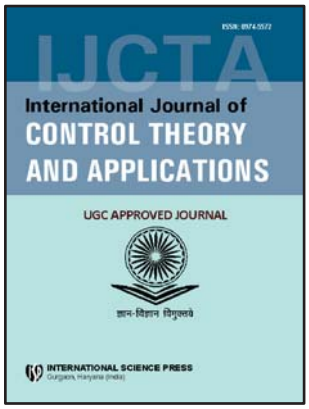

International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 31 • 2017

An Efficient Hard Logarithmic Based Dynamic Auditing Protocol for Secure Data Storage in Clouds

MeenuTahilyani[a] and Amit Dutta[b]

[a]*Department of Computer Science, SantHirdaram Girls College, Bhopal, India*

E-mail: meenu_mgh@yahoo.co.in

[b]*Deputy Director, AICTE, New Delhi, India*

E-mail: amitdutta07@gmail.com

Abstract: Here an effectualmethod is implemented for the dynamic possession of data at the data centers. The procedureapplied here starts with the creation of cloud and allots various users and statistics centers at the virtual machine to send their information in a protected manner. First of all the data from various users are set up and load is computed at each end of the record centers then setup and key generation takes place, a certain access policy is applied to each users of the cloud, hence when users needs to access Data he may fulfill the access policy applied over the cloud and lastly encryption and decryption of the information is done. The planned tactic applied here delivers less computational time for the numerous Dynamic Processes to achieve on Multiple Copies. The organization also proofs to be more protected since it resolves the problem of User Revocation and Escrow Problem. It also delivers less Computational time for Verification and Proof.

Keywords: *Cloud Service Provider, Cloud computing, Third Party Auditor, Elliptic Curve Cryptography, Hard Logarithmic, Access Policy.*

1. INTRODUCTION

Cloud computing is an evolving term that describes the transformation of many existing technologies and approaches to computing into something different. Cloud computing has establishedsubstantialconsideration from research communities in academia andtrade; on the other hand there are various challenges facing cloud computing to be widely deployed and used.

The major challenge is security, which is related toinfrastructureanddata. Cloud computing splits application and information resources from the basic infrastructure, and the methods used to deliver them [1]. However, the datum that data proprietors no longer physically enjoy their delicateinformationpromotions new contests to the tasks of information confidentiality and integrity in cloud computing systems. Unauthorized access and misuse of customers' confidential data are seriousconcerns regarding data outsourcing; hence, it is of significant importance to be awareof data administrators (CSPs) and become wider of data access right. The cloud data storage model in cloud computing consists of three entities namely Clients, Cloud Service Provider (CSP) and Third Party Auditor (TPA) as illustrated in Figure. 2: as the following activities[17].

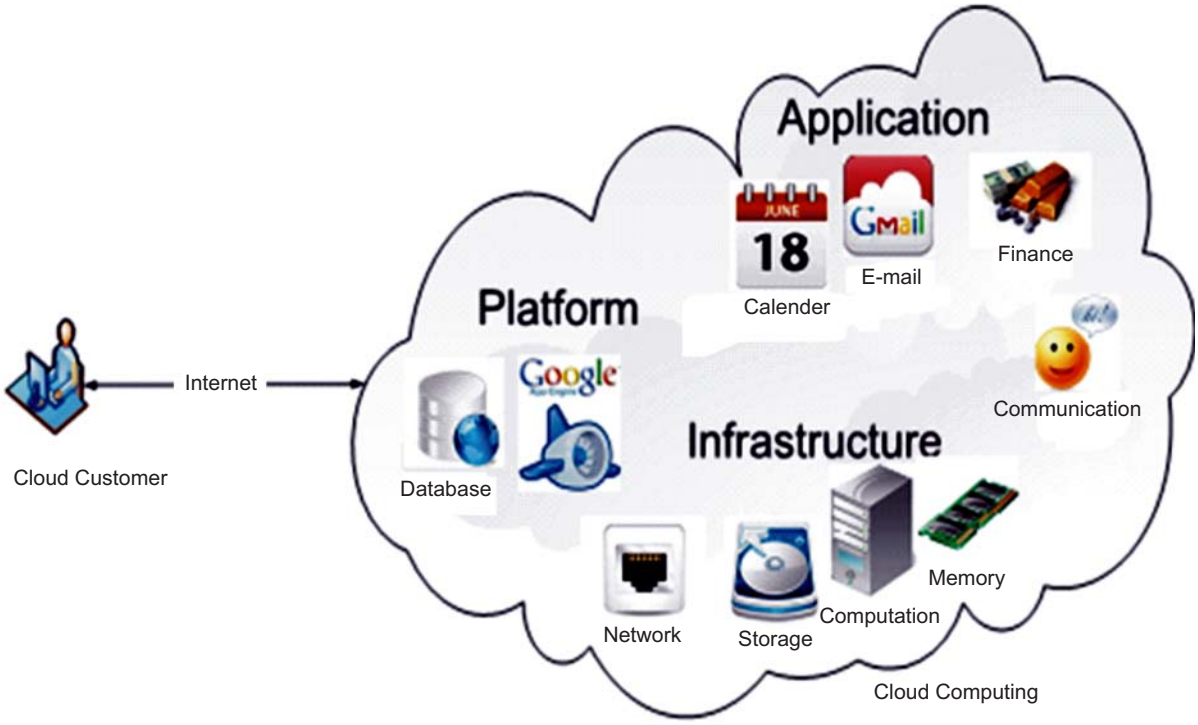

Figure 1: Cloud Computing

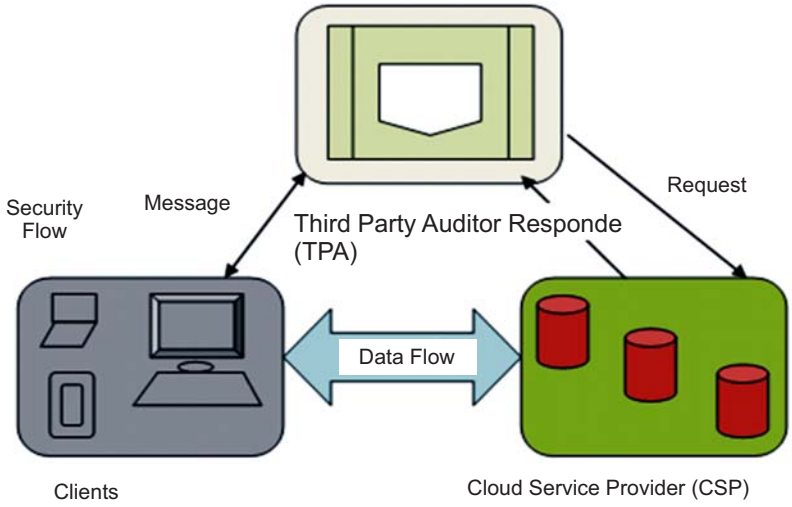

Figure 2: Cloud Data Storage Architecture

Clients: The Clients are those who have data to be stored, and access with help of Cloud Service Provider (CSP). They are typically desktop computers, laptops, mobile phones, tabletcomputers, etc.

Cloud Service Provider (CSP): Cloud Service Providers (CSPs) are those who have major resources and expertise in building, managing distributed cloud storage servers and provideapplications, infrastructure, hardware, enabling technology to Clients as a service via internet.

Third Party Auditor (TPA): Third Party Auditor (TPA) who has knowledge and competence that client may not have and confirms the truthfulness of informationstored in cloud on behalf of clients. Foundedon the inspectionconsequence, TPA might release a check report to the Client.

In the cloud paradigm, by putting the large data files on the remote servers, the clients can be relieved of the burden of storage and computation. As customers no slowerhold their informationnearby, it is of dangerous standing for the customers to safeguard that their information are being appropriately stored and preserved. That is, clients should be fortified with convincedsafety means so that they can occasionally authenticate the accuracy of the inaccessible information even without the presence of indigenous copies [16].

For instance, in *e*-Health submissions inside the USA the custom and contact of threatened health material would meet the strategiesapproved by Health Insurance Transportability and Answerability Act (HIPAA), and thus possession the data private on the isolatedstoragewaitpersons is not just a decision, but a request.

In Cloud computing, privacy plays a most important component mainly in sustaining manage over associations' data positioned across multiple distributed cloud servers or CDS [2]. It is a necessity when utilizing a public cloud dueto public clouds ease of access environment. Emphasizing confidentiality of cloud users' outlines and keeping their information, that is practically right to used, permits for cloud data security protocols to be put into effect at different unusual levels of cloud applications [3].

The objective of accurateness promise to make sure cloud users that their cloud data are definitely accumulated correctly and reserved integral all the instance in the cloud to get better and sustain the similar stage of storage space exactness promise even if cloud customers modify, delete or append their cloud information files in the cloud [4]. Availability is one of the most significant information security conditions in Cloud computing for the reason that it is a key decision issuewhen deciding along withcloud vendors within the delivery models [2]. The service level agreement(SLA) is the main document which emphasizes the apprehension ofavailability in cloud services and resourcesbetween the CSP andclient. Consequently by exploring the materialsanctuarynecessitiesat each of the different cloud deployment, delivery models, vendors and organizations can becomeself-assuredin encourage anextremelyconfined safe and sound cloud structure[3].

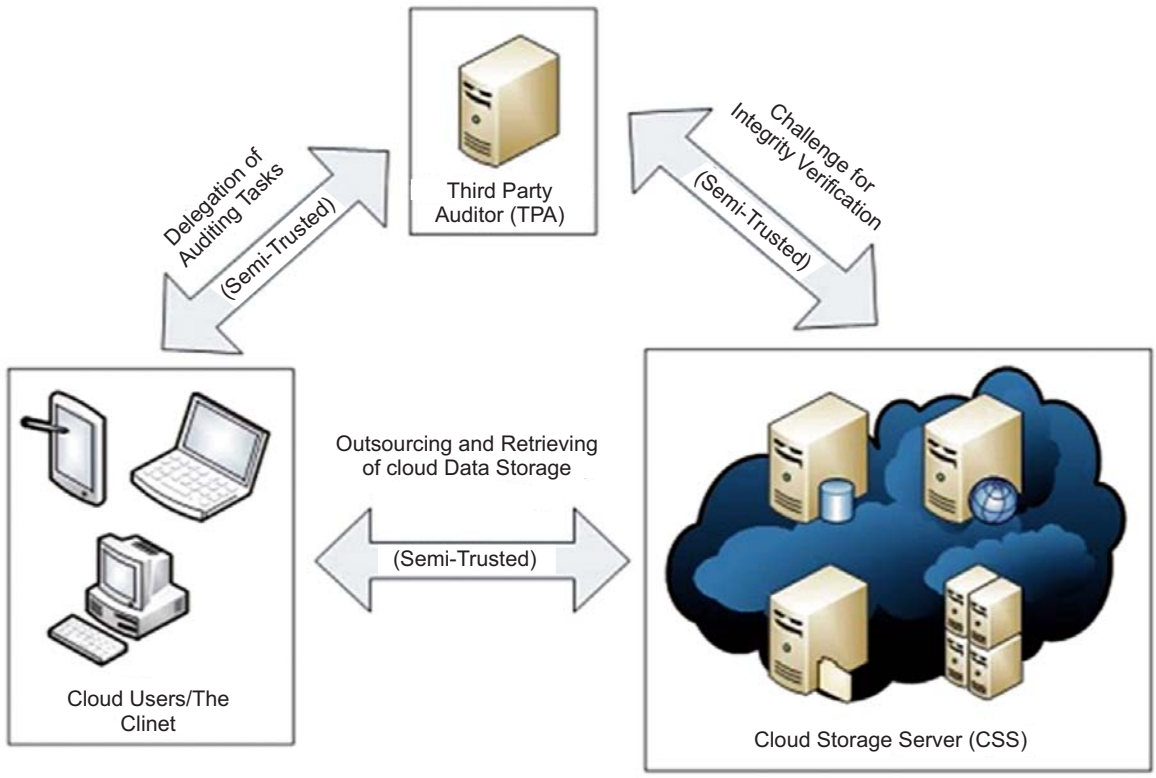

Figure 3: Participating parties in public auditing of cloud data

Pointing at integrity declaration, public reviewing of cloud data has been alengthily investigation unruly infresh years. As user datasets stored on cloud storage servers (CSS) are out of the mist users' reach, reviewing from the customer himself or a third gathering accountant is a shared demand, no substance how secure and powerful the server-side instrumentsentitlement to be. With Demonstrable Information Ownership (DIO) and Proofs Of Retrieveability (POR), the data owner or a third-party auditor is able to confirm the truthfulness of their information without obligating to recover their information. Moreover, when the customer needs a third gathering to authenticate the information on his behalf, all information will be unprotected to the third get-together. To discourse these glitches, scientists are emerging arrangements based on outdated digital autographs to help users authenticate the truthfulness of their information without having to repossess it, which they term as provable data possession (PDP) or evidences of retrieve ability (POR). There are three participating parties in integrity verification game: client, CSS and TPA. The client provisions her data on CSS, while TPA's impartial is to prove the truthfulness of theclient's information deposited on CSS. Having a specialized TPA to authentiate information truthfulness is well-organized, but it may also familiarize supplementary jeopardizes as the third-party accountantmay not be totally dependable by itself.

Figure-3 shows the relations between the participating parties in public auditing, which demonstrates that the three parties in a public auditing game -- the client, the cloud service provider and third-party auditor -- do not fully trust each other. This has been a widely researched problem over recent years.In such schemes, a small piece of metadata baptized 'homomorphic authenticator or 'homomorphic tags' are stored along with each data block. When the client needs to authenticate data truthfulness, the waitperson will produce a waterproof with the authenticators of the selected data blocks, and data auditing is doneby the client or a third-party auditor through verifying the proof with public keys.

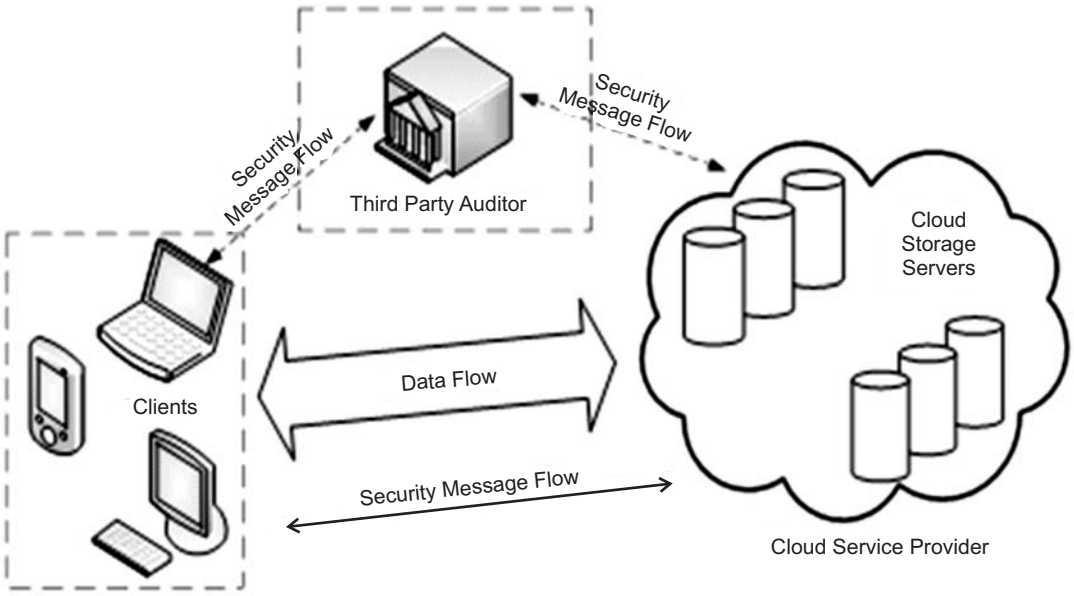

Figure 4: Cloud data storage architecture [5]

As stated above, the majority of datasets in big data applications are dynamic. Therefore, it is of great importance for public checking schemes to be scalable and accomplished of secondary dynamic data updates. Current public checkingarrangements can previouslysustenanceconfirmation of numerous kindsof full self-motivatedinformationinforms[5, 6]. However, there are security and efficiency difficulties that we aim to discourse in our research. Existing public reviewing schemes allow the integrity of a dataset stored in cloud to be externally verified without retrieval of the whole original dataset. However, in practice, there are many contests that hinder the application of such schemes.

Several security solutions have been recently developed, in order to provide data confidentiality in cloud storage environments [7-10], while considering access control challenges and user revocation concerns.In [9], Yu et al. proposed a characteristic based admission regulator strategy to firmly outsource sensitive client data to cloud servers. In this method, information is encrypted using a symmetric encryption procedure, while the enciphering key is protected by a KP-ABEscheme [11]. To accomplishactivecollections, they representative the key re-encryption actions to the cloud, without revealing the content of outsourced data. As such, the association cancellation instrument transports supplementary calculation upstairs. That is, our design conveys performance advantages for large scale sharing groups.

Several stowage organizations are based on the proxy re-encryption algorithms, in instruction to achieve fine grained access control [7, 11]. When a beneficiary wants to recover sub contracted information from the depositor, he has first to ask the cloud server to re-encrypt data file using its public key and the public master key, while considering the granted privileges. Ateniese et al. [12] propose a bi-directional proxy re-encryption arrangement to protected disseminated stowage systems and achieve efficient access control. However, aaccident attack amongst the untrusted storage server and a revoked group member can be hurled, which permits to absorb the decryption answers of all encoded blocks. In [7], the authors design an end-to-end content confidentiality protection mechanism for large scale data storage and distribution. They comprise many cryptographic instruments, specifically the proxy re-encryption and transmission cancellation. Inappropriately, the donation of a new user or the revocation of a group member requires the update of the entire group with new parameters and secret keys. That is, the complexity of user contribution and cancellation in their approach is linearly cumulative with the quantity of data proprietors and the quantity of cancelled users, respectively.To name a few of these, first, the server still has to aggregate a proof with the cloud controller from data blocks that are distributed stored and processed on cloud instances and this means that encryption and transfer of these data within the cloud will become time-consuming.

2. LITERATURE SURVEY

In this paper [13], author has recommended a proficient and make safe for cloud storage schemes as well as they recommended a privacy-preserving and proficient storage auditing protocol, which can assemble the above-listed conditions. To explain the data privacy difficulty, their technique is to produce an encrypted verification with the challenge stamp by using the Bilinearity property of the bilinear combination, such that the accountant cannot decrypt it but can authenticate the exactness of the verification. Without using the mask method, their method supported on auditing procedure to sustenance batch auditing for not only several clouds but also multiple owners. Our multicloud batch auditing does not need any additional trusted manager. The multi-owner batch auditing can significantly progress the auditing concert, particularly in huge-scale cloud storage schemes. Alternatively that their technique, they assume the server calculate the confirmation as atransitionalimportance of the confirmation, such that the auditor can honestlyutilize this intermediary importance to confirm the exactness of the confirmation. Consequently, theirtechnique can significantlydecrease the computing weights of the auditor by affecting it to the cloud server.

This exertion educations the tricky [5] of confirming the truthfulness of information stowage in cloud calculating and propose a protocol supporting for fully active information processes, especially to support block insertion, which is missing in most existing schemes. The overview of TPA eradicates the participation of the customer through the checking of whether his information stowed in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. The sustenance for informationsubtleties via the most universal forms of informationprocess, such as chunkalteration, supplement, and obliteration, is also a noteworthystageto practicality, since services in Cloud Computing are not limited to archive or backup data only.

In this paper author proposed a new multi-agent system (MAS) architecture [2] is significant to make sure high protection facilitation based on the method of its expansion. A safety measures structure supported on MAS architecture to make easy confidentiality, exactness declaration, availability and reliability of mutual CDS environment is anticipated. To create the protection structure for collaborative CDS security, the parts on MAS, cloud consumer and CSP are accumulated from different literatures. An early representation of customized MAS parts for mutual CDS security is offered. The connections between these parts are utilized to build the questionnaire. Rasch was utilized in analyzing pilot questionnaire thing dependability is found to be reduced and a few acts in respondents and things were recognized as rebels with indistinct dimensions.

In this paper [14] author has focused on the problems associated to security characteristics in cloud computing his research effort proposes a novel classical called Multi-clouds Databases (MCDB) which uses multi-clouds as an alternative of single cloud service provider, for instance in Amazon cloud service which utilizes Shamir's secret sharing algorithm with multi-clouds as an alternative of a single cloud. Besides, MCDB model assumed TMR methods with sequential method to develop the consistency of their model which improves security. This paper talks about the architecture with the parts of the representation. Author aim of the proposed representation is to reduce the security hazards that occur in cloud computing and get better system consistency. Besides, it concentrates on the problems associated to data integrity, data confidentiality, and service availability.

In this paper [15], author has propose a novel map-based provable multi-copy dynamic data possession (MB-PMDDP) method that has the following characteristics: 1) it presents confirmation to the clients that the CSP is not deceiving by storing smaller amountof copies; 2) it sustains outsourcing of dynamic information, i.e., it sustains block-level process, such as block modification, insertion, deletion, and add on; and 3) it permits allowedcustomers to effortlesslyright to use the file copies accumulated by the CSP. They give a comparative study of the proposed MB-PMDDP scheme with existing scheme provable control of dynamic single-copy methods.A file that is replica and stored intentionally on multiple servers – located at different geographic positions – can assist reduce access time and communication charge for customers. In addition, a server's copy can be restructured even from anentireharm using replica copies on other servers. The hypotheticalstudy is authenticated through experimental effects on a profit-making cloud platformas well as theydemonstrate the refuge against plotting servers and deliberate how to distinguish besmirched duplicates by to some extent altering the proposed method.

Curtmolaet, al. [18] proposed a scheme named MR-PDP that can prove the honesty of numerousimitations along with the innovative information file. Although the scheme needs only one authenticator for each chunk, it has two Spartan drawbacks. First, since the verification process requires secret material, there will be security problems when extending the MR-PDP scheme to support public auditing. Second, it does not support verification for dynamic data updates. In order to allow a third-party auditor to verify datasets with multiple replicas without any secret material, the client still needs to store and build different ADS for every replica, which will incur heavy communication overheads. As an improvement to MR-PDP, Barsoumet. al. [19] proposed a series of PDP schemes. These schemes are based on the BLS signature with support of public verifiability, data dynamics and multiple replicas at the same time. However, they do not provide a verification process for updates. Furthermore, their construction of the MHT structure is not efficient for update verifications as each single update will incur updates on all branches. Joseph [20] provided a privacy-preserving information integrity defense by permitting public auditability for cloud stowage and riggings a ascendable agenda that discourses the building of an communicating inspection etiquette to avoid the deceitfulness of prover and the escape of substantiated information in cloud stowing by dropping the upstairs in subtraction, announcement and storage.

3. PROPOSED METHODOLOGY

The Auditing Scheme proposed here is based on the concept of Sharing Data over Public Clouds with Multi Receiver Identity based Signcryption.

Signcryption is a technique of encrypting the data and apply signatures at the same time and send to Receiver. The Receiver on the other hand will apply Signatures and decrypts the data.

The Algorithm implemented here is based on the concept of Signcryption, which contains number of phases such as Setup and Key Generation and Encryption and Decryption with Access Policy Matching.

Setup Phase: In this phase Elliptic Curve Equations with the Selection of Elliptic Curve Parameters are chosen. All the Access Policies are decided in the setup phase to decide the Access Permission levels of the Users.

Key Generation Phase: Here in this paper Sender and Receiver agree on a common Base Point G (x, y) from the elliptic Curve and Choose their respective Private and Public Key. Let us suppose 'E' is the General Elliptic Curve Equation then 'Pk' is the Public key and 'Sk' is the Secrete key for Sender and receiver.

The Elliptic Curve Equation is given by:

$$y^2 = x^3 + ax + b$$

Where, $$4a^3 + 27b^2 \neq 0$$

Sender Selects any random Key point over elliptic Curve E(F) which is supposed to be the Private Key for Sender'Sk', using private key and Common Base Point 'B', public key is generated.

$$\text{Pk} = \text{Sk.B}$$

Signcryption: Here in this phase for the Encryption of Message or Data Signatures are generated for the respective Receivers based on the Identity of the receiver and Apply Signatures and Encryption Simultaneously at the same time on the Message to encrypt the data.

UnSigncryption: Here in this phase for the Decryption of Message or Data Signatures are generated for the respective Receivers based on the Identity of the receiver and Apply Signatures and Decryption Simultaneously at the same time on the Message to decrypt the data.

Signature Generation: The Message or Data to be Shared, for that random integer value 'u' is selected and from the integer value Tag value is generated.

$$\text{Tag}_m = \text{name } ||n||u|| \text{ Sig}_{sk}$$

Sender Generates Signatures Sig_g for each of the message m_i,

$$\text{Sig}_g = (\text{H}(m_i).um_i)^{\alpha}$$

4. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic Curve Cryptography is a technique which is based on the Concept of Elliptic curve theory which is based Hard Logarithmic Problem that can be used to create faster, smaller and more effective Cryptographic Keys. Elliptic Curve Cryptography is used for the generation of Keys by using the Elliptic Curve Equations. Elliptic Curve Cryptography yields a level of Security from 164-bits keys to 1024 bits depends on the System Requirements.

The General Equation of the Elliptic Curves is given as:

$$y^2 = x^3 + ax + b$$

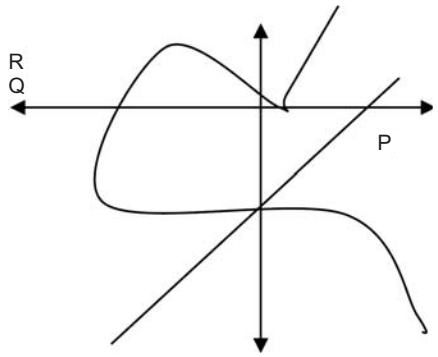

Figure 5: General Elliptic Curve Equations

Key Generation using Elliptic Curve Cryptography : Since ECC is based Asymmetric Key Cryptography hence is used to generate both pairs of Public and Private Keys. The Data Owner uses the receiver's public key for the encryption of the Message and receiver uses it private key for decryption. Let '*n*' is the maximum limit and must be a prime number, select a number '*d*' (private key) within the range of '*n*' which is the private key for the Data Owner, hence using this private key and the Base Point 'P' (which is any point on Curve) public key 'Q' is generated.

$$Q = d*P$$

Encryption using Elliptic Curve Cryptography : For the Encryption operation to be performed using ECC, public and private key pairs are used. Suppose a Message 'M' needs to be encrypted using ECC, take any point 'm' on the point 'M' on the Elliptic Curve 'E'. Choose any random point on the Elliptic Curve '*r*' within the range from [1-(n-1)].

$$C1 = r * P$$

$$C2 = M + r * Q$$

Decryption using Elliptic Curve Cryptography : For the Decryption of the CipherText 'C1 & C2' the following operations needs to be performed at the receiver side:

$$M = C2 - d * C1$$

Signcryption Phase: The various Steps involved during Signcryption phase for the identity IDi.

1. The Receiver's public key U_B(Selected from Private Key and Base Point) is verified by using generated Signatures.
2. Random Integer *r* is selected randomly, r $\in_R$ [1, $n - 1$].
3. Now Computes S = $r \cdot B = (r_1, r_2)$.
4. Computes T = $r \cdot U_B = x_1$, if S = O (point at infinity, then go to Step 2.
5. k_1 = Hash ($x_1 \| ID_A \| ID_B$).
6. A symmetric encryption algorithm is used to generate the cipher text Ciphertext = E_{k1} (M), where the secret key k_1 is the encryption key.
7. Generates *v* = Hash (Ciphertext $\| r_1 \| ID_A \| r_2 \| ID_B$).
8. Computes $s = d_A - vr \bmod q$.
9. Sends the signcrypted text (T, Ciphertext, *s*) to receiver.

Unsigncryption Phase : The Unsigncryption algorithm involves the following steps which are performed by the recipient of the message.

1. Sender's public key U_A is verified by using identity of the sender.
2. Computes $K = d_B \cdot R = x_1$.
3. $k_1 = H(x_1 \| ID_A \| ID_B)$.
4. A symmetric decryption algorithm is used to generate plain text $M = D_{k1}(C)$, where the secret key k_1 is used for decryption.
5. Computes v = Hash (Ciphertext $\| r_1 \| ID_A \| r_2 \| ID_B$).
6. Verifies $s \cdot B + v \cdot T = U_A$, If it is true then accept the message, since M is correct plain text which is sent by sender ; otherwise reject message M.

5. RESULT ANALYSIS

The table given below is the analysis and comparison of Communication Cost of Batch Auditing for 'K' number of Owner's and 'C' number of Clouds. Here '*t*' defines the total number of challenged data blocks from each of the Data Owner at each Cloud Server. '*s*' defines the total number of sectors at each of the data block. '*n*' defines the total number of data blocks of file. The comparison given here is on the basis of Four Auditing Schemes. The Analysis proves that the proposed scheme seems to be more efficient in comparison to the existing Auditing Protocols.

Table 1
Analysis and Comparison of Communication Cost of Batch Auditing Protocols

Scheme	*Challenge*	*Proof*
Wang's Audit [4,5]	O (KC*st*)	O (KC*st* log *n*)
Zhu's IPDP [21,22]	O (KC*t*)	O (KCs)
Existing Scheme [13]	O (KC*t*)	O (C)
Proposed Scheme	O (K*t*)	O (log C)

The Table given below is the analysis of Computation Cost of the auditor for $s = 50$ and for Single Owner and Single Cloud. The Analysis done here is based on three Schemes which provides Auditing in Cloud. Here number of Challenged Data blocks are taken for Single Owner and Single Cloud and on the basis of that Computation Cost is computed. The Proposed Scheme implemented here proves to be more efficient and provides less Computation Cost in comparison to other Auditing Schemes.

Table 2
Analysis of Computation Cost for *s* = 50 Single Owner, Single Cloud

	Computation Cost (s = 50)		
# of Challenged Data Blocks	*Zhu's IPDP*	*Existing Scheme*	*Proposed Scheme*
100	0.15	0.13	0.1
150	0.2	0.17	0.14
200	0.24	0.21	0.18
250	0.28	0.25	0.23
300	0.32	0.28	0.25
350	0.35	0.32	0.29
400	0.4	0.37	0.34
450	0.45	0.41	0.38
500	0.48	0.45	0.42

The Table given below is the analysis of Computation Cost of the auditor for *s* = 50 and for Single Owner and 5 blocks / Cloud. The Analysis done here is based on three Schemes which provides Auditing in Cloud. Here number of Challenged Data blocks are taken for Single Owner and 5 blocks / Cloud and on the basis of that Computation Cost is computed. The Proposed Scheme implemented here proves to be more efficient and provides less Computation Cost in comparison to other Auditing Schemes.

Table 3
Analysis of Computation Cost for *s* = 50 Single Owner, 5 blocks / Cloud

	Computation Cost (s = 50)		
# of Challenged Data Blocks	*Zhu's IPDP*	*Existing Scheme*	*Proposed Scheme*
5	0.25	0.04	0.03
10	0.52	0.08	0.06
15	0.76	0.11	0.09
20	1.1	0.15	0.12
25	1.27	0.18	0.14
30	1.52	0.2	0.17
35	1.75	0.27	0.23
40	2.15	0.29	0.26
45	2.25	0.34	0.32
50	2.5	0.38	0.35

The Figure given below is the analysis of Computation Cost of the auditor for *s* = 50 and for Single Owner and Single Cloud. The Analysis done here is based on three Schemes which provides Auditing in Cloud. Here number of Challenged Data blocks are taken for Single Owner and Single Cloud and on the basis of that Computation Cost is computed. The Proposed Scheme implemented here proves to be more efficient and provides less Computation Cost in comparison to other Auditing Schemes.

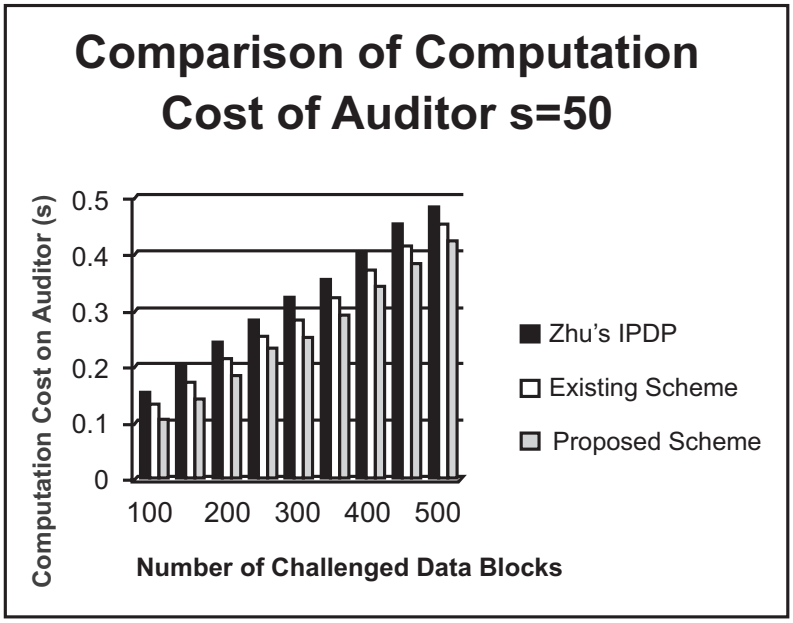

Figure 6: Comparison of Computation Cost for *s* = 50 single Owner, Single Cloud

The Figure given below is the analysis of Computation Cost of the auditor for $s = 50$ and for Single Owner and 5 blocks / Cloud. The Analysis done here is based on three Schemes which provides Auditing in Cloud. Here number of Challenged Data blocks are taken for Single Owner and 5 blocks / Cloud and on the basis of that Computation Cost is computed. The Proposed Scheme implemented here proves to be more efficient and provides less Computation Cost in comparison to other Auditing Schemes.

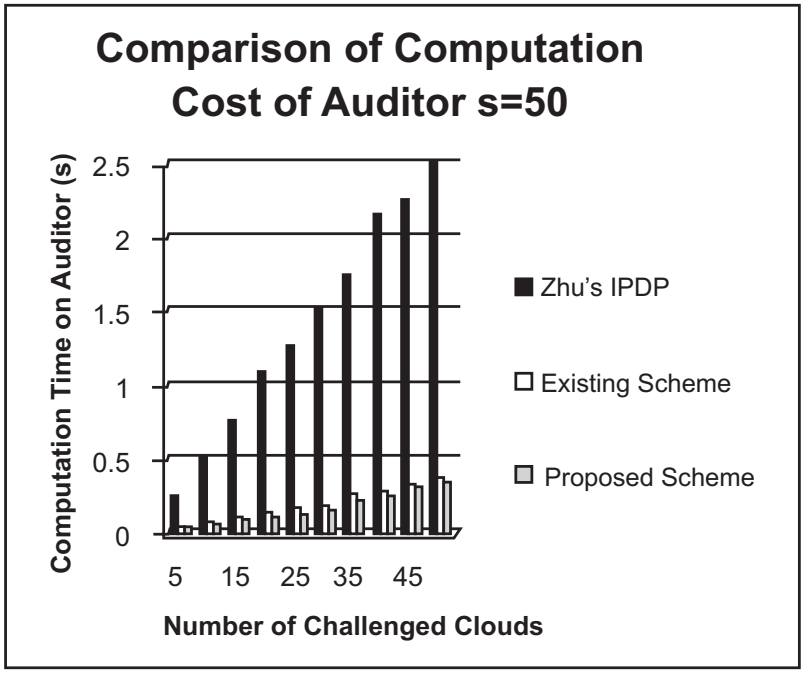

Figure 7: Comparison of Computation Cost for *s* = 50 single Owner, 5 blocks / Cloud

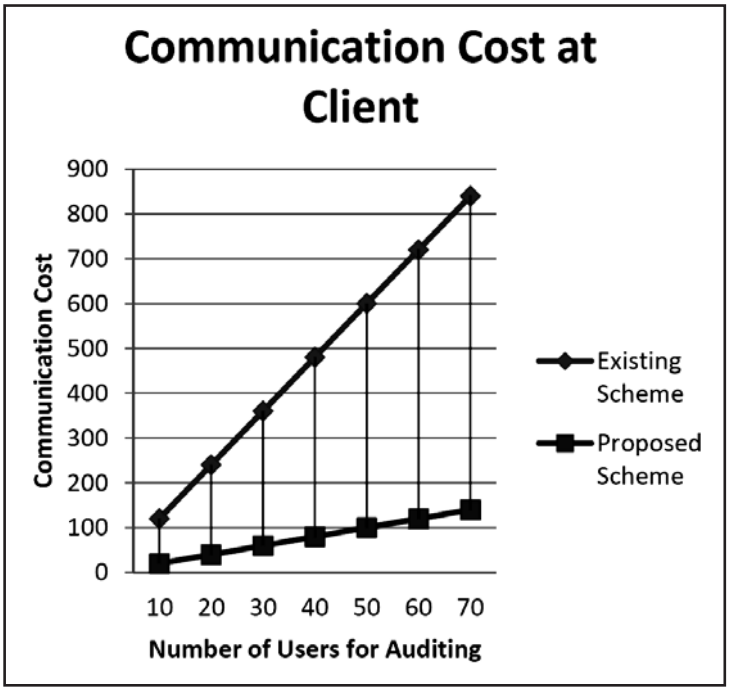

Figure 8: Comparison of Communication Cost at Client Side

The Figure 8, shown above is the analysis and comparison of Communication Cost at Client Side. The Communication Cost computed here at the Client Side includes all the phases required for the Scheme to process Auditing including Registration, Login and Authentication. The Proposed Scheme implemented provides less number of operations to be performed for auditing at the client side hence take less communication cost in comparison to the existing scheme.

The Figure 9, shown below is the analysis and comparison of Communication Cost at Server Side. The Communication Cost computed here at the Server Side includes all the phases required for the Scheme to process Auditing including Registration, Login and Authentication. The Proposed Scheme implemented provides less number of operations to be performed for auditing at the Server side hence take less communication cost in comparison to the existing scheme.

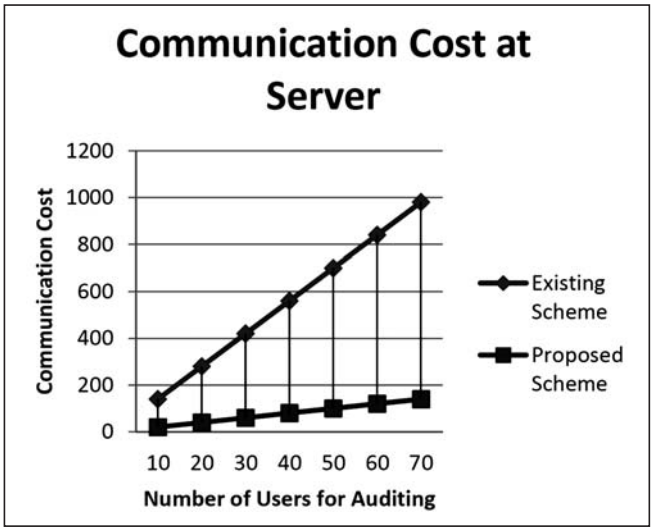

Figure 9: Comparison of Communication Cost at Server Side

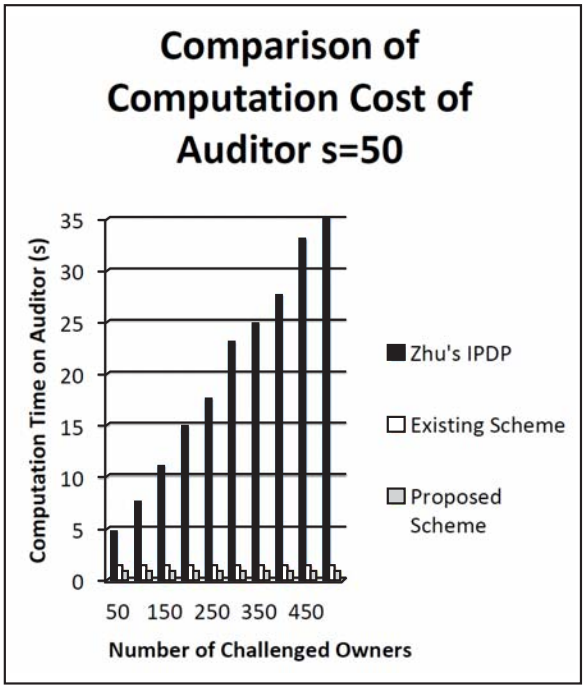

Figure 10: Comparison of Computation Cost for *s* = 50 single Cloud, 5 blocks / Owner

The Figure 10, given above is the analysis of Computation Cost of the auditor for s = 50 and for Single Cloud and 5 blocks / Owner. The Analysis done here is based on three Schemes which provides Auditing in Cloud. Here number of Challenged Data blocks are taken for Single Cloud and 5 blocks / Owner and on the basis of that Computation Cost is computed. The Proposed Scheme implemented here proves to be more efficient and provides less Computation Cost in comparison to other Auditing Schemes.

6. CONCLUSION

Data Sharing is a way of sharing data or resources in the cloud so that the user can access the data in an easy manner. But During the sharing of data users needs to be authenticated, hence various techniques are implemented to ensure the accountability of communalinformation in the cloud. The plannedprocedure implemented here for the distribution of information using Message Authentication Code and Key Generation using Elliptic Curve Cryptography provides efficient results as compared to the existing technique.

The plannedprocedurerealized here provides less computational time and security from various attacks as well as perform Efficient Dynamic Operations on various Copies to be shared. It also provides Efficient User revocation and Security from Escrow Problem.

REFERENCES

[1] Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing v3.0, Nov 2011.

[2] A.M. Talib, R. Atan, R. Abdullah, and M.A. Azmi Murad. Multi Agent System Architecture Oriented Prometheus Methodology Design to Facilitate Security of Cloud Data Storage. Journal of Software Engineering 5 (3), 2011, pp. 78-90 .

[3] S. Ramgovind, M.M. Eloff, and E. Smith, "The Management of Security in Cloud Computing," IEEE, 2010, pp. 1-7 .

[4] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," IEEE, 2009, pp. 1-9.

[5] WANG, Q., WANG, C., REN, K., LOU, W. & LI, J. Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing. IEEE Transactions on Parallel and Distributed Systems, 22, 847 - 859.

[6] LIU, C., CHEN, J., YANG, L. T., ZHANG, X., YANG, C., RANJAN, R. & RAMAMOHANARAO, K. Authorized Public Auditing of Dynamic Big Data Storage on Cloud with Efficient Verifiable Fine-grained Updates. IEEE Transactions on Parallel and Distributed Systems, 25, 2234 - 2244.

[7] H. Xiong, X. Zhang, D. Yao, X. Wu, and Y. Wen. Towards end-to-end secure content storage and delivery with public cloud. CODASPY '12, pages 257–266. ACM, 2012.

[8] S. Zarandioon, D. Yao, and V. Ganapathy. K2c: Cryptographic cloud storage with lazy revocation and anonymous access. In SecureComm, volume 96, pages 59–76. Springer, 2011.

[9] Shucheng Yu, CongWang, Kui Ren, andWenjing Lou. Achieving secure, scalable and fine-grained data access control in cloud computing. In Proceedings of the 29th conference on Information communications, INFOCOM'10, pages 534–542, Piscataway, NJ, USA, 2010. IEEE Press.

[10] S. Fugkeaw. Achieving privacy and security in multi-owner data outsourcing. Pages 239–244. IEEE, 2012.

[11] Vipul Goyal, Omkant Pandey, and et al. Attribute-based encryption for fine-grained access control of encypted data, 2006.

[12] G. Ateniese, K. Fu, M. Green, and S. Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. ACM Trans. Inf. Syst. Secur., 9:1–30.

[13] Kan Yang, XiaohuaJia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing" IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 9, September 2013.

[14] Mohammed A. AlZain, Ben Soh and Eric Pardede, "A New Approach Using Redundancy Technique to Improve Security in Cloud Computing" in Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on , vol., no., pp.230-235, 26-28 June 2012. Doi: 10.1109/CyberSec.2012.6246174.

[15] Ayad F. Barsoum and M. Anwar Hasan, "Provable Multicopy Dynamic Data Possession in Cloud Computing Systems" IEEE Transactions On Information Forensics And Security, Vol. 10, No. 3, March 2015.

[16] A. Juels, J. Burton, and S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. ACM CCS '07, Oct. 2007, pp. 584–97.

[17] G.Ateniese et al., "Provable Data Possession at Untrusted Stores," Proc. ACM CCS '07, Oct. 2007, pp. 598–609.

[18] CURTMOLA, R., KHAN, O., BURNS, R. C. & ATENIESE: G. Year. MR-PDP: Multiple-Replica Provable Data Possession. In: Proceedings of the 28th IEEE International Conference on Distributed Computing Systems (ICDCS '08), 2008 Beijing, China. 411-420.

[19] BARSOUM, A. F. & HASAN, M. A. Year. Integrity Verification of Multiple Data Copies over Untrusted Cloud Servers. In: Proceedings of the12thIEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID '12), 2012 Ottawa, Canada. 829-834.

[20] N.M. Joseph, E. Daniel and N.A. Vasanthi, "A Scalable Privacy-Preserving Verification Correctness Protocol to Identify Corrupted Data in Cloud Storage," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2013, 2(3): pp: 0951-0956.

[21] [21] Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative Provable DataPossession for Integrity Verification in Multi-Cloud Storage,"IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 12,pp. 2231-2244, Dec. 2012.

[22] [22] Y. Zhu, H. Wang, Z. Hu, G.-J.Ahn, H. Hu, and S.S. Yau, "DynamicAudit Services for Integrity Verification of Outsourced Storages inClouds," Proc. ACM Symp.Applied Computing, W.C. Chu, W.E.Wong, M.J. Palakal, and C.-C. Hung, eds., pp. 1550-1557, 2011.