gopi	8	rlooked wa...	228474718	290	false	30644.058...

Fig 3: Data Stored in server

E. Dynamic Data Modification

The authorized user can dynamically modify the data stored at the cloud storage server. The cloud storage provides static storages only. The user can't modify the data dynamically at storage server. In the proposed scheme the user can perform the operations like insert, delete and update dynamically at storage server. The modifications can perform at the particular block. It avoids the user to read the entire file for modification.

1) Insert:
The authorized user can insert the new data with the already stored file. To insert the data the user should generate the insert () message and sent it to the server. The insert message contains the details like the block number, number of character's to insert, and text going to insert, then the position where the data should place on that particular block. These details are send to the server, the server verifies the user authentication then execute the insert () operation and calculate the hash value for newly changed block .Then the server update this new hash value with the old one and send the proof to the user.

2) Update:
The authorized user can modify the data blocks stored in the cloud storage server from its current value to a new one. For update the data the user generates an update request message update () and send to server. The update message should specify the details like block number and the text to update. The server verifies user authentication by signature verification and execute the update () message operation returns the result to the user. The hash value for the newly modified block is also calculated and updated in to the server.

3) Delete:
The authorized user can perform delete operation to delete the file from the cloud storage server. To delete the file the user generates the message delete () and send to the server. The delete () message should specify the details like the block number, and file name to delete. The server gets the input from the user and executes the delete operation; the MHT replaces the root based on the available blocks and returns the result to the user.

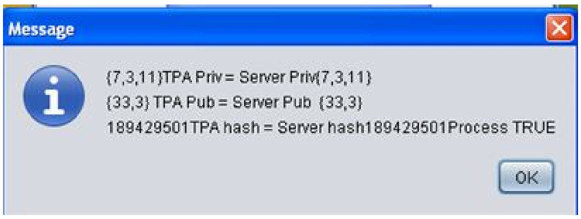
F. Data integrity verification by Third Party Auditor

The Third Party Auditor (TPA) is a trusted third party acting as a verifier to verify the data integrity. Normally the user is an entity, store large volumes of data in to storage server. The storage server receives the data from the user and stores in it. Perform modification on the stored data is unavoidable. At that time the data owner wants to know about the data integrity and data security. For that the user request the TPA for performs the auditing. The TPA is an entity performs the business of auditing, is independent and reliable. Verify the integrity of the data by perform auditing for the user's. Based on the user request the TPA gets the privilege to access the cloud storage data and perform auditing. Initially the TPA verifies the signature, if this verification fails it returns as false. otherwise it access the data from the storage server by data owner privilege It calculates the hash value for the data stored in the cloud storage and matches that value with the hash value stored in the storage server. If both the values are same means it returns the result as true. Fig 4 shows the TPA auditing result for single user.

V. BATCH AUDITING FOR MULTIUSERS

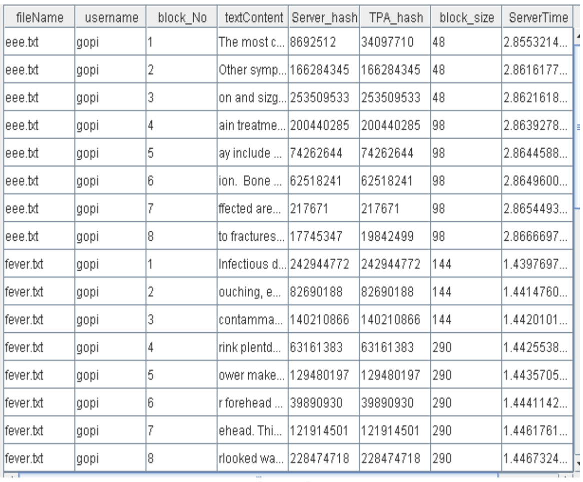
In cloud computing more users access the cloud servers at same time. K user's can access the cloud at same time, it will generate K messages. Perform auditing for each individual user takes more time and it will reduce the efficiency. For that the TPA performs auditing for multiple users' at same time. It will reduce the communication cost and increase the performance of the cloud storage server. For perform batch auditing the TPA use the aggregate signature scheme [10]. The aggregate signature scheme consist of two algorithms: aggregation (), aggregate veri(). Assume K users are participated in the cloud.

Aggregation (): It aggregate K user's participated in the cloud assigning an index i for each user. It ranges from 1…. K. Each user u_i Є U has its own signature σ_i Є G_1 on a message. The algorithm computes aggregate signature $\sigma \rightarrow \Pi^{k}_{i=1}$ the aggregate signature is σ Є G_1



{7,3,11}TPA Priv = Server Priv{7,3,11}
{33,3} TPA Pub = Server Pub {33,3}
189429501TPA hash = Server hash189429501Process TRUE

Fig 4: TPA result for single user



fileName	username	block_No	textContent	Server_hash	TPA_hash	block_size	ServerTime
eee.txt	gopi	1	The most c...	8692512	34097710	48	2.8553214...
eee.txt	gopi	2	Other symp...	166284345	166284345	48	2.8616177...
eee.txt	gopi	3	on and sizg...	253509533	253509533	48	2.8621618...
eee.txt	gopi	4	ain treatme...	200440285	200440285	98	2.8639278...
eee.txt	gopi	5	ay include ...	74262644	74262644	98	2.8644588...
eee.txt	gopi	6	ion. Bone ...	62518241	62518241	98	2.8649600...
eee.txt	gopi	7	ffected are...	217671	217671	98	2.8654493...
eee.txt	gopi	8	to fractures...	17745347	19842499	98	2.8666697...
fever.txt	gopi	1	Infectious d...	242944772	242944772	144	1.4397697...
fever.txt	gopi	2	ouching, e...	82690188	82690188	144	1.4414760...
fever.txt	gopi	3	contamma...	140210866	140210866	144	1.4420101...
fever.txt	gopi	4	rink plentd...	63161383	63161383	290	1.4425538...
fever.txt	gopi	5	ower make...	129480197	129480197	290	1.4435705...
fever.txt	gopi	6	r forehead ...	39890930	39890930	290	1.4441142...
fever.txt	gopi	7	ehead. Thi...	121914501	121914501	290	1.4461761...
fever.txt	gopi	8	rlooked wa...	228474718	228474718	290	1.4467324...

Fig 5: Batch Auditing Report

Aggregate Veri (): The aggregate signature, the original message and the public keys of the entire user's given as an input to verify the signature σ

1. If the signature verification fails it return as false.
2. Compute $h_{i\rightarrow}$ (HM$_i$) for all the K users and accept if the hash value stored in the server matches with the newly generated value. Fig 5 shows on batch auditing report.

VI. CONCLUSION

This work studies about the problem of data confidentiality, data integrity and dynamic data modification. The ECC signature algorithm provides the high security to cloud storage data. It provides data origin authentication and data integrity. The Merkle hash tree function used to perform the dynamic data modification at cloud storage server. Here the cloud storage server does not remain as static. Finally consider the task of allowing a Third party auditor instead of client to verify the data integrity. The TPA performs multiple auditing tasks simultaneously. Our proposed scheme shows that the cloud storage system is highly secure and efficient.

VII. FUTURE ENHANCEMENT

In future research on this area several techniques can be applied. One of the most important one is public verifiability. It allows the Third Party auditor to audit the cloud storage data without requesting the user's time. It will increase the efficiency of the time. Further study on detailed cooperation is required.

REFERENCES

[1] Aqeel Khalique ,Kuldip Singh,Sandeep Sood "Implementation of Elliptic Curve Digital Signature Algorithm" *International Journal of Computer Applications (0975 – 8887)* Vol 2 – No.2, May 2010

[2] *Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li "Enabling Public Auditablity and Data Dynamics for Storage Security in Cloud Computing"* IEEE Transactions on Parallel and Distributed Systems, Vol. 22, No. 5, May 2011

[3] Balakrishnan.S,Saranya.G,Shobana.S,Karthikeyan.S "Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud" *IJCSt* Vol. 2, Issue 2, June 2011

[4] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," *Proc. 14th ACM Conf. Computer and Comm. Security (CCS'07),* pp. 598-609, 2007.

[5] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,"Plutus: Scalable Secure File Sharing on Untrusted Storage," *Proc.Second USENIX Conf. File and Storage Technologies (FAST),* pp. 29-42, 2003.

[6] C.Wang, Q.Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," *Proc. IEEE 29th Int'l Conf. Computer Comm. (INFOCOM),* pp. 525-533, 2010.

[7] Don Johnson and Alfred Menezesand Scott Vanstone "The Elliptic Curve Digital Signature Algorithm (ECDSA)" Certicom Corporation 2001

[8] Erway C, Kupcu A, Papamanthou C, and Tamassia R, "Dynamic provable data possession," in *Proc. of CCS'09*. Chicago, IL, USA: ACM, 2009.

[9] *Cong Wang,Qian Wang,Kui Ren,Wenjing Lou (2009) , "Ensuring Data Storage Security in CloudComputing".* IEEE 17'th International Conference July 2009.

[10] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," *Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic techniques (Eurocrypt '03),* pp. 416-432, 2003.

[11] Oprea, M.K. Reiter, and K. Yang, "Space-Efficient Block Storage Integrity," *Proc. 12th Ann. Network and Distributed System Security Symp. (NDSS'05),* 2005.

[12] Timothy A. Hall Sharon S. Keller "The FIPS 186-3 Elliptic Curve Digital Signature Algorithm Validation System (ECDSA2VS)" National Institute of Standards and Technology Information Technology Laboratory,Updated:January9,2013

[13] GeorgBecker "Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis"SeminararbeitRuhr-Universit at Bochum, 18.07.08.