Volume 1, Issue 4 November 2015 ISSN NO: 2454 - 7514

North Asian International Research Journal Consortium

North Asian International Research Journal

Of

Science, Engineering and Information Technology

Welcome to NAIRJC

ISSN NO: 2454 -7514

North Asian International Research Journal of Science, Engineering & Information Technology is a research journal, published monthly in English, Hindi, Urdu all research papers submitted to the journal will be double-blind peer reviewed referred by members of the editorial board. Readers will include investigator in Universities, Research Institutes Government and Industry with research interest in the general subjects

Editorial Board

Address: - Dr. Ashak Hussain Malik House No. 221 Gangoo, Pulwama, Jammu and Kashmir, India - 192301, Cell: 09086405302, 09906662570, Ph. No: 01933-212815,
Email: nairjc5@gmail.com, nairjc@nairjc.com, info@nairjc.com Website: www.nairjc.com

REGENERATING-CODE-BASED CLOUD STORAGE BY PRIVACY-PRESERVING PUBLIC AUDITING

VIKRAM AJABE[1]
NMVPM's, Nutan Maharashtra Institute of Engineering and Technology, Talegaon Dabhade, Pune. 410507

DHIRAJ DHAKAD[2]
NMVPM's, Nutan Maharashtra Institute of Engineering and Technology, Talegaon Dabhade, Pune. 410507

AVDHUT KULKARNI[3]
NMVPM's, Nutan Maharashtra Institute of Engineering and Technology, Talegaon Dabhade, Pune. 410507

MAULI SHELAR[4]
NMVPM's, Nutan Maharashtra Institute of Engineering and Technology, Talegaon Dabhade, Pune. 410507

ABSTRACT

To secure outsourced information in distributed storage against debasements, adding adaptation to non-critical failure to distributed storage together with information honesty checking and disappointment reparation gets to be basic. As of late, recovering codes have picked up fame due to their lower repair data transfer capacity while giving adaptation to internal failure. Existing remote checking strategies for recovering coded information just give private evaluating, requiring information proprietors to dependably stay online and handle evaluating, and in addition repairing, which is now and then unfeasible. In this paper, we propose an open reviewing plan for the recovering code-based distributed storage. To take care of the recovery issue of fizzled authenticators in the nonattendance of information proprietors, we present an intermediary, which is advantaged to recover the authenticators, into the customary open inspecting framework model. In addition, we plan a novel open undeniable authenticator, which is created by two or three keys what's more, can be recovered utilizing fractional keys. In this manner, our plan can totally discharge information proprietors from online weight. Likewise, we randomize the encode coefficients with a pseudorandom capacity to protect information security. Broad security examination appears that our plan is provable secure under irregular prophet model also, test assessment shows that our plan is very effective and can be attainably coordinated into the regenerating code-based Cloud Storage.

Keywords—*Cloud Computing, Remote Data Checking, Proofs of Retrievability, Data Integrity.*

I. INTRODUCTION

distributed storage is presently picking up prominence in light of the fact that it offers an adaptable on-interest information outsourcing administration with engaging advantages: alleviation of the weight for capacity administration, all inclusive information access with area autonomy, what's more, evasion of capital consumption on equipment, programming, what's more, individual maintenances, etc., [1]. In any case, this new worldview of information facilitating administration additionally brings new security dangers toward clients information, in this manner making people or

enterprisers still feel reluctant. It is noticed that information proprietors lose extreme control over the destiny of their outsourced information; along these lines, the accuracy, and accessibility what's more, respectability of the information are being put at danger. On the one hand, the cloud administration is typically confronted with an expansive reach of interior/outside foes, who might perniciously erase on the other hand degenerate clients' information; then again, the cloud administration suppliers may act untrustworthily, endeavoring to conceal information misfortune then again defilement and guaranteeing that the records are still accurately put away in the cloud for notoriety or money related reasons. Hence it bodes well for clients to execute a proficient convention to perform periodical checks of their outsourced information to guarantee that the cloud to be sure keeps up their information effectively. Numerous components managing the trustworthiness of outsourced information without a nearby duplicate have been proposed under diverse framework and security models up to now. The most noteworthy work among these studies are the PDP (provable information ownership) model and POR (evidence of retrievability) model, which were initially proposed for the single-server situation by Ateniese et al. [2] and Juels et. al. [3], individually. Considering that documents are normally striped and repetitively put away crosswise over multi-servers or multi-mists, investigate uprightness confirmation plans suitable for such multi-servers or multi clouds setting with distinctive excess plans, for example, replication, deletion codes, and, all the more as of late, recovering codes. In this paper, we concentrate on the uprightness confirmation issue in recovering code-based distributed storage, particularly with the practical repair technique [11]. Comparative studies have been performed by Bo Chen et al. [7] and H. Chen el al. [8] independently and autonomously. [7] broadened the single-server CPOR scheme(private adaptation in [12]) to the regenerating code-situation; [8] outlined and executed an information respectability protection(DIP) plan for FMSR [13]-based distributed storage what's more, the plan is adjusted to the meager cloud setting. Notwithstanding, the two are intended for private review, just the information proprietor is permitted to check the honesty and repair the defective servers. Considering the vast size of the outsourced information and the client's obliged asset capacity, the errands of reviewing what's more, reparation in the cloud can be impressive and costly for the clients [14]. The overhead of utilizing distributed storage ought to be minimized however much as could reasonably be expected such that a client does not need to perform an excess of operations to their outsourced information (in extra to recovering it) [15]. Specifically, clients may not need to experience the many-sided quality in confirming and reparation. The reviewing plans in [7], [8] suggest the issue that clients need to dependably stay on the web, which may block its selection in practice, particularly for long haul archival storage. data blocks and authenticators) are implemented by a third-party auditor and a semi-trusted proxy separately on behalf of the data owner. Instead of directly adapting the existing public auditing scheme [12] to the multi-server setting, we design a novel authenticator, which is more appropriate for regenerating codes. Besides, we”encrypt” the coefficients to protect data privacy against the auditor, which is more lightweight than applying the proof blind technique in [14], [15] and data blind method in [16]. Several challenges and threats spontaneously arise in our new system model with a proxy (Section II-C), and security analysis shows that our scheme works well with these problems. Specifically, our contribution can be summarized by the following aspects: • We design a novel homomorphic authenticator based on BLS signature [17], which can be generated by a

couple of secret keys and verified publicly. Utilizing the linear subspace of the regenerating codes, the authenticators can be computed efficiently. Besides, it can be adapted for data owners equipped with low end computation devices (e.g. Tablet PC etc.) in which they only need to sign the native blocks. • To the best of our knowledge, our scheme is the first to allow privacy-preserving public auditing for regenerating code-based cloud storage. The coefficients are masked by a PRF (Pseudorandom Function) during the Setup phase to avoid leakage of the original data. This method is lightweight and does not introduce any computational overhead to the cloud servers or TPA.

• Our scheme completely releases data owners from online burden for the regeneration of blocks and authenticators at faulty servers and it provides the privilege to a proxy for the reparation.

• Optimization measures are taken to improve the flexibility and efficiency of our auditing scheme; thus, the storage overhead of servers, the computational overhead of the data owner and communication overhead during the audit phase can be effectively reduced.

• Our scheme is provable secure under random oracle model against adversaries illustrated in Section II-C. Moreover, we make a comparison with the state of the art and experimentally evaluate the performance of our scheme.

II. EXISTING METHODLOGY

Compare with the Traditional Public Auditing System model, our framework model includes extra intermediary operators. In request to uncover the judiciousness of our outline and make our taking after depiction in Section below to be all the more clear and solid, we think about, for example, a reference situation: An organization utilizes a business recovering code-based open cloud also, gives long haul archival capacity administration for its staffs, the staffs are furnished with low end calculation devices(e.g., Portable workstation PC, Tablet PC, and so forth.) and will be every now and again disconnected from the net. For open information evaluating, the organization depends on a trusted outsider association to check the information uprightness; Similarly, to discharge the staffs from substantial online weight for information and authenticator recovery, the organization supply an intense workstation(or bunch) as the intermediary and give intermediary reparation administration to the staffs' information.

III. PROPOSED SYSTEM

A. Overview

In spite of the fact that an immediate expansion of the strategies, can understand open unquestionable status in the multi-servers viewing so as to set every piece as an arrangement of sections and performing spot keeping an eye on them, such a direct strategy makes the information proprietor create labels for all sections freely, along these lines bringing about high computational overhead. Considering that information proprietors usually looks after constrained calculation and memory limit, it is entirely critical for us to lessen those overheads. Second, dissimilar to distributed storage taking into account customary eradication code or replication, an altered record format does not exist in the recovering code-based cloud capacity. Amid the repair stage, it registers out new pieces, which are very surprising from the broken ones, with high likelihood.

The accompanying parts of this area demonstrate our answer for the issues above. To start with, we develop a BLS-based [17] authenticator, which comprises of two sections for every fragment of

coded squares. Using its homomorphic property and the linearity connection amongst the coded hinders, the information proprietor is ready to produce those authenticators in another system, which is more proficient contrasted with the clear approach.

Our authenticator contains the data of encoding coefficients to keep away from information contamination in the reparation with off-base coefficients. To decrease the data transfer capacity expense amid the review stage, we perform a bunch confirmation over all α hinders at a sure server instead of checking the honesty of each piece independently as [7] does. In addition, to make our plan secure against the supplant assault and replay assault, data about the server's lists, pieces, and portions are all implanted into the authenticator. In addition, our primitive plan can be effortlessly enhanced to bolster protection safeguarding through the coding's veiling coefficients with a keyed PRF.

B. Construction of Our Auditing Scheme

Considering the recovering code-based distributed storage with parameters (n, k, ℓ, α, β), we expect β = 1 for effortlessness. Let and GT be multiplicative cyclic gatherings of the same huge prime request p, and e : G × G → GT be a bilinear matching map as presented in the preliminaries. Let g be a generator of G and H(·) : {0, 1}∗ → G be a safe hash work that maps strings consistently into gathering G. Table I list the essential documentations and phrasings utilized as a part of our p

Setup: The review plan related parameters are introduced in this strategy.

KeyGen(1κ) → (pk, sk): The information proprietor creates a arbitrary marking key pair (spk, ssk), two irregular components x, y R ←− Zp and processes $pk_x \leftarrow g^x$, $pk_y \leftarrow g^y$. At that point the mystery parameter is sk = (x, y, ssk) and people in general parameter is pk = (pk_x, pk_y, spk). Delegation (sk) → (x): The information proprietor sends encoded x to the intermediary utilizing the intermediary's open key, then the intermediary decodes and stores it locally after accepting.

The information proprietor consistently picks an irregular identifier ID R ←− {0, 1}∗, an irregular image u R ←− G, one set ſ = {w1,w2, ...wm} with components w_i R ←− G, and a record label t =(ID||u||w1||...||wm)||Sigssk(ID||u||w1||...||wm) for F. Sig() implies a standard mark plan. Review that the first record F is part into m squares, {w_i} mi =1; The customer figures and stores nα coded squares amongst n cloud servers. Review every portion of the pieces as a solitary image for effortlessness, our mark is produced all the while with the encoding procedure as takes.

Augmentation: The data owner properly augments the native m blocks as Eq.(3).

Signing for Native Blocks: The data owner views the data parts of the augmented blocks as a set of segments and computes authenticator for each segment, i.e. the symbols i, j, k denote the index of the server, the index of the block at a server and the index of a segment in a certain coded block.

Empowering Privacy-Preserving Auditable:

The security assurance of the proprietor's information can be effectively accomplished through coordinating with the irregular verification blind strategy [15] or other procedure [9]. In any case, all these protection safeguarding systems acquaint extra calculation overhead with the reviewer, who as a rule needs to review for some mists and an expansive number of information proprietors; accordingly, this could make it make an execution bottleneck. Hence, we lean toward to present a novel technique, which is all the more light-weight, to relieve private

information spillage to the inspector. Notice that in a recovering code-based distributed storage, information pieces put away at servers are coded as direct mixes of the first squares {wi}mi =1 with irregular coefficients. Assuming that the inquisitive TPA has recouped m coded hinders by intricately performing Challenge-Response strategies and illuminating frameworks of direct mathematical statements [14], the TPA still requires to tackle another gathering of m directly free comparisons to determine the m local squares. We can use a keyed pseudorandom capacity fkey (·) : {0, 1}∗ × K → GF(p) to veil the coding coefficients and along these lines keep the TPA from effectively g

Alleviating The Overhead Of Data Owner:

Despite that the information proprietor has been discharged from online weight for evaluating also, repairing, regardless it bodes well to diminish its calculation overhead in the Setup stage on the grounds that information proprietors generally keep up exceptionally constrained computational and memory assets. As already depicted, authenticators are created in another system which can diminish the computational many-sided quality of the proprietor to some degree; in any case, there exists a substantially more productive system to present further diminishment. Considering that there are such a variety of particular example number juggling operations amid the authenticator era, the information proprietor can safely delegate a piece of its registering undertaking to the intermediary in the accompanying way: The information proprietor first legitimately enlarges the m local squares, signs for them as Eq.(6), and along these lines acquires the $\{\sigma^{**}_{j_o k_o}\}_{1\le j_o\le m\ 1\le k_o\le s}$, then it sends the enlarged local squares and $\{\sigma^{**}_{j_o k_o}\}$ to the intermediary. Subsequent to getting from the information proprietor, the intermediary executes the last two stages of SigAndBlockGen(·) lastly produces whole authenticators σ_{ijk} for every fragment v_{ijk} with mystery esteem x. Along these lines, the information proprietor can move the costly encoding and authenticator era assignment to the intermediary while itself keeping up just the initial two lightweight steps; in this way, the workload of information proprietor can be significantly alleviated.. Moreover, Theorem 4 contends that the intermediary cannot fashion legitimate authenticators for invalid sections.

IV. RELATED WORK

The issue of remote information checking for uprightness was initially presented in [26], [27]. At that point Ateniese et al. [2] and Juels et al. [3] offered ascend to the comparable thoughts provable information ownership (PDP) and verification of retrievability (POR), individually. Ateniese et al. [2] proposed a formal definition of the PDP model for guaranteeing ownership of documents on untrusted capacity, presented the idea of RSA-based homomorphic labels and recommended haphazardly examining a couple pieces of the document. In their resulting work [28], they proposed an element adaptation of the earlier PDP plan taking into account MAC, which permits exceptionally fundamental square operations with constrained usefulness however piece insertions. All the while, Erway et al. [29] gave a formal structure for element PDP and gave the first completely powerful answer for bolster provable upgrades to put away information utilizing rank-based validated play records and RSA trees. To enhance the proficiency of element PDP, Q. Wang [30] proposed another system which utilizes merkle hash tree to bolster completely changing information. To discharge the information proprietor from online weight for confirmation,[2] considered the general population auditability in the PDP model interestingly. Be that as it may, their variation convention uncovered the

direct mix of tests and along these lines gives no information security ensure. At that point C. Wang et al. [14], [15] built up a irregular visually impaired strategy to address this issue in their BLS mark based open examining plan. So also, Solomon et al. [31] presented another protection safeguarding technique, which is more effective since it abstains from including a computationally serious blending operation for the purpose of information blinding. Yang et al. [9] introduced an open PDP plan, where the information protection is given through consolidating the cryptography strategy with the bilinearity property of bilinear matching. [16] used arbitrary veil to visually impaired information obstructs in blunder amending coded information for protection saving inspecting with TPA. Zhu et al. [10] proposed a formal structure for intuitive provable information possession (IPDP) and a zero-learning IPDP arrangement for private mists. Their ZK-IPDP convention underpins completely information elements, open undeniable nature and is additionally protection safeguarding against the verifiers.

Considering that the PDP model does not ensure the retrievability of outsourced information, Juels et al. [3] portrayed a POR model, where spot-checking and blunder rectifying codes are utilized to guarantee both "ownership" and "retrievability" of information records on remote chronicle administration frameworks. Later, Browers et al. [32] proposed an enhanced system for POR conventions that sums up Juels' work. Dodis et al. [33] likewise gave a study on diverse variations of POR with private auditability. A delegate work upon the POR model is the CPOR introduced by Shacham and Waters [12] with full evidences of security in the security model characterized in [3]. They use the openly irrefutable homomorphic straight authenticator manufactured from BLS marks to accomplish open reviewing. Be that as it may, their methodology is not security safeguarding because of the same reason as [2].

To present adaptation to non-critical failure in down to earth distributed storage, outsourced information records are regularly striped and needlessly put away crosswise over multi-servers or even multi-mists. It is fancied to outline effective evaluating conventions for such settings.In particular, [4]–[6] develop those uprightness checking plans for the single-server setting to the multi-servers setting under replication and eradication coding individually. Both B. Chen et al. [7] and H. Chen et al. [8] endeavor to plan inspecting plans for recovering code-based distributed storage, which is like our commitment aside from that our own discharge the information proprietor from online weight for confirmation and recovery.

Moreover, Zhu et al. [10] proposed a proficient development of helpful provable information possession(CPDP) which can be utilized as a part of multi-mists, and [9] amplify their primitive reviewing convention to bolster group reviewing for both numerous proprietors also, various mist

V. SYSTEM ARCHITECTURE

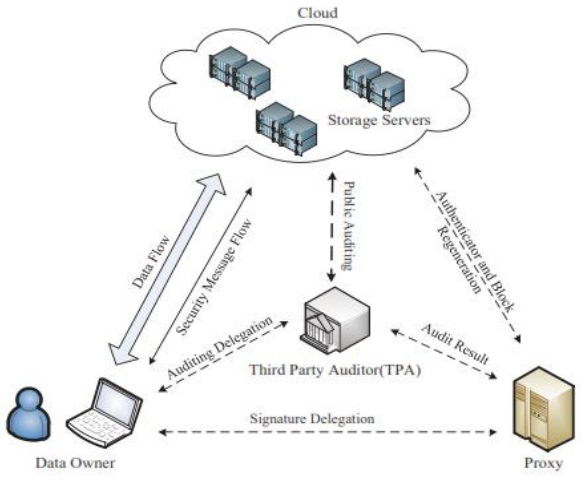

Fig 1: System Model

We consider the evaluating framework model for Regenerating Code-based distributed storage as Fig.1, which includes four elements: the information proprietor, who possesses a lot of information documents to be put away in the cloud; the cloud, which are overseen by the cloud administration supplier, give stockpiling administration and have noteworthy computational assets; the outsider auditor(TPA), who has aptitude and abilities to direct open reviews on the coded information in the cloud, the TPA is trusted and its review result is fair for both information proprietors and cloud servers; and an intermediary operators, who is semi-trusted and follows up on benefit of the information proprietor to recover authenticators and information hinders on the fizzled servers amid the repair methodology. Notice that the information proprietor is confined in computational and stockpiling assets contrasted with different substances and may gets to be disconnected from the net indeed, even after the information transfer system. The intermediary, who might continuously be on the web, should be a great deal all the more effective than the information proprietor however not exactly the cloud servers in wording of calculation and memory limit. To spare assets as well as the online weight conceivably brought by the occasional examining and unintentional repairing, the information proprietors resort to the TPA for respectability check and delegate the reparation to the intermediary.

VI. ALGORITHM / PROTOCOL / MATHEMATICAL INDUCTION / METHODS USED

A. Correctness

There are two verification processes in our scheme, one for spot checking during the Audit phase and another for block integrity checking during the Repair phase.

Theorem 1: Given a cloud server i storing data blocks Ψ_i and accompanied authenticators Φ_i , TPA is able to correctly verify its possession of those data blocks during audit phase, and the proxy can correctly check the integrity of download blocks during repair phase.

B. Soundness

Definition 1: Our authenticator as Eq. (10) is existentially unforgivable under adaptive chosen message attacks if no PPT adversary has a non-negligible advantage in the following game-Game 0:

1. Setup: The challenger runs the KeyGen() algorithm on input 1 κ and gives the public parameter (pkx, pky) to adversary A.
2. Queries: The challenger maintains the following oracles which can be queried by the adversary A :

• Hash Oracle (Ohash): provide result of H(·) for hash queries.

• UW Oracle (Ouw): produce the random parameters u, wλ($1 \le \lambda \le m$) for signature or forgery.

• Sign Oracle (Osign): produce authenticators on adaptively chosen tuple {ID, i, j, k, vijk, {$\varepsilon_{ij\lambda}$} m λ=1}, and return an authenticator σijk.

3. Output: Eventually, the adversary A produces a tuple {ID∗ , i,∗ j ∗ , k∗ , v∗ , {ε ∗ λ } m λ=1, σ∗}, and we say that A wins the game if Eq.(23) holds while the input tuple {ID∗ , i,∗ j ∗ , k∗ , v∗ , {ε ∗ λ } m λ=1} was not submitted to the Sign Oracle Osign.

$$e(\sigma * , g) = e(Hi * j * k * , pkx) \cdot e(u v * \prod m \lambda=1 w \varepsilon * \lambda \lambda , pky) \quad (23)$$

In the following theorem, we will show that our authenticator is secure under the CDH (Computational Diffie-Hellman) assumption.

Theorem 2: If the adversary A is able to win Game 0 with non-negligible advantage ϵ after at most qh hash queries and quw UW queries(quw = qh implied by our assumption in footnote 5), then there exist a PPT algorithm S that can solve the CDH problem with non-negligible probability ϵ'. 6

Definition 2: Our auditing scheme is sound if no PPT adversary has a non-negligible advantage in the following game-Game 1:

1. Setup: The challenger runs the KeyGen() algorithm on input 1 κ and gives the public parameter (pkx, pky) to adversary A

2. Store Query: The adversary A queries store oracle on data $F*$, the challenger implements the SigAndBlockGen() algorithm of our protocol and returns $\{\Phi * i, \Psi * i, t\}$ to A.

3. Challenge: For any $F*$ on which A previously made a store query, the challenger generates a challenge $C = \{Qi, \Lambda i\}$ and requests A to provide a proof of possession for the selected segments and corresponding coefficients.

4. Forge: Suppose the expected proof P should be $\{\mu i, \sigma i, \{\rho_{i\lambda}\}\ m\ \lambda=1\}$, which can pass the verification with Eq.(15). However, the adversary A generates a forgery of the proof as $P' = \{\mu'_i, \sigma'_i, \{\rho'_{i\lambda}\}\ m\ \lambda=1\}$. If the P' can still pass the verification

• Case 1: $\sigma' i \neq \sigma i$;

• Case 2: $\sigma' i = \sigma i$, but at least one of the following inequalities should be satisfied : $\mu' i \neq \mu i$, $\rho' i\lambda \neq \rho i\lambda$ with $1 \leq \lambda \leq m$; then adversary A wins this game, otherwise, it fails.

Theorem 3: If the authenticator scheme is existentially unforgeable and adversary A is able to win Game 1 with non-negligible probability ϵ, then there exist a PPT algorithm S that can solve the CDH problem or DL(Discrete Logarithm Problem) problem with non-negligible probability ϵ'.

Proof: See Appendix D. C.

C. Regeneration-unforgeable

Noting that the semi-trusted proxy handles regeneration of authenticators in our model, we say our authenticator is regeneration-unforgeable if it satisfies the following theorem.

Theorem 4: The adversary (or proxy) can only regenerate a forgery of authenticator for invalid segment from certain coded block(augmented) and pass the next verification with negligible probability, except that it implements the Repair procedure correctly.

D. Resistant to Replay Attack

Theorem 5: Our public auditing scheme is resistant to replay attack mentioned in [[7], Appendix B.], since the repaired server maintains identifier η' which is different with the corrupted server η. V.

VII. CONCLUSION

In this Paper we propose an open evaluating plan for the recovering code-based distributed storage framework, where the information proprietors are favored to assign TPA for their information legitimacy checking. To secure the first information protection against the TPA, we randomize the coefficients before all else rather than applying the visually impaired strategy amid the inspecting procedure. Considering that the information

proprietor can't generally stay online in rehearse, so as to keep the capacity accessible and undeniable after a pernicious debasement, we present a semi-trusted intermediary into the framework show and give a benefit to the intermediary to handle the reparation of the coded squares and authenticators. To better fitting for the recovering code-situation, we outline our authenticator in light of the BLS signature. This authenticator can be proficiently created by the information proprietor at the same time with the encoding methodology. Broad examination demonstrates that our plan is provable secure, and the execution assessment demonstrates that our plan is exceedingly effective and can be attainably coordinated into a recovering code-based cloud capacity framework.

VIII. REFERENCES

[1] A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "Above the clouds: A berkeley view of cloud computing," Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS, vol. 28, p. 13, 2009.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07. New York, NY, USA: ACM, 2007, pp. 598– 609.

[3] A. Juels and B. S. Kaliski Jr, "Pors: Proofs of retrievability for large files," in Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 584–597.

[4] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "Mr-pdp: Multiplereplica provable data possession," in Distributed Computing Systems, 2008. ICDCS'08. The 28th International Conference on. IEEE, 2008, pp. 411–420.

[5] K. D. Bowers, A. Juels, and A. Oprea, "Hail: a high-availability and integrity layer for cloud storage," in Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009, pp. 187–198.

[6] J. He, Y. Zhang, G. Huang, Y. Shi, and J. Cao, "Distributed data possession checking for securing multiple replicas in geographicallydispersed clouds," Journal of Computer and System Sciences, vol. 78, no. 5, pp. 1345–1358, 2012.

[7] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote data checking for network coding-based distributed storage systems," in Proceedings of the 2010 ACM workshop on Cloud computing security workshop. ACM, 2010, pp. 31–42.

[8] H. Chen and P. Lee, "Enabling data integrity protection in regeneratingcoding-based cloud storage: Theory and implementation," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 407–416, Feb 2014.

[9] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 9, pp. 1717–1726, 2013.

[10] Y. Zhu, H. Hu, G.-J. Ahn, and M. Yu, "Cooperative provable data possession for integrity verification in multicloud storage," Parallel and Distributed Systems, IEEE Transactions on, vol. 23, no. 12, pp. 2231– 2244, 2012.

[11] A. G. Dimakis, K. Ramchandran, Y. Wu, and C. Suh, "A survey on network codes for distributed storage," Proceedings of the IEEE, vol. 99, no. 3, pp. 476–489, 2011.

[12] H. Shacham and B. Waters, "Compact proofs of retrievability," in Advances in Cryptology-ASIACRYPT 2008. Springer, 2008, pp. 90– 107.

[13] Y. Hu, H. C. Chen, P. P. Lee, and Y. Tang, "Nccloud: Applying network coding for the storage repair in a cloud-of-clouds," in USENIX FAST, 2012.

[14] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in INFOCOM, 2010 Proceedings IEEE. IEEE, 2010, pp. 1–9.

[15] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013. IEEE TRANSACTIONS ON INFORMATION AND SECURITY Vol 1 No 2015

[16] C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards secure and dependable storage services in cloud computing," Service Computing, IEEE Transactions on, vol. 5, no. 2, pp. 220–232, May 2012.

[17] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," Journal of Cryptology, vol. 17, no. 4, pp. 297–319, 2004.

[18] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," Information Theory, IEEE Transactions on, vol. 56, no. 9, pp. 4539–4551, 2010.

[19] T. Ho, M. Medard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and ´ B. Leong, "A random linear network coding approach to multicast," Information Theory, IEEE Transactions on, vol. 52, no. 10, pp. 4413– 4430, 2006.

[20] D. Boneh, D. Freeman, J. Katz, and B. Waters, "Signing a linear subspace: Signature schemes for network coding," in Public Key Cryptography–PKC 2009. Springer, 2009, pp. 68–87.

[21] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in Advances in CryptologyłCRYPTO 2001. Springer, 2001, pp. 213–229.

[22] A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for fr-reduction," IEICE transactions on fundamentals of electronics, communications and computer sciences, vol. 84, no. 5, pp. 1234–1243, 2001.

Publish Research Article

Dear Sir/Mam,

We invite unpublished Research Paper,Summary of Research Project,Theses,Books and Book Review for publication.

Address:- Dr. Ashak Hussain Malik House No-221, Gangoo Pulwama - 192301 Jammu & Kashmir, India
Cell: 09086405302, 09906662570,
Ph No: 01933212815
Email:- nairjc5@gmail.com, nairjc@nairjc.com , info@nairjc.com
Website: www.nairjc.com