ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

Proxy Based Resource Allocation and Access in Cloud Environment

[1] M.R. Yuvaraj, [2] G. Adiline Macriga, [3]S. Veenadhari

[1] Research Scholar, Dept. of Computer Science and Engineering, AISECT University, Bhopal, India

[2] Professor, Sri Sairam Engineering, Chennai, India

[3] Associate Professor, Dept. of Computer Science and Engineering, AISECT University, Bhopal, India

ABSTRACT : Data integrity maintenance is the major objective in cloud storage. It includes audition using TPA for unauthorized access. The data of the users will be stored in public and private areas of the cloud. So that, only public cloud data will be accessed by user and private cloud will remain more secure. Once any unauthorized modification is made, the original data in the private cloud will be retrieved from the cloud server and will be returned to the user. Every data stored in the cloud will be generated with a Hash value using the Merkle Hash Tree technique. So modification in content will make changes in the Hash value of the document as well. The proxy also performs signature delegation work by generating private and public key for every user using Polynomial Reduction Algorithm so that the security will be maintained. This scenario is implemented in a multi owner environment in which one document will be accessed by user groups. In this context, the access limit should be properly maintained so that no user of other group should be allowed to modify a particular group's data. Also, if any modifications made to that data will be identified by the proxy and the user is revoked.

KEYWORDS: Cloud Computing, Proxy, TPA, Polynomial Reduction

I. INTRODUCTION

1.1 Motivation

With evolution of computers the life of people became more and more easily. They where able to keep there data on there devices, and started finding ways to make them accessible to others, for example say by using floppy, writable disks, which was followed by portable hard-disk, all these where expensive in there own way during there time. The data was very much private on personal devices like PC, laptops, mobile phones etc, therefore sharing data with others was considered to be expensive. As the world of computing got more advanced the ways for sharing data started becoming cheaper and cheaper. In recent years a new term has evolved call ”Cloud” which is provided by different provides, and which is nothing but facility or service of different resources or components like hardware, platform, storage’s, software etc, and it is gaining importance because it frees the user from maintenance perspective on a investment of some money for the use of these services provided by cloud service providers[3]. Now to provide such service to the client, naturally the provider’s must have and rather can have access to resources which are used by the people/clients. Among the reasons these access are greatly required are for maintenance perspective. And definitely since billions of clients will be thinking about using such service, the infrastructure ought to be capable enough to support them, and these resources ought to be shared between billions of client’s. Service availability, data synchronization between different devices, availability of data via any devices which includes browser facility makes cloud more attractive. Now since the info gets shared or stored in providers area, the client gets worried about privacy of its data, although there are certain agreements and SLA which are agreed by cloud provider and client[4]. Now although client has a platform to generally share the info, the expense of securing his/her data or in a nutshell making its data private gets costlier.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

The cloud term is of interest not just to the patient clients but to organizations as well. With organization as a consumer the concern of data security becomes multifold. Consider a typical example of small scale business that has different departments like HR, Finance, etc. We will focus on finance department since finance details of any business/company/organization are considered to be very sensitive and must be confidential. Therefore if the little scales company thinks of using the cloud services like storage. Storing all account/finance related information in cloud stored makes it prone to leakage of sensitive information tells un-authorized users. Therefore securing this finance data is vital before it gets uploaded to the storage cloud, and just in case the data stored in cloud storage gets tampered there should be a method to verify the integrity of the data, moving further specific band of people should have access to this data which may be folks from finance department of client company or special auditors. Simply speaking the client must have the ability to store the data securely, verify the integrity of the data, share the data securely with specific band of people[7].

1.2 Problem Definition

The clients concern about data security, data integrity, and sharing data with specific band of men and women must be addressed. You can find multiple means of achieving this, example encrypting data on client machine and then storing the information to cloud storage server, computing hash of the information on client machine and storing hash of data in client machine, client trying out the responsibility of sharing the trick key about encryption with specific band of people. Therefore it becomes more tedious for client to keep these information and share such information, more over in the event the device which stores such information is lost or stolen it pose a threat to the total data. Another way could be same storage cloud provider providing the service for secured sharing, hashing, encryption/decryption, but since administrative can have use of both services for maintenance, the security service provided by the cloud storage provider, the information might be compromised. The aforementioned approches burdens the client by which makes it additionally accountable for securing it data before storing it to the cloud storage[13].

1.3 Problem Description

Cloud computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public auditablity for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy. In this work, we utilize and uniquely combine the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. For data uploading and accessing we use the proxy key which temporary instance key for the user for current task. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient[8].

1.4 Objectives

Our objective is to build a security service which will be provided with a trusted 3rdparty, and would lead to providing only security services and wouldn't store any data in its system. Detailing it further[14].

1. To construct Web service system which would provide data integrity verification, provide encryption/decryption of the consumer data.
2. Defining access list for sharing data securely with specific band of individuals.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

3. To construct thin client application which would call this web service before uploading/downloading the data to and from cloud.

II. PROPOSED SYSTEM

In this paper, the TPA will be fully automated and will be able to properly monitor confidentiality and integrity of the data and uniquely integrate it with random mask technique to achieve a privacy-preserving public auditing system for cloud data storage security while keeping all above requirements in mind. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient. There are many challenges in Cloud Computing, if not well resolved, may impede its fast growth. In this work the challenges of the existing techniques are addressed by using some techniques of Key-policy RSA encryption (KP) and Proxy re-encryption. KP is proposed to resolve the problem of data access control in one-to-many communications, while proxy re-encryption is a technique which is mainly used to protect the data from its disclosure in the cloud storage server. This technique is based on the **Polynomial Reduction Algorithm**. This technique helps the cloud servers to provide the requested data to the client without knowing the underlying content. Our Framework used facilitates ease of use, reduces development efforts and supports improved security and communication features platform remoting allows objects to interact with each other across application domains. The proposed cloud architecture are

DATA OWNER:
An entity, which has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation, can be either individual consumers or organizations[19].

CLOUD STORAGE SERVER (CSS):
An entity, which is managed by Cloud Service Provider (CSP) .It, has significant storage space and computation resource to maintain client's data.

EFFECTIVE THIRD PARTY AUDITOR (ETPA):
A TPA is an entity which maintains records for clients and data owner. Records include login, file access and logout information.

PROXY:
An entity, which is authorized to process the Original Client's data and upload them, is selected and authorized by Original Client. When Proxy satisfies the warrant m_ω which is signed and issued by Original Client, it can process and upload the original client's data; otherwise, it cannot perform the procedure.

KGC (Key Generation Center):
An entity, when receiving an identity, it generates the private key which corresponds to the received identity.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

2.1 Proposed System Block diagram

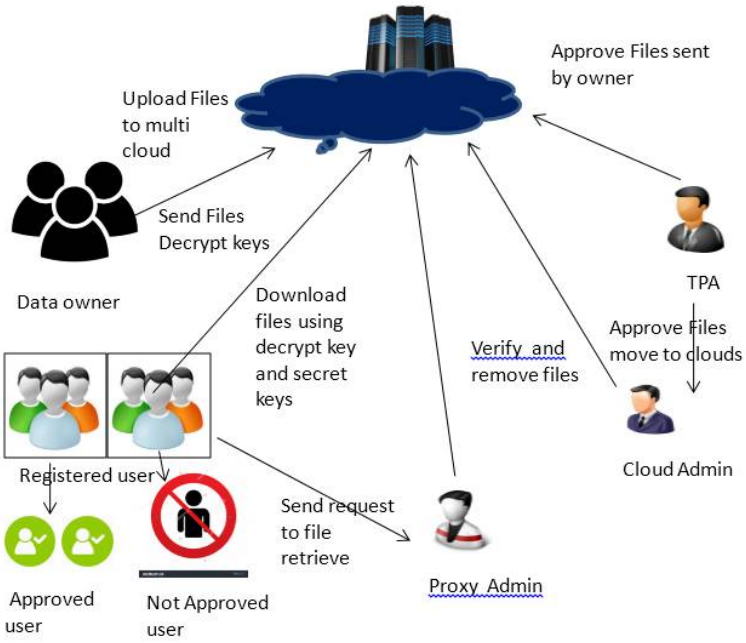

Figure 2.1 Overall Block Diagram after Secret key Generation

Data Owner:
Person who has bulk amount of data files to be loaded in the cloud. Before storing the data into cloud user should be registered. Assigns the responsibility and authority to TPA. While storing the cloud file data is encrypted by AES-256 bit algorithm is used.

Third Party Auditor
TPA is allowed to inspect the correctness of the stored data on request without reclaiming a copy of the stored data and make the data owners always free from online burden. For integrity checking SHA-1 algorithm is used. After integrity check the results are sent to data owner and proxy. 5.3 Cloud Service Provider It is equipped with sufficiently great storage space which provides data storage service and numerous resources for computation.

Proxy
It is semi-trusted and follows up in the interest of the information proprietor to recover authenticators and information hinders on the fizzled servers during the repair technique.

Cloud Storage Server (CSS)
An entity, which is managed by Cloud Service Provider (CSP) .It, has significant storage space and computation resource to maintain client's data.

Key Generation Center (KGC)
An entity, when receiving an identity, it generates the private key which correspondsto the received identity. **Polynomial Reduction Algorithm.(Key Generation Algorithm)**

Cloud admin
Cloud admin verifies and approves the files of data owners. It also checks the status of every file and keeps monitoring the users. When a threat is possessed by an user, it is alarmed and it has the ability to block that particular user, who possess threat to the stored data.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

Users

Users register themselves to the data owner and acquire credentials with their accessibility rights. Each user's activity is monitored by session ID (V-B) and a log information about their credentials are maintained. An user who tries to violate the protocols are notified to the cloud admin along with their system details.

We focus on the respectability check issue in regenerating code-based distributed storage; in particular with the utilitarian recover methodology. To completely guarantee the information uprightness and recovery the clients calculation assets and also online weight, we propose an open evaluating plan for recovering code-based distributed capacity, in which the respectability examining and recovery of fizzled information pieces and authenticators are actualized by an outsider inspector and a semi-trusted intermediary independently for the information proprietor. Rather than specifically adjusting the current open reviewing plan to the multi-server setting, we outline a novel authenticator, which is more suitable for recovering codes. Also, we "encode" the coefficients to secure information protection against the reviewer, which is more insignificant than applying the evidence blind strategy and information blind technique. We outline a novel homomorphic authenticator in light of BLS mark, which can be produced by two or three mystery keys and confirmed freely.

2.2 Proposed Architecture:

Large systems are always decomposed into subsystems that provide some related set of services. The initial design process of identifying these sub-systems and establishing a framework for sub-system control and communication is called Architecture design and the output of this design process is a description of the software architecture. The architectural design process is concerned with establishing a basic structural framework for a system. It involves identifying the major components of the system and communications between these components. The system architecture shows the blocks required for the paper. Figure 3 shows the existing system architecture.

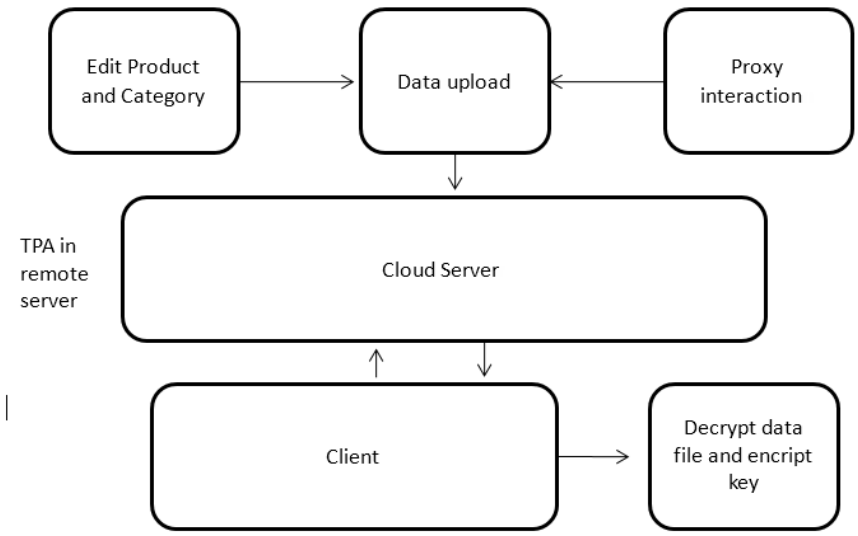

Figure 2.2 Cloud Computing System Architecture

The data owner is the one who encrypts the document (text, image and word document) that he wants to upload on the cloud server. After which he performs the AES encryption to encrypt the plain document, proxy reencryption and attribute based encryption to provide unique access structure to each client. Then he categorizes the data into different categories by linking different proxy key generated using the proxy reencryption technique. The data owner is the one who has the priority of editing and also deleting the contents stored on the cloud server. Then he performs the attribute based encryption to provide unique access structure to each client. After all these steps the data

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

owner uploads the encrypted file, re-encryption key and access structure on to the cloud server. Only authorized client can log in using his private key. After successful he gets a unique access structure that has been assigned by the data owner. Clients request the cloud server for the re-encryption key and files that he wants to download. Finally client decrypts the reencryption key and then decrypts the encrypted file using this key.

SYSTEM IMPLEMENTATION

A. ESTABLISHING CLIENT AND TPA

An entity, which has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation, can be either individual consumers or organizations. TPA which has expertise and capabilities that clients do not have, is trusted to assess and expose risk of cloud storage services on behalf of the clients upon request

B. ALGORITHM FOR OVERALL IMPLEMENTATION:

Step 1: Initially the cloud server is started.
Step 2: User register its authentication via TPA.
Step 3: Get the proxy key by polynomial reduction algorithm from PKG.
Step 4: Then the data owner login using the data upload interface.
Step 5: He encrypts the data.
Step 6: Perform PRE (Proxy Re-Encryption), using client's public key.
Step 7: Further he performs KP (Key Policy).
Step 8: He then generates different categories using the proxy key generated during the PRE, Upload the data.
Step 9: Authorized clients who are authenticated by the data owner login using their private key.
Step 10: Each client gets access structure of separate files based on access policy defined by the data owner to that particular client.
Step 11: Download required files.

2.3 Algorithm of Proposed System

Polynomial Reduction Algorithm

Step 1. authui (y,z)=αfi(u,y,z) // authentication polynomial of cluster Ci for u.
Step 2. verfu j (x,z)=βfj(x,u,z) // For each cluster j(j = i), the designer computes the check polynomial verfu j (x,z) with a probability P, and stores these check polynomials in node u.
Step 3. KCi = FC(KC|CHi) // the cluster key of cluster Ci stored in u1 is
Step 4. CHi −→ u :(CHi|u|cji) // Cluster-head CHi sends the local ID assignment message to every nodes u in its cluster,
Step 5. u −→ CHi :(u|cji) // After receiving the message, node u stores the local ID and sends the following response message.
Step 6. z = H((E)KCi) // For example, node u first computes the report z by applying the hash function to the encrypted measurement, which has been encrypted by the key KCi.
Step 7. MAP = authui (y,z)=αfi(u,y,H((E)KCi)) // H(·) is the hash function stored in node u and KCi is the cluster key for the cluster, to which u belongs. Then node u generates MAP for the measurement.
Step 8. r =((E)KCi|u|cji|MAP) // generating the sensing report r, every sensing node sends the report to the cluster-head CHi. The report r is.
Step 9. R =((E)KCi|Ci|u1|···|uT|cj1 i |···|cjTi |authu1 i (y,H((E)KCi))|···|authuTi (y,H((E)KCi))|Time) // After receiving all sensing reports generated by the sensing nodes, the cluster-head randomly chooses T reports v from them and merges these T measurement reports to an integrated measurement report R and sends it to the controller. The measurement report R is formed by
Step 10. A^{um},vi = authumi (v,H(E)KCi)= αfi(um,v,H(E)KCi)) // the intermediate node first calculates the values of Aum,vi and Vv,^{um}i with the value of z calculated by
Step 11. $V^{v,um}_{i}$ = verfvi (um,z)=βfi(um,v,z) = βfi(um,v,H(E)KCi)).

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

III. RESULT AND ANALYSIS

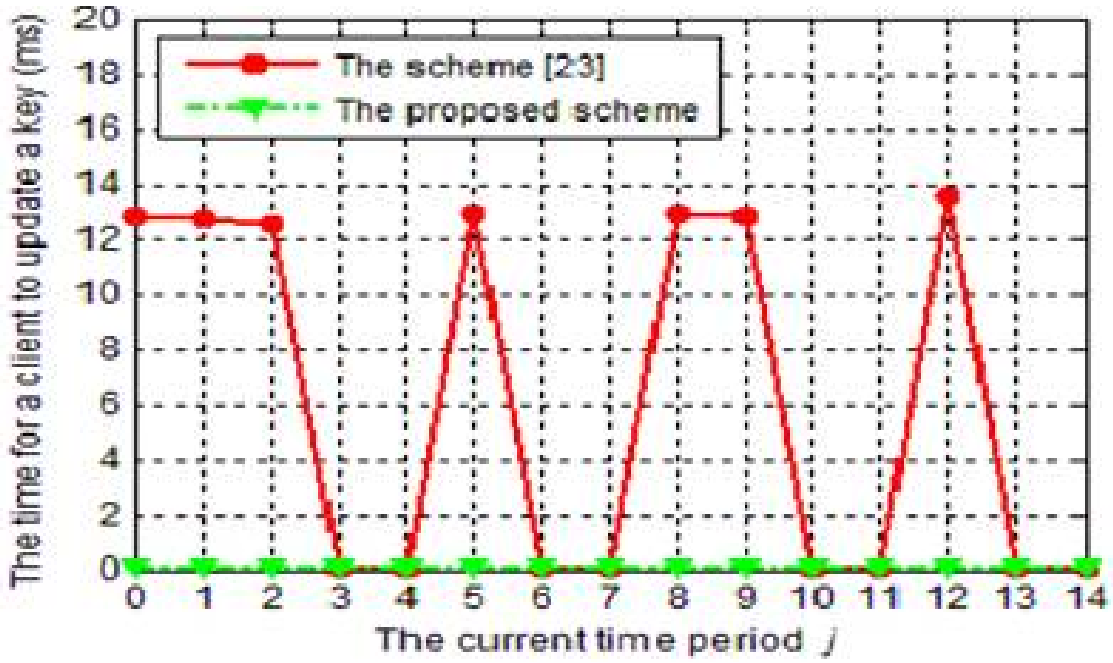

Fig. 3. The key update time on client side in the proposed scheme and thescheme [23]

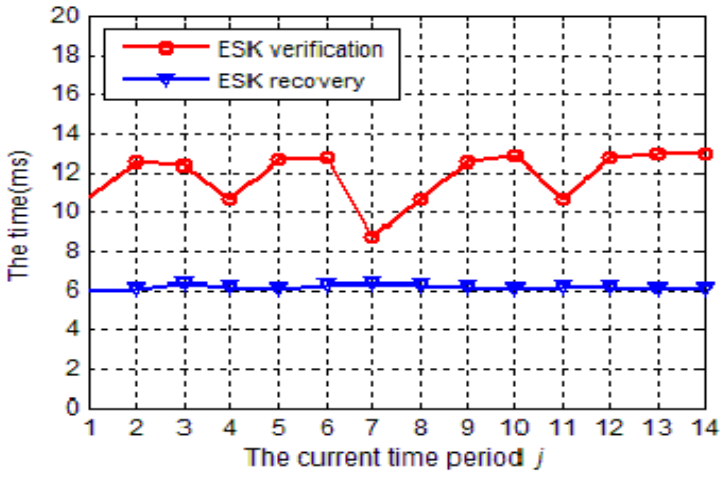

Fig. 4. The time to verify and recover an encrypted secret key (ESK) in different time periods

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

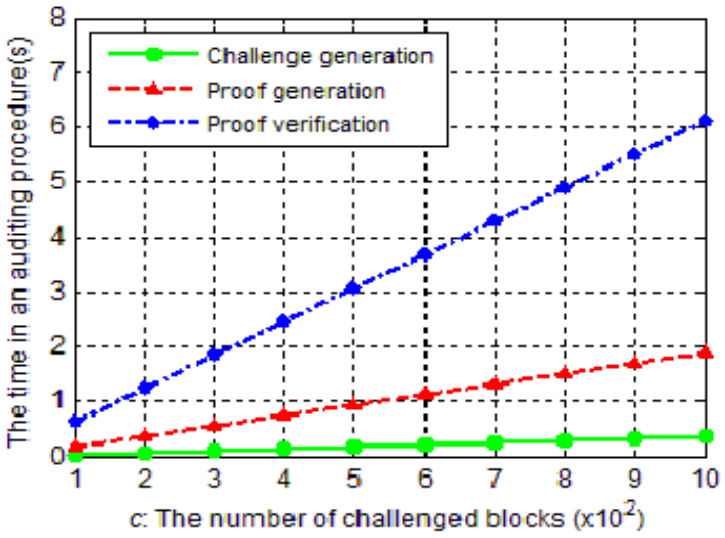

Fig. 5. The time of auditing procedures with different number of checked Blocks.

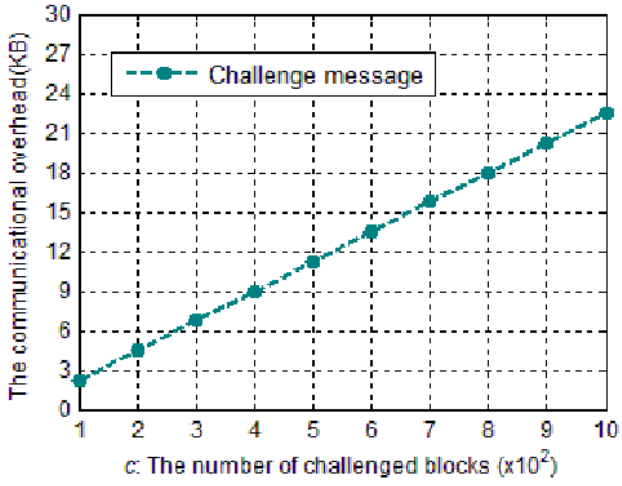

Fig 6.a

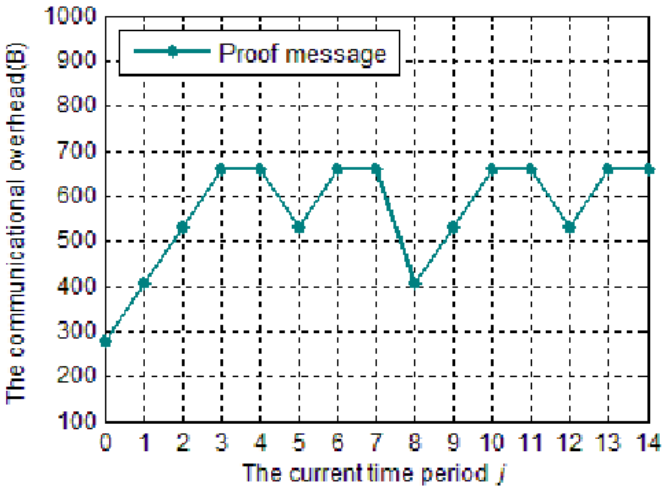

Fig 6.b

Performance Analysis We evaluate the performance of the proposed scheme through several experiments that are implemented with the help of the Pairing-Based Cryptography (PBC) library [31]. We carry out these experiments on a Linux server with Intel processor running at 2.70 GHz and 4 GB memory. The elliptic curve picked to realize bilinear mapping is a super singular curve with fast pairing operation, and the order of the curve group has 160 bits. In this case, the size of an element in Z∗ q is 20 bytes, and the size of an element in G1 is 128 bytes. The data file in our experiments is 20 M comprising 1,000,000 blocks. For simplification, we set the total time period T = 14 which means we can use a full binary tree with depth 2 to associate with these time periods. All experimental results are taken as the mean values from multiple executions. In the proposed scheme, the key update workload is outsourced to the TPA. In contrast, the client has to update the secret key by itself in each time period in scheme [17]. We compare the key update

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

time on client side between the both schemes in Fig. 3. In scheme [17], the key update time on the client is related to the depth of the node corresponding to the current time period in binary tree. When the depth of node corresponding to the current time period is 0 or 1 (the node is internal node), the update time is about 12.6ms; when it is 2 (the node is leaf node), the update time is almost zero. In our scheme, the key update time on client side is zero in all time periods. When the client wants to upload new files to the cloud, it needs to verify the validity of the encrypted secret key from the TPA and recover the real secret key. We show the time for these two processes happened in different time periods in Fig. 4. In practice, these processes do not happen in most of time periods. They only happen in the time periods when the client needs to upload new files to the cloud. Furthermore, the work for verifying the correctness of the encrypted secret key can fully be done by the cloud if we use the method in the end of Section 3. We demonstrate the time of the challenge generation process, the proof generation process, and the proof verification Fig. 4. The time to verify and recover an encrypted secret key (ESK) in different time periods Fig. 5. The time of auditing procedures with different number of checked blocks process with different number of checked data blocks in Fig. 5. In our evaluation, the number of checked block varies from 100 to 1,000. All the time of these processes increase linearly with the number of checked blocks. The challenge generation process spends the least time, which is 0.35s at most; the proof generation process spends more time, varyingfrom0.19s to 1.89s; the proof verification process spends the most time varying from 0.62s to 6.12s. In our scheme, the communicational messages comprise the challenge message and the proof message. From Fig. 6 (a), we can see that the challenge message is linear with the number of checked blocks. The size of challenge message is 2.25 KB when the checked blocks are 100, and increases to 22.5 KB when the checked blocks are 1,000. As analyzed in [18], when the number of checked blocks is 460, the TPA can detect the data abnormity in the cloud with a probability at least 99%. In this case, the challenge message would be 10.318 KB. From Fig. 6 (b), we can see that the size of proof message varies with the depths of nodes corresponding to time periods. In period 0, the proof message is the shortest, which is 276.5 bytes, since the depth of the corresponding node is 0. And the longest proof messages appear at the leaves of the tree, which is 0.66 **KB.**

IV. CONCLUSION

We have seen how delegation of responsibility trusted 3rd party which provides security services secures user data. It reliefs the client from maintaining any kind of key information and allowing the client for using any browser enabled device to access the cloud services. It allows the client to verify the integrity of the data stored on download or retrieval of its own stored data in cloud. The client can share the data securely with specific band of people with minimized overhead of key distribution.

FUTURE WORK

1. To enhance the security more, a mechanism to secure the keys in security cloud can be an area of research.
2. Simply change our environment towards Hadoop(big data), which inbuilt the concept of Cloud Computing.
3. It will reduce the overhead of network traffic can be another area of research.

REFERENCES

1. Huaqun Wang, Debiao He, Shaohua Tang, “Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity Checking in Public Cloud”, 1556-6013 (c) 2015 IEEE.
2. Jia Yu, Kui Ren, Senior Member, IEEE, and Cong Wang, Member, IEEE, “Enabling Cloud Storage Auditing with Verifiable Outsourcing of Key Updates”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. , NO. , 2015
3. Jing-Jang Hwang, Hung-Kai Chuang,Yi-Chang Hsu, Chien-Hsing Wu, “A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service,” Proceedings of the 2011 International Conference on Information Science and Application, April 2011.
4. Qian Wang ,Cong Wang ,Kui Ren ,Wenjing Lou ,Jin Li, “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 5, MAY 2011.
5. Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr. Atanu Rakshit, “Cloud Security Issues”, IEEE International Conference on Services Computing, pp. 517 520, September 2009.
6. Peter Mell, Timothy Grance, “The NIST Definition of Cloud Computing”, NIST Special Publication 800-145
7. Ling Li, Lin Xu, Jing Li, Changchun Zhang, “Study on the Third-party Audit in Cloud Storage Service”, 2011 International Conference on Cloud and Service Computing

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

8. L. M. Vaquero,L. Rodero-Merino,J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition", ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50-55, January 2009.
9. A. Parakh and S. Kak, "Online data storage using implicit security", Information Sciences, vol. 179, issue 19, pp. 3323-3333 ,September 2009.
10. C. Weinhardt, A. Anandasivam, B. Blau, N. Borissov, T. Meinl, W.Michalk, and J. Stober, "Cloud computing ? a classification, business models, and research directions", Business & Information Systems Engineering (BISE), vol. 1, no. 5, pp. 391-399, 2009.
11. L. Lamport, "Password authentication with insecure communication", Communications of the ACM, vol. 24, no. 11, pp. 770-772, 1981.
12. "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", Federal In formation Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST). November 26, 2001. Retrieved October 2, 2012.
13. William Stallings, "Cryptography and Network Security", 2009.
14. Salesforce.com, Inc., "Force.com platform", Retrieved Dec. 2009, from
15. http://www.salesforce.com/tw/.
16. http://www.cs.utsa.edu/ wagner/laws/AESintro.html
17. J. Yu, K. Ren, C. Wang, V. Varadharajan, "Enabling Cloud Storage Auditing with Key-Exposure Resistance," IEEE Transactions on Information Forensics and Security. vol. 10, no. 6, pp. 1167-1179, Jun. 2015.
18. 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, pp. 598-609, 2007.
19. Kamlesh Kumar Pathak and Manik Chandra Pandey, "International Journal of Engineering Research ISSN: 2348-4039 & Management Technology", ISSN: 2348-4039, May-2015 Volume 2, Issue-3