Finger Print Authentication For Improved Security And Public Auditing For Cloud Storage

Ankush Shrirao[1], Ayushi Bawankar[2], Apeksha Panwelkar[3], Priyanka Banswani[4]
[1, 2, 3] Dept of Electronics & Telecommunication Engineering
[4]Assistant Professor, Dept of Electronics & Telecommunication Engineering
[1, 2, 3, 4] G.H. Raisoni College of Engineering, Nagpur

Abstract- *Cloud computing is one of the rising innovations, that takes set of associations clients to the following level. One of the real difficulties in this innovation is Security. Biometric frameworks give the response to guarantee that the rendered administrations are gotten to just by a legitimate client or an approved client and nobody else. Biometric frameworks perceive clients based on behavioural or physiological attributes. Likewise, information honesty upkeep is the significant target in cloud storage. It incorporates try out utilizing TPA for unapproved get to. This work executes ensuring the information and recovery of information in the event that somebody misuses it. This activity will be doled out to a Proxy server. The information of the clients will be put away in public and private region of the cloud. With the goal that lone public cloud information will be gotten to by client and private cloud will stay more secured. Once any unapproved adjustment is made, the first information in the private cloud will be recovered by the Proxy server and will be come back to the client. This paper achieves another imitation of a security framework where in clients bring to the table numerous biometric finger prints amid Enrolment for an administration. The way toward consolidating conventional client id and secret word instrument alongside bio metric picture preparing method finger print acknowledgment is completely investigated for enhancing security in public cloud foundation. The likelihood of presenting another cloud benefit as "Bio-metric as a Service" is additionally investigated.*

Keywords- Cloud Computing, Data Security, Regenerating Codes, Public Audit, Privacy Preserving, Finger Print Authentication

I. INTRODUCTION

Cloud computing is perceived as another option to conventional data innovation because of it is inherent asset offering to low support qualities. In cloud computing, the cloud specialist co-ops (CSPs, for example, Amazon and others can convey different support of cloud clients with the assistance of capable server farms. By moving the nearby information administration frameworks into cloud servers and clients may appreciate superb administrations and spare critical ventures on them neighbourhood foundations. A standout amongst the most key administrations is offered by cloud suppliers was information storage. How about we consider a constrained information application the organization permits its staffs in a similar gathering or office to put away and shared records in the cloud. By using the cloud that the staffs could be totally discharged from the troublesome nearby information storage facility and upkeep. Notwithstanding, it is likewise represents a noteworthy hazard to the privacy of those put away records. Particularly the cloud servers is overseen by cloud suppliers isn't completely trusted by clients while the information records put away in the cloud may be private and delicate, for example, marketable strategies. To jelly information privacy is essential answer for scramble information records and after that transferred the encoded information into the cloud [2]. Shockingly, the outlining of the proficient and secure information sharing plan for bunches in the clouds isn't a simple errand because of the accompanying testing issues.

As a matter of first importance character the privacy is being a standout amongst the most critical confinement for the wide organization of cloud computing. Here not holding the ensured of character privacy client might be unwilling to attach in cloud computing frameworks in light of the fact that their genuine personalities can be effectively unveil to cloud suppliers and furthermore assailants. Then again its unrestricted character privacy may bring about the mishandle of privacy for instance the wrongdoing staff could misdirect others on the organization to sharing false records without being traceable. In this way, traceability and which are empowers the TPA to uncover the genuine personality of a client's are likewise profoundly attractive. Second, it is profoundly prescribed that any part in the gatherings should ready to completely appreciate the information putting away and in addition sharing administrations gave by the cloud which are characterized as the different proprietor way. Contrast and the single proprietor way where just the gathering supervisor could store and alter information in the cloud, the various proprietor conduct are more adaptable in handy applications.

All the more solidly, every client in the gatherings can not just read information and furthermore change his or her piece of information in the whole information document shared to the organization. Last yet not the slightest so bunches are ordinarily powerful practically speaking, e.g., new staff collaboration and current worker disavowal in the organization. The progressions of enrolment make secure information sharing to a great degree tricky. On one hand, the unknown frameworks can challenges present day conceded clients can take in the substance of information documents put away before their participation, since it isn't workable for new allowed clients to contact with mysterious information proprietors and access the relating unscrambling keys. Then again the effective enrolment annuls system without refreshing the characterized keys of the rest of the clients wants to limit the intricacy of key administration. Numerous security plans for information sharing on untrusted servers had been proposed. In these methodologies, information proprietors can store the encoded information records in sceptical storage with conveyed the comparing unscrambling keys are just too approved clients. In this manner, unapproved clients and in addition storage servers couldn’t take in the substance of the information records since they don't know about the decoding keys.

Be that as it may, the many-sided quality of client cooperation and annulment in these plans are directly expanding with the quantities of information proprietors and the quantity of repudiated clients, separately. By setting the gathering with a solitary characteristic, we proposed a protected provenance conspire is set up on the figure content strategy trait built up encryption procedure, which are enables any part in a gathering to impart information to others.

Be that as it may, the issue of client disavowals are not tended to in their plan. We exhibited a versatile and fine grained information get to control plot on cloud computing based on the key arrangement properties based on by encryption method with the execution of Proxy Server. Lamentably, the single proprietor way prevents the reception of theirs plan into the case, where all clients are conceded to store and offer information. Consequently we are executing a gathering based Data proprietor framework.

This paper concentrates on a cloud based system for taking care of the subtle elements of any element: an individual, an association's information and application in the cloud in a more secured way utilizing enhanced biometric picture handling procedures. The utilization of cloud benefits by an association or an individual client decreases the capital venture cost to the repeating costs. Since the cloud client does not claim any assets; rather utilize the administrations from the cloud on pay/utilize premise or generally alluded as membership premise. When we don't possess any physical assets, the association is calmed of support of assets as well; in this manner, an association may focus on its standard business; as opposed to IT foundation.

The significance of biometrics-based confirmation frameworks that are intended to withstand security issues when utilized in basic applications, particularly in free remote applications, for example, online business, keeping money is to be unmistakably tended to. Our concentration is towards utilizing such bio-metric validation frameworks in cloud condition where an endeavour’s business information is put away in remote servers.

II. RELATED WORK

A. The Need for Bio-metrics

The connection amongst man and man has diminished and the connection amongst man and machine has expanded. The advanced separation is narrowing down. While discussing the discussion amongst man and machine, the procedure of recognizable proof emerges. When we utilize machines in public condition say the cloud, and after that recognizable proof of the client is particularly vital. The thin hole amongst man and machine is lessened utilizing different strategies and bio-measurements verification is likewise one vital innovation among them. The different bio-metric systems utilized as a part of the present day are: confront, fingerprint, iris picture, voice acknowledgment, hand geometry, retinal example, signature, thermo-grams and so forth [2] Some bio-metric procedures are still in pipeline viz. scent, ear, keystroke, DNA, hair. In our paper, fingerprint validation instrument is broke down and the best approach to consolidate such verification component in a cloud domain to give secured administrations to the information proprietor is talked about.

B. Finger-print Identification

The procedure of recognizable proof in this organized world is unavoidable. When we utilize web administrations like mail, keeping money, online business, and for the present day, when we utilize cloud, we have recognizable proof systems like client id, watchword, one time stick and so forth. Recognizable proof process [2] can be surely knew as: 'something you have's and 'something you know'. An illustration situation is: we have ATM card and we know its PIN number. Consider the possibility that we lose our A TM card and the vast majority of the clients have their PIN as year of birth sort of information. On the off chance that a sham has our A TM and has our PIN, at that point the distinguishing proof process falls flat.

With a specific end goal to enhance this defenceless distinguishing proof process, we utilize bio-measurements to fortify the ID procedure in this organized world. What could be taken as bio-metric recognizable proof? The appropriate response is any human physiological or behavioural trademark could be accounted as a bio-metric recognizable proof gave that fulfils couple of properties as nitty gritty: I) all-inclusiveness - all human ought to have, ii) uniqueness - no two humans have the same, iii) perpetual quality - ought not fluctuate with time and iv)collectability-quantifiable. The bio-metric based verification is broadly utilized as a part of a significant number of the applications: managing an account, internet business and now in cloud condition too to guarantee security of information in storage too amid correspondence.

C. Finger Print - Authentication

Fingerprints are remarkable among people. In the field of Astrological Science, fingerprints give imperative data to anticipate about future existence of a person. Finger prints are graphical stream like edges in palm of a human. Finger print is caught carefully utilizing a finger print scanner, such equipment segments are being joined in the present day cell phones. Consequently adding biometrics security to the cloud framework won't be an issue for the present day as its equipment partner is more affordable and can likewise be effortlessly interfaced with the current framework. Edge consummation and edge bifurcation are the two essential trademarks includes in finger print of any human client. A typical calculation has been produced and generally utilized: “programmed fingerprint recognizable proof framework" that comprises of two stages: disconnected and on-line. In the disconnected stage, a fingerprint is caught utilizing the equipment gadget, and the caught picture's quality is enhanced utilizing distinctive calculations; at that point noteworthy highlights of the fingerprint are removed and put away in a database as a layout. In the on-line stage, the fingerprint of the client is caught, upgraded and highlights of the fingerprint are extricated, and is contrasted and the layout put away in the database amid on-line stage. The means are shown in the figure 1.

Despite the fact that we have numerous other biometric arrangements, fingerprint recognizable proof framework is generally utilized for some reasons. Contrasting with other biometric methods, the benefits of fingerprint-based ID are as definite underneath:

1) Uniqueness of the fingerprint - the particulars points of interest of individual edges and wrinkles are perpetual and constant.
2) The fingerprint is effortlessly caught utilizing minimal effort fingerprint scanner.
3) Fingerprint is one of a kind for each individual.

So it can be utilized to shape various levels of security to enhance cloud frameworks.

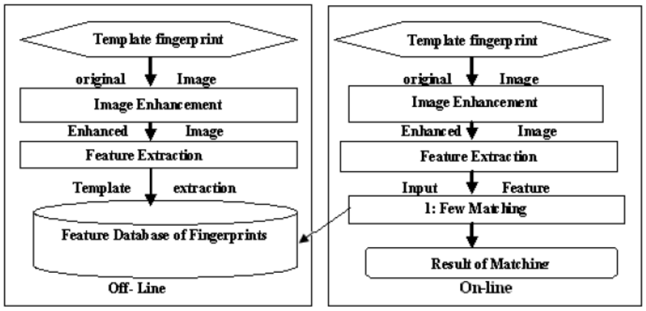

Figure 1 Stream of Diagram speaking to the Fingerprint Identification

The above figure obviously clarifies the straightforward approach of fingerprint check. In disconnected process, the fingerprint of all clients are caught and put away in a database. Before putting away the crude or unique picture, the picture is upgraded. The fingerprint picture when caught out of the blue may contain undesirable information i.e. commotion. Since our hands being the most utilized piece of our body may contain wetness, dry, sleek or oil; and these pictures might be dealt with as clamor while catching the first finger print. Furthermore, thus, to expel the commotion, picture improvement methods like versatile separating and versatile thresholding.

Figure 2 Unique Fingerprint Image

The standard shape factor for the picture estimate is 0.5 to 1.25 inches square and 500 dabs for every inch. In the above unique picture, the procedure of versatile sifting and thresholding are completed. The repetition of parallel edges is a helpful trademark in picture improvement process. We can decide the stream by applying versatile, coordinated channel even though there might be discontinuities in a specific edge. This channel is connected to each pixel in the picture and the off base edges are expelled by applying coordinated channel. In this manner, the commotion is evacuated and the upgraded picture is appeared in figure 3.

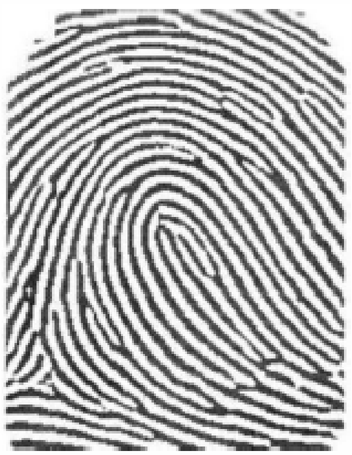

Figure 3 Upgraded Fingerprint Image

The upgraded picture experiences highlight extraction process wherein: binarization and diminishing happen. All fingerprint pictures don't share same differentiation properties as the power connected while squeezing may change for each case. Consequently, the difference variety is evacuated by this binarization procedure utilizing neighborhood versatile thresholding. At the point when the width of the edges is decreased down to a solitary pixel, an enhanced fingerprint picture is acquired and this component extraction process is called Thinning. The resultant component extraction is appeared underneath figure 4.

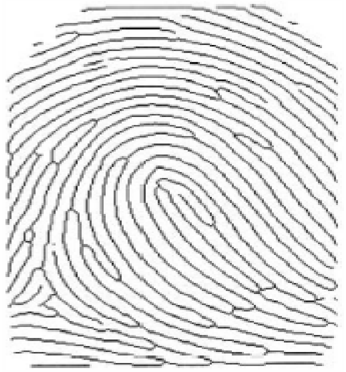

Figure 4 Highlight Extractions - After Binarization and Thinning

The procedure of particulars extraction is done as the last advance in includes extraction and after that the last picture is put away in database. At the point when the picture is weakened, it is anything but difficult to remove the highlights: the particulars are direct to identify and the endings are found at the end purposes of thin lines and the bifurcations are found at the intersections of three lines. When we can recognize substantial minutia focuses in a diminished picture, at that point we need to separate two critical information from the improved, diminished picture based on the huge minutia focuses: they are edge finishing (x,y) area, and the bearing of the closure bifurcation. Despite the fact that minutia sort is generally decided and put away, many fingerprint coordinating frameworks don't utilize this data since separation of one from the other is regularly troublesome. The aftereffect of the element extraction organize is what is known as a minutia layout, as appeared in figure 5. This is a rundown of particulars with going with characteristic esteems. An estimated go on the quantity of details found at this stage is from 10 to 100. On the off chance that every minutia is put away with sort (1 bit), area (9 bits each for x and y), and bearing (8 bits), at that point each will require 27 bits - say 4 bytes - and the layout will require up to 400 bytes. It isn't remarkable to see format lengths of 1024 bytes.

Presently, the online procedure begins. At the confirmation organize, the fingerprint of the cloud client who needs to get to cloud administrations is caught and his layout is contrasted and the fingerprint database. Details are gathered based on their closeness and alluded as neighborhood particulars. Or maybe checking every last prepared minutia with the put away minutia, this gathering of neighborhood details helps in simple and snappier coordinating procedure. Normally, at least three particulars are gathered as one neighborhood details.

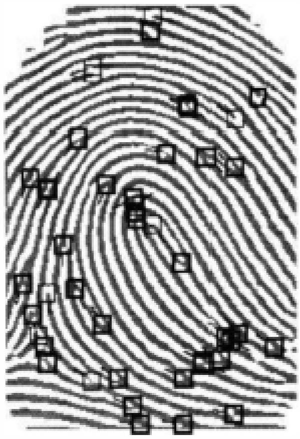

Figure 5 Details Template

Each of the area details is situated at a specific separation and relative introduction from each other. To start with coordinating of neighborhood particulars is done between the two pictures; if closeness is found to an acceptable edge, at that point few neighborhood details are tested and the individual minutia in the area details of the clients current fingerprint picture and the database put away picture are looked at further. As every minutia has its own qualities of sort and minutia heading, individual details are likewise analysed. In the event that correlation shows just little contrasts between the area in the put away fingerprint and that in the present client's fingerprint, at that point these areas are said to coordinate. This procedure is done for all the area designs comprehensively and if enough similitudes are discovered, at that point the fingerprints are said to coordinate. Another strategy for coordinating the fingerprint pictures is called layout coordinating. A diagram design must be brought about by interconnecting the particulars and is contrasted and the states of charts joining fingerprint details. This is represented in Figure 6. An I: 1 coordinating can't be completed and we utilize edge esteem - named as match score, for the most part a number going in the vicinity of 0 and 1. Higher the esteem, higher is the match.

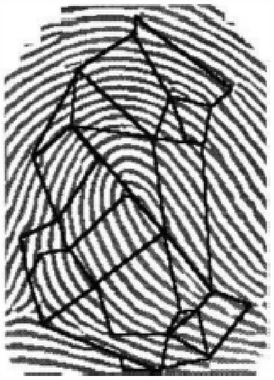

Figure 6: Few-Matching in online process

III. LITERATURE REVIEW

Jian Liu, Kun Huang, Hong Rong, Huimei Wang and Ming Xian in [1] proposes a public auditing plan for the regenerating-code-based cloud storage framework, where the information proprietors are special to appoint TPA for their information legitimacy checking. To secure the first information privacy against the TPA, They randomize the coefficients at the outset instead of applying the visually impaired procedure amid the auditing procedure. Existing remote checking strategies for regenerating-coded information just give private auditing, requiring information proprietors to dependably remain on-line and handle auditing, and repairing, which is now and then unreasonable. Accordingly an intermediary is utilized who works without information proprietor for taking care of the recovery issue of fizzled authenticators. In this manner information proprietor has no compelling reason to dependably remain on-line. Two or three keys produce a novel public certain authenticator which ensure unique information privacy against the outsider examiner and safeguard the privacy in cloud storage.

M. Li, S. Yu, K. Ren, and W. Lou in [3] proposed a patient-driven structure and a suite of components for information get to control to PHRs put away in semi put stock in servers. To infer fine-grained and versatile information get to control for PHRs, they impact ascribe based encryption calculation to encode every patient's PHR record. They isolate the clients in the PHR framework into various security spaces that enormously lessens the key administration multifaceted nature for proprietors and also clients. A high level of patient's privacy is guaranteed at the same time by abusing multi specialist ABE. Individual wellbeing record is a patient-driven system for wellbeing data trade, which is constantly outsourced to be put away at outsider cloud storage. Be that as it may, there is a wide privacy worry as individual wellbeing data could be presented to those outsider cloud servers and to unapproved parties. This plan gives versatile and secure sharing of individual wellbeing records in cloud computing utilizing Attribute-Based Encryption.

H. Chen and P. Lee outline and execute a useful information trustworthiness security conspire [4] for a particular regenerating code, while preserving its central properties of adaptation to non-critical failure and repair-movement sparing. Plunge plot is planned under a portable Byzantine antagonistic system, and empowers a customer to confirm the respectability of irregular subsets of outsourced information against malevolent debasements. It works under the basic supposition of thin-cloud storage and enables distinctive parameters to be tweaked for an execution security exchange off. This executes and assesses the overhead of DIP plot in a genuine cloud storage test bed under numerous parameter decisions. These further breaks down the security qualities of DIP conspire through scientific models. It exhibits that remote honesty checking can be plausibly coordinated into regenerating codes in down to earth arrangement. This assess the running circumstances of various essential operations, for example, Upload, Check, Download, and Repair, for various parameter decisions.

C. Wang, Q. Wang, K. Ren, and W. Lou [5] proposes a viable and adaptable circulated storage confirmation systems with unequivocal dynamic information support to guarantee the accessibility of clients information in the cloud. It relies upon eradication amending code in the document dispersion readiness model to supply redundancies and affirmation about the information steadfastness against Byzantine servers, where a storage server can be bomb in irregular ways. This development exceedingly limits the correspondence and additionally storage overhead when contrasted with the old replication-based document appropriation show. By utilizing Homomorphic token with dispersed check of deletion coded information, this accomplishes the accuracy of storage protection and additionally information mistake confinement, when the information defilement has been distinguished amid the confirmation of storage rightness. This plan can give the assurance of concurrent restriction of information mistakes and the distinguishing proof of the getting into mischief servers.

J. He, Y. Zhang, G. Huang, Y. Shi, and J. Cao [6] gives speculations to settling the Finding an Optimal Spanning Tree in a Complete Bidirectional Directed Graph (FOSTCBDG) issue through tallying all the accessible ways that infections assault in clouds organize condition. Additionally, This assistance the cloud clients to accomplish productive numerous imitations information ownership checking by a rough calculation for handling the FOSTCBDG issue, and the viability is exhibited by a test think about. This paper, give a novel proficient Distributed Multiple Replicas Data Possession Checking (DMRDPC) plan to conquer the two weaknesses of focus arranged checking. The DMRDPC plot initially finds an ideal traversing tree to characterize the fractional request of booking numerous reproductions information ownership checking. This is an exceptionally complex assignment, since data transfer capacities have geological assorted variety on various connections of various imitations and the transmission capacities between two copies are deviated, and subsequently it is important to locate an ideal spreading over tree with the verifier as the root in a Complete Bidirectional Directed Graph (CBDG), which associates the verifier and every one of the reproductions. At that point, as per the planning halfway request, the information ownership checking from the verifier, who checks the majority of its kids, is begun. Those reproductions that have passed the confirmation can continue checking the information ownership of their youngsters. On the off chance that a few imitations flop in the checking, they can acquire one duplicate from its parent before they keep checking the information ownership of their own youngsters.

The objective of Fox, R. Grifth, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica [7] to clarify different terms, gives basic equations to evaluate connection between of cloud and traditional Computing, and distinguish the best specialized and non-specialized hindrances and additionally chances of Cloud Computing. IT associations have communicates the worries of major basic issues, for example, security that exist with the broad execution of cloud computing. These sorts of concern originate from the way that information is put away remotely from the client's area; it can be put away at any area. Security is most contended about issues in the cloud computing field; many endeavours take a gander at cloud computing watchfully because of anticipated security dangers.

IV. PROPOSED SYSTEM

The framework comprises of cloud server and numerous clients. This framework is valuable for business applications. Cloud server enables clients to store their encoded squares of records and regarded hash. For this encryption of record obstructs, there is an appropriated KDC. Framework utilizes dispersed KDC, in light of the fact that on the off chance that one KDC is occupied another will be utilized. Along these lines, the heap on KDC is appropriated and execution in moved forward. By utilizing key, client can encode the squares of document. Before putting away the square records on cloud storage, client produce the hash of piece documents and store it on server.

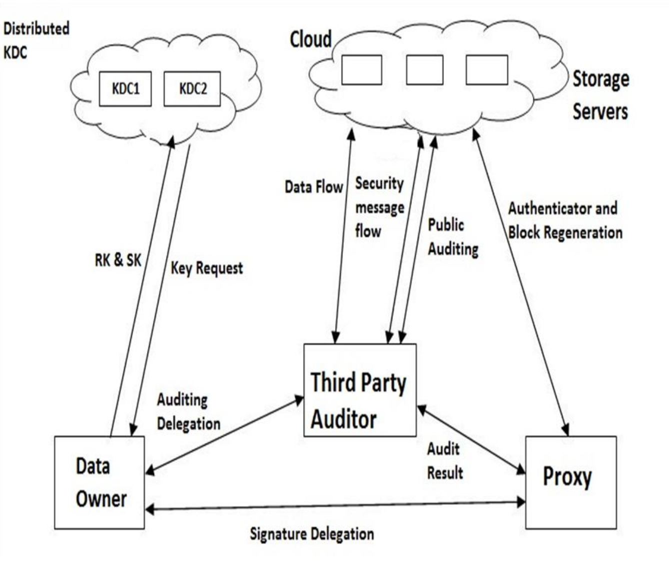

Figure 1 System Architecture

Client can demand to TPA for record square honesty checking, store at cloud server. TPA stores the hash of pieces. It asks for hash of specific document asks for by client for uprightness checking. It thinks about the got hash of document obstruct with hash store in its database. In the event that the hash is matches, it sends the message to client, which shows that the documents store on server isn't defiled. In the event that the document is tainted, TPA asking for intermediary to adjust it. Intermediary having recovery code. By utilizing this recovery code, intermediary recuperate the records debased on server. And afterward TPA again confirms that, regardless of whether that record is recoup or not. At long last TPA tells the client that the record is recuperated.

V. CONCLUSIONS

To keep up the adequacy and to keep up information defilement from data debasement in information storage reinforcement system are debate assignments. Putting away information parts on various servers diminishes the odds of data misfortune however these information piece storage on different server for data reinforcement extends storage space. This information pieces may be debased store on cloud server. To recuperate the tainted information hinders, our proposed framework executes regenerating coding procedure at intermediary, if any pieces is misfortune or degenerate. Likewise to diminish the computation cost, framework utilizes cloud servers for putting away the data, since cloud server has a few advantages, for example, security, ease, high accessibility, and so on. Framework utilizes conveyed KDC, to limit the heap at single KDC. In this, if any one KDC is occupied, client asking for key to another KDC. To compute the execution of our framework, different testicles did on dataset including number of records. The document measure shifts from 1 kb to 100 MB. The test outcomes demonstrates that, our framework is perform best than existing one, regarding, storage space, cost, accessibility of information, limit over-burden at KDC and recuperation of records.

REFERENCES

[1] 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 ˆa07. 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] 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. 1717ˆa1726, 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] 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] 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, andW. Lou, “Privacy-preserving public auditing for secure cloud storage,” Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362-375, 2013.

[16] 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. 220ˆa232, May 2012.

[17] Boneh, B. Lynn, and H. Shacham, “Short signatures from the weil pairing,” Journal of Cryptology, vol. 17, no. 4, pp. 297ˆa319, 2004.

[18] 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. 4539ˆa4551, 2010.

[19] T. Ho, M. MAˆ ´edard, 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. 4413ˆa 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 Cryptology CRYPTO 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.

[23] R. Gennaro, J. Katz, H. Krawczyk, and T. Rabin, “Secure network coding over the integers,” in Public Key Cryptography-PKC 2010. Springer, 2010, pp. 142-160.

[24] S. Goldwasser, S. Micali, and R. Rivest, “A digital signature scheme secure against adaptive chosen message attacks,” SIAM Journal of Computing, vol. 17, no. 2, pp. 281-308, 1988.

[25] Neha T, P.S Murthy, “A Novel Approach to Data Integrity Proofs in Cloud Storage”, Volume 2, Issue 10, October 2012.