ISSN (e): 2250 – 3005 || Volume, 06 || Issue, 09|| September – 2016 ||
International Journal of Computational Engineering Research (IJCER)

An Auditing Protocol for Protected Data Storage in Cloud Computing

Anush Sharma[1], Er.Munish Katoch[2]
[1]Student M.Tech(CSE), Sri Sai University Palampur(H.P.)
[2]Astt.Prof.(CSE), Sri Sai University Palampur(H.P.)

ABSTRACT
Cloud computing is a mechanism which provides us resources, information as per user requirement by the help of internet. Cloud is used to store important content material for a longer period of time which requires trust and safety of content that is stored in cloud. The main issue of cloud computing is security of data. Many techniques proposed earlier were beneficial for static archived data. Some encryption techniques were introduced later for dynamic data which includes masking technique, bilinear property with dynamic auditing. This paper proposed an effective auditing protocol to maintain the dynamic operations on data with RSA, MD5 and ID3 algorithms for enhancing data safety. The analysis and simulation results are effectual and protected as it incurs least communication cost and least computation cost of the auditor.

Keywords: *Batch auditing, cloud computing, communication cost, computation cost, dynamic auditing, ID3, MD5, RSA.*

I. INTRODUCTION

Cloud computing is the utilization of computing resources (hardware and software) that are pooled as services over the internet. Cloud storage is an essential facility of cloud computing [1], which allows data owners (owners) to shift information from their confined computing systems to the cloud. Cloud computing is being determined by a lot of which includes Google, Amazon and Yahoo also some traditional vendors including IBM, Intel and Microsoft [2]. Once data goes into cloud, the customer drops the control over the data. This lack of control raises new fearsome and difficult issues related to privacy and reliability of data placed in cloud [3]. Sometimes, cloud service providers may be fraudulent. They may remove the data that have not been used for a longer period of time to save the storage space and state that the data is still perfectly stored in the cloud [1].

1.1 Clouds are of three types, depending on their ease of access: Public Cloud, Private Cloud and Hybrid Cloud:

A public Cloud is made accessible in a pay-as-you-go method to the common public users. A private Cloud's usage is limited to members, workers, and trustworthy partners of the association. A hybrid Cloud uses both private and public Cloud in a flawless way. Examples of public cloud are Amazon, Microsoft and Google. Examples of private cloud are particular organisation like financial, trade etc and example of hybrid cloud is processing of big data.

1.2 There are three types of cloud providers: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) as follows:

1. Software as a Service -A SaaS backer gives subscribers admission to both resources and applications. SaaS makes it disposable for you to attempt a spry echo of software to instal on your furnishings. SaaS other than makes it easier to strive the selfsame software on wide of your devices at in advance by accessing it on the cloud. In a SaaS pact, you try the slightest administrate over the cloud.

2. Platform as a Service - A PaaS organization goes a counterpoise exposed to the Software as a Service setup. A PaaS benefactress gives subscribers entr to the happy ramble they entreat to affect and operate applications over the internet [4].

3. Infrastructure as a Service - An IaaS agrees, as the delegate states, deals at bottom with computational infrastructure. In an IaaS be consistent, the proponent totally outsources the storage and sure, such as armaments and software that they need.

II. RELATED WORK

In [2] proposed an obstruction which is based on Elliptic Curve Cryptography (ECC) and Sobol Sequence. It permits auditor to attest the facts eccentric stored at CSP without retrieving original data but ECC increases the block of the quiet bulletin much alongside than RSA encryption. Annexe, the ECC algorithm is yon hectic and back exhausting to administrate than RSA, which increases the contingency of realization errors, thereby reducing the security of the algorithm.
In [4] improved RSA cryptography with bilinear property of computational bilinear Diffie Hellman to guarantee the data privacy is projected. Diffie-Hellman is a fundamental succession algorithm and allows yoke parties to choose, forsake an disoriented communications incline, a garden closely guarded underlying digress only the two parties know, even without having universal anything beforehand. The shared underlying is an asymmetric central, but, manner about asymmetric essential systems; it is openly hinder and impractical for bulk encryption.
In [10] introduced a secure and efficient dynamic auditing procedure by means of File segmentation and allocation, Tag generation, and Random Challenge and verification algorithms. File segmentation technology cannot magically solve all downloading problems. Forth are rigorous sticks on the influence of the technology. In contrive of users deviate has inferior upload-bandwidth, wide demand higher than supply. Jointed downloading tushy setting aside how unequivocally well conduct point peaks, and it duff as well, to varied scope, let up loaders utilize their connection safely. Aside from a appropriate to the sufficient amidst of data tags, their auditing scheme can bring a deep storage slide on the server.
In [1] bilinear pairing-based cryptography shall lose its competitive advantages although it looks very beautiful.

III. PROPOSED WORK

We plan an evaluating structure for distributed storage frameworks and propose a protection safeguarding and effective capacity inspecting protocol. Our examining convention guarantees the information security by utilizing RSA, Md5 and Id3. Our reviewing convention acquires less correspondence cost between the evaluator and the server. It likewise lessens the registering heaps of the examiner by moving it to the server. We extend our re-examine principle to strengthen the information dynamic procedure, which is effective and provably secure in the irregular prophet model. We further extend our inspecting convention to bolster clump examining for numerous mists as well as various proprietors. Our multicloud group reviewing does not require any extra trusted coordinator. The multiowner cluster evaluating can significantly enhance the inspecting execution, particularly in extensive scale distributed storage frameworks. The security of RSA depends on the computational trouble of figuring substantial whole numbers. As registering force increments and more effective figuring calculations are found, the capacity to consider bigger and bigger numbers additionally increments. Encryption quality is straightforwardly fixing to key size, and multiplying key length conveys an exponential increment in quality, in spite of the fact that it impairs execution. MD5 (message digest calculation) create a "exclusive identify notion". Mostly, they describe a great deal of bits down to only a couple of bits (128 on account of MD5) in a manner that crashes are as uncommon as could reasonably be expected. This is helpful in light of the fact that you can analyze and store these little hashes a great deal more effortlessly than the whole unique groupings. In cryptography, one-way hashes are utilized to confirm something without essentially giving ceaselessly the first data. eg Unix stores hashes of passwords rather than the passwords themselves. at the point when a client enters their secret key, the framework processes the hash of it and analyzes it to the hashes recorded in/and so forth/passed. Since you can't run the hash capacity in converse, the framework realizes that the secret key you entered is the right one. The grave that UNIX utilizes doesn't generally diminish the size yet is a comparable thought. Hashes and processes like MD5 are an indispensable piece of digital signatures. ID3 calculation permits an abnormal state of security and performance. This methodology is essentially to plan unique reason secure multiparty calculations; subsequently protection will be ensured the length of the genuine gatherings frame an adequately substantial majority. Whereas, ID3 convention will guarantee that the whole information exchanges stays mystery with the exception of the data spilled from the choice tree yield by the convention. The execution of the tradition is redesigned broadly while meanwhile confining the information spillage from the decision tree.

IV. PRIVACY PRESERVING AUDITING PROTOCOL

In this area, we first present a few methods we connected in the outline of our effective and security protecting reviewing convention [1]. At that point, we depict the calculations and the definite development of our reviewing convention for distributed storage frameworks. We consider a reviewing framework for distributed storage as appeared in Figure 1, which includes data owners (proprietor), the cloud server, and the third party auditor (examiner). [2]The proprietors make the information and host their information in the cloud. The cloud server stores the proprietors' information and gives the information access to clients (information buyers). The auditor is a trusted third party that has skill and capacities to give information stockpiling evaluating administration to both the proprietors and servers. The auditor can be a trusted association oversaw by the legislature, which can give fair-minded evaluating result to both information proprietors and cloud servers [4].

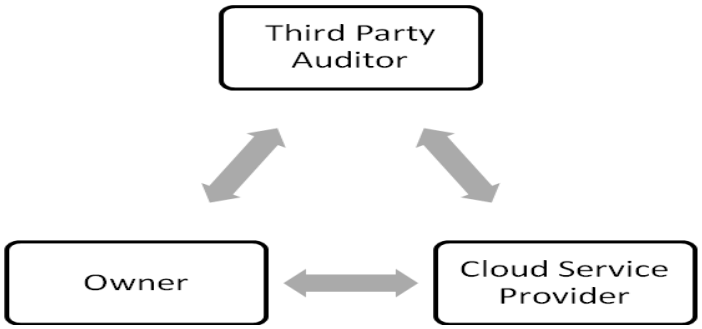

Figure1. Basic model of data storage auditing

Table1: Describes some notations listed below [1]:

Symbol	Meaning
Sk_t	Secret tag key
Pk_t	Public tag key
Sk_h	Secret hash key
M	Data component
T	Set of data tags
n	Number of blocks in every component
s	Number of sectors in each information block
M_{info}	theoretical detail of M
C	Challenge generated by auditor
P	Proof generated by server

4.1 A storage auditing protocol consists of the following five algorithms:

We acknowledge the reviewer is direct yet curious. It performs genuinely in the midst of the whole reviewing method, yet it is curious about the got data. In any case,[4][1] the different could be exploitative and might dispatch the going with attacks:

1) KeyGen (□)= (sk_h, sk_t, pk_t) [1]

This key time estimation [1] takes no data other than the comprehended security parameter λ. It outputs a secret hash key sk_h and a pair of secret-public tag key (sk_t, pk_t).

2) TagGen (M, sk_t, sk_h**) = T** [1]

The tag generation algorithm we insert the value of encrypted file *M*, the secret (private) tag key sk_t and the secret hash key sk_h.[4] For every data block m_i, it computes a data tag t_i based on sk_h and sk_t. It outputs a set of data tags $T = \{t_i\}_{i \in |1,n|}$ where $\mathbf{t_i = (\, h(sk_h, W_i) \,.\, \prod_{j=1}^{s} uj^{\,mij}\,)^{\,skt}}$

3) Chall (M_{info}**) = C** [1]

The challenge algorithm we put the only data of informationM_{info}. It returns a challenge

C = ({i,v}$_{i \square Q}$**,R) where R=(pk$_t$)^r i.e (r** □ **Z$^*_p$) , (v$_i$** □ **Z$^*_p$)** [4]

4) Prove (M, T, C) = PЄ

The verify algorithm takes as inputs the file *M*, the tags *T*, and the challenge *C* from the auditor. It outputs a proof P. where **C = ({i,v}$_{i \square Q}$,R)** .Now the tag proof TP and data proof DP are [4]

TP= $\prod_{i \in Q} t_i^{vi}$

For generating data proof let us first compute the linear combination of challenged data blocks [4] MP_j for j€ [1,s]

MP_j = $\sum_{i \in Q} v_i m_{ij}$ then it produces **DP =** $\prod_{j=1}^{s} e(u_j, R)^{MPj}$

It generates [2] the proof P = (TP, DP).

5) Verify (C, P, sk_t, pk_t, M_{info}**) = 0/1**

The verification algorithm [5]takes as inputs *P* from the server, the secret hash key sk_t, the public tag key pk_t, and the conceptual information of the data M_{info}.It computes identifier hash values h(sk_h,W_i) of challenged data blocks and calculates the challenge hash H_{chal} **as** $H_{chal} = \prod_{i \in Q} h(sk_h, W_i)^{rvi}$ .It verifies the proof by the equation **DP.e(H_{chal},pk_t) = e(TP,g_2^r).**It outputs the auditing result as *0 or 1*.

Figure 2 show frame of privacy maintaining auditing protocol [1][4]. It comprises of the following parts: owner initialization, confirmation auditing, and sampling auditing.

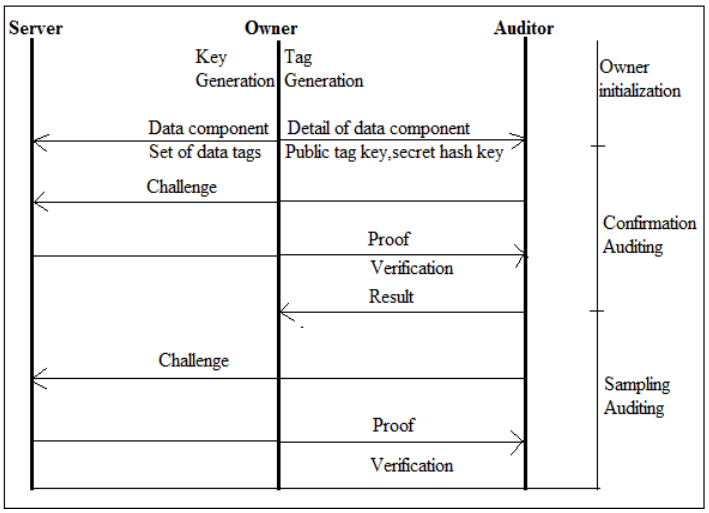

Figure2: Frame of privacy maintaining auditing protocol

Stage 1: Owner initialization: The proprietor runs the key era calculation KeyGen to get the key hash key and in this manner the pair of mystery open label key.

Stage 2: Confirmation auditing: In proposed examining development, the evaluating convention exclusively includes two-way correspondence: Challenge and Proof. Calculation the affirmation reviewing sporadically, the proprietor fancies the evaluator to see regardless of whether the proprietor's data unit legitimately hangs on the server.

Stage 3: Sampling auditing: The auditor will do the examining reviewing occasionally by troublesome an example set of information pieces. The recurrence of taking evaluating operation relies on upon the administration understanding between the information proprietor and in this manner the auditor (and moreover relies on upon the amount of trust the information proprietor has over the server). Much the same as the affirmation examining to a limited extent, the testing evaluating strategy likewise contains two-way correspondence. For sampling auditing with t challenged data blocks [1], the probability of detection can be generated as $Pr(t,s) = 1- (1 - p)^{t.s}$, it can detect any data corruption with a probability Pr(t,s). Let us assume a file F having m data components [1][2][3][4] as $F=(F_1,F_2,.....,F_n)$. Every data component can be restructured with dynamism through the data owners. For public data mechanism, the data owner does not encrypt it, but for private data component, the data owner encrypts it with its matching key. Each data component F_k is separated into n_k data blocks termed as$F_k=(m_{k1},m_{k2},...,m_{knk})$ .For the security motive, the data block size is limited by the security constraint. Taking example the security level is set 160 bit (20 Byte), the data block size as 20 Byte. A 50-KByte data component is partitioned into 2,500 data blocks and produces 2,500 data tags, which incurs 50-KByte storage overhead. By utilizing the data fragment technique, we promote split every data blocks into areas. The part size is confined by the security parameter. We produce one information tag for each information hinder

that comprises of (s) segments, such that less information labels are produced..For instance, if an information square (m_i) will be as often as possible read, then (s_i) could be expansive, yet for those every now and again redesigned information squares, (s_i) could be moderately little. For effortlessness, one and only information segment is considered in proposed development and consistent number of divisions for every information piece. Assume there is an information part (M), which is separated into (n) information squares, and every information piece is further split into (s) segments. For information obstructs that have distinctive number of divisions, the greatest number of parts among S_{max} all the segment numbers S_i is chosen first. Now, for every data block mi with sectors S_i , $S_i < S_{max}$,$m_{ij} <0$ for $S_i<j<=S_{max}$.Because the size of each sector is constant and equal to the security parameter p, the number of data blocks can be calculated as n =sizeof(M)/ s.logp. The encrypted data component is represented as M = $[m_{ij}]$, i Є[1,n], j Є[1,s] . Let G1,G2 and G_t be the multiplicative groups with the identical prime bid p and e G1 xG2 ~ G_t be the bilinear map. Let g1 and g2 be the generators of G1 and G2, respectively. Let h :{0, 1}*~G1 be a keyed secure hash function that maps the M_{info} to a point in G1.

V. PRIVACY PRESERVING DYNAMIC AUDITING PROTOCOL

To keep away the replay attack, [1] we present an index table (ITable) to record the dynamic data of the data [1]. The ITable comprises of four segments: Index, Bi, Vi, and Ti. The Index means the present block number of data block mi in the data segment M. Bi signifies the first block number of data block mi, and Vi means the present rendition number of data block mi. Ti is the time stamp utilized for creating the data tag. This ITable is made by the owner amid the owner initialization and oversaw by the auditor. At the point when the owner finishes the data dynamic operations, it sends a redesign message to the auditor for redesigning the ITable that is put away on the auditor. After the affirmation auditing, the auditor sends the outcome to the owner for the affirmation that the owner's data on the server and the deliberation data on the auditor are both avant-garde. This finishes the data dynamic operation. To manage the forge attack, we can alter the tag era calculation TagGen. In particular, while creating the data label ti for the data block mi, we embed all the conceptual data into the data tag by setting Wi = FID‖i‖Bi‖Vi‖Ti ,[4] such that the server can't get enough data to forge the data tag from element operations. The itemized verification will be given in the supplemental document, accessible online. The dynamic auditing protocol comprises of four stages that are owner initialization, confirmation auditing, sampling auditing, and dynamic auditing. The first three phases are similar to our privacy preserving auditing protocol as discussed in the above part. Only the tag generation algorithm (TagGen) and the ITable generation vary during the first stage. Figure 3, describes the dynamic auditing phase [1], which contains three steps: information update, index update, and update confirmation.

Step1: Information update- Information can be updated by applying modification, insertion, and deletion operations on the data. For every update operation there is a specified algorithm [4]. Each algorithm takes as inputs the new version of data block m_i^*, the secret tag key sk_t, and the secret hash key sk_h.
Modify $(m_i^*, sk_t, sk_h) \rightarrow (msg_{modify}, t_i^*)$
Insert $(m_i^*, sk_t, sk_h) \rightarrow (msg_{insert}, t_i^*)$
Delete $(m_i) \rightarrow (msg_{delete})$

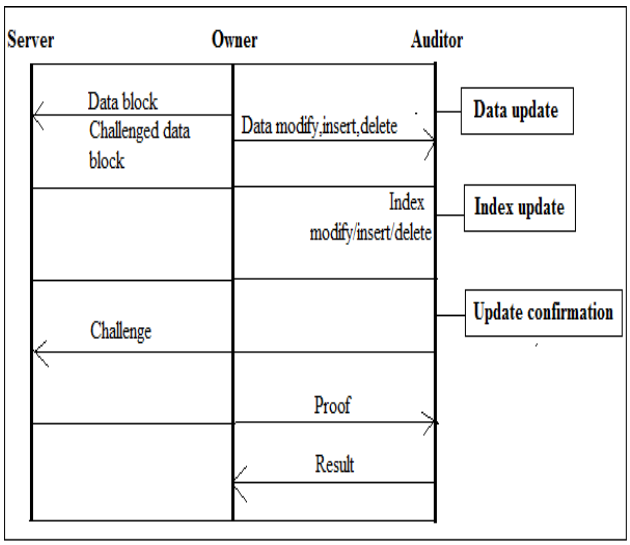

Figure3: Frame of privacy preserving dynamic auditing protocol

Step2: Index update-After obtaining the three parts of information update [4]. The following algorithms are applied to update the I Table, which takes the update message msg $_{modify}$ as input. It changes the number v_i by v_i^* and modifies t_i by t_i^* the new time stamp as
Imodify (msg_{modify})
Iinsert (msg_{insert})
Idelete (msg_{delete})

Step3: Update confirmation-Once the auditor updates the I Table, it directs an affirmation inspecting for the updated data and sends the outcome to the owner [4]. At that point, the owner will support to erase the local adaptation of data as per the update confirmation auditing result. Table 2 describes the index table of abstract information of data M [1] as follows:

Table 2: Index Table

Initial abstract information of M				After modifying m_2,V_2 and T_2 are updated				After inserting before m_2 all items before m_2 move backward with index increased by 1				After deleting m_2 all items after m_2 move forward with index decreased by 1			
Index	B_i	V_i	T_i	Index	B_i	V_i	T_i	Index	B_i	V_i	T_i	Index	B_i	V_i	T_i
1	1	1	T_1	1	1	1	T_1	1	1	1	T_1	1	1	1	T_1
2	2	1	T_2	2	2	2	T_2^*	2	n+1	1	T_{n+1}	2	2	1	T_2
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
n	n	1	T_n	n	n	1	T_n	n + 1	n	1	T_n	n - 1	n	1	T_n

VI. BATCH AUDITING FOR MULTIOWNER AND MULTICLOUD

Data storage evaluating is a critical administration in cloud registering that helps the owners check the data honesty on the cloud servers. As an aftereffect of the gigantic assortment of data owners, the auditor could get numerous reviewing demands from various owners. In this circumstance, it may enormously enhance the framework execution, if the auditor could consolidate these evaluating demands along and exclusively lead the batch examining for different owners in the meantime. As an aftereffect of parameters for creating the information labels utilized by each owner is very surprising, and along these lines, the auditor can't join the information labels from different house owners to direct the batch auditing. On the other hand, a few data owners could store their data on entirely one cloud servers. To affirm the owner's data honesty through and through the clouds, the auditor can send the examining difficulties to each cloud server that has the owner's data and check all the evidences from them. To cut back the calculation cost of the auditor; it's exceptionally interesting to combine of these reactions and do the batch verification.

6.1 Algorithm for Batch Auditing for Multi owner and Multi cloud

Give O a chance to be the arrangement of owners and S be the arrangement of cloud servers [1][2][3][4]. The batch examining for multi owner and multi cloud can be developed as takes after:

Stage1: Owner initialization. Every owner O_k(k Є O) runs the key era calculation KeyGen to create the pair of secret-public tag ($skt_{t,k}$,$pk_{t,k}$) and an arrangement of secret hash key$\{sk_{h,kl}\}_{l\epsilon s}$

Stage2: Batch auditing for multi owner and multi cloud. Let O_{chal} and S_{chal} signify the included arrangement of owners and cloud servers required in the batch reviewing, separately. The batch evaluating likewise comprises of three stages: batch challenge, batch proof, and batch verification.

VII. PERFORMANCE ANALYSIS

7.1 Communication cost

Storage auditing is an exceptionally troublesome administration as far as computational cost, correspondence expense, and memory space. In this segment, the communication price and calculation many-sided quality correlation between proposed conspire and existing works are portrayed. Since the communication cost amid the instatement is practically the same in these three auditing protocols, we as it were think about the communication cost between the reviewer and the server, which comprises of the challenge and the proof. Consider a batch auditing with K owners and C cloud servers. Assume the quantity of challenged data block from every proprietor on various cloud servers is the same, meant as t, and the data block are part into s

segments in our plan. We do the correlation under the same likelihood of location. Our plan and Kan Yang have the same aggregate communication cost amid the challenge stage. Amid the proof stage, the communication cost of the proof in our scheme is just direct to C. The result is described in figure 4.

7.2 Computation convolution

We recreate the calculation of the proprietor, the server, and the auditor on a Linux framework with an Intel Core Duo CPU at 3.16 GHz and 4.00-GB RAM. The code uses the RSA, Md5 and Id3 to simulate planned auditing format.

7.3 Computation cost of the auditor

The computation time of the auditor versus the quantity of data blocks, the quantity of clouds, and the quantity of owners are thought about as appeared in Figure 4. And Figure 4(a) demonstrates the computation time of the inspector versus the quantity of challenged data blocks in the single cloud and single owner case. In this figure, the quantity of data blocks goes to 500 (i.e., the challenged data size equivalents to 500 Kbyte), however it can delineate the direct relationship between the computation cost of the evaluator versus the challenged data size. From Figure 4, it is demonstrated that the proposed plan acquires less computation cost of the auditor. Figure 4(b) portrays the computation cost of the evaluator of the multi cloud batch auditing plan versus the quantity of challenged clouds. Figure 4(c) additionally shows that the batch auditing for numerous owners can extraordinarily lessen the computation cost. In spite of the fact that in proposed re-enactment the quantity of data owners goes to 500, it can outline the pattern of computation cost of the reviewer that proposed plan is considerably more effective. Figure 4 shows the Comparison of computation cost of the auditor (s = 50) as follows:

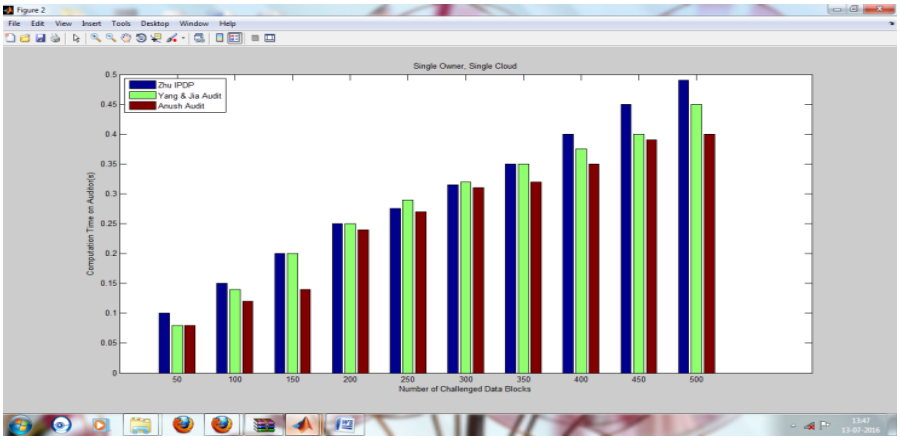

Figure 4(a). Single owner, Single cloud

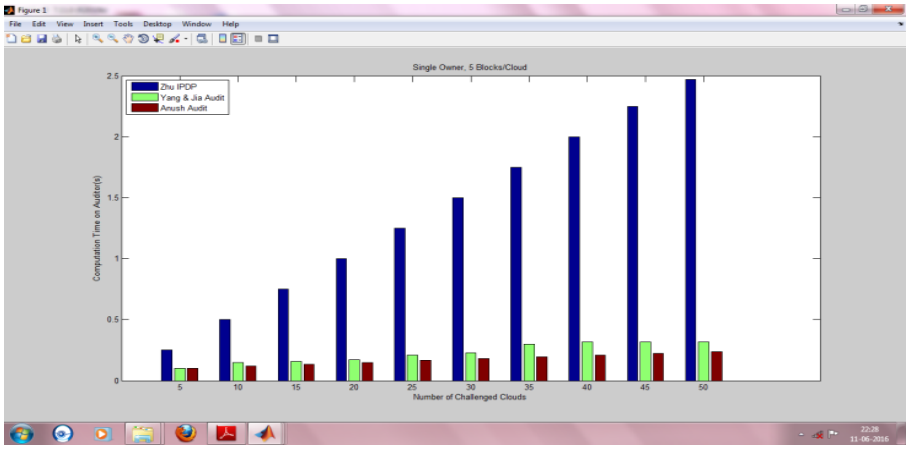

Figure 4(b). Single owner, 5 block/cloud

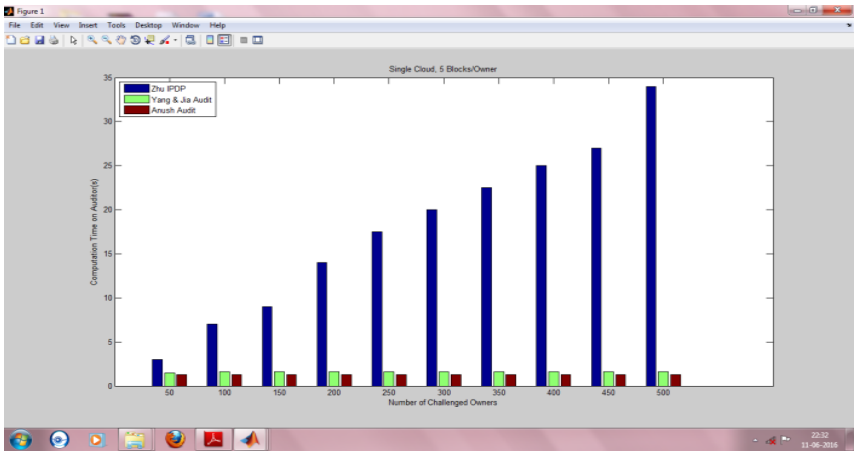

Figure 4(c). Single Cloud, 5Block/Owner

7.4 Computation cost of the server

The computation cost of the server versus the quantity of data blocks in Figure 5(a) and the quantity of data owners in Figure 5(b) are compared. The Proposed plan moves the processing heaps of the auditing from the auditor to the server, such that it can significantly diminish the computation cost of the auditor. Following are the graphical results that concluded:
Figure 5 shows the Comparison of computation cost on the server (s =50)

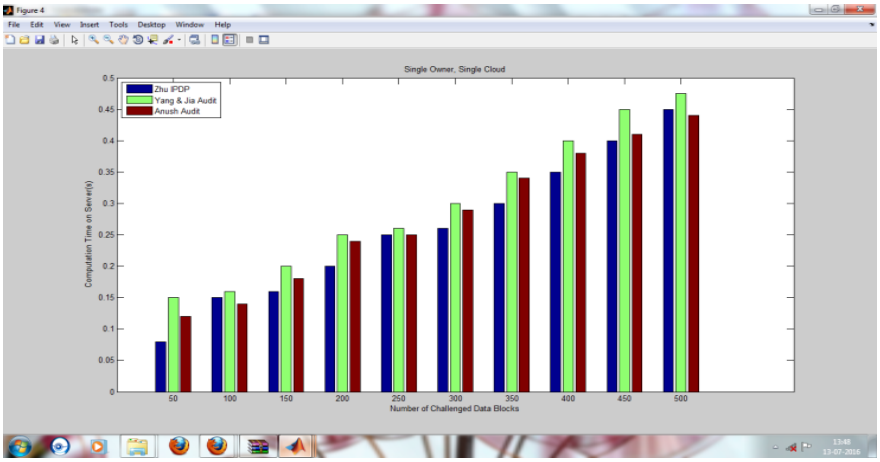

Figure 5(a). Single owner, single cloud

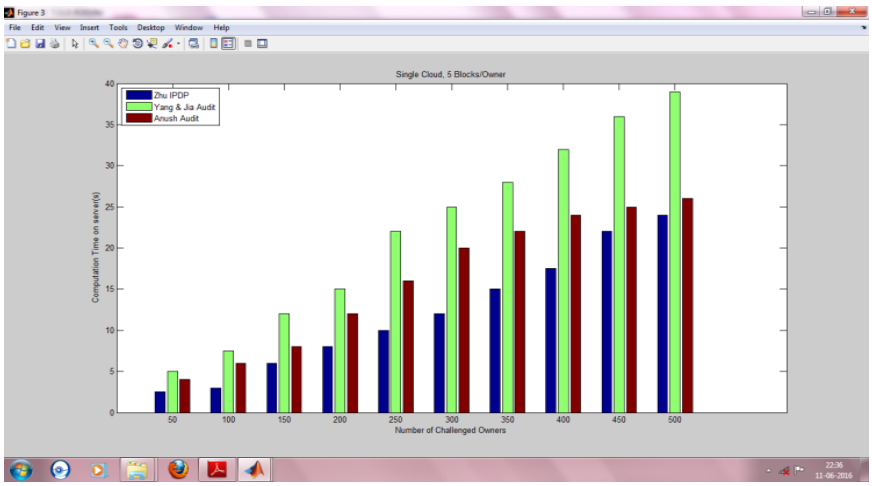

Figure 5(b). Single cloud, 5block/owner

VIII. CONCLUSION

In this paper we projected an efficient and essentially protected dynamic auditing protocol. It maintains the confidentiality of data by combining the cryptographic technique with RSA, Md5 and Id3 approach sooner than applying bilinearity property of bilinear pairing. It protects the data confidentiality next to the auditor and chains the batch auditing for several owners. Our auditing protocol fulfils all security and presentation needs of cloud data storage. In addition, proposed auditing theme incurs less communication cost and less computation cost of the auditor by moving the computing loads of auditing from the auditor to the server that significantly improves the auditing performance and can be functional for large-scale cloud storage scheme. Table 3 defines the comparison of auditing schemes used in [1] and proposed scheme as under:

Table3. Comparison of Auditing Schemes

Scheme	Privacy	Batch operation Multiowner/Multicloud	Approach	Feature
Yang [1]	Yes	Yes	Bilinearity property of bilinear pairing Challenge stamp	Long and Complicated
Our scheme	Yes	Yes	Rsa,Md5,Id3	Simplified approach

REFERENCES

[1]. Kan Yang and Xiaohua Jia.An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing.IEEE Transactions on Parallel and Distributed Systems.Volume-24.No.9, September 2013.

[2]. Priyanga R, Maheswari B and Karthik S. Efficient and Secure Dynamic Auditing Protocol for Integrity Verification in Cloud Storage.Proceedings of International Conference on Global Innovations In Computing Technology. Volume-2.Special Issue 1, March 2014.

[3]. Syam Kumar P, Subramanian R. An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computin. IJCSI International Journal of Computer Science Issues. Volume-8, Issue- 6.No 1.November 2011.

[4]. Dr. R Manickachezian and S Hemalatha. Dynamic Auditing Protocol using Improved RSA and CBDH for Cloud Data Storage International Journal of Advanced Research in Computer Science and Software Engineering, Volume-4, Issue-1, January 2014 ISSN: 2277 128X.

[5]. Prof. Umesh B Chavan and Lokesh P Chaudhari. Survey Paper on Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud. International Journal of Computer Science and Mobile Computing, Volume-1 Issue.1, January- 2014.

[6]. T Prasanthi, C Balasubramanian, S Kimsukha Selvi and K Kala. An Efficient Auditing Protocol for Secure Data Storage in Cloud Computing. Proceedings of the World Congress on Engineering 2014 Volume-1.

[7]. Rakhi Bhardwaj and Vikas Maral. Dynamic Data Storage Auditing Services in Cloud Computing. International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-4, April 2013.

[8]. Gaurav Raj and Munish Katoch. Security Implementation through PCRE Signature over Cloud Network Advanced Computing. An International Journal (ACIJ) Volume-3, No.3. 2012.

[9]. J Noorul Ameen, J Jamal Mohammed and Nilofer Begam. Dynamic Auditing Protocol for Efficient and Secure Data Storage in Cloud Computing. COMPUSOFT, An international journal of advanced computer technology, Volume-3, Issue-6.June-2014.

[10]. Md. Tajuddin and K China Busi. An Enhanced Dynamic Auditing Protocol in Cloud Computing. International Journal of Engineering Trends and Technology (IJETT) Volume-4 Issue-7. July 2013.

[11]. R K Ramesh and R Jegadeesan. N^{TH} Third Party Auditing For Data Integrity in Cloud. Asia Pacific Journal of Research Volume-1, Issue-13, January 2014 ISSN: 2320-5504, E-ISSN-2347-4793.