IJCTA, 9(36), 2016, pp. 327-336
© International Science Press

Block–Based Diagonal Hashing Scheme with One Step Verification for Efficient Public Auditing and Data Management of Cloud Resources

V. Joseph Michael Jerard* and P. Manimegalai Vairavan**

Abstract : The problem of public auditing and data management has been studied in a number of research articles previously. The methods use various schemes of data management and the author discussed different approaches to ensure the correctness of data, but suffers from the problem of poor accuracy and higher time complexity. To overcome the issue of public auditing, an efficient block-based diagonal hashing scheme has been proposed. The method splits the input data into a number of blocks and for each block, the diagonal hashing scheme has been used to encrypt the data. The users of the cloud environment can access the data published, and they can modify the data with the possession of keys being provided. The public auditing of cloud resource is ensured using a one-step verification approach performed by the third party auditor and cloud resource provider who maintains entire verification keys. The data management is performed in block based approach and the modified data will be indexed to the previous blocks after the successful completion of one-step verification process.

Keywords : Cloud Computing, Public Auditing, Data Management, One Step Verification, Block Based Approach.

1. INTRODUCTION

Cloud as the term suggest is the group of resources formulates a resource medium where the cloud user can post their resources and can fetch whenever required. The cloud is a loosely coupled environment where the identity is not known to the environment. The service provider provides various services in the cloud environment at different levels as infrastructure (IaaS), platform (PaaS) and database (DaaS). Whatever the service being provided, the user can access the service on registration, and the environment maintains the various identity for the cloud users. In general, the user identity is maintained by a third party, which performs verification of user identity at all the situation. The cloud service provider generates keys for the successful access of the cloud resource and user details who were authorized to access to the third party auditor. The user details and key details are maintained by the third party auditor, upon verification request from the cloud service provider or cloud manager, the details are verified and based on the result from the TPA, and the user access will be granted.

The user identity may be verified by the TPA, but there are many challenges present in the cloud environment. In particular, when the resource becomes sharable and collaborative working, then auditing the correctness called public auditing becomes more important. By providing public auditing, the user assured with the correctness of data and user can trust the value of data. To perform such task the third

* Research scholar, Karpagam University, Coimbatore, Tamil Nadu, India.

** Professor, ECE Dept., Karpagam University, Coimbatore, Tamil Nadu, India

party auditor communicates with the data owner to verify the correctness of the data. This situation arises when the cloud user modifies the data and before updating the original data, the cloud manager performs the verification by communicating with the TPA and Cloud service provider (CSP). Based on the result of verification, the modification of the data is performed.

Data management is another issue in cloud computing, which ensures the proper storage of the cloud resources. There are many approaches being discussed for the data management which focuses on how the resource being stored. The efficiency of cloud environment is highly based on how the data being stored and how fast they can be retrieved or modified. To improve the performance of cloud computing, the environment has to ensure higher accuracy in data management and public auditing. The public auditing focuses on the security of data in the cloud environment where the data management focuses on the storage of data in the cloud.

For the security improvement, there are many strategic approaches being discussed earlier like public/ private key based mechanism, session based approaches, Attribute based mechanism and so on. Each of the approaches has many flaws in their performance, and they produce more inaccurate results in public auditing and data management. Also, the approaches struggle with the problem of higher time complexity which is a more affecting factor of cloud performance. To reduce such time complexity, the one step verification can be used. The one step verification approach is about verifying the correctness of the content in single step. In this approach, the TPA communicates with the data owner and request to verify the content. Based on the result of data owner the original content will be modified.

For the data management, the cloud has many storage mechanisms. We talk about the block based approach, where the content of the entire resource will be split into number of blocks. For each block the data owner generates keys to access the block. By registering the service the user will be able to get the keys allocated to the resource and even the user could be restricted in accessing specific blocks of the resource. The cloud stores the blocks of resource in scattering manner to overcome the risk of accessing the resource by guessing attacks.

2. RELATED WORKS

There are a number of methods has been discussed for the development of security measures in cloud computing and to improve the performance of cloud environment. This section discusses about few of the approaches related to public auditing and data management in cloud environment.

Secure Privacy Preserving Public Auditing for Cloud storage [1], proposes secure public auditing scheme for cloud storage provide more security compared previous technology. In this paper public Auditing system and discuss two straightforward schemes and their demerits. Then they present our main result for privacy preserving Public auditing to achieve the before mentioned design Goals. This paper provides an abstract view of different schemes proposed in recent past for cloud data security using third party auditor. Most of the authors have proposed schemes which rely on encrypting the data using some encryption algorithm and make third party auditor store a message digest or encrypted copy of the same data that is stored with the service provider. The third party is used to resolve any kind of conflicts between service provider and client.

Public Auditing of Big Data with Fine Grained Updates on Cloud [5], presents an overview of trusting a third party. It focuses on privacy-preserving which means TPA cannot derive user's data during the process of public data auditing. The proposed system uses a signature scheme which cannot be forged so that it will prevent malicious TPAs. It provides a feature of fine-grained dynamic data update which increases the efficiency of update process.

Privacy Preservation and Public Auditing for Cloud Data Using Ass [8], a privacy-preserving mechanism is designed which supports public auditing on shared data stored in the cloud. In particular, aggregate signatures are used which computes the verification metadata needed to audit the correctness of shared data. With this mechanism, the identity of the owner who signs each data block in shared data is kept private from public verifiers. These public verifiers are able to efficiently verify integrity of shared data without downloading the entire file. In addition, this mechanism can efficiently perform multiple auditing tasks at same time instead of verifying them one by one.

Third Party Auditing for Secure Data Storage in Cloud through Trusted Third Party Auditor Using RC5 [12], ensure reliable data storage using cloud services. It mainly focuses on the way of providing computing resources in form of service rather than a product and utilities are provided to users over internet. In the cloud, application and services move to centralized huge data center and services and management of this data may not be trustworthy, into cloud environment the computing resources are under control of service provider and the third-party-auditor ensures the data integrity over out sourced data. In this paper, we proposed encryption method at TPA side to protect the privacy and integrity of outsourced data in cloud environment. To ensure the correctness of data, we consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the data stored in the cloud., the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy preserving public auditing. This shows the proposed scheme is highly efficient. Here Work is focuses on RC5 Encryption Algorithm for stored data in cloud. Resulted encrypted method is secure and easy to use.

Implementation of Privacy-Preserving Public Auditing and Secure Searchable Data Cloud Storage [13], identify the system requirements and challenges toward achieving privacy-assured searchable outsourced cloud data services, usable design and practically efficient search schemes for encrypted cloud storage. We are presenting a general methodology for these using searchable encryption techniques, which allows encrypted data to be searched by users without leaking information about the data itself and user’s request. Enabling public audit ability for cloud storage is of critical importance so that users can use up to a third party auditor (TPA) to check the integrity of outsourced data and can be worry free. To efficiently introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and help to avoid additional online burden to user. We propose a secure and efficient cloud storage system supporting privacy-preserving public auditing. We will further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently.

Tcloud : A Trusted Storage Architecture for Cloud Computing [14], present a trusted architecture of cloud data storage. The architecture presents a unique way of secure storage and accessing of data from the cloud data center. It also ensured that only authorized user will be able to access the data. Additionally, if there is any violation of the security parameter at the data center, the data will still be safe i.e. the data will be stored in encrypted form.

In Access Controlled Data Security in Cloud Environment [15], Third Party Auditor (TPA) mechanism thus the user is able to share the data while having the facility to allow/ deny access along with the read write permission to a single user and group of users. The data which is shared by user is encrypted and secret shares are generated and some but not all secret shares are stored on the distributed cloud Environment. Thus TPA has the complete data to authenticate the integrity of the data. Thus as per our approach the TPA will be able to do the auditing without asking for the local copy of the data which in turn will result in less communication and computational load.

All the above discussed methods has the problem of ensuring the correctness of data and produces poor data management and takes more time complexity.

3. BLOCK BASED DIAGONAL HASHING SCHEME

The block based diagonal method splits the entire file into number of blocks with fixed size. For each block of the data, the method generates encryption keys using the diagonal hashing scheme. The diagonal hashing scheme works as follows: The method maintains different level of keys according to the size of file. For instance, the method maintains N number of keys and the value of N is 27, where the size of file is within the range of 27 megabits. How the value of N is computed is as follows:

$$K = \{3, 4, 5, 6,\ldots., P\} \tag{1}$$

K represents the set of integer number.

$$N = \varnothing(K)^3 \tag{2}$$

The symbol ∅- is the subset of K with size 1.

The value of N represent the cube value of subset from K.

Once the size of file has been identified then the method determines the number of block X as follows:

$$S = \text{Size}(R) \tag{3}$$

R is the resource and the value S represents the size of file.

Now select the value N from K based on the size of file S as follows:

$$N = \int_{i=1}^{\text{size (K)}} k(i)^3 > S \tag{4}$$

After computing the value of N, now the method generates key matrix using different key values. Generated key matrix will be used to perform hashing and generate encryption keys.

For example for the value of N = 64, the method generates the key matrix as follows:

Table 1

Sample Key Matrix

a	*b*	*c*	*d*	*e*	*f*	*g*	*h*
i	*j*	*K*	*l*	*m*	*n*	*o*	*p*
q	*r*	*s*	*t*	*u*	*v*	*w*	*x*
y	*z*	*aa*	*ab*	*ac*	*ad*	*ae*	*af*
ag	*ah*	*ai*	*aj*	*ak*	*al*	*am*	*an*
ao	*ap*	*aq*	*ar*	*as*	*at*	*au*	*av*
aw	*ax*	*ay*	*az*	*ba*	*bb*	*bc*	*bd*
be	*bf*	*bg*	*bh*	*bi*	*bj*	*bk*	*bl*

The Table 1, shows the sample key matrix being generated for the value of N=64 and the same can be computed for any value of N.

Now the method computes the number of blocks B to be generated.

The number of blocks to be generated is identified using a random generator, where the random generator takes the size of file as input and generates a random number within the range of file size.

$$\text{Rand} = \int \text{Random Generator } (N)^2 \tag{4}$$

The equation (4) computes the number of blocks the file has to be split and the value of Rand is the square of any random number within the range of N.

Now for each block of the file, the method performs number of transpose operation on the key matrix and performs generation of M^{-1} for B number of times, where B is the number of block. If the value of B is 1, then the key matrix is transposed for 1 time, for the value of B = 2, the key matrix is transposed for 2 times. Finally from the transposed matrix of keys, the method computes the average value of diagonal elements and the element at the index of average value will be selected as the key for the block.

Generated key will be used to produce encrypted block and the method stores the resultant key in separate key matrix to be used in the verification phase.

3.1. Cloud Controller

The cloud controller is the functional component which operates and controls the overall functionality of the cloud environment. The service provider could be able to post their resource and upon submission of the resource the CSP generates the key using the Block Based Diagonal Hashing Function and shares the key set with the third party auditor and intimates the resource with the cloud controller. Similarly the cloud user will be able to access the cloud resource based on the resource id and the request will be handled by the controller.

```
Pseudo Code of Cloud Controller :
Input : Resource Request/Deployment, Resource Table Rt
Output : Boolean/Boolean
Start
        Receive Resource Request Req.
        If Req.Type == Upload Then
                Update the resource Table Rt.
                        $Rt = \sum(Ri \in Rt) \cup Req. Resources$
        Else if Req.Type == Access Then
                Verify with TPA.
                If True then
                        Return References.
                End
        End
Stop.
```

Above discussed pseudo code performs the cloud resource handling and request handling. The method handles different request types and acts according to the request type submitted.

3.2. Third Party Auditor TPA

The Third party auditor performs the identity management of the entire cloud environment. Upon uploading any resource the CSP shares the list of users and their id with them. Whenever the user request arises, the TPA receives the identity key and verifies the key for its trustworthy. If the key verification becomes successful then the request comes to the next stage. In the second stage, if the request is read type then the reference will be returned to the user and if the resource is write type then the TPA receives the block and communicates with the CSP. Based on the result from the CSP the TPA returns results to the user.

```
Pseudo Code of TPA:
Input : Key Set Ks, Resource Set Rs
Output : Null
Start
    Receive Request Rs.
    If Rs.Type == Upload Then
            Update Resource set Rs.
            $Rs = \sum(Res \in Rs) \cup Rsi$
            Receive Key set Ksi.
            Update key set Ks.
            Ks =
    Else if Rs.Type == Access Then
            If $\int_{=1}^{\text{size(Ks)}} ks(i) == Reqeust.key$ Then
                    Return true.
            End
```

```
        Return false
    Else if Rs.Type == Modify Then
        If $\int_{=1}^{\text{size(Ks)}} ks(i) == Reqeust.key$ Then
            Communicate with CSP.
            If True Then
                Return True.
            Else
                Return False.
            End
        End
        Return false
    End
    Stop.
```

The pseudo code displayed above performs the operation of Third party auditor and controls the access of any resource and maintains the identity of the system.

3.3. One Step Verification

The one step verification is the process of verifying the correctness of the data in single step. In this the TPA communicates with the CSP whenever it receives the modification request. The TPA receives the modification request and communicates with the CSP to perform one step verification. Upon receiving the request from the TPA the CSP invokes this one step verification approach. The functional module receives the modified block and sends to the CSP to verify the correctness of data.

```
Pseudo Code of One Step Verification:
Input : Modified Block Mb, Request req.
Output : Boolean
    Receive request Req.
    Identify the resource Id Rid.
    Receive the modified block Mb.
    Send (Rid, Mb).
    Receive (flag).
    If flag == true then
        Return true.
    Else
        Return false.
    End
Stop.
```

The above discussed one step verification approach verifies the correctness of data using the support of CSP and returns flag to the TPA.

3.4. Cloud Service Provider (CSP)

The CSP plays the vital role in the cloud environment by providing various services and whenever It receives the modification request from the TPA, it claims the user id, modified block and resource id. Using all these information, the method verifies the presence of two bit integer at the end of each block.

For the modified block, the method reads the last two decrypted with the decryption key for the block. Now the decrypted data is verified by computing the number of ones and zeros throughout the block. If the value of number of ones and zeros are equal in both then the block is modified in proper manner and returns true value to TPA otherwise the TPA will be sent with the false flag.

```
Pseudo Code of TPA :
Input : Key Set Ks, Modified Block Mb
Output : Boolean
Start
    Read Modified Block Mb.
    Identify the key for the block from ks.
    Ki = Π Key (Mb) ∈ Ks
    Read the last two bits of Mb.
    Nones = Integer (Mb (Mb (size)-2)).
    Nzeros = Integer (Mb (Mb (size)-1)).
    Decrypt Mb using the key.
    Compute Tones from Mb.
    Tones = $\sum^{\text{size(block)}} bit\ (mb) == 1$
    Compute Tzero from Mb.
    Tzero = $\sum_{i=1}^{\text{size(block)}} bit\ (mb) == 0$
    If Tones == Nones && Tzero == Nzeros Then
        Return true
    Else
        Return false.
    End
Stop.
```

The above discussed algorithm performs the verification process by computing the number of ones and zeros. The computed values are used to verify the correctness of the data.

4. RESULT AND DISCUSSION

The proposed block based diagonal matrix approach has been implemented and designed using different simulation scenarios. The method has been evaluated for its performance using the CloudSim simulator and the performance of the proposed mechanism has been evaluated.

Table 2

Details of simulation parameter

Parameter	*Value*
Simulator Name	Cloud Sim
Number of resources	1000
Number of users	500

The Table 2, shows the details of simulation parameter being used to evaluate the performance of the proposed approach.

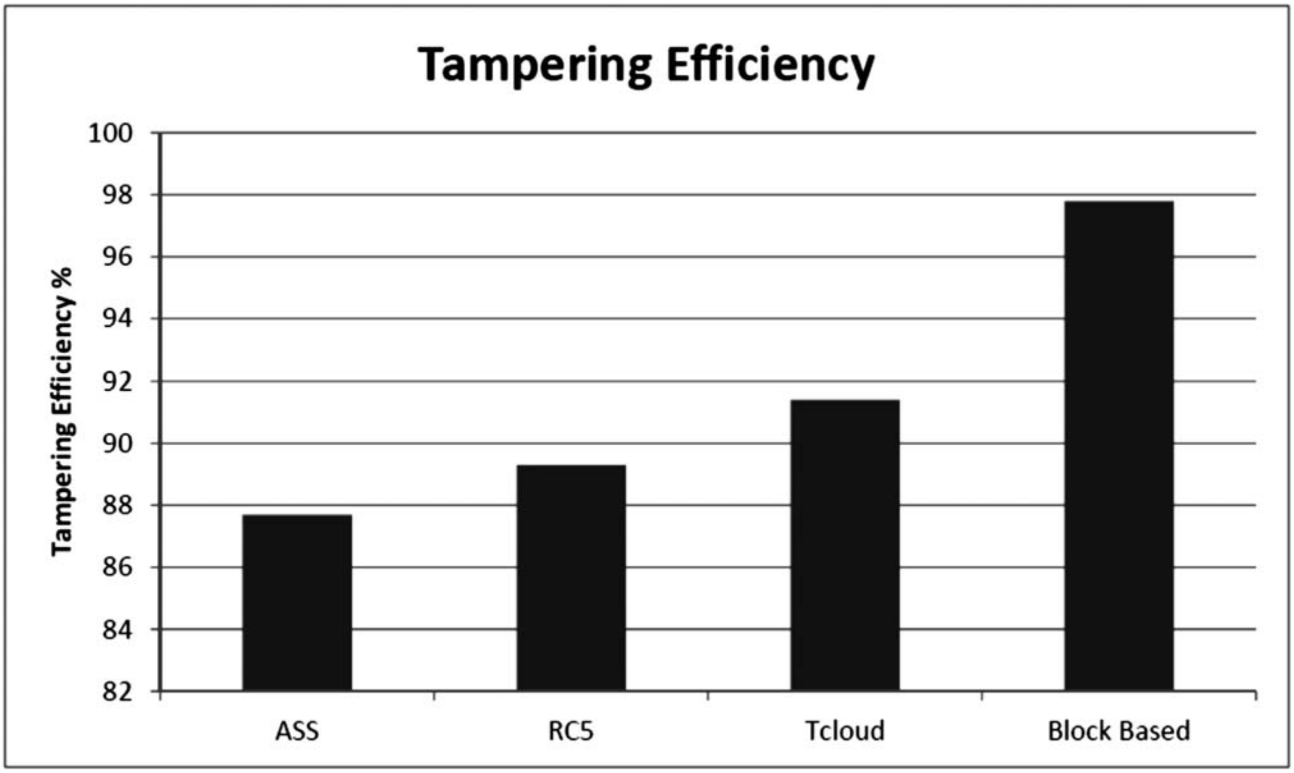

Figure 1: Comparison of tampering efficiency

The Graph 1, shows the tampering efficiency produced by different methods and it shows that the proposed block based approach has produced efficient results than other methods.

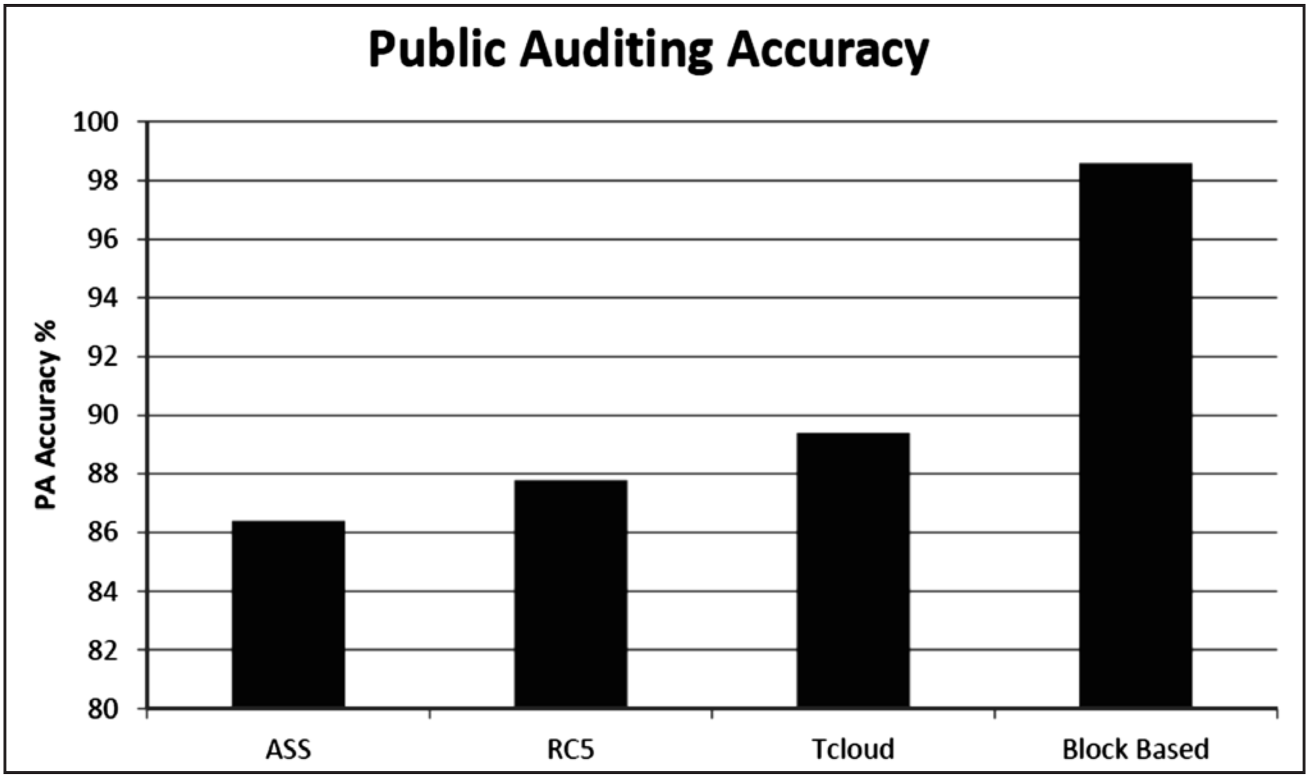

Figure 2: Comparison of public auditing accuracy

The Graph2 shows the comparative result on public auditing accuracy produced by different methods and it shows clearly that the proposed method has produced more auditing accuracy than other methods.

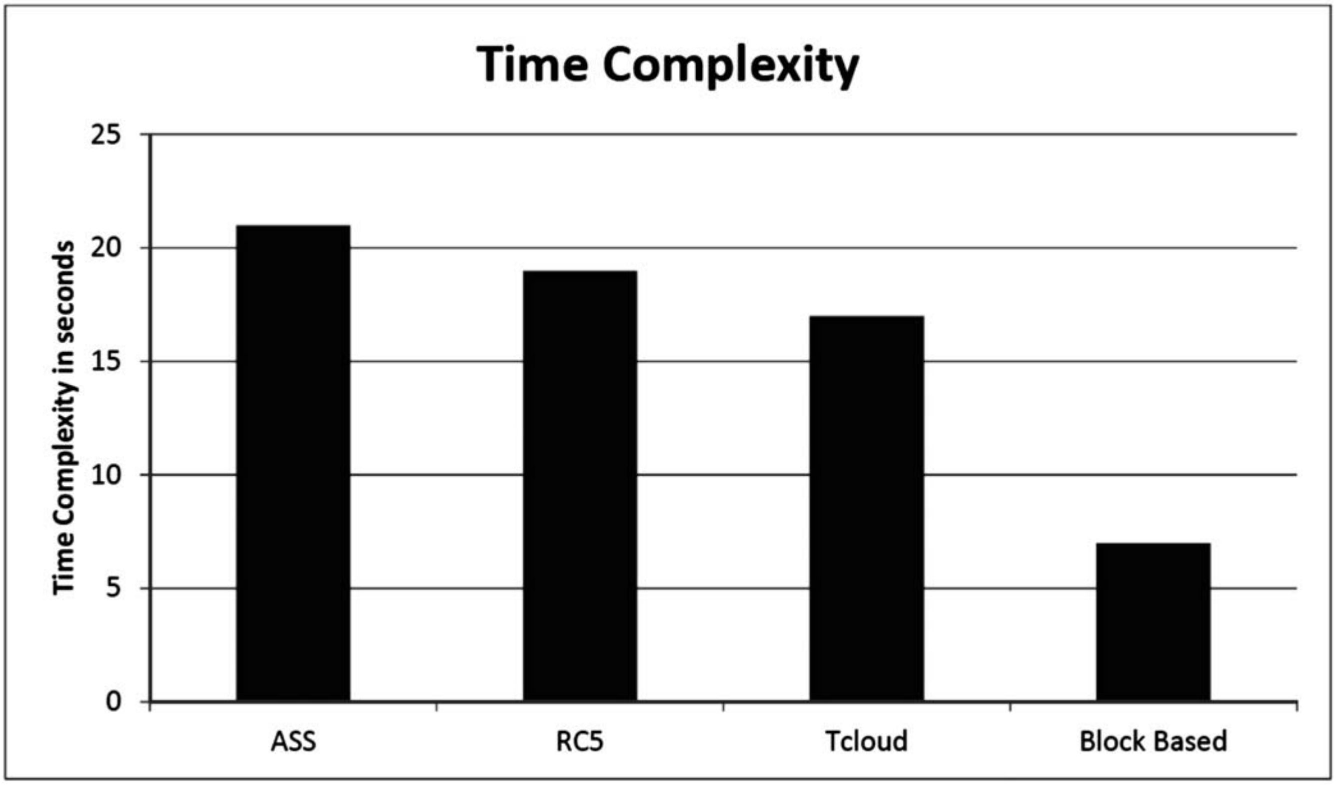

Figure 3: Comparison of time complexity

The Graph 3 shows the comparative result on time complexity in verification and the result shows that the proposed method has reduced the time complexity of verification than other methods.

5. CONCLUSION

This paper presents a block based diagonal key based one step verification scheme for the development of public auditing in cloud environment. The method splits the entire resource into number of blocks and for each block the method selects an encryption key and encrypts using the diagonal hashing function. The cloud user is provided with the keys and whenever the user has modified the block of data then the request will be handled by the TPA. The TPA communicates with CSP, instead the CSP performs one step verification which verifies the originality and correctness of the data. Based on the result of CSP the TPA handles the user request. The proposed method produces more accurate result in public auditing and produces efficient result in time complexity also.

6. REFERENCES

1. Sathiskumar R1 , Dr.Jeberson Retnaraj, Secure Privacy Preserving Public Auditing for Cloud storage, International Journal of Innovative Research in Science, Engineering and Technology, Volume 3, Special Issue 1, January 2014.
2. C. Wang, K. Ren, W. Lou, and J. Li, “Toward Publicly Auditable Secure Cloud Data Storage Services,” IEEE Network, vol. 24, no. 4,pp. 19-24, July/Aug. 2010.
3. K. Yang and X. Jia, “Data Storage Auditing Service in Cloud Computing: Challenges, Methods and Opportunities,” World Wide Web, vol. 15, no. 4, pp. 409-428, 2012.
4. C. Wang et al., “Privacy-Preserving Public Auditing for Storage Security in Cloud Computing,” Proc. IEEE INFOCOM ‘10, Mar.2010.
5. Surapriya Swain, Public Auditing of Big Data with Fine Grained Updates on Cloud, International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 12, December 2014.

6. Q. Wang, C.Wang, K. Ren, W. Lou, and J. Li, ‘‘Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,’’ IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 5,pp. 847-859, May 2011

7. Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren, and Wenjing Lou, “Privacy-Preserving Public Auditing for Secure Cloud Storage,” IEEE Transactions On Cloud Computing, Year 2013.

8. Dr. J. SUGANTHI, ANANTHI J, S. ARCHANA, PRIVACY PRESERVATION AND PUBLIC AUDITING FOR CLOUD DATA USING ASS ,International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 3, Issue 6, November-December 2014.

9. B. An Efficient Utilization of Spectrum in Wireless Mobility by Retransmission Mechanism” in Central government NISCAIR, Journal of Scientific & Industrial Research (JSIR), New Delhi, india in September 2015 issue.

10. S Archana and Ananthi J, “Privacy-Preservation and Public Auditing for Cloud Data - A Survey”, International Journal of Science and Research (IJSR), Vol. 3, No. 10, October 2014, pp-1989-1992.

11. 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: Advances in Cryptology (EUROCRYPT’03), pp. 416-432, 2014.

12. Nupoor M. Yawale , Prof. V. B. Gadicha, Third Party Auditing For Secure Data Storage in Cloud through Trusted Third Party Auditor Using RC5, International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 3, March 2014.

13. A. MsVaishali Patil, 2B. Prof. Archana Lomte, Implementation of Privacy-Preserving Public Auditing and Secure Searchable Data Cloud Storage, International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 7, July 2014.

14. Sultan Ullah and Zheng Xuefeng, TCLOUD: A Trusted Storage Architecture for Cloud Computing, International Journal of Advanced Science and Technology Vol.63, (2014), pp.65-72.

15. Challenges and Surveys in Key Management and Authentication Scheme for Wireless Sensor Networks“ in Abstract of Emerging Trends in Scientific Research 2014– 2015.