ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Shared Spreadable Cloud Data with Efficient Group User Revocation

Phasale Priyanka, Dr.Ranmalkar Vrushali

M.E Student, Dept. of Computer, Vishwabharti College of Engineering Ahmednagar, India

Assistant Professor, Dept. of Computer, Vishwabharti College of Engineering Ahmednagar, India

ABSTRACT: This paper concern with cloud for storage of large data. Some explorations assume security and efficiency problem of sharing dynamic data. Collusion attack occurs in cloud server side and data owner not able to take part in user revocation phase, and not provided more secrecy of owner data in existing system. Propose scheme overcome this attack and provide secure system with the help of contribution to extract specific keywords while file uploading. When user enters those specific extracted keyword are displayed to user (not all files display) with the help of Elliptic curve cryptography for group signature, Advanced encryption standard for file encryptions, Word count for keyword extraction algorithm. This system construct not only support group data encryption and decryption during the data modification processing, but also realize efficient and secure user revocation. Also provide some nice property avoid file de-duplication that is save the memory space of cloud storage, another is keyword extraction, experimental result shows that confidentiality of our scheme, as compared to other relative scheme our scheme provide efficiency and security.

KEYWORDS:*Public* integrity auditing, Cloud service provider, Third party auditor, Group signature, advanced encryption standard, Elliptic curve cryptography, File de-duplication, keyword extraction.

I. Introduction

Cloud computing is the on demand delivery of computer power, database storage, applications, and other IT resources through a cloud services platform via the internet. Cloud provides services to improve storage limitation. Sometime server return invalid result like server hardware software failure, malicious attack so data integrity and accessibility necessary to protect the security and privacy of cloud user's data. For avoiding critical security challenge solutions is system support two schemes first dynamic scheme which supports data modification, second is static scheme not modify data. System provides data integrity for data owners as well as TPA. Dynamic schemes allowed to only data owner could modify the data. In development platform multiple users in a group need to share, access, modify, compile and run the shared source code at anytime and anywhere. In existing scheme support only plaintext data not cipher text so not consider the data secrecy of group user's problem. Not allow to data owners to take part in the user revocation phase, so collusion occurs server gives the chance to attacker [1].

The deficiency of problem motivates how to design an efficient and reliable scheme, Propose scheme overcome this attack and provide secure system with the help of contribution to extract specific keywords while uploading. When user enters those specific extracted keyword that belongs from specific, only those files associated with that specific keyword are displayed to user (not all files display)with the help of Elliptic curve cryptography for group signature ,Advanced encryption standard for file encryption, Word count for keyword extraction algorithms. Propose system gives authority to only data owners for user revocation phase, and CSS does not take part in user revocation phase. When data owner upload their own file at that time specific keywords are extracted automatically those comes in file mostly. So owner get access to selected users in group only those user able to access file with searching file with extracted keyword, Belong to that keywords associated file display to users not all files.

1.1 Cloud Storage model

Figure show CSS model divided into three different parts, first is cloud server second is group users third is TPA. Under group users two types of users is present that is data owner and group users but some revoked group users want to access the data by data owner. The cloud server is semi trusted because they provide all storage services to numbers of group users, TPA is any third person in the cloud, TPA check the data integrity of the shared data which

DOI: 10.15680/IJIRCCE.2017. 0506087

data stored in the cloud storage server[1]. The TPA could efficiently verify the integrity of the data stored in the cloud storage server; even the data is frequently updated by the group users. The data owner is different from the other group users, data owner could securely revoke a group user when a group user is found malicious or the contract of the user is expired [2].

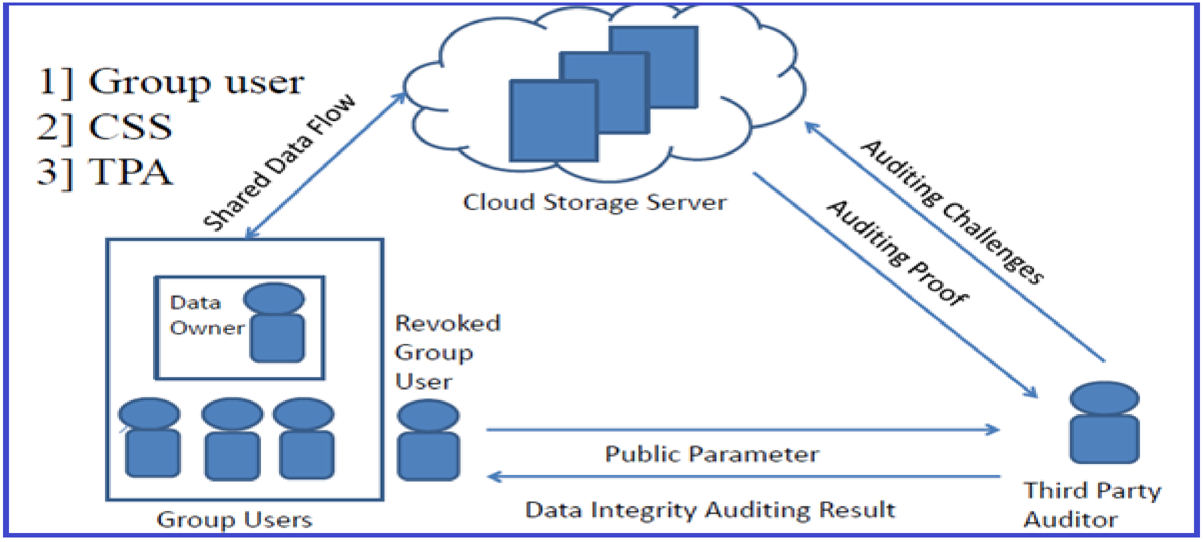


Figure 1.1: The Cloud Storage model.

1.2 Security Goals:

1) **Security:** Large number of policy, technology, and control to protect data, applications, and the associated infrastructure of cloud computing. Storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centres.

2) **Correctness**: Scheme iscorrect when efficiently support encrypted any db for any updated data by valid group user.

3) **Efficiency**: Efficiency measure the ratio of useful output to total input, which expressed with the mathematical formula E=P/C, P is the amount of useful output of product produced per the amount cost of resources consumed.

4) **Count ability**: Scheme is countable if TPA provides the proof for misbehaviour of cloud storage server with the db.

5) **Traceability**: In traceability always data owner capable to trace out who is the last user updated the data item, when data is generated by generation algorithm also each signature generate by user is valid or not.

II. Related work

Recently in collaboration platform some cloud service cloud services use so many users in group want access of file sharing and modification. In cloud only data owner update owner for group so computation overhead increase and data auditing become infeasible. Result support only data owner operation not multi-user Wang et al[2]design new scheme ring signature based on data integrity but big drawback of this scheme does not consider the problem of user revocation. Wang at al[2]reconstruction proxy-re-signature authentication channel occurs. But still scheme not efficient and secure. Yuan and yu [3] design proxy and polynomial tag, but secrecy of group user is not considered means support only plaintext not cipher text. Data owner share group key, problem occur because any revoke group user force to another group user to share their key, any CSS take part in user revocation phase not data owner. So cloud server get chance for attacker and system not more secure CSSallowed group user data modification. To overcome above problem we design secure scheme with the help of ASGKA by using this protocol group user encrypt and decrypt share DB. Data owner able to conduct user revocation phase that is CSS not able to modify data [1].

III.Proposed SYSTEM OVERVIEW

The proposed system designs an efficient and reliable scheme, while achieving secure group user revocation. To the end, we propose a construction which not only supports group data encryption and decryption during the data modification processing, but also realizes efficient and secure user revocation. Our idea is to apply vector commitment scheme over the database. Then we leverage the Asymmetric Group Key Agreement (AGKA) and group signatures to support cipher text data base update among group users and efficient group user revocation respectively. Specifically, the group user uses the AGKA protocol to encrypt/decrypt the share database, which will guarantee that a user in the group will be able to encrypt/decrypt a message from any other group users. The group signature will prevent the collusion of cloud and revoked group users, where the data owner will take part in the user revocation phase and the cloud could not revoke the data that last modified by the revoked user. We explore on the secure and efficient shared data integrate auditing for multi-user operation for cipher text database. By incorporating the primitives of vector commitment, asymmetric group key agreement and group signature, we propose an efficient data auditing scheme while at the same time providingsome new features, such as traceability and count ability.

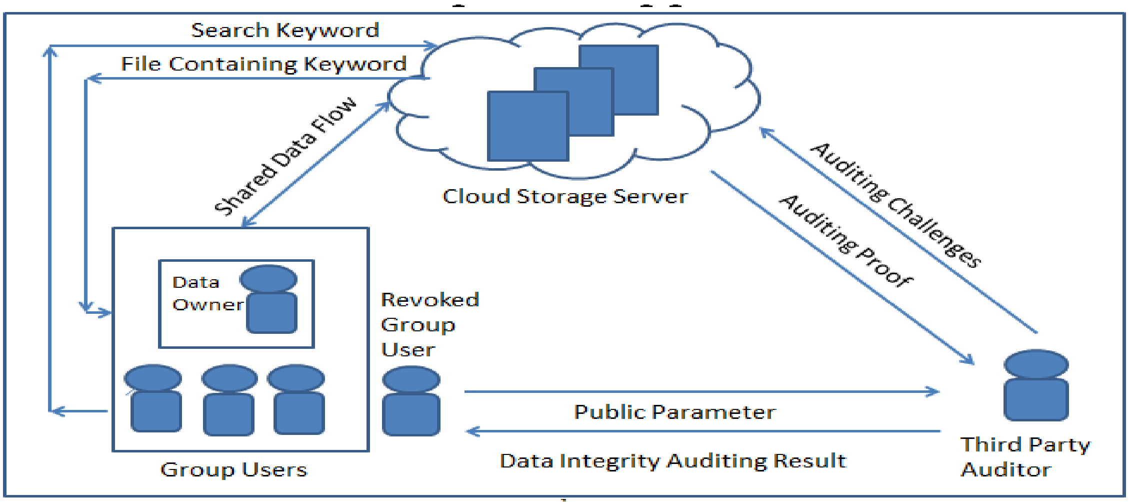


Fig 3.1 Proposed System Overview

In this project our contribution to extract keywords while file uploading. When user enters keyword that is from file, only files associated with that keyword are displayed to user (not all files) with the help of ECC, AES, Word count algorithms. We provide the security and efficiency analysis of our scheme, and the analysis results show that our scheme is secure and efficient. Propose system gives authority to only data owners for user revocation phase, and CSS does not take part in user revocation phase, because CSS is semi trusted model. When data owner upload their own file at that time specific keywords are extracted automatically those comes in file mostly. So owner get access to selected users in group only that user able to access file with searching file with extracted keyword, Belong to that keywords associated file display to users not all files.

Design Considerations:

- Initial data owner login as admin.
- Data owner upload own file on cloud(that time specific keyword extracted automatically)during process of file uploading admin select group as well as group user to give the access of file sharing. If file de-duplicate then uploading fail.
- Group user search file with extracted keyword, belong to that word associate file show to user not expose all data owner file to user.
- If user is revoke by owner then those users not able to access data.
- Cloud service provider not able to take part in user revocation phase, because revocation phase handle

  By owner.

- Data check by TPA, data owner send request to TPA, then TPA check request then verify data and send result back to owner is data is real or modified by CSS.
- If data is modified then owner reset AGKA, update to other group users.

Description of the Proposed Algorithm:

1. ECC Algorithm For Group Signature:

Step 1: Generation of both public and private key. Then select a number d within the range of n, using the following equation we can generate the public key

Q = d * P

Where

d = the random number that we have selected
Within the range of (1 to n-1) private key.
P = is the point on the curve.
Q = is the public key.

Step 2: encryption of message M Randomly select k from [1 (n-1)].
Step 3: Two cipher texts will be generated let it be C1 and C2.C1 and C2 will be send.
C1 = k*P C2 = M + k*Q
Step 4: Decryption process get back the message m that was send to us M is the original message that we have send.
M = C2 d * C1
Step 5: Proof is howwe gets back the message,
M = C2 d * C1
M can be represented as (C2 d * C1)
C2 d * C1 = (M + k * Q) d * (k * P)
(C2 = M + k * Q and C1 = k * P)
= M + k * d * P d * k *P (cancelling out k * d * P)
= M (Original Message)

2. AES for file encryption:

Step 1: Key Expansions: round keys are derived from the cipher key using key schedule.
AES requires a separate 128-bit input block occupy the first column in the 4 4
Matrix of bytes. The next four bytes occupy the second column, and so on.
Byte [][] state = new byte[4][Nb]
Step 2:Initial Round: - 1.AddRoundKey each byte of the state is combined with a block
Of the round key using bitwise xor. AddRoundKey (state, w, 0, Nb - 1)
2. Rounds
For (in round = 1; round Nr; round++)
A) Sub BytesA non-linear substitution step where each byte is replaced
With another according to a lookup table.
Sub Bytes (state)
B) Shift Rows
A transposition step where the last three rows of the state are
Shifted cyclically a certain number of steps.
Shift Rows (state)
C) Mix Columns A mixing operation which operates on the
Columns of the state, combining the four bytes in each column.
Mix Columns (state)
D) AddRoundKey
AddRoundKey (state, w, round*Nb, (round+1)*Nb - 1)
Step 3: Final Round (no Mix Columns)
1. Sub Bytes

```
        2. Shift Rows
        3. AddRoundKey
Step4: stop. out = state
```

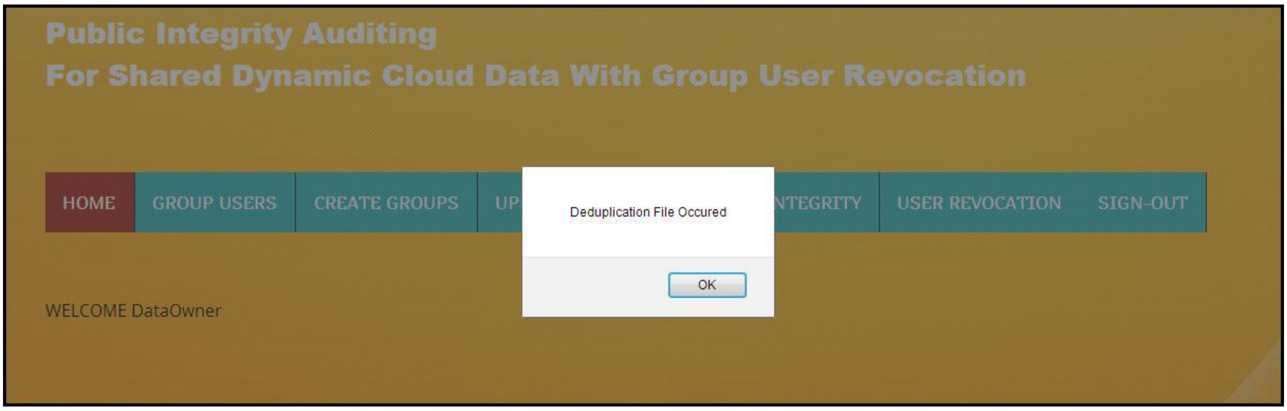
3. Wordcount for keyword extraction algorithms:

```
Step 1: Start from beginning of the Ext file.
Step 2: Traverse through entire file.
        String [] words = new String [arr.length];
Step 3: On each word create separate entry array
        int [] counts = new int [arr.length];
Step 4: If word occur again, thenincrement its counter
        Counts [0] = 1;
        For (int i = 1, j = 0; i arr.length; i++)
Step 5:  Else create separate entry for that word
        Words[j] = arr[i];
Step 6: After traversing whole file.
        Counts[j] ++;
Step 7: Display word that having higher frequency.
        Counts[j] = 1;
```

IV.TEST RESULT

Module 1: File de-duplication:

When data owner upload as own file on cloud server, file name and content of file check with other file which store in server, if content match the message will be display that the DE duplication of file, already occur, so this is nice property to save the storage space of sever, avoid file de-duplication.



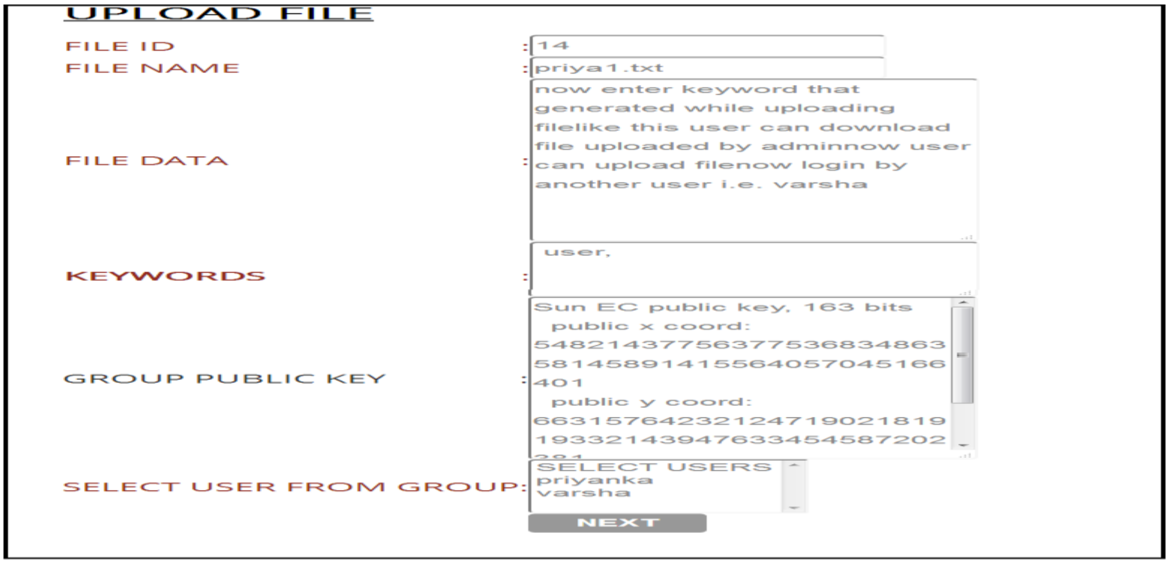
Public Integrity Auditing
For Shared Dynamic Cloud Data With Group User Revocation

Deduplication File Occured

WELCOME DataOwner

Module 2: File upload with automatic keyword extraction:

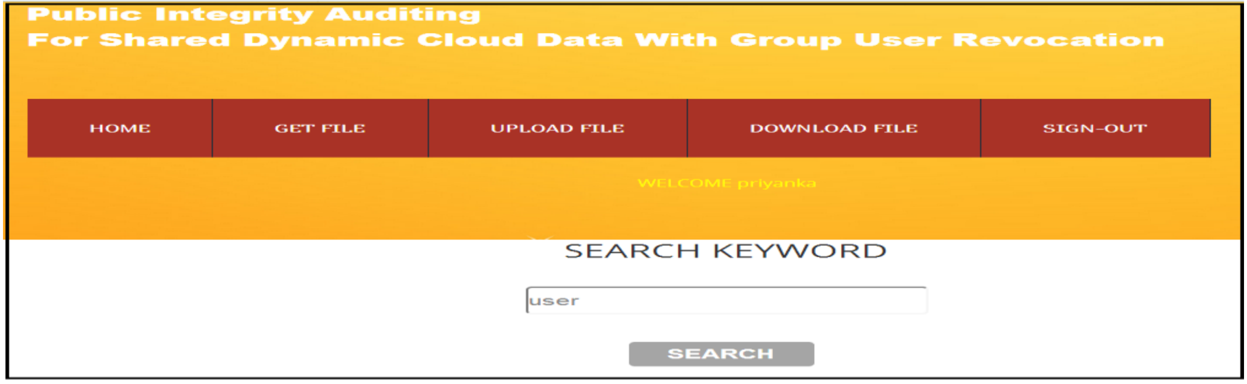
When data owner upload their own file with real content at that time some specific keyword extracted at the time of file uploading, that extracted keywords knows only data owner and those users who have selected by owner only not have access for all group user. So those user have access they have knowledge about file content. This is nice feature we propose only selected user able to access file, owner shows result of files those belong from specific extracted keyword, not all file display to user. Secrecy of data maintain by data owner.



UPLOAD FILE

FILE ID	:14
FILE NAME	:priya1.txt
FILE DATA	:now enter keyword that generated while uploading filelike this user can download file uploaded by adminnow user can upload filenow login by another user i.e. varsha
KEYWORDS	: user,
GROUP PUBLIC KEY	:Sun EC public key, 163 bits public x coord: 548214377563775368348635814589141556405704516640l public y coord: 66315764232124719021819193321439476334545872022
SELECT USER FROM GROUP:	SELECT USERS priyanka varsha

Module 3: Search keyword: Extracted keyword search by user who have access for share data, otherwise revoke user not able to access the data uploaded by data owner.



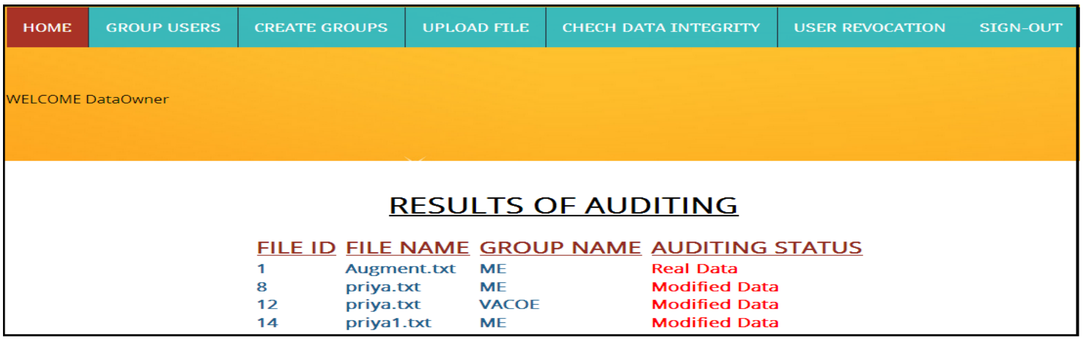
Public Integrity Auditing
For Shared Dynamic Cloud Data With Group User Revocation

WELCOME priyanka

SEARCH KEYWORD

user

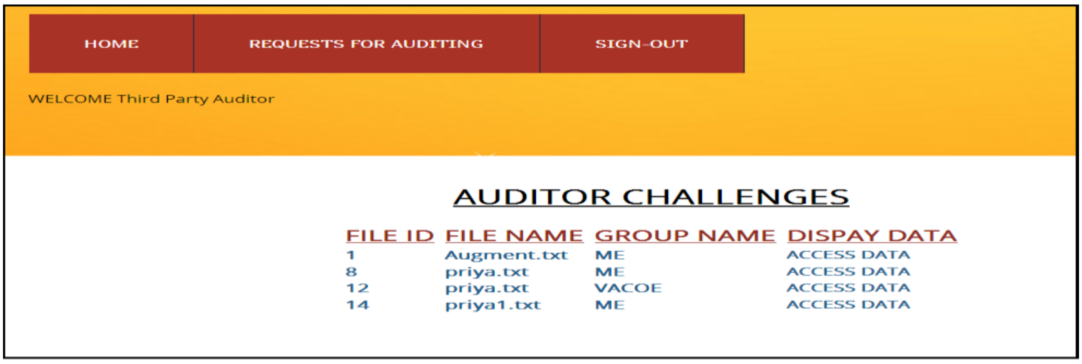
Module 4: Auditing Result : If data owner want to check the data integrity of uploaded data, owner sent auditing request to TPA, then TPA access data and sent result to data owner that data is real or modified by CSS(cloud storage server).



WELCOME DataOwner

RESULTS OF AUDITING

FILE ID	FILE NAME	GROUP NAME	AUDITING STATUS
1	Augment.txt	ME	Real Data
8	priya.txt	ME	Modified Data
12	priya.txt	VACOE	Modified Data
14	priya1.txt	ME	Modified Data



HOME | REQUESTS FOR AUDITING | SIGN-OUT

WELCOME Third Party Auditor

AUDITOR CHALLENGES

FILE ID	FILE NAME	GROUP NAME	DISPAY DATA
1	Augment.txt	ME	ACCESS DATA
8	priya.txt	ME	ACCESS DATA
12	priya.txt	VACOE	ACCESS DATA
14	priya1.txt	ME	ACCESS DATA

V. Simulation Results

1. Query Time Cost:

Query time cost of our scheme is taking exactly 3 second to query about 1000 data item. The server does not need to run the whole Query algorithm every time. Efficient than existing scheme.

2. Verify Time Cost:

Verify time cost, the computation overhead comes from the group signature. Verify the validity is most important of this phase, first of all verify the integrity of the signature, the computational cost of our scheme is 5 times efficient than scheme [2].

3. Update Time Cost:

When number of block increases then computational cost increase in our scheme.

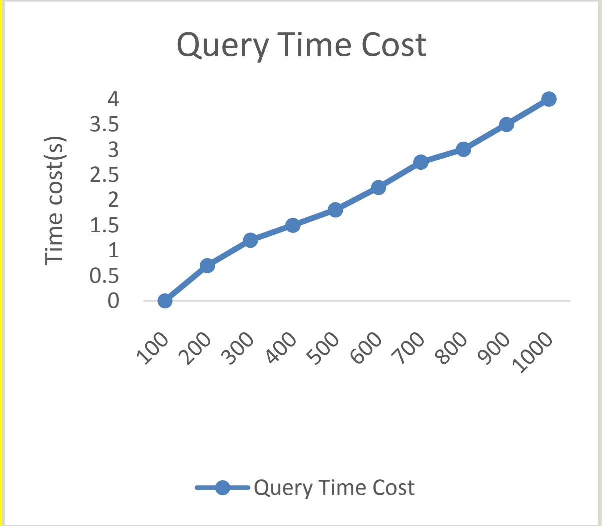


Fig.1.Query Time Cost

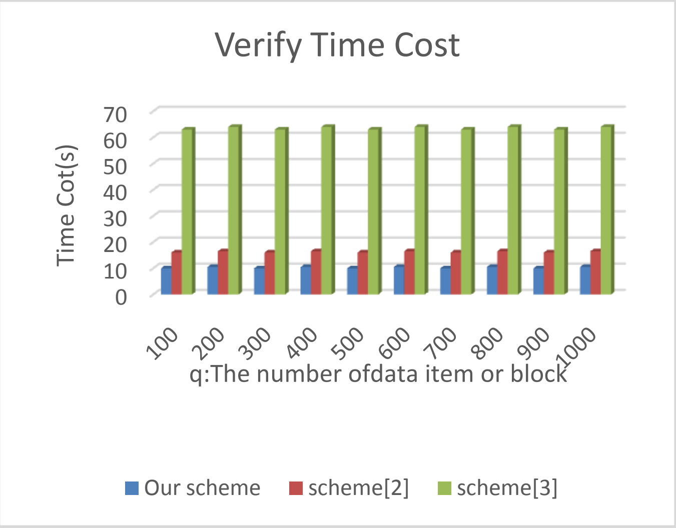
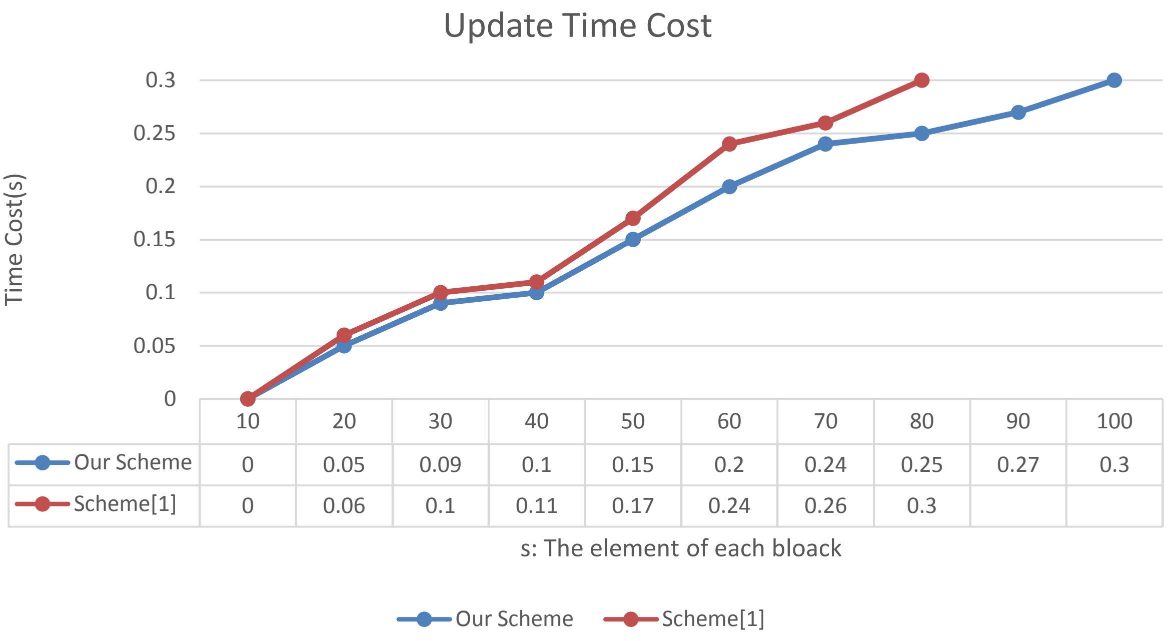


Fig. 2. Verify Time Cost



	10	20	30	40	50	60	70	80	90	100
Our Scheme	0	0.05	0.09	0.1	0.15	0.2	0.24	0.25	0.27	0.3
Scheme[1]	0	0.06	0.1	0.11	0.17	0.24	0.26	0.3		

Fig. 3. Update Time Cost

VI. CONCLUSION AND FUTURE WORK

Scheme provides security analysis and data confidentiality for group users, securely and efficiently shared data integrate auditing for multi-user operation for cipher text database. It is also secure against the collusion attack and revoked group users cloud storage server. The propose scheme uses VC, (AGKA), Elliptic curve cryptography for group signature ,Advanced encryption standard for file encryption, Word count for keyword extraction algorithms with user revocation are achieve the data integrity auditing of remote data using multiple authorities in the cloud computing system more secure. In this paper our contribution to extract keywords while file uploading. When user enters keyword that is from file, only those files associated with that keyword are displayed to user not all files display to user. Also provide some nice property avoid file de-duplication that is save the memory space of cloud storage, another is keyword extraction, experimental result shows that confidentiality of our scheme, as compare to other relative scheme our scheme provide efficiency and security. We propose an efficient data auditing scheme while at the same time providing new features such traceability and count ability to provide the security and efficiency analysis of our scheme.

In our research attempt, we have focused to provide security analysis and data confidentiality for group users However, the cloud is growing tremendously via use of the Internet.Growing the use of TPA for key generation and for key agreement.TPA is central system, if it fails then whole system get failed.The whole attribute set is divided into *N* disjoint sets and controlled by each single authority, therefore each authority is aware of only part of attributes. If we are working with cloud, user identity is major concern; user doesn't want to reveal his personal information to public. This concept not included in it.In this sense, systemis semi-anonymous since, but we can achieve as full-anonymity.

REFERENCES

1. Tao Jiang, Xiao Feng Chen, and Jian Feng Ma, "Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation," IEEE Transactions, vol. 10, pp. 99, 2015.
2. B. Wang, L. Baochun, and L. Hui, "Public auditing for shared data with efficient user revocation in the cloud," IEEE INFOCOM Italy, Apr. 2013.
3. J. Yuan and S. Yu, "Efficient public integrity checking for cloud data sharing with multi-user modification," in Proc. of IEEE INFOCOM 2014, Toronto, Canada, Apr. 2014, pp. 2121–2129.
4. Giuseppe Ateniese, Randal Burns, Reza Curtmola, Joseph Herring, "Provable Data Possession at Untrusted Stores," IEEE Transaction, 2007.
5. Yevgeniy Dodis, Salil Vadhan, Daniel Wichs, "Proofs of Retrievability via Hardness Amplification," J anuary 26, 2009.

6. Chris Erway, Alptekin Kupcu, Charalampos Papamanthou, Roberto Tamassia, "Survey on: Dynamic Provable Data Possession," reseedings of the 16th ACM conference on Computer and communications security,Chicago, Illinois, USA, November, 2009.

7. C. Wang, Q. Wang, K. Ren, W. Lou, "Privacy-preserving public auditing for storage security in cloud computing," IEEE, Mar 2010.

8. Elaine Shi, Emil Stefanov, Charalampos Papamanthou, "Practical Dynamic Proofs of Retrievability," D. Catalano and D. Fiore, "Vector commitments and their applications in Public-Key Cryptography - PKC", Mar. 2013.

9. Q. Wu, Y. Mu, W. Susilo, B. Qin, and J. Domingo-Ferrer, "Asymmetric group key agreement," in Proc. of EUROCRYPT Cologne, Germany 2009.

10. Madhuri R. Rokade et al, "Providing Data Utility on Cloud using Slicing approach and Dynamic Auditing Protocol using TPA to maintain Integrity of Data", IJCSIT 2014.

11. Giuseppe Ateniese, Dawn Song, and Gene Tsudik, "Quasi-Efficient Revocation of Group Signatures.

12. Jan Camenisch, Anna Lysyanskaya,, "Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials" February 2002.

13. Xiaofeng Chen, Jin Li, Xinyi Huang, Jianfeng Ma, and Wenjing Lou, "New Publicly Verifiable Databases with Efficient Updates," IEEE Transactions on Dependable and Secure Computing 2013.

14. Technical Guideline TR-03111, Elliptic Curve Cryptography.

15. Avi Kak,"AES: The Advanced Encryption Standard Lecture Notes on Computer and Network Security" April 2016.

16. K.Suresh Babu, J. Mahalakshmt et al., "Group User Revocation and Integrity Auditing" (IJITR) Volume No.4, Issue No.4 July 2016.

17. Priyanka A. Phasale and Prof M.C.Kshirsagar, "A Survey on Dynamic Data Sharing in Public Cloud using Multi- Authority System", IJIERT,PP NO- 2394-3696, 2015.

BIOGRAPHY

Mrs. Phasale Priyanka A. The success of this paper depends largely on the encouragement and guidelines of many others. We express our heartfelt gratefulness to Dr. L. B. Abhang principal and head of computer engineering department, Vishwabharati Academy's College Of Engineering, Ahmednagar, for their inspire supervision whenever required during this work. Also thankful to the staff of Computer Engineering Department of VACOEA for their cooperation and support. I would like to put forward our heartfelt acknowledgement to all our friends and all those who have directly or indirectly provided their overwhelming support during the work of this paper.