Deduplication Supporting Strong Privacy Protection for Cloud Storage

K.Makanyadevi[a], S.Divya[b], P.Janani[c], V.Pooranya[d] and R.Savitha[e]

[a] Department of Computer Science and Engineering , M.Kumarasamy College of Engineering, Karur, Tamil Nadu, India -39113

[b,c,d,e] Department of of Computer Science and Engineering , M.Kumarasamy College of Engineering, Karur, Tamil Nadu, India -639113

Article History: Received: 11 January 2021; Accepted: 27 February 2021; Published online: 5 April 2021

Abstract: Cloud computing is developing as the following disruptive utility worldview. It gives broad capacity capabilities and an environment for application engineers through virtual machines. Third-party inspectors (TPAs) are becoming more common in cloud computing implementations. Consequently, including reviewers comes with its issues such as belief and preparing overhead To achieve productive examining, we ought to (1) fulfill efficiently auditing without asking the information area or introducing preparing overhead to the cloud client; (2) avoid presenting unused security vulnerabilities amid the auditing handle There are various security models for safeguarding the CCs (Cloud Client) information within the cloud. The TPA methodically analyzes the prove of compliance with set up security criteria within the connection between the CC and the Cloud Benefit Supplier (CSP). A novel strategy to create the record for a copy check, and utilize a modern methodology to create the key for the record encryption. In expansion, the client as it were must perform lightweight computation to produce information authenticators, verify cloud information keenness, and recover the information from the cloud.

Keywords: deduplication, Cloud storage auditing, deduplication, strong privacy protection, data security, cloud storage.

1. Introduction

Data deduplication is one of the maximum well-preferred technologies in the garage right now as it allows organizations to store plenty of lots of coins on garage prices to save the data and at the bandwidth prices to move the data whilst replicating it offsite for DR. After all, if you store less, you would like less hardware. If you'll deduplicate what you store, you'll better utilize your existing space for storing, which may economize by using what you've got more efficiently.

If you store less, you furthermore may copy less, which again means less hardware and backup media as computers spread, heaps of gadget identity techniques taking advantage of the virtual processor is developed, and identification for discrete-time systems has been studied due to the facility for analysis and processing. Cloud computing is an evolving technology that has helped several companies and developers save money and time while also providing comfort to end-users.

As a result, cloud capacity incorporates a wide extend of applications since businesses can for all intents and purposes store their information without disturbing the whole framework. Cloud computing offers the best clients a few benefits, counting fetched investment funds, the capacity to get to data in any case of the scene, productivity, and security. The majority of existing authentication schemes has flaws. As a result, graphical passwords are the most common authentication method, in which users verify the image by clicking on it.

Image-based successful authentication is the foundation of our proposed framework. When the administrator uploads the cloud, the picture is divided into four bits. The admin will have two parts, and users in that community will be able to see the other two parts. The pseudo-random generator technique is used to split the images at random. When a user wants to download a file, the user will submit a requisition to the appropriate admin, which is split into two sections. The administrator will check both pieces, and if the authentication is effective, the file will be sent to the user in an encrypted format. Information deduplication is one of the strategies utilized to unravel the issue of data redundancy. Deduplication methods are frequently utilized interior the cloud server to diminish the server's separation.

To dodge unauthorized get to information and the creation of copy information within the cloud, the encryption procedure is utilized to scramble information until it is put away on a cloud server. Business-critical data and processes are often stored in cloud storage. As a result, maintaining good trust relationships between cloud users and cloud service providers necessitates a high degree of protection. As a result, this paper suggests various cloud storage to combat security threats.

As a result, traditional types of data storage, such as files and databases, are separated and stored in different cloud storage services. There are a variety of deduplication techniques available, including 1) location-based deduplication. 2) Deduplication based on time 3) Deduplication of Blocks Client-side and server-side deduplication are the two forms of location-based deduplication. On the client-side, the information is deduplicated and sent to the server-side. On the server-side, the data is sent to the server first, and then de-duplicated at the server-side. In time-primarily based totally, there are inline and postfixes. In bite primarily based totally, the facts are cut up into numerous chunks, and information is deduplicated.

2. Literature Survey

[1]GNU Multiple Precision Arithmetic Library is an unfastened library for arbitrary-precision arithmetic, going for walks on signed integers, rational numbers, and floating-aspect numbers. There aren't any real limits to the precision besides those implied with the aid of using the to be had a memory.

[2] A shopper that has spared data at an endowed server can affirm that the server has the interesting data without recovering it. The adaptation produces probabilistic proofs of proprietorship by means of a implies of examining arbitrary units of pieces from the server, which strikingly diminishes I/O costs. The customer proceeds a steady amount of metadata to affirm the confirmation.

[3]MLE gives a manner to obtain stable deduplication (space-green stable outsourced garage), an intention presently centered with the aid of using several cloud garage providers. We offer definitions each for privateness and for a shape of integrity that we name tag consistency.

[4]Attribute-primarily based encryption (ABE) has been broadly utilized in cloud computing wherein a records backer outsources his/her scrambled records to a cloud carrier backer, and may rate the records with clients owning exact accreditations (or properties). In any case, the rise to vintage ABE machines is not a valuable resource for steady deduplication, usually vital for evacuating copy duplicates of the break-even with actualities to shop capacity area and arrange transmission capacity.

[5]With the developing require for wonderful healthcare and the developing esteem of care, unavoidable healthcare is taken into thought as a mechanical alternative to manage around world wellness issues. In particular, the most recent propels within the Web of Things have caused the advancement of the Web of Therapeutic Things (IoMT). In spite of the fact that such low-value and unavoidable detecting contraptions may need to likely adjust the cutting-edge responsive care to preventative care, the security and privateness issues of such detecting machines are regularly neglected.

[6](1) convergent encryption, which allows reproduction files to be grouped into a single record gap even though the files are encrypted with unique user keys; and (2) SALAD is a Self-Arranging Lossless format Associative Database (SALAD) that aggregates document information, fabric, and area information in a decentralized, adaptable, and fault-tolerant way. The reproduction-report coalescing method is scalable, highly accurate, and fault-tolerant, according to large-scale simulation experiments.

[7]Compared with conventional neighborhood garage, cloud garage is an extra budget-friendly preference due to the fact the faraway information middle can update customers for information control and maintenance, which could keep money and time at the collection of work. However, turning in information to an unknown Cloud Service Provider (CSP) makes the integrity of information come to be capability vulnerability.

[8]The Computerized Universe, which includes all information produced by PCs, Sensor Systems, GPS/Wi-Fi Area, Web Metadata, Web-Sourced Historical Information, Portable, Smart-Connected Gadgets, and Next-Generation Applications (to title many), is changing the way we devour and learn IT, as well as disturbing conventional trade models. The unparalleled and quick development of information is giving businesses with modern openings particular conceivable outcomes and challenges.

[9]Irrefutable Searchable Symmetric Encryption, as a pivotal cloud security method, permits clients to recover the scrambled records from the cloud by means of key terms and confirm the legitimacy of the diminish of comes about. Energetic substitution for cloud data is one of the greatest not unordinary places and necessities for data proprietors in such plans.

[10]With the appearance of information outsourcing, a way to effectively affirm the integrity of information saved at an entrusted cloud carrier provider (CSP) has emerged as a huge hassle in cloud storage. Provable statistics possession (PDP) is a version that lets in customers or a relied on the auditor to confirm whether or not or now no longer or no longer has CSP possessed the outsourced statistics without downloading it.

[11]Cloud carport structures are getting increasingly prevalent. A promising era that keeps up their cost down is deduplication, which shops best an single reproduction of rehashing information. Client-facet deduplication tries to ended up mindful of deduplication conceivable outcomes as of now on the buyer and shop the transmission capacity of bringing in duplicates of display records to the server.

[12]As the quantity of records increases, so does the call for online garage offerings, from easy backup offerings to cloud garage infrastructures. Although deduplication is simplest while carried out throughout more than one user, cross-consumer deduplication has severe privateness implications.

[13]The multi-author version, in which a large number of clients collaborate on shared files collaboratively and any company member may update the statistics through alteration, addition, and deletion operations have not been adequately studied as a significant safety property of cloud storage. Existing works beneath one of these multi-creator versions might carry massive garage prices to the third-celebration verifiers.

[14]The open cloud carport examining with deduplication is proposed to test the judgment of cloud records underneath beneath the circumstance that the cloud shops handiest a single generation of the indistinguishable archive from particular clients. To the first-class of our information, the show plans roughly cloud carport reviewing with deduplication cannot help semantic security for cloud records.

[15]We outline and discover non - polar compounds proof in this article (POR). A POR plot empowers an file or reinforcement benefit (verifier) to supply brief confirmation that an person (verifier) can recoup a rationale record F, i.e., that the archive preserves and accurately transmits document information necessary for the individual to obtain better F in its entirety.

[16] Deduplication is utilized by cloud capacities benefit suppliers such as Dropbox, Mozy, and others to hold locales with the asset of as it was putting away one copy of each report transferred. Customers, on the other hand, would lose money if they traditionally encrypt their files. This pressure is settled by message-locked encryption (the foremost unmistakable appearance of which is concurrent encryption).

[17] Information dseduplication may be a procedure for evacuating copy duplicates of information that has been broadly utilized in cloud carports to diminish capacity space and increment transfer speed.

[18]As the cloud storage generation matures over the next decade, outsourcing records to a cloud carrier for the garage will become a popular trend, enabling garage owners to save time and money on record maintenance and management.

[19]Data integrity has gotten a lot of attention as a middle-of-the-road security problem in dependable cloud storage. Data auditing protocols allow a verifier to examine the integrity of outsourced data without having to download it.

[20]The challenge of judgment reviewing for cloud deduplication capacity is examined in this paper. Particularly, within the same way, that we ensure the privacy of outsourced information, we moreover arrange to guarantee the security of deduplicated cloud capacity. With current works centered completely on Provable Information Ownership (PDP)/Proof of Retrievability (POR), we're either constrained to depend on a completely dependable intermediary server or compromise security and execution.

[21]The PBC (Pairing-Based Cryptography) library could be a free C library (discharged beneath the GNU Lesser Common Open Permit) based on the GMP library that performs the numerical operations that support pairing-based cryptosystems.

[22]An instrument known as Farther Information Astuteness Checking (RDIC) was concocted to confirm whether the outsourced records are kept intaglio without being completely downloaded, much appreciated to a prepare known as Inaccessible Information Keenness Checking (RDIC). At the time, A few RDIC plans empowered record proprietors with restricted computation or communication control to designate the confirmation venture to a third-party verifier.

[23]Clients can keep their data within the cloud rather than paying for neighborhood information capacity and support by utilizing cloud capacity services. Many insights astuteness inspecting plans have been proposed to guarantee the judgment of the statistics put away inside the cloud. A client should rent his private key to deliver insights verification tokens for data judgment inspecting in most, on the off chance that not all, of the winning schemes.

[24]Utilizing cloud capacity administrations, clients can protect their data inside side the cloud to dodge the use of community data capacity and upkeep. To create beyond any doubt the keenness of the measurements spared inside side the cloud, numerous insights judgment reviewing plans were proposed.

[25]Using cloud garage services, customers can keep their statistics within side the cloud to keep away from the expenditure of nearby statistics garage and maintenance. Numerous insights astuteness inspecting plans have been proposed to guarantee the judgment of the information put away within the cloud.

[26]The dynamic adjustment approach to the acknowledgment threshold is planned for knowledge uploading on this foundation. The proposed scheme, which is focused primarily on threshold dynamic modification, has excellent scalability and practicability, according to the results of the experiments and evaluation.

[27]Advertising durable records security to cloud clients while allowing well off programs may be a troublesome assignment. Analysts find different cloud stage structure alluded to as Information Assurance as a Benefit.

[28]The residences of the ultimate convergent encryption layer permit deduplication to take place naturally. Security is as a result traded for garage performance as for each record that transits from unpopular to famous status, garage area may be reclaimed.

[29]While Cloud Computing makes those blessings extra attractive than ever, it additionally brings new and hard protection threats toward users' outsourced data.

[30]With the quick development of cloud computing, increasingly more agencies would like to feature and maintain their records within side the general public cloud. When the components of the monetary organization of a business enterprise are bought via the method of any other business enterprise, the corresponding facts may be transferred to the acquiring business enterprise.

[31]Cloud garage offerings permit customers to place away facts and experience the excessive nice on-call for cloud packages without the pressure of consistent control in their software, hardware, and facts.

[32]To guard the user's privacy information, non-prevent information chains are decomposed into discrete information chains, and discrete information chains are prevented from being synthesized into non-prevent information chains.

[33]In this convention, we depend on eradication code for the accessibility, unwavering quality of insights, and utilize token pre-computation utilizing Sobol Grouping to confirm the astuteness of erasure-coded measurements within the locale of Pseudorandom Information in modern frameworks.

[34]Dispensed steady multi-celebration computation (SMC), wherein every peer is handiest concerned in steady computations with a number of the peers. We hypothesize dispensed SMC should permit us to obtain greater green and scalable computing solutions.

[35]Many present auditing schemes constantly expect TPA is dependable and independent. These paintings research the hassle of if positive TPAs are semi-depended on or maybe probably malicious in a few situations.

[36]The accessibility and keenness of customers' records spared inside side the cloud carport; clients need to assert the cloud carport remotely and intermittently, with the help of the pre-saved verification measurements and without putting away an adjacent reproduction of the records or recovering lower back the records all through confirmation.

[37]Remote statistics possession checking protocols permit trying out that a far-off server can access an uncorrupted file in this form of way that the verifier does now not need to comprehend earlier the complete file is being verified.

[38]Cloud computing may be a special computing show that gives helpful and on-demand get to a pool of configurable computing assets. Examining offerings are exceptionally pivotal to guarantee that the records are effectively facilitated inside side the cloud.

[39]With cloud computing and carport administrations, records are not most viably spared inside side the cloud, be that as it may routinely be shared among a gigantic amount of clients in a gather. It remains slippery, in any case, to put out an unpracticed component to review the keenness of such shared measurements, at break-even with time as in spite of the fact that holding character protection.

[40]In cloud capacity frameworks, reality proprietors have their truths on cloud servers, and clients (realities buyers) can get appropriate get to the actualities from cloud servers. Due to the data outsourcing, in any case, this unused worldview of data web site facilitating supplier moreover presents unused assurance challenges, which calls for a fair-minded examining supplier to test the data judgment inside side the cloud.

[41]Manage cloud-primarily based applications, services, and your whole infrastructure and get records on performance, security, and patron behavior. Uncover malicious activities, if any, with AI-powered reporting, optimize cloud environment with integrated quality exercise recommendations, and automate incident remediation for a man or woman AWS resources.

[42]Allowing the cloud carrier users (CSUs) to offer their protection alternatives with the favored cloud services, supplying a conceptual mechanism to validate the protection controls and internal safety hints of cloud provider providers.

[43]A fault-tolerant, self-healing storage device that auto-scales up to 128TB by the database case. With up to 15 low-latency research replicas, point-in-time healing, non-prevent backup to Amazon S3, and replication through three Availability Zones, it can provide extreme typical overall efficiency and availability.

[44]Never stress almost losing a record once more, with amplified form history and erasure recuperation that's super simple for end-users — so IT can center on more imperative work than reestablishing records.

[45]Astuteness checking turns into significant to steady records in a cloud environment. It is basic to create certain that the spared truths are not one or the other compromised nor debased. Numerous current conventions screen clients ' tricky realities through sharing the encryption and unscrambling keys with the cloud server.

[46]Detect and prevent malware attacks to keep your stored data secure. Seamlessly integrate multiple storage instances to review and manage the health of all your data in one unified view

[47]Designed mainly to optimize your workloads for the cloud, Rapid Scaling debts for pace and license availability to scale cloud assets back down to zero even as they'll be now not needed, bringing cloud charges closer than ever to a particular demand.

[48]Expanse partners with exclusive Internet groups to leverage the wonderful to have records on malware command and control and exclusive malicious pursuits like net application attacks. We display for communications among your community and infrastructure already recognized to be attacking your peers.

[49]The light-weight dependable privacy-preserving (LAPP) convention. Our proposed convention is light-weight in expressions of handling and communique costs. The objective of the time complexity and computation time on inspecting reenactments is to the recognition the lightweight inconvenience of our proposed convention advance to beautify the first-class of benefit.

[50]Cloud computing presents large garage capabilities, the improvement of surroundings for software builders thru digital machines. It is likewise the house of software programs and databases which are accessible, on-demand. As protection is the principal constraint maintaining agencies to have interaction into the cloud fully, third-celebration auditors have become an increasing number of not unusual places in cloud computing implementations.

3. Proposed System

The proposed plot effectively accomplishes records deduplication and authenticator deduplication. Moreover, to decrease the computation burden on the client-side, the client as it were ought to perform the lightweight computation to create information authenticators, confirm the judgment of the cloud information, and recover it from the cloud capacity. We allow the security examination of the proposed plot, appearing that the proposed conspire fulfills rightness, soundness, and solid security assurance In this paper, we examine how to completely stand up to the brute-force word reference assaults and realize deduplication with solid protection security in cloud capacity inspecting and employing a plot called a concrete.

To realize deduplication with solid protection security, we plan a novel strategy to produce the record list and utilize an unused technique to create the key for record encryption. Within the point-by-point plan, the record index is created with the assistance of an Office Server (AS) rather than straightforwardly being created by the hash esteem of the record. The key for record encryption is created with the record and the record name. The record name is kept by the client furtively. In this way, the security of the user's record is ensured against the cloud and the AS. To make strides the capacity effectiveness, the clients, who possess the same record, can produce the same cipher text and the same authenticators.

Moreover, to reduce the computation burden on the individual side, the individual most viably wants to carry out the light-weight Computation to make records authenticators, affirm the keenness of cloud records and get their records from the cloud.

4.SystemModel

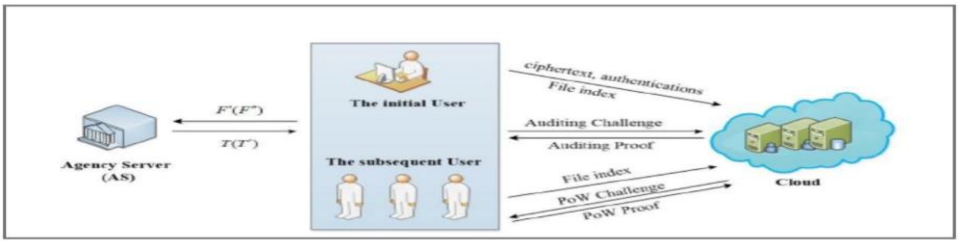

Figure 1: System model

The contraption form incorporates 3 assortments of substances: The Office Server, the cloud, and the client,

(1)Office Server: It is in charge of assisting users in developing the file index and file mark using their private key. The index allows the cloud to determine whether or not the file submitted by the user is duplicated. The user will create keys for encryption and an authentication server using the file label.

(2) Cloud: The cloud has tremendous capacity space and gives clients with capacity and uploading administrations.

(3) Customer: The shopper is gathered into two classes. One is the primary individual, who transfers records that did not already exist within the cloud. The other is consequent clients who transfer records that have been spared within the cloud. The introductory client makes verification tokens for each scrambled record some time recently uploading the scrambled record, verification tokens, and record tag to the cloud(figure 1). Only a copy of a duplicate file can be stored in the cloud, according to a deduplication cloud storage audit. After that, both the beginning and ensuring clients can get to their information by downloading it from the cloud. Clients may moreover utilize the cloud to check the exactness of their information by utilizing the cloud capacity examining convention. Duplicate files are deduplicated in the cloud to increase storage performance. To put it another way, the cloud as it were keeps a single duplicate of each copied report, and it's comparing verification tokens and gives the client an association to the comparing.

5. Conclusion

This proposed plot has predominant security spillage in cloud capacity reviewing with deduplication indeed as brute-strain word reference assaults are propelled. We format a light-weight cloud carport inspecting plot with deduplication helping strong privateness assurance. Within the proposed plot, the privateness of the buyer may be legitimately protected towards the cloud and distinctive parties. The buyer diminishes the overwhelming computation burden for creating data authenticators and confirming data keenness. The assurance proves shows that the proposed conspire are secure. We moreover offer indicated comparisons among our proposed plot and diverse show plans with the help of utilizing tests.

References

1. The Gnu Multiple Precision Arithmetic Library (GMP). Accessed: Oct. 2019. [Online]. Available: http://gmplib.org/
2. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Ownership of verified data in untrusted branches," in Proc. 14th ACM Conf. Comput. Commun.Secure. (CCS), 2007, pp. 598_ 609.
3. M. Bellare, S. Keelveedhi, and T. Ristenpart, "Message blocking Secure encryption and deduplication ", in Proc . Annu. Int. Conf. Theory Appl. Crypto- graph. Techn. Berlin Germany: Springer, 2013, pp. 296_ 312.
4. H. Cui, R. H. Deng, Y. Li, and G. Wu, "Attribute-based storage to support secure deduplication of encrypted data in the cloud", IEEE Trans. Big Data, vol. 5, no. 3, pp. 330_342, Sep. 2019.
5. R. Ding, H. Zhong, J. Ma, X. Liu, and J. Ning, "Lightweight IoT based IoT Storage to Protect Privacy", IEEE Internet Thing J., vol. 6, no. 5, pp. 8393_8405, Oct. 2019.

6. J. R. Douceur, A. Adya, W. J. Bosky, P. Simon, and M. Theimer, "Reclaiming space from duplicate _les in a serverless distributed _lesystem," in Proc. 22nd Int. Conf. Distrib. Comput. Syst., Jul. 2002, pp. 617_624.
7. Y. Fan, X. Lin, G. Tan, Y. Zhang, W. Dong, and J. Lei, "Secure Data Integrity Check Scheme for Cloud Storage", Future Gener. Comput. Syst., vol. 96, pp. 376_385, Jul. 2019.
8. Murugesan, M., Thilagamani, S. ," Efficient anomaly detection in surveillance videos based on multi layer perception recurrent neural network", Journal of Microprocessors and Microsystems, Volume 79, Issue November 2020, https://doi.org/10.1016/j.micpro.2020.103303
9. X. Ge, J. Yu, H. Zhang, C. Hu, Z. Li, Z. Qin, and R. Hao, "Towards Achieving keyword search over dynamic encrypted cloud data with symmetric-key based veri_cation," IEEE Trans. Dependable Secure Com-put., to be published.
10. Thilagamani, S., Nandhakumar, C. ." Implementing green revolution for organic plant forming using KNN-classification technique", International Journal of Advanced Science and Technology, Volume 29 , Isuue 7S, pp. 1707–1712.
11. S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, ''Proofs of ownership in remote storage systems,'' in Proc. 18th ACM Conf. Comput. Commun. Secure. (CCS), New York, NY, USA, 2011, pp. 491–500
12. Thilagamani, S., Shanti, N.," Gaussian and gabor filter approach for object segmentation", Journal of Computing and Information Science in Engineering, 2014, 14(2), 021006, https://doi.org/10.1115/1.4026458
13. K. He, J. Chen, Q. Yuan, S. Ji, D. He, and R. Du, ''Dynamic group-oriented provable data possession in the cloud,'' IEEE Trans. Dependable Secure Comput., to be published
14. Rhagini, A., Thilagamani, S. ,"Women defence system for detecting interpersonal crimes",International Journal of Advanced Science and Technology, 2020, Volume 29,Issue7S, pp. 1669–1675
    A. Juels and B. S. Kaliski, ''Pors: Proofs of retrievability for large files,'' in Proc. 14th ACM Conf. Comput. Commun. Secure. (CCS), 2007, pp. 584–597
15. K.Deepa, S.Thilagamani, "Segmentation Techniques for Overlapped Latent Fingerprint Matching", International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume-8 Issue-12, October 2019. DOI: 10.35940/ijitee.L2863.1081219
16. J. Li, X. Chen, X. Huang, S. Tang, Y. Xiang, M. M. Hassan, and AL elaiwi, ''Protect distributed deduplication systems with greater reliability,'' IEEE Trans. Comput., vol. 64, no. 12, pp. 3569–3579, Dec. 2015.
17. Santhi, P., Mahalakshmi, G., Classification of magnetic resonance images using eight directions gray level co-occurrence matrix (8dglcm) based feature extraction, International Journal of Engineering and Advanced Technology, 2019, 8(4), pp. 839–846.
18. Santhi, P., Priyanka, T.,Smart India agricultural information reterival system, International Journal of Advanced Science and Technology, 2020, 29(7 Special Issue), pp. 1169–1175
19. X. Liu, W. Sun, W. Lou, Q. Pei, and Y. Zhang, ''One-tag checker: Message-locked integrity auditing on encrypted cloud deduplication storage,'' in Proc. IEEE Conf. Comput. Commun., May 2017, pp. 1–9
20. Pandiaraja, P, Vijayakumar, P, Vijayakumar, V & Seshadhri, R 2017, 'Computation Efficient Attribute Based Broadcast Group Key Management for Secure Document Access in Public Cloud', Journal of Information Science and Engineering, 33, No. 3, pp. 695-712
21. S. Peng, F. Zhou, J. Li, Q. Wang, and Z. Xu, ''Efficient, dynamic and identity-based remote data integrity checking for multiple replicas,'' J. Netw. Comput. Appl., vol. 134, pp. 72–88, May 2019. [23] H. Shacham and B. Waters, ''Compact proofs of retrievability,'' J. Cryptol., vol. 26, no. 3, pp. 442–483, Jul. 2013.
22. Vijayakumar, P, Pandiaraja, P, Balamurugan, B & Karuppiah, M 2019, 'A Novel Performance enhancing Task Scheduling Algorithm for Cloud based E-Health Environment', International Journal of E-Health and Medical Communications (IJEHMC), Vol 10,Issue 2,pp 102-117.
23. P. Singh, N. Agarwal, and B. Raman, ''Protect data deduplication with cloud secret sharing schemes,'' Future Gener. Comput. Syst., vol. 88, pp. 156–167, Nov. 2018.
24. D. Song, E. Shi, I. Fischer, and U. Shankar, ''Cloud data protection for the masses,'' Computer, vol. 45, no. 1, pp. 39–45, Jan. 2012.
25. P. Pandiaraja, N Deepa 2019 ," A Novel Data Privacy-Preserving Protocol for Multi-data Users by using genetic algorithm" , Journal of Soft Computing , Springer , Volume 23 ,Issue 18, Pages 8539-8553.

26. S. Bhagyashri and P. Y. B. Gurav, ‘‘Privacy-preserving public auditing for secure cloud storage,’’ IOSR J. Comput. Eng., vol. 16, no. 4, pp. 33–38, 2014.
27. N Deepa , P. Pandiaraja, 2020 ,” Hybrid Context Aware Recommendation System for E-Health Care by merkle hash tree from cloud using evolutionary algorithm” , Journal of Soft Computing , Springer , Volume 24 ,Issue 10, Pages 7149–7161.
28. R. Singh, S. Kumar, and S. K. Agrahari, "Ensuring Data Storage Security in Cloud Computing," IOSR Journal of Engineering, 2012, vol. 2, p. 12.
29. K Sumathi, P Pandiaraja 2019,” Dynamic alternate buffer switching and congestion control in wireless multimedia sensor networks” , Journal of Peer-to-Peer Networking and Applications , Springer , Volume 13,Issue 6,Pages 2001-2010
30. P. Syam Kumar, R. Subramanian, and D. Thamizh Selvam, "Ensuring data storage security in cloud computing using Sobol Sequence," in Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on, 2010, pp. 217-222. 93
31. B. Gilburt, A. Schuster, and R. Wolff, "k-TTP: New data protection model for large distributed environments," in Proceedings der 10. ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2004, pp. 563-568.
32. K. Huang, M. Xian, S. Fu, and J. Liu, "Securing the cloud storage audit service: defending against the frame and collude attacks of third party auditor," Communications, IET, 2014, vol. 8, pp. 2106-2113.
33. J. Xu, "Auditing the Auditor: Secure Delegation of Auditing Operation over Cloud Storage," IACR Cryptology EPrint Archive, 2011, vol. 2011, p. 304.
34. F. Sebé, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.-J. Quisquater, "Effective validation of remote data ownership in critical IT infrastructures, IEEE transactions for knowledge and data engineering, 2008, vol. 20, pp. 1034-1038.
35. Y. Yu, L. Niu, G. Yang, Y. Mu, and W. Susilo, "On the security of auditing mechanisms for secure cloud storage," Future Generation Computer Systems, 2014, vol. 30, pp. 127- 132.
36. B. Wang, B. Li, and H. Li, "Knox: Control the confidentiality of data shared with large groups in the cloud," in International Conference on Applied Cryptography and Network Security, 2012, pp. 507-525.
37. K. Yang and X. Jia, "TSAS: Third-Party Storage Auditing Service," in Security for Cloud Storage Systems, ed: Springer, 2014, pp. 7-37.
38. Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Dynamic monitoring services to verify the integrity of external cloud storage," in Proceedings of the 2011 ACM Symposium on Applied Computing, 2011, pp. 1550-1557. 94
39. Kumararaja, V., Deepa, K.,” Pap smear image classification to predict urinary cancer using artificial neural networks” , Annals of the Romanian Society for Cell Biology, ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 1092 – 1098
40. S. Rizvi, K. Cover, and C. Gates, "A Trusted Third-party (TTP) based Encryption Scheme for Ensuring Data Confidentiality in Cloud Environment," Procedia Computer Science, 2014, vol. 36, pp. 381-386.
41. N. Shimbre and P. Deshpande, "Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES Algorithm," in Computing Communication Control and Automation (ICCUBEA), 2015 International Conference on, 2015, pp. 35-39.
42. P. Varalakshmi and H. Deventhiran, "Integrity checking for cloud environment using an encryption algorithm," in Recent Trends In Information Technology (ICRTIT), 2012 International Conference on, 2012, pp. 228-232.
43. M. Kaur and M. Mahajan, "Using encryption algorithms to enhance the data security in cloud computing," International Journal of Communication and Computer Technologies, 2013, vol. 1, pp. 56-59.
44. K. Suresh and K. Prasad, "Security Problems and Security Algorithms in Cloud Computing ”, International Journal of Advanced Research in Computer Science and Software Engineering. , 2012, vol. 2, pp. 12-15.
45. S. Rizvi, J. Ryoo, Y. Liu, D. Zazworsky, and A. Cappetta, "Central trust approach for cloud computing," in 2014 23rd Wireless and Optical Communication Conference (WOCC), 2014, pp. 1-6.
46. M. Ben Haj Frej, J. Dichter, and N. Gupta, "Lightweight Accountable Privacy-Preserving Protocol Allowing the Cloud Client to Audit the Third-Party Auditor for Malicious Activities," Applied Sciences, 2019, vol. 9, p. 30-34. 95
47. M. Ben Haj Frej, J. Dichter, and N. Gupta, "Light-weight accountable privacy-preserving (LAPP) protocol to determine the dishonest role of third party auditor in cloud auditing," in 2018 IEEE International Conference on Consumer Electronics (ICCE), 2018, pp. 1-6.