RESEARCH ARTICLE OPEN ACCESS

Third Party Public Auditing For Shared Data InThe Cloud Using ECC

*Divya R Nair[1],Syam Gopi[2]
[1]*ResearchScholar,Departmentof Computer Science &Engg., AmalJyothi College of Engg. ,Kanjirappally, Kerala, India*
[2]*Assistant Professor,Departmentof Computer Science &Engg., AmalJyothi College of Engg. ,Kanjirappally, Kerala, India*
Corresponding Author: Divya R Nair

ABSTRACT
A Third Party Auditor audits the shared data in thecloud without any modification of the data content.To provide thesecurity for cloud data a TPA can check the integrity of shareddata.The third party auditor can be able to audit the integrity ofdata without accessing the entire data from the cloud.The filesare divided into blocks and allow the TPA to audit the data witha specified block.If a new user wishes to join the group, TPAapproves the user and added to the group.A public auditingmechanism that verifies the integrity of data stored in the cloudwith the help of a digital signature, which can be aggregatedto each block of data.The proposed scheme provides an efficientuser revocation mechanism i.e. when a user revoked from thegroup, to resign the blocks that are signed by that revokeduser.The proposed scheme also supports dynamic operations suchas update, delete and insert operations.The TPA handles multipleauditing tasks at a time with batch auditing protocol.

Keywords: *Public auditing, user revocation, cloudcomputing, digital signature, batch auditing.*

Date of Submission: 11-07-2017 Date of acceptance: 01-08-2017

I. INTRODUCTION

Cloud computing[1] is an on demand internet based computing that provides shared computer processing data[2] and resources to other devices or computers. Cloud computing estimates the need of administrators to manage computing resources. It allows users to pay only for used resources. There are services like private, public or hybrid cloud computing models. The private cloud provides services from a business data center to internet users. In public cloud, a third party delivers the services over the internet. Hybrid services are a combination of both private and public models.

There are so many mechanisms to provides a public auditing scheme [8] that promises the data integrity in the cloud by checking the correctness of shared data.A third party auditor [3], [6] is assigned to check the integrity of data in the cloud.The third party auditor can perform the audit task without retrieving the whole data [8].The uploaded files are divided into a number of blocks and each block is signed bythe user.If anyone can modify the block, the user needs to resign the modified block by using her private key.To promise the data confidentiality the auditor allows theauditing task by select a particular block.

One of the users in the group may misbehave or exit from the group then revokes the user from the group.The proposed system introduces a public auditing mechanism [9] for shared data in the cloud.In this scheme a third party auditor for shared data in the cloud, a digital signature is used to verify the integrity of shared data without retrieving the whole data.The system model also manage the revocation of users [12] in the group.

The proposed system overcome the disadvantages of some existing mechanisms such as to perform multiple auditing tasks at a time by using batch auditing scheme[7] and handle efficient user revocation.An elliptic curve digital signature algorithm(ECDSA)[4] is used to generate the signature ofeach block.The elliptic curve Diffie-Hellman algorithm is used to generate the secreted key and the data encryption standard supports the encryption and decryption process. This scheme supports dynamic operations [10] such as update, delete and insert operations. The proposed scheme is asecure one, which supports an efficient user revocation[4] and handles auditing task efficiently.It also promises to reduce the auditing time of the data in the cloud.

The remainder of this work organizedas follows.The system and threat model is described in section 2, and the cryptographic methods are

explained in section 3.Section 4 describes the proposed methodology and the performance evaluation is explained in section 5. Section 6 provides the description of the relatedwork in the field.Section 7 concludes this paper.

II. PROBLEM STATEMENT

2.1 System and Threat model

The system and threat models of the proposed system are described in this section. The proposed systemmodel is shown in Fig. 1.To ensures the data integrity and save the cloud users from the online burden, here introduce a third party auditor to audit the data stored in the cloud when needed.The auditor can check the correctness of data on behalf of the user.The proposed scheme includes three entities suchas the user, the cloud, and the third party auditor.

Fig. 1. The Public AuditingSystem Model

1)The User: The user is one of the main entities in the proposedsystem.The user first registers into the system.Afterthe approval from the admin, log in with a valid userid and password.The user can be able to perform fileoperations such as upload and download the file.Theusersplits the files according to its size and divided intodifferentblocks.The user signs the file blocks and sendsan audit request to the auditor.

2) The Cloud Service: To provide computational resourcesand other services for users.The cloud sends the file detailsto the auditor and shares the data between users.Thecloud generates the metadata and provides services forusers.

3) The TPA: A trusted service that checks the data integrityin the cloud through public auditing mechanism onbehalf of the user.The TPA generates a valid signatureand performs auditing task effectively.The audit result issent back to the user.

The data integrity is threatened by several factors. Due to some human or system errors, the cloud provider may corrupt the data. A revoked user is another factor that affectthe data integrity. The revoked user may try to modify the data by an illegal way. To guarantee the data integrity, a signature is attached with each block of data. One of the users who modify a block, there need to sign the block with his/her private key. The misbehaving user must need to remove or revoke from the group and blocks signed by this revoked user are resigned by the existing user.

2.2 Design Goals

To handle the revoked user and provides data integrity in the cloud, the proposed mechanism must follow**1)Correctness:** The auditor can periodically check the data integrity and provide audit results to the user. **2) Efficient user revocation:** The misbehaving user must be revoked from the group and signature is recalculated. **3) Batch auditing:**To audit one or more files at a time.

III. ELLIPTIC CURVE CRYPTOGRAPHY

The Elliptic Curve Cryptography [4] is an alternative mechanism for implementing public key cryptography the equation of an elliptic curve is

$$y^2 = x^3 + ax + b \quad (1)$$

E is the elliptic curve, P is the point on the curve and n is the maximum limit.The Elliptic Curve Cryptography is used to generate a private and public key pair.

3.1. Key generation with ECC

The ECC is used to generate both public key and private key.ECC will work in a cyclic subgroupof an elliptic curve over a finite field.The main parameters are:

1. The size of the finite field p.
2. The co-efficient a and b .
3. G is the base point of the subgroup.
4. n is the order of the subgroup.
5. h is the co-factor of the subgroup.

Thus the parameters are (p,a,b,G,n,h)

1.The private key generation:The private key is selected as a random integer (d) and chosen from (1,...n-1). Thus d is theprivate key and n is the order of the subgroup.

2.The public key generation**:**The public key is denoted as H.This is calculated as:

$H = dG$

Thus the generated key pair is denoted as (d, H).

3.2. The encryption with ECDH

ECDH is the Elliptic Curve Diffie-Hellman algorithm [4].It is a variant of the Diffie-Hellmanalgorithm.It describes the encryption of data with generated key pair and works as:

1. Consider A and B wants to share a secret .A have the private key d_A and public key.AlsoB have the private key d_B and public key H_B.
2. A calculate $S = d_A H_B$ and B calculates $S = d_B H_A$

Thus S is the same key for both A and B.If a and b have obtained the secret S, they can exchange the data with DES algorithm.

IV. PROPOSED METHOD

4.1. Public Auditing

The public auditing module includes key generation, signaturegeneration and signature verification.In key generationphase, users generate their own private key and public key byusing elliptic curve cryptography. The Elliptic Curve Cryptography is used to generate aprivate and public key pair.The ECC is used to generate bothpublic key and private key.The generated key pair is denoted as (d,H).

4.1.1. ECDSA

The signature generation and verification are performed byusing elliptic curve digital signature algorithm (ECDSA).TheECDSA[4] contains two phases such as signature generationprocess and verification process.A digital signature is used to audit the data integrity and byusing this signature a user signs a block of the message.TheECDSA is the Elliptic Curve Digital Signature Algorithm andit consists of mainly two algorithms such as:

1) Signature Generation Algorithm
2) Signature verification Algorithm

1) Signature Generation Algorithm

- Take a random integer k from (1...n-1).
- The point (x_1,y_1) is calculated as $(x_1,y_1) = kG$.
- Calculate $r = x_1 \bmod n$.
- If r = 0,then choose another k and repeat the steps.
- Calculate $s = k^{-1} (z + r\, dA) \bmod n$, where $k^{-1}$is the multiplicative inverse of k modulo n.
- If s = 0, then choose another k and repeatthe steps.

Thus the generated pair (r,s) is considered as signaturepair.

2) Signature Verification Algorithm

To verify the signature, we need H_A,z and (r,s).

The algorithm works as;

- Calculate the integer $u_1 = s^{-1}z \bmod n$ and $U_2 = s^{-1}r \bmod n$.
- Calculate the point $(x_2,y_2) = u_1G + u_2H_A$.
- Calculate $v = x^{-1} \bmod n$.
- If v = r; then the proof is accepted.

The TPA collects the metadata and generate signatures for eachblock.Finally, the auditor verifies the signatures and sendstheresults to the user.The result contains details of both authorizedand suspicious data blocks.If one of the users is revoked fromthe group, the blocks signed by that revoked user is consideredas the suspicious block.The auditor checks the suspiciousblock and included in the audit request.

4.2. User Revocation

The proposed system is efficient and secure during userrevocation.When a user is revoked from the group, the blockssigned by the revoked user is resigned by a resigning key,recomputed the signature on those blocks and attach the signatureto each block.The revocation of the user is secure becausethe existing users are able to sign the data blocks.Duringtheauditing, the blocks signed by the revoked user are consideredas suspicious blocks.

4.3. Batch Auditing

The TPA must handle multiple auditing tasks [5] at a time.Itreduces the auditing time of TPA.The TPA can performauditing of different file blocks at a time [13] and reducesthe computation cost of the auditor.TPA views the list offiles uploaded by the user, selects all the files and performsauditing.

4.4. Data Dynamic Operation

The dynamic module supports dynamic operations [11] on file blocks. To enable each user to modify the data stored in the cloud.The dynamic operations include an insertion, deletionand update operations.After the modification of a file block,the new signature is calculated and attached to the modifiedblock.

V. PERFORMANCE EVALUATION

5.1. Performance of Public Auditing

To perform the auditingwe need to log in the TPA console.The user selects a file ormultiple files and submits for auditing.The user1 submits thefiles such as file1.java, file2.java, and file3.java for auditingtask.The blocks signed by the revoked user areconsidered as asuspiciousblock.Here the file1.java and file2.java are found assuspiciousblocks.The result showthat total percentage of both suspicious and verified blocks asshown in Fig. 2, Fig. 3 and Fig. 4.

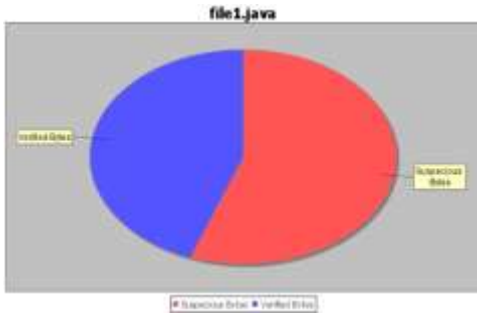

Fig. 2. Audit result for file1.java

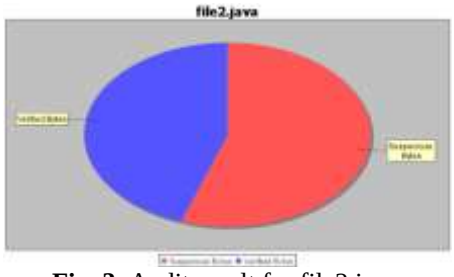

Fig. 3. Audit result for file2.java

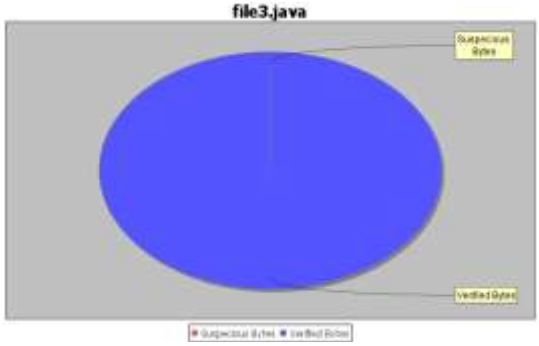

Fig. 4. Audit result for file3.java

The file1.java contains two modified blocks signed by therevokeduser.The file2.java contains one modified block signedby the revoked user and the file3.java contains no modifiedblocks.The total number of verified and suspicious bytes ismentioned in Table I.

Table I Audit Result

Filename	File1.java	File2.java	File3.java
Total blocks	4	2	3
Modified blocks	(1,2)	0	Nil
Total bytes	3696	1896	2904
Verified bytes	1640	848	1048
Suspicious bytes	2904	2904	0

5.2. Performance of Batch Auditing

The TPA can perform both individual auditing and batchauditing as per the user's wish.The independent auditing,the auditor needs more time and communication overheadto perform auditing task.In order to reduce the time and communication overhead, TPA performs batch auditing.The experimental results show that the batch auditing helps to performauditing task effectively.

5.3. Efficiency Analysis

Here compare the efficiency of the proposed system withthe RSA-based scheme.The proposed system uses ECC forencryption and decryption.Wecompare the encryption anddecryption process with the RSA algorithm.The comparison isdescribed in Fig.5.To compare the time taken for initialization,encryption and decryption process of both ECC and RSA algorithm.

Fig. 5. Performance Analysis of RSA and ECC

The RSA takes 357 ms, 94 ms and 1888 ms for initialization, encryption, and decryption respectively. But ECC takes 16 ms, 219 ms and 172 ms for initialization, encryption, and decryption respectively. Thus the analysis shows that ECC takes less time than RSA for initialization and encryption process.

VI. RELATED WORK

A secure data sharing in clouds, SeDaScmechanismthat provides data confidentiality and integrity.Inthisscheme [2] encrypts a file with a single encryption key. In Ensuring data storage security in Cloud Computing [11], that introduces the new security threats in the cloud andsome techniques that provides data security in the cloud. Thedata owner submits the data, the list of the users, and theparameters to the cryptographic server.In this scheme thecryptographic server is the third party and it is responsible forkey management, encryption and decryption.This scheme alsohandles the user inclusion and revocation in the cloud.Thisscheme ensures the data confidentiality but its needs securechannel for secret key exchange.The third party public auditing scheme for cloud storage [3],proposed a public auditing mechanism for data in thecloud.This scheme verifies the correctness of the cloud data withthe help of a TPA, without retrieving the entire data.Theproposedsystem consists of three entities such as the owner, thecloud server and the TPA.This ensures that no data content isleaked to TPA during the public auditing.This scheme reducesthe overhead of the client.The user selects a file and splits into blocks.The TPA performs auditing of a block when a usersends an audit request.The TPA verifies the signature generatedby itself with the user generated signature and sendsthe result to the user.It maintains the storage correctness ofdata but do not support data dynamic operations.A new scheme, An Efficient Public verifiability and DataIntegrity Using Multiple TPAs in Cloud Data Storage [4], aremote data storage correctness scheme based on an ellipticcurve digital signature algorithm(ECDSA) that supportsthe public auditing.This scheme identifies the misbehavingservers.Here proposed a main TPA and a secondary TPA forchecking the data integrity.ECDSA used to generate the signatureto verify the data integrity.It consists of KeyGen, SignGen,ProofGen and VerifyProofalgorithms.In this scheme, if mainTPA will fail to work, the secondary TPA must be able tohandle the audit process.The Privacy-Preserving Public Auditing for Secure CloudStorage [7], ensures the data integrity as well as the onlineburden of the user in the cloud. The TPA canperiodicallycheck the integrity of the data stored in the cloud. A privacy preserving auditing mechanism, Oruta [8]that uses a homomorphic ring signature method for signature generation and

verification. This scheme supports batch auditing task. Another scheme, Public auditing for shared data with efficient user revocation in the cloud [9] that handles the user revocation efficiently. InPrivacy-preserving public auditing for shared cloud data supporting group dynamics [10], proposed an auditing scheme that provides data privacy and supports dynamic groups in the cloud. Another auditing scheme,Efficientintegrity auditing for shared data in the cloud with Secure User Revocation [12]that supports revocation of the user from the group.An Efficient Public Batch Auditing Protocol for Data Security in Multi-cloud Storage [13], to perform multiple audits task simultaneously and supports multi cloud data.

VII. CONCLUSION

Here propose TPA for shared data in cloud, the publicauditing mechanism for shared data in the cloud.Theproposedscheme verifies the integrity of data stored in the cloud. Thesystem utilizes digital signatures algorithm to construct andverify the signature.The third party auditor is assigned to audit the integrity of shared data and handles the user revocationprocess. To performs multiple auditing tasksat a time by batch auditing mechanism.The proposed schemealso supports dynamic operations on the files.Aninterestingproblem in our future work is how to efficiently audit theintegrity of shared data with multiple users' requests.Batchauditing performs the multiple audit tasks at a time and reducesthe computation cost on the auditor side.

ACKNOWLEDGEMENTS

The authors would like to thank Boyang Wang,StudentMember, IEEE, Baochun Li, Senior Member, IEEE, and HuiLi, Member, IEEE.

REFERENCES

[1] Michael Armbrust, Armando Fox, ReanGriffith,Anthony D. Joseph, Randy Katz, AndyKonwinski,Gunho Lee, Dav id Patterson, Ariel Rabkin, Ion Stoica,andMateiZaharia, A View of Cloud Computing,*Communications of the acm* ,2010, pp50-58.

[2] Mazhar Ali, RevathiDhamotharan, Eraj Khan, SameeU. Khan Athanasios V. Vasilakos, SeDaSC: Secure Data Sharing in Clouds, *IEEE transaction on Knowledge and Data Eng*., 2013, pp 1-10.

[3] SwapnaliMorea, SangitaChaudharib, Third Party Public Auditing scheme for Cloud Storage,*Procedia Computer Science* , 2014, pp 69-76.

[4] S. H. Abbdal, An Efficient Public Verifiability and Data Integrity Using Multiple TPAs in Cloud Data Storage,*IEEE transaction on Big Data Security on Cloud*, 2016, 412-417.

[5] D. S. Kasunde and A. A. Manjrekar, Verification of multi-owner shared data with collusion resistant user revocation in cloud, *Computational Techniques in Information and Communication Technologies (ICCTICT)*, 10,2015, 182-185.

[6] Priya K and Gunavathi I,, Ensure cloud storage correctness based on public auditing mechanism,*Communications and Signal Processing (ICCSP)*,2015,1468-1472.

[7] C.Wang, S. S. M. Chow,Q.Wang, K. RenandW. Lou, Privacy-Preserving Public Auditing for Secure Cloud Storage, *IEEE Transactions on Computers*, 2, 2013, 362-375.

[8] B.Wang, B. Li and H. Li,Oruta: privacy-preserving public auditing for shared data in the cloud,*IEEE Transactions on Cloud Computing*, 1,2014, 43-56.

[9] B.Wang, B. Li and H. Li, Public auditing for shared data with efficient user revocation in the cloud, *IEEE INFOCOM*, 2013, 2904-2912.

[10] B.Wang, H. Li and M. Li, Privacy-preserving public auditing for shared cloud data supporting group dynamics, *IEEE Transactions on Communications (ICC)*,2013, 1946-1950.

[11] Cong Wang, Qian Wang, KuiRen and Wenjing Lou, Ensuring data storage security in Cloud Computing,*Quality of Service, Charleston*, 2009,1-9.

[12] Y. Luo, M. Xu, S. Fu, D.Wang and J. Deng, Efficient Integrity Auditing for Shared Data in the Cloud with Secure User Revocation,*IEEE Trustcom/BigDataSE/ISPA*,2015, 434-442.

[13] H. Kai, An Efficient Public Batch Auditing Protocol for Data Security in Multi-cloud Storage, *China Grid*,2013,51-56.

International Journal of Engineering Research and Applications (IJERA) is UGC approved Journal with Sl. No. 4525, Journal no. 47088. Indexed in Cross Ref, Index Copernicus (ICV 80.82), NASA, Ads, Researcher Id Thomson Reuters, DOAJ.

Divya R Nair. "Third Party Public Auditing For Shared Data InThe Cloud Using ECC." International Journal of Engineering Research and Applications (IJERA) 7.8 (2017): 01-05.