International journal of Master of Engineering Research and Technology | Vol-2, Issue-5, 2015
ISSN (ONLINE) 2394-6172

Privacy Preserving Efficient Multiple TPA Verification Protocol for Secure Cloud Storage

Rahul Mahajan
M.Tech. Scholar, Computer Science
Patel Institute of Engineering and Science
Bhopal, India
rahulmahajansa@gmail.com

Deepak Rathore
Assistant Professor CSE Dept
Patel College of Science and Technology
Bhopal, India
rathore.rath@gmail.com

Abstract: **Cloud computing is an evolving area in the field of computer science, day by day the systems becoming compact and efficient same way the computation is also changing rapidly, users don't want to keep the earlier days bulky systems with them and hence they are looking for the system which provide them solution for outsourcing their data for portability and convenience so that their outsourced data can be accessible to them at any geographical location in the world as well as their data must available to all devices. For achieving solution for this problem there is only option is cloud computing environment. In this system the user has to upload data on cloud storage space which is provided by the cloud server providers such as Google, azure etc. the users can delete the local copy of their outsourced data and save their local computational and storage resources. The data can be access anytime and anywhere by using internet. The system is advantageous for this era of technology but there is a challenge of providing security, privacy and integrity to user's private data. The Privacy preserving public auditing schemes are used to overcome these problems by providing third party auditors, who are in the business of auditing and who are expertise in the field of auditing. But this system is not full proof because the user's data may be revealed to TPA and may harm to user's data privacy, so for overcoming this problem we have provided a solution which is base on multiple third party auditors. That is An Efficient Multiple TPA Verification Protocol EMTVP. We show that our proposed architecture possesses these properties based on the privacy–preserving system. We have also showed that the dynamic auditing and efficient verification has reduced the security threats and is highly secured than the previous methodologies. In addition, we have presented the arbitrarily selecting TPA from multiple TPAs to protect the privacy of user's data and efficient auditing task.**

Keywords: **cloud computing; Privacy preserving; public auditing; data dynamics; batch auditing; Multiple TPA.**

I. INTRODUCTION

Cloud computing is an emerging technology in the computer world where the computing is enthused to a group of computers [13]. It becomes popular word in the market. The core concept of cloud computing is, simply, that there is large collection of computational devices which reside at some location the cloud of computers that is group of computers and we have to get access from them and use them as when needed. With innovations of personal computer the autocracy of centralized computing systems was ended. There was a somewhat easiness in using personal computers. But the system was replaced with the centralized server architecture. All the computational tasks are performed on servers and the clients enjoy the service provided by server. This approach of server architecture grows Internet in the world. Cloud computing is similar appearance as that of old era centralized computational system with dumb terminals but this time the server is easily accessible over the internet anywhere from the world.

Cloud computing is the most important concept for every small, medium or large scale industry. As many cloud users wants the services of cloud computing, but there is concern of security of users personal information which will be uploaded on the server. Data management, data privacy and security are concerns for every cloud user, and the cloud provider too [6], [7], [18]. With more and more companies looking into cloud computing, understanding cloud data security issues is important. Cloud computing is network based architecture which uses computational architecture.

Biggest challenge in adoption of cloud technology is data security and privacy. Cloud computing provides cloud storage as a service which stores and manages data for their customers. There is a risk when trusting cloud provider to store important data/files with third party. There are many other issues as in case if user want to change cloud provider, situation when cloud provider close their business and other issues we face while using different services in cloud [14].

We focus on privacy issue here. As companies start using the cloud servers and resources for their business development, the leaders in this cloud based business focuses on improving the privacy and security to the cloud users. The security should be provided for the data of companies that to be stored on the cloud as well as the efficient ways to store the data efficiently and also protect the resources that are to be granted for particular cloud user. The appropriate care should be taken for granting the access rights to the authorized users so that misuse should be avoided [2]. Privacy is the level of confidentiality provided to user in a system. Privacy not only guarantees the fundamental confidentiality of company important secured data, but also makes sure the different levels of data privacy [15]. Intentionally making the companies private data public or misusing the network access rights the privacy can be violated. The threat of data privacy is more in the cloud than traditional technology, because the more number of interactions over the network the risk and challenges are associated with it. This is because of the functional or operational properties of the cloud storage environment. For privacy preservation we need to have strong system which will prohibit unauthorized users from gaining access to sensitive data. Due to large number of

incidents of information leakage and identity theft it generated awareness about data security and privacy breaches and their impacts on business [13]. Data loss can have devastating impact on a business or individual. It will not only make damage to reputation and brand of a well known company but also can make significant impact on the customers trust, employees of company and partners.

II. PROBLEM STATEMENT

1. The System Model

The system model consists of four different things for provided that more competent and confidentiality preserving model: the CSP, the data user, the data owner, and the TPA. The data owner uploads the encrypted blocks of file M to n different cloud servers represented as storage servers. If the data owner needs maintain the data content concealed, the file M can be first encrypted prior to encoding. The data file is then converted into the metadata akin to verification tags for providing veracity test ability. Subsequent to that the data user picks any cloud server for retrieving the data file from the number of data sources. The TPA regularly verifies the integrity of the data file kept on the cloud server [7]. Network architecture for secure cloud data storage can be shown in Figure 1.1. The important three objects can be identified as follows:

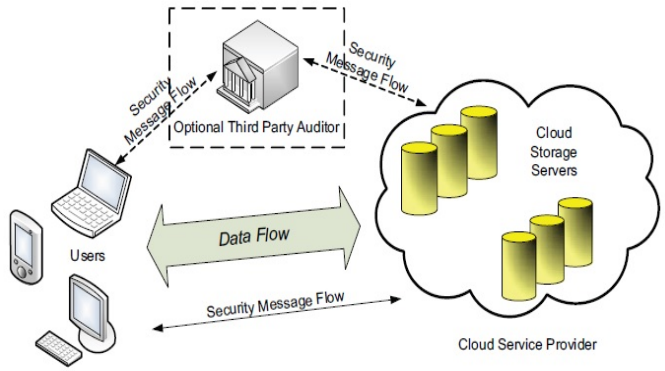

Figure 1: Architecture of Cloud Computing Environment with TPA.

- **Clients**

The Clients are those who have data to be stored and interact with the Cloud Service provider (CSP) to manage their data on the cloud. They are typically: computers, laptops, mobile phones. After, storing the data in cloud, the Client should take care of their stored data in cloud, which means, they can frequently verify the security of their data without having a local copy of the data. In case Clients do not have the time to verify the security of their data in cloud, they can assign this job to trusted Third party Auditor (TPA).

- **Cloud Service Provider (CSP)**

Cloud Service Provider (CSP) are those who have major resources and expertise in building, managing distributed cloud storage servers and offers storage or software services to customers via the Internet. The CSP is responsible for data maintenance. The CSP also responds to Verifier queries honestly.

- **Third Parity Auditors (TPA)**

The TPA [5], [6], who has expertise and capabilities that Clients may not have, is trusted and monitoring the risk of cloud data storage services on behalf of Clients. The auditor is free, therefore has no inducement for support (or collude with) the service provider or Client in conveying culpability. To permit contract intercession, the storage facility as well as Client is required to mutually faith on the auditor in conveying fault. It is the fact that auditor, having its identity in and position in the commerce of auditing, is extra trustworthy than Clients and, therefore, be able to keep a minute quantity of audit results for the long term. Finally, Client data and results gained as of it encompass exterior worth; consequently the auditor has an excitement to become skilled at about its contents [17].

2. Design Goals

Towards offering protected as well as consistent cloud data storage space services, Design must at the same time accomplish performance assurance all through data recovery as well as repair.

To make sure the safety as well as reliability meant for cloud data storage beneath the abovementioned adversary based technique, we intend to propose proficient method for dynamic data authentication as well as process and get the subsequent goals [9]:

- **Storage accuracy**

For make sure users so as to their data are to be sure stored correctly also kept integral over the time in the cloud.

- **Prompt localization of data inaccuracy**

For efficiently establish the improper server when data corruption has been identified.

- **Dynamic ways for supporting data access**

To preserve the similar stage of storage accuracy guarantees still if users vary, delete or add its data files in the cloud.

- **Reliability**

To improve data accessibility beside complex crash, malevolent data alteration as well as server conspiring threats, i.e. reducing the consequence conveyed with data faults or else server crash.

- **Lightweight**

For allowing users for perform storage accuracy verification with minimum overhead.

- **Accessibility and Dependability**

With admittance a few k-permutation with n storage servers, the data user might effectively get back encoded data also recuperate the entire unique data. The data recovery provision remnants purposeful as equal to $n - k$ storage servers be polluted within one round as well as polluted servers can be renovate from other vigorous servers.

- **Protection**

The intended storage provision defends the data privacy as well as at regular intervals makes convinced the truthfulness of data in cloud servers for avoids data failure or altered form.

- **Offline Data possessor**

Data owners can go offline immediately after data outsourcing, which means they are not required to be involved in tasks such as data integrity check and repair at a later stage.

- **Privacy-Protecting**

For avoiding the cloud server from getting knowledge of data stored extra information as of the dataset as well as the catalogue, with to convene privacy needs.

3. Security Concerns in Cloud

Each coin have two side, and cloud computing is no exclusion. There is disapproval concerning confidentiality in cloud scheme, since the reality is that administrator has admittance to data stored on the cloud. They can accidentally or purposely get the client data. Traditional security or protection techniques need reconsideration for cloud. Apart from for confidential cloud where association do not have be in charge of the resources, the development of cloud is appears slight deliberate, since businesses believe as an alternative of conciliations on the safety of the data, they are ready to spend in buying private resources for setup their individual infrastructure. Security matters that worry to the client can be classified into sensitive data access, data segregation, bug exploitation, recovery, accountability, malicious insiders, and account control issues. Like different disease have different medicines, different cloud security issues have different solutions, like cryptography, use of more than one cloud provider, strong provision stage accord among client and CSP. Profound venture is essential to protect the conciliation data in cloud. The business can be developed only if the trust is built in the minds of clients which will be possible only if safety concerns are being solved. Following are some of the concerns [18].

1) System Complexity

Compared to traditional data centre the cloud architecture is much more complex. Therefore while considering protection of all these resources and data also the dealings of these resources with each other requirements.

2) Shared Multi-tenant Environment

Since the cloud needs to provide service to millions of client, a rational parting of data is made at different level of the application stack. Because of which attacker in the face of client able to utilize the bugs getting hold of admittance to data from other institutes.

3) Internet-based Services

As the cloud services are offered online through internet there is a concern of quality of services over the network.

4) Failure of control

We know that data is spread over World Wide Web so it is difficult to have control over the physical and logical resources over cloud and alternative control to client's assets, mismanagement of assets are some additional concerns.

III. EXISTING SCHEME

1. Notations and preliminaries

Notations: In this thesis, N denotes the set of natural numbers {1, 2 ...} and ℤ denotes the set of integers {... , -2,-1,0,1,2,.....}. ℤp denotes the set {0 ... p-1} and ℤp* the set of integers smaller than p. That is,

$$ℤp^* = \{n | 1 \le n \le p \text{ and } gcd(n,p) = 1\}.$$

The notation [1, k] denotes the set {1, ..., k}.

Functions and Algorithms

Let $f: X_1 \rightarrow X_2$ are the function f with input X_1 and output X_2. Let A denotes an algorithm. Let A(.) to denote that A has several inputs. $Y \leftarrow A(x)$ denotes that y is the output of algorithm A on input x. Following is the introduction of important crypto graphical background for proposing scheme.

Bilinear Maps

The necessary facts about bilinear maps and groups are briefly reviewed, in the notations: Bilinear chart or map can be explained as, let's consider G1, G2, along with GT exists as a multiplicative cyclic clusters of primary order of p. Now consider **g1** as well as **g2** exist as generators or producers for G1 and G2 correspondingly. The bilinear chart is a chart such that there exists **e:** G1×G2 —> GT used for each **u** ϵ G1, **v** ϵ G2 along with **a, b** ϵ $ℤ_p$, $\mathbf{e(u^a,v^b) = e(u,v)^{ab}}$. The above bilinearity entails for whichever **u1,u2** ϵ G1, **v** ϵ G2, $\mathbf{e(u_1 . u_2, v) = e(u_1, v) . e(u_2, v)}$. Definitely there exists capably quantifiable algorithm for calculating e in addition to the chart should be non inconsequential, i.e., e is non degenerate: $e(g_1,g_2) \neq 1$ [9].

2. Privacy-Preserving Public Auditing for Cloud Data Security

Existing approach for this is a privacy-preserving public audit scheme [9], [11] for cloud data security in cloud computing. By using this approach homomorphic linear authenticator with random masking technique as in [4] is used to make sure that the TPA [1] would not get any knowledge about the data stored on the cloud server during the cloud data auditing process. It reduces the users' dilemma about expensive auditing process and outsourced data leakage.

Properties of Protocol

This approach accomplishes the public auditability [18]. In this method they don't make use of the undisclosed key they employ the public –private key pairs for maintaining the audits so that user is liberated from the worry of maintaining the authentication of its outsourced data. This method guaranteed the confidentiality of data contents of user throughout the auditing task by using the arbitrary masking γ to hide μ, a linear arrangement of the data blocks. This have to be prominent that the importance R in this protocol, which is necessary for maintaining privacy-preserving, will not affect the equation, because of the circular relationship between R and γ in γ = h(R) and the verification equation. The size of (σ, μ, R) is autonomous of the number of sampled blocks c. If the server is omitted a small part of the data, then the number of blocks that requests to be checked in order to detect server acting up with high chance is in the order of Þ. In fastidious, if t part of data is dirtied, then arbitrary sampling c blocks would achieve the

recognition probability P = 1-(1-t) ^{c}. Here, every block is preferred homogeneously at arbitrary. When t = 1% of the data F, the TPA only requests to audit for c = 300 or 460 arbitrarily chosen blocks of F to detect this misbehaviour with prospect well-built than 95 and 99 percent, respectively. Given the enormous volume of data outsourced in the cloud, checking a portion of the data file is more affordable and practical for both the TPA and the cloud server than checking all the data, as long as the sampling strategies provides high-probability guarantee. We will present the experimentation result based on these sampling strategy. For some cloud storage providers, it is possible that definite information dispersal algorithms (IDA) may be used to portion and physically dispense the user's outsourced data for increased accessibility.

TPA		Cloud Server
1. Retrieve file tag t, verify its signature, and quit if fail;		
2. Generate a random challenge $chal = \{(i, \nu_i)\}_{i \in I}$;	$\xrightarrow{\{(i,\nu_i)\}_{i\in I}}$ challenge request $chal$	3. Compute $\mu' = \sum_{i \in I} \nu_i m_i$, and $\sigma = \prod_{i \in I} \sigma_i^{\nu_i}$;
		4. Randomly pick $r \leftarrow \mathbb{Z}_p$, and $R = e(u, v)^r$ and $\gamma = h(R)$;
	$\xleftarrow{\{\mu,\sigma,R\}}$ storage correctness proof	5. Compute $\mu = r + \gamma\mu' \mod p$;
6. Compute $\gamma = h(R)$, and then verify $\{\mu, \sigma, R\}$ via Equation 1.		

Table 1: Privacy Preserving Public Auditing.

IV. PROPOSED METHODOLOGY AND ARCHITECTURE

1. Overview

The architecture of cloud computing environment has the security audit by third party auditor. For ensuring the data reliability and protecting the users computational resources the third party auditor are most important because they have hands on practice in the field of data integrity scrutiny and validating, hence it is necessary for cloud user to assign the auditing task to TPA and be relax. The TPA will audit the user's data periodically or as per the requirement of the user. furthermore, it will assist users to assess the threat of their pledged cloud data services, the audit end results from Trusted third party auditor are also be advantageous for the CSP for getting better their business by maintaining its reputation in the world of cloud based business. In a world, allowing public auditing schemes will engage in recreation a vital role for this promising cloud market to turn out to be completely well-known; where users will require traditions to consider threat in addition to put on confidence in the cloud.

2. Proposed Architecture

The network representative architecture for data storage in cloud systems used in existing systems, it consists of three entities: Client, Cloud Service Provider (CSP) and Third Party Auditor Array (TPA_1, $TPA_{2, ---,}$ TPA_n). In propose model, we are using the same storage architecture with TPA along with some significant modification in the existing system to ensure more reliable and efficient system.

MTPA is an array of independent TPAs who are in the business of auditing for users by using multiple TPA we are distributing the auditing task between multiple independent TPAs so that we achieve simultaneous auditing for multiple users multiple data blocks at a time. By using such model we enable more promising system for user's data privacy preservation than that of preceding algorithms [8].

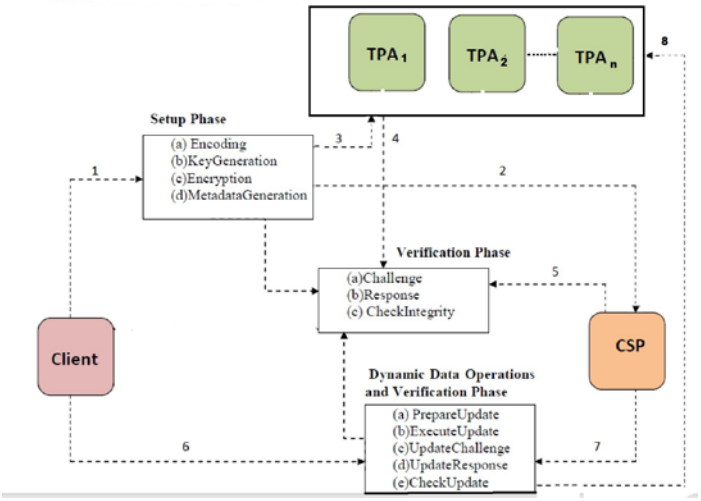

Figure 2: Architecture of EMTVP for Secure Cloud Storage.

1) Clients

The Clients are those who have data to be stored and interact with the Cloud Service Provider (CSP) to manage their data on the cloud. They are typically: computers, laptops, mobile phones. After, storing the data in cloud, the Client should take care of their stored data in cloud, which means, they can frequently verify the security of their data with not encompassing a local reproduction of the data. In case Clients do not have the time to verify the security of their data in cloud, they can assign this job to trusted Multiple Third party Auditor (MTPA).

2) Cloud Service Provider (CSP)

Cloud Service Provider (CSP) are those who have major resources and expertise in building, managing distributed cloud storage servers and offers storage or software services to customers via the Internet. The CSP is responsible for data maintenance. The CSP also responds to the number of various queries submitted for integrity, confidentiality and consistency checks honestly.

3) Multiple Third Parity Auditors (MTPA)

Here there is major change in our scheme instead of using single TPA we are using multiple TPA and distribute the data blocks randomly among TPAs so that each TPA only possess some random block of data from random cloud user and cannot retrieve the original data file F at all, the TPA, who has knowledge as well as potential that Clients may not have, is trusted and monitoring the risk of cloud data storage services on behalf of Clients. The auditor seems to be self-regulating, hence does not has motivation to support (or collude with) the

service provider or Client in conveying responsibility. We suppose that auditor is more reliable than Clients and, therefore, be able to preserve some of audit results for the long term[5].

3. An Efficient Multiple TPA Verification Protocol Algorithm

Algorithm for proposed scheme is as follows

1. The Client pre-processes the file and sends metadata to the MTPA or keeps locally for later Integrity verification and sends the file to the CSP.
2. The CSP stores the file.
3. The MTPA stores the Metadata blocks randomly to any TPA from multiple TPA array.
4. The verifier (Client/MTPA) generates a challenge and sends to the CSP and checks the validity of response, if it is valid returns 1 otherwise return 0.
5. The CSP generates a response and sends to the verifier.
6. The Client generates an update request and sends to the CSP and verifies the whether the CSP has updated the data successfully or not? If yes it sends updated metadata to the MTPA or resends challenge to the CSP.
7. The CSP updates data and generates an update response based on Client requests.
8. The MTPA stores the updated metadata in c0ase of modification or insertion.

Our auditing scheme has four algorithms which are (Key Gen, Sig Gen, Gen Proof, and Verify Proof) [10].

To generate the key which is required for encryption Key Gen algorithm is used. This generation algorithm is executed by the customer for setup the system. User has to use SigGen for the purpose of generation of verification metadata. This verification metadata may include digital signatures. Cloud server runs the GenProof for generating a proof for data storage accuracy; TPA executes the VerifyProof for the purpose to verify the proof. The detailed descriptions of these algorithms in these three phases are described in the following sections.

3.1 Setup Phase

By running the KeyGen algorithm the client starts the scheme and initialize public and secret factors of the system, user selects an arbitrary signing key duo (spk, ssk), an arbitrary component $x \leftarrow \zeta_p$, an arbitrary $u \leftarrow G1$ as well as calculates $v \leftarrow g^x$. The secret factor is sK =(x,ssK). For generating authentication metadata the user uses the SigGen by using data file F. After that the user stores the data file F as well as the authentication metadata on cloud server, and erases its local replica. In the pre-processing the user is able to modify, expansion the data file F or together with added metadata to be stored at server [23].

For ensuring the Confidentiality, Availability and Integrity of the file, the Client pre-processes the file before storing it in the cloud in setup phase. The setup phase consists of four methods as shown:

a) Encoding

To achieve the guarantee of the Availability of data stored in the cloud, the Client encodes the file blocks (b1, b2... bn).

b) Key Generation

In this algorithm, the Client generates private and public key pair for the later processing of the file blocks in the propose system.

c) Encryption

In case, the Client wants to ensure the data Confidentiality, the Clients encrypts the data file blocks using public key cryptography. [13].

d) Metadata Generation

To verify the reliability of data stored on the cloud, the Client computes the metadata for each block of file.

3.2 Verification Phase (Audit Phase)

The MTPA member TPA sends an audit challenge to the CS to ensure that the CS has maintained the data file block (b_i) intact, which is arbitrarily assigned to it. The CS has to issue a reply message with running the Gen Proof by means of block (b_i) and its verification metadata as inputs. The MTPA then verifies the response via Verify Proof.

The verification phase consists of three methods as shown in Figure 3:

a) Challenge

In order to authenticate the truthfulness of data block which is randomly assigned to the member of TPAs array, the auditor member (MTPA) first creates a random challenge and sends it to the CSP.

b) Response

Upon receiving a challenge request from the verifier (MTPA), the CSP generates response as Integrity proof corresponds to the challenge and sends back to the verifier.

c) Check Integrity

After receiving a response from the CSP the verifier checks if the update proof is valid or not by comparing response with previously computed metadata. To hold the Integrity [16], the response must be equal with the metadata otherwise it indicates data has corrupted.

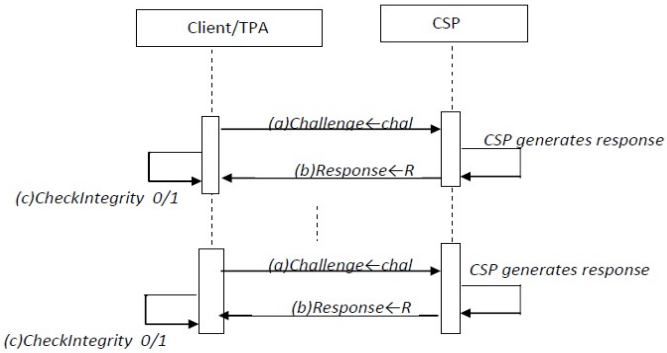

Figure 3: Verification Phase.

Our framework assumes that the MTPA is stateless. Due to the independent TPA members in the MTPA they does not have complete block and they does not know which users data block is assigned to them and as the data blocks of one file are distributed among the TPAs, no TPA has the complete data file of user. Due to this the cloud user's identity is protected as well as file blocks identity is also protected from the TPA [4].

Parameter	Existing System		Proposed EMTVP	
Number of blocks	220	140	220	140
Server computation time (ms)	118.14	93.4	115.28	91.5
TPA computation time (ms)	290.6	158.3	270.35	138.95
Communication cost (bytes)	120	120	110	110

Table 2: Performance comparison for different number of sampled blocks between existing system and proposed EMTVP.

Table 2 gives the experiment result for performance of our scheme over the existing scheme [11]. It can observed that our scheme as more efficient as of existing scheme and also our scheme gives privacy guarantee as we have different multiple TPA that audits the only blocks assigned to them.

4. Dynamic Data Operations and Verification Phase

One of the core design principles of cloud data storage is to give dynamic functionality of the data for different practical applications. One obvious solution to support all dynamic data operations is for the Client to download the entire data from the CSP and update it. This would be secure but highly inefficient.

1. Prepare Update

Suppose the Client wants to update the data in the cloud, the Client runs Prepare Update algorithm to create an update request and sends to the CSP. The update request specifies the particular data operation (modification, insert, delete) which has to perform.

2. Execute Update

Upon receiving an update request from the Client, the CSP runs the Execute Update algorithm to update the data in the cloud.

3. Update Challenge

The update operations may also introduce additional threats to the auditing system. So, in order to verify whether CSP has performed the update operation successfully, the Client immediately challenges the CSP for the proof of update operation.

4. Update Response

Upon receiving an update challenge, the CSP generates a proof for update operation and return to the Client.

5. Check Update

After receiving an update response from the CSP, the Client runs the Check Update algorithm to check the security of update operation by comparing response with pre-computed metadata for new updated block.

V. Implementation Details and Result

For getting the system results we have to follow the existing systems details like privacy preserving public auditing using third party auditor here the only change in our system is we are using multiple TPA for auditing task instead of single TPA based system.

As shown in the figure 5 the individual auditing has higher auditing time overhead as compared to batch auditing.

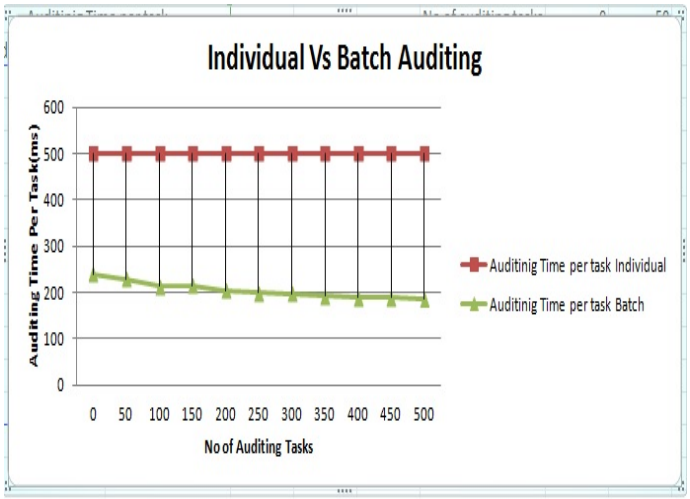

Figure 4: Comparison of Individual Vs Batch Auditing.

Experiment by choosing various numbers of blocks as input parameters gives the result which proves that the result generated from the proposed scheme is producing slightly better results than that of existing system with higher security guarantee over the privacy and integrity of cloud user's private data which is stored on the cloud server as shown in figure 6.

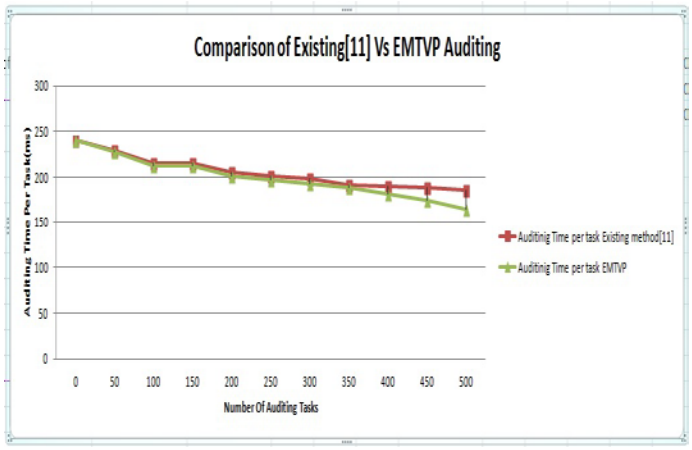

Figure 5: Comparison of auditing time between existing method and EMTVP Auditing.

VI. CONCLUSION

In this paper, we have provided a solution which is base on multiple third party auditors. That is An Efficient Multiple TPA Verification Protocol (EMTVP). We prove that by using multiple TPA we can split the user's data blocks and arbitrarily assign blocks to TPAs so that the TPA cannot identify and relate the information in the data blocks.

Our system can be followed in cloud computing environment to change the traditional approach of TPA for cloud storage environment. More prominently, we proposed a new audit approach which is based on Efficient Multiple TPA Verification Protocol, This protocol is same as that of privacy preserving public auditing protocol with enhanced security and efficiency due to random distribution of data blocks in multiple TPA. This approach greatly reduces the risk of revealing the user's data privacy by TPA, while still achieves the privacy protection and higher security. Our experiments clearly showed that our approach is more promising in terms of privacy protection than that of previous approach.

VII. FUTURE WORK

In future Efficient Multiple TPA Verification Protocol approach can be further enhanced by adding more flexibility in arbitration process of file data blocks assignment to number of TPAs from the set of members from MTPA pool. By adding this efficient arbitration the performance can be enhanced as well as improved the integrity of our system.

VIII. REFERENCES

[1] Giuseppe Ateniese, Randal Burns, Reza Curtmola, Joseph Herring, Lea Kissner, Zachary Peterson, Dawn Song, "Provable Data Possession at Untrusted Stores", 14th ACM Conference on Computer and Communications Security pp1-11, (CCS 2007).

[2] Ari Juels , Burton S. Kaliski, "Pors: proofs of retrievability for large files", In CCS '07: Proceedings of the 14th ACM conference on Computer and communications security, Pp 584—597,2007.

[3] Hovav Shacham, Brent Waters, "Compact Proofs of Retriavability", ASIACRYPT: 90-107, 2008.

[4] Jachak K. B., Korde S. K., Ghorpade P. P. and Gagare G. J. ,"Homomorphic Authentication with Random Masking Technique Ensuring Privacy & Security in Cloud Computing", Bioinfo Security Informatics, vol. 2, no. 2, ISSN. 2249-9423, pp. 49-52, 12 April 2012.

[5] Chandinee Saraswathy K. , Keerthi D. , Padma G., "HLA Based Third Party Auditing For Secure Cloud Storage", Chandinee Saraswathy K. et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) pp 1-7,, 2014.

[6] Chandinee Saraswathy K. , Keerthi D. , Padma G, "HLA Based Third Party Auditing For Secure Cloud Storage" International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1526-1532.

[7] Abhishek Mohta ,Ravi Kant Sahu,Lalit Kumar Awasthi, " Robust Data Security for Cloud while using Third Party Auditor", International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 2, , pp 1015-1028, February 2012.

[8] Sadia Marium, Qamar Nazir, Aftab Ahmed, Saira Ahthasham Mirza Aamir Mehmood, "Implementation of EAP with RSA for Enhancing The Security of Cloud Computing" ,International Journal of Basic and Applied Sciences, 1 (3) pp 177-183, (2012).

[9] K.Kiran Kumar, K.Padmaja, P.Radha Krishna, "Automatic Protocol Blocker for Privacy-Preserving Public Auditing in Cloud Computing" ,International Journal of Computer Sci ence And Technology IJCST Vol. 3, Issue 1, Spl. 5, pp 936-940, Jan. - Mar 2012.

[10] Jachak K. B., Korde S. K., Ghorpade P. P. and Gagare G. J. ,"Homomorphic Authentication with Random Masking Technique Ensuring Privacy & Security in Cloud Computing", Bioinfo Security Informatics, vol. 2, no. 2, ISSN. 2249-9423, pp. 49-52, 12 April 2012.

[11] Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, and Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 2, pp 362-375,FEBRUARY 2013.

[12] Y. Zhu, H. Hu, G.-J. Ahn, and S. S. Yau, "Efficient audit service outsourcing for data integrity in clouds," In Journal of Systems and Software, vol. 85, no. 5, pp. 1083-1095, May 2012.

[13] 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.

[14] Wang Shao-hu, Chen Dan-we, Wang Zhi-weiP, Chang Su-qin, "Public auditing for ensuring cloud data storage security with zero knowledge Privacy" College of Computer, Nanjing University of Posts and Telecommunications, China, 2009.

[15] H. Tianfield, "Security issues in cloud computing", IEEE International Conference on Systems, Man, and Cybernetics, October 2012, pp- 1082-1089, 2009.

[16] D. Attas, and O.Batrafi, "Efficient integrity checking technique for securing client data in cloud computing", International journal of electrical & computer science, pp. 43-48, 2011.

[17] J. J. Wang, and S. Mu, "Security issues and countermeasures in cloud computing", in IEEE International Conference on Grey Systems and Intelligent Services, September 2011, pp.843-846. 2010.

[18] Cong Wang, Qian Wang, Kui Ren,Wenjing Lou, “Privacy Preserving Public Auditing for Data Storage Security in Cloud Computing ” IEEE, 2010.

[19] Y. Jadeja, and K. Modi, “Cloud computing-concepts, architecture and challenges” in IEEE International Conference on Computing,Electronics and Electrical Technologies, March 2012, pp. 877-880.

[20] Ling Li, Lin Xu, Jing Li, Changchun Zhang,"Study on the Third-party Audit in Cloud Storage Service", International Conference on Cloud and Service Computing,pp 1-13,2011.