IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 4, April 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304069 |

An Efficient Deduplicate Removal Technique in Cloud Storage with Secure Data Sharing

J.Noorul Ameen M.E., M.Mohamed Javed Yasar, S. Prabakaran, F. Yusuff Aseher

Assistant Professor, E.G.S. Pillay Engineering College, Nagapattinam, India

UG Student, Department of Computer Science and Engineering, E.G.S. Pillay Engineering College, Nagapattinam. India

ABSTRACT: Data deduplication stands as a pivotal technique, pivotal in curbing storage expenses and boosting the efficiency of data management. Within the realm of cloud storage, it's imperative to scrutinize redundant files upon upload.

To this end, a fresh approach is proposed, centered around chunk-based partitioning for deduplication in cloud data storage. This method involves segmenting data into uniform-sized chunks, followed by deduplication processes to identify and purge duplicate chunks.

Duplicate verification is carried out using file attributes such as name and size. Moreover, security enhancements are integrated into the system through the utilization of Base64 encoding for data representation and the implementation of Advanced Encryption Standard (AES)-based re-encryption techniques, fortifying the security of cloud data storage and enabling secure data sharing.

Introducing an innovative method leveraging data chunk partitioning to streamline data processing on the cloud. This technique involves chunk-based compression, which identifies intricate data partitions and patterns during compression operations.

It's designed to handle diverse file formats including text, documents, and images. Additionally, it employs block-based variable chunk similarity while ensuring security through a Base64-based encoding algorithm.

Furthermore, it implements a Proxy Re-encryption method for secure data sharing. In the re-encryption process, the AES algorithm is utilized to encrypt the ciphertexts generated by Base64, thereby generating new decryption keys that are securely delivered to the intended recipients via email.

I. INTRODUCTION

Cloud computing has emerged as a widely adopted IT service, offering extensive resources such as storage and computing tailored to users' needs. Among these services, cloud storage stands out as particularly popular. With the exponential growth of global data volumes, efficient utilization of cloud storage has become imperative. Duplicate data storage is a significant contributor to storage wastage in the cloud, where multiple users may store identical files or different files containing identical data segments. Data deduplication presents a promising solution to this challenge. In a deduplication setup, the Cloud Service Provider (CSP) collaborates with users to determine whether an uploaded file already exists in storage, enabling users with duplicate data to access files without storing additional copies in the cloud. However, concerns about security and privacy arise due to the semi-trusted nature of CSPs. There's a risk that CSPs may tamper with or delete uploaded data for their gain, potentially resulting in significant losses for data owners and stakeholders. Therefore, ensuring the integrity of data stored in the cloud, particularly in deduplicated storage, is paramount

Verification procedures involve users issuing random challenges to the CSP, which computes a response based on the data stored for the corresponding files. Users then verify file integrity using these responses. However, existing Proofs of Retrievability (PoR) solutions often focus on enhancing user-side performance and assume infinite computation and storage resources on the CSP's end. In reality, CSPs employ data deduplication for optimal storage utilization,

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304069 |

rendering current solutions incompatible. This is because verification tags in existing schemes are generated using user-specific private keys, resulting in different tags for the same file held by different users, thus preventing deduplication at the CSP level.

To prevent CSP exploitation and ensure fair data duplication checks, an effective mechanism must be devised. This mechanism should safeguard users against deceptive practices by CSPs, thereby preserving storage space and promoting equitable service provision.

II. RELATED WORKS

Our research primarily aligns with proof of retrievability (PoR) solutions within cloud data deduplication. Juels and Kaliski introduced a sentinel-based PoR scheme, utilizing Error Correcting Code (ECC) and inserting indistinguishable sentinels alongside encrypted blocks. While supporting limited PoR queries, this scheme necessitates periodic file downloads and sentinel updates. Ateniese et al.
Proposed Provable Data Possession (PDP) based on homomorphic tags, allowing public verifiability but incurring high computation costs. Subsequent efforts aimed at enhancing PoR schemes, such as Shacham and Waters' Compact PoR, Xu and Chang's polynomial commitment enhancement, and Azraoui et al.'s StealthGuard utilizing Private Information Retrieval (PIR).
Message-locked proofs of retrievability emerged as a solution, with Bellare et al. formalizing Message-locked Encryption (MLE) and Chen et al. proposing a secure deduplication mechanism based on an improved MLE scheme. Zheng et al. introduced a proof of storage scheme with deduplication, albeit vulnerable to weak key attacks. Vasilopoulos et al.

Transformed existing PoR into a message-locked form, integrating it with deduplication functions. However, these approaches may generate different verification tags for the same file, impacting deduplication efficacy.

Formalized Message-locked Encryption (MLE), while Chen et al. proposed a secure deduplication mechanism based on an enhanced MLE scheme. Zheng et al. introduced a proof of storage scheme with deduplication, although susceptible to weak key attacks. Vasilopoulos et al. adapted existing PoR into a message-locked format, integrating it with deduplication functions.

However, these methods might produce disparate verification tags for identical files, impacting deduplication efficiency. Our scheme, as outlined, stands out from existing ones by offering support for unlimited queries, facilitating tag deduplication, providing flexibility in tag generation, and ensuring the correctness of duplication checks. This critical aspect has been overlooked in prior schemes, potentially exposing opportunities for CSP exploitation for profit motives.

III. PROPOSED METHODOLOGY

Builds upon our previous deduplication scheme [14], enhancing it by incorporating Private Set Intersection (PSI) and Private Information Retrieval (PIR) techniques to ensure data integrity and accuracy in duplicate checks for encrypted data deduplication. In contrast to prior approaches, we introduce a PSI-based challenge and response mechanism to the duplication check process, allowing the data holder to determine the duplication status of uploaded blocks instead of relying solely on the Cloud Service Provider (CSP).

Additionally, we employ Auditability Assurance (AA) to validate the CSP's computations during duplication checks, preventing potential manipulation of users into uploading already stored data blocks. Moreover, we propose a note insertion mechanism leveraging PIR, enabling the data holder to embed a specific set (referred to as a note set) of randomized bit sequences, adhering to a concealed function, as verification tags within the encrypted blocks of an uploaded file.

Data owners/holders with proven ownership of corresponding blocks can verify block integrity by challenging the conformity of notes to the hidden function.

It's noteworthy that verification tags are generated by multiple data holders for increased security. In VeriDedup, content holders with diverse sets of notes can also undergo deduplication, alleviating the need for the CSP to manage

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

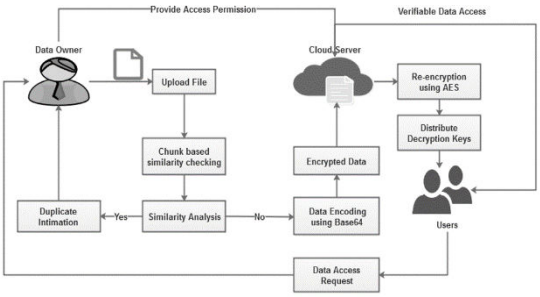
| DOI:10.15680/IJIRSET.2024.1304069 |

numerous verification tags from different data holders for integrity checks.

This reduces storage overhead associated with deduplication operations. Subsequently, we present the two innovative protocols, namely TDICP and UDDCP, followed by a comprehensive explanation of the entire VeriDedup framework.

IV. OVERVIEW

The TDICP protocol encompasses the following core procedures: System initialization, Note generation and embedding, Check initialization, Response calculation, and Integrity verification. System initialization: Given the security parameter-, AA produces a concealed function f, which is subsequently utilized for note generation.



Note generation and embedding: Given the concealed function f and the data holder's secret keys, the data holder generates a randomized note set S and a position set P corresponding to the uploaded blocks of its file. These note sets are then inserted into the encrypted blocks at their respective positions. Check initialization: Given the check indexes of the blocks, the data holder computes a coefficient set e and derives the challenge set v = b * e mod m, where gcd(m, b) = 1. Response calculation: Given the challenge set v, the CSP computes the response Resp = v * D. Integrity verification: Given the response Resp, the data holder computes the check result by evaluating Res = Resp * b^(-1) mod m to extract the note set and validate whether these notes adhere to the concealed function f. Upon successful verification, the data holder confirms the integrity of the stored file.

4.1 TDICP Design Brief

The TDICP protocol encompasses several pivotal procedures System setup, Note generation and insertion, Check Initialization, Response calculation, and Integrity check.

During System setup, upon entering the security parameter lambda, the Authority Agent(AA) generates a retired function f, which is latterly employed for note generation.

In Note generation and insertion, the data holder utilizes the retired function f and their secret keys to produce a randomized note set S and a position set P corresponding to the uploaded blocks of their train. These note sets are also fitted into the translated blocks at their separate positions.

For Check initialization, given the check indicators of the blocks, the data holder generates a measure set e and computes the challenge set v = b * e mod m, where gcd(m, b) = 1.

During Response calculation, upon entering the challenge set v, the Cloud Service Provider(CSP) computes the response Resp = v x D.

In the Integrity check phase, upon entering the response Resp, the data holder computes the check result Res = Resp * 1/ b mod m to prize the note set and corroborate whether these notes cleave to the retired function f. However, the data holder confirms the integrity of the stored train, If the verification succeeds.

4.2 VeriDedup Construction

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304069 |

VeriDedup consists of the following primary procedures: System initialzation, Data preprocessing, Duplication Check, for Note set insertion and Data upload, Data integrity verification and Data Download. The scheme's intricacies explained as follows:

- First, the System initialzation is crucial to the process.
- Data preprocessing, although time-consuming and tedious, is essential for accurate results.
- The Duplication Check is for ensuring no repeated data is present.
- Note set insertion and Data upload play significant roles in the overall process.
- Data integrity verification checks the validity of the uploaded information.
- Lastly, Data Download provides access to the verified data.

Overall, these procedures are vital to maintaining data accuracy and efficiency in VeriDedup operations.

System Initialization (4.2.1):

In the system setup, assuming the actuality of a bilinear chart e G1 x G1 → GT where G1and GT are two groups of high order q, the system parameters involve arbitrary creators g ∈ G1 and Z = e(g, g) ∈ GT. Each data holder uw generates their secret crucial sk_w = aw and public key pkw = gaw for Proxy Re-Encryption (PRE), where aw is chosen aimlessly from Zp *. The public key pkw is employed for creating there-encryption key at the Authority Agent (AA) for uw. Also, an elliptic wind Eq(a, b) over GF(q), a base point P, the elliptic wind secret key s ¬ w of uw where s_w ∈{ 0,., 2s- 1}, and $V_w = s_wP$ as the corresponding public key are established, with s being a security parameter. The keys(pk_w, sk_w) and(V_w, s_w) of uw are linked to a unique identifier of the data holder, which can serve as a pivotal alias for stoner identity verification.

AA generates a agreement- hidden function f which will be latterly used by all data holders to induce their distinct note sets Swi, and disseminates f among them. It's notable that f can be any function chosen grounded on the needed security position by the data holders. Also, AA generates pk_{AA} and sk_{AA} for PRE and shares pk_{AA} with the data holders.

The Cloud Service Provider(CSP) initiates an RSA algorithm with a public-private crucial brace(e, d) under the modulus N. This crucial brace is employed to cipher the uploaded markers of the data holders and the CSP for duplication check purposes.

Data Preprocessing and Duplication Check (4.2.2):

Suppose data holders u1 and u2 wish to upload their data lines F1 and F2 to the CSP. However, it performs the following way.
If u1 is the first to upload the train.
1. Divide F1 into several splits, each containing m blocks. Use Error Correcting Code(ECC) to extend the blocks to m + d - 1 blocks to handle crimes efficiently.
2. induce a block label $y_{1,\ i}$ = H(H($B_{1,\ i}$) x P *) for each block B_1,i.
3. shoot the set of markers{ $y_{1,\ i}$} to the CSP.
4. CSP interacts with AA and u1 to perform a duplication check using the label set{ x_j } maintained by CSP.
5. For each x_j, CSP generates a_j = H(x_j) d mod N and sends{ a_j, H(x_j), sign(H(x_j)), Δ} to AA.
6. AA verifies the correctness of CSP calculations and creates a ditz sludge CF as input of{a_j}.
7. For each y_1, i, u_1 selects arbitrary figures and computes r_1^{inv}, i and r_1, i,.
8. cipher A(1, i) = H(y ¬ 1, i) * r1, i mod N and shoot them to CSP.
9. CSP computes C(1, i) = (A(1, i)) d mod N and e spends to u1. 10. u1 verifies the correctness of CSP calculation and checks duplication with the ditz sludge CF.

This process ensures data integrity and duplication checks for uploaded lines. Aimlessly opting N 1, v non-overlapping subsets from the sets{fa1, i},{fH($y_{1,\ i}$) = Q a1, i^e holds in each subset. However, AA confirms the correctness of CSP's calculation and updates the ditz sludge CF by fitting {a_1, i}, If the verification succeeds. This streamlined sludge is used in the posterior duplication check rounds. Upon a positive duplication check and if thepre-stored blocks belong to the same data holder, the data holder instructs the CSP to maintain its block without farther action.still, if the blocks belong to a different data holder, the CSP is informed to perform deduplication. Upon being informed of duplication from a different stoner u_2, the CSP originally verifies block power by assigning power verification tasks to AA. AA challenges data holder u_2 to prove power of the blocks $B^2_i = B^1_i$ using an power verification protocol grounded on a cryptoGPS identification scheme.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304069 |

After verification, if power is verified, AA generates are-encryption crucial $rk_{AA} \rightarrow u_j$ = RG(pk_{AA}, sk_{AA}, PK_2) and sends it to CSP. CSP also transfers CK_1 to CK_2 by calculating R($rk_{AA} \rightarrow u_2$, E(pk_{AA}, DEK_1)) = E(pk_2, DEK_1) for u_2. latterly, both u_1 and u_2 can pierce the same data blocks stored at the CSP and perform the ensuing integrity check.

Each data holder, u_1 and u_2, generates a unique(m0, b0) as a secret along with unique(d_1, i, 0,., d_1, i, z) and(d_2, i, 0,., d_2, i, z) independently. They use these secrets to induce other sets(e_1, i, 0,., e_1, i, z) and(e_2, i, 0,., e_2, i, z) grounded on their position indicators. They further produce Req1, i and Req2, i independently and cooperate with CSP to gain the note sets grounded on their position indicators to check whether the notes conform to the retired function. also, if u1 and u_2 partake a same duplicated block B, i from different data holders, u1 verifies f(h_1, i, 0,., h_1, i, k) = 0 to check the integrity of $B_{1,\ i}$, while u2 verifies f(h_2, i, 0,., h_2, i, k) = 0 for B2,i.However, they both corroborate f(h, i, 0, If $B_i \in B_i$, h, i, k) = 0 to check the integrity of B,i. therefore, the protocol not only deduplicates identical blocks uploaded to the CSP but also deduplicates verification markers of duplicated blocks generated by multiple data holders. As ECC is applied to prop in train recovery, an integrity check is performed over allblocks.However, the protocol ensures the integrity of F1 and F2, If u1 and u2 successfully perform g times arbitrary verification in all corresponding block sets. Each B1, i is only associated with a single $CTI_{1,i}$ i.e., $CTI_{1,\ i} = CTI_{2,i}$.

V. DATA DOWNLOAD

When u1 initiates a download request for F1, it sends a request along with the file name to the CSP. Upon receiving the request, the CSP first verifies if u1 has the authorization to download the file. If the verification is successful, the CSP returns the corresponding block sets $\{CTI_{1,\ i}\}$ to u1. u1 then extracts all the notes based on the position indexes P1;i for each block to retrieve the ciphertexts $\{CT_{1,\ i}\} = \{CT_{1,\ i}\} \cup \{CT_i\}$ and decrypts each $CT_{1,i}$ directly using DEK_1 to obtain $\cup\{B_{1,i}\} = \{B_i^*\} \cup \{B_i^1\}$. Due to the application of ECC, u1 can recover F1 from $\{B_i^1\}$ with errors no more than d^2. For u2, following similar steps to obtain the ciphertexts $\{CT_2^1\} = \{CT_i\} \cup \{CT_i^2\}$

it also receives a re-encrypted DEK1 key D(sk_2, E(pk_2, DEK_1)) from the CSP. u2 then uses its key pair (pk_2, sk_2) to obtain the key DEK_1 and decrypt each CT_i to retrieve the duplicated original blocks $\{B_i$ and its unique original blocks $\{B_i^2\}$ by directly utilizing DEK2. Finally, u2 can obtain the original file $\cup\{B_i^2\} = \{B_i\} \cup \{ B_i^2\}$ and recover F2 using ECC.

The experimental findings unequivocally demonstrate the superiority of our proposed algorithms over benchmark algorithms in three pivotal aspects. Firstly, they consistently achieve an average EC reduction of 15.49%, signifying their efficacy in minimizing energy consumption. Secondly, there is a notable average reduction in Service Level Agreement Violation (SLAV) of 7.85%, illustrating improved adherence to desired Quality of Service (QoS) levels. Lastly, the algorithms effectively decrease the number of VM migrations by an average of 83.32%, which is essential for minimizing system overhead and migration costs. These results firmly establish the superiority of our approaches over benchmark algorithms, highlighting their potential for enhancing energy efficiency and overall system performance.

Our future endeavors will prioritize three main aspects:

- Exploring the application of multi-objective optimization techniques to address VM consolidation migration, which involves multiple objectives such as load balancing, performance optimization, and cost reduction.

- Further evaluation in large-scale real-world deployments is essential to authenticate the effectiveness and feasibility of our proposed approaches. Such real-world testing can offer invaluable insights into the challenges and advantages associated with implementing these approaches in production environments.

- With the escalating popularity of container technology for resource virtualization, we aim to enhance the migration algorithm developed in this study to ensure its compatibility with containers.

VI. SECURITY ANALYSIS

In this section, we establish the correctness and soundness of TDICP. Correctness refers to the ability of the integrity check algorithm to accurately extract a queried column, while soundness ensures that the original file can be

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304069 |

reconstructed if the corresponding TDICP integrity check is successful. We also demonstrate the soundness and privacy of UDDCP, omitting the proof of correctness as it is self-evident. Soundness implies that the Cloud Service Provider (CSP) cannot produce fraudulent computation results throughout the procedure, privacy ensures that neither the CSP nor the data holder divulge any information to each other except for the shared intersection, and correctness guarantees that the data holder accurately retrieves all intersections between its tag set and the CSP's tag set.

VII. CONCLUSION

In this study, we presented VeriDedup, a solution designed to verify the integrity of an outsourced encrypted file and ensure the accuracy of duplication checks in a unified manner. VeriDedup's integrity check protocol, TDICP, enables multiple data holders to independently verify the integrity of their outsourced files using their verification tags, We utilized a new challenge and response mechanism within the duplication check protocol, UDDCP, of VeriDedup. This mechanism allows the data holder, rather than the CSP, to determine whether a file is a duplicate, ensuring the accuracy of duplication checks. Security and performance analyses demonstrate that VeriDedup maintains security and efficiency within the defined security model. Additionally, computer simulations confirm its efficiency when compared to closely related prior work.

REFERENCES

1)Z. Yan, L. Zhang, W. Ding, and Q. Zheng, “miscellaneous data storehouse operation with deduplication in pall computing,” IEEE Trans. Big Data, vol. 5,no. 3,pp. 393 – 407,Sep. 2019. Public- crucial encryption with suggestive multi-keyword hunt(PEMKS) is secure against the adaptive chosen keyword attack and the offline keyword guessing attack, The practical computational outflow is analogous to the other schemes.

2)Z. Yan, W.X. Ding, and H.Q. Zhu, “A scheme for managing translated data stores using deduplication in Pall,” in Proc. Int. Conf. Algorithms Archit. Resemblant Process., 2015, pp. 547 – 561. Secure Cloud Data Deduplication with Effective Re-Encryption, Data deduplication scheme with effective re-encryption saves inordinate calculation outflow. The pall stoner needs to store hash values, which increases the storehouse cost

3)Z. Yan, M. Wang, Y. Li, and A.V. Vasilakos," Encrypted data operation with duplication in pall computing," IEEE Cloud Comput., vol. 3,no. 2,pp. 28 – 35,Apr. 2016. An Effective and Secure Public crucial Authenticated Encryption With Keyword Search in the Logarithmic Time Lidong Han, Junling Guo, Guang Yang Public crucial authenticated searchable encryption scheme Encryption and lattice algorithms are nearly fast There are still some security problems that do.

4)W. Shen, Y. Su, and R. Hao, “Featherlight pall storehouse auditing with deduplication supporting strong sequestration protection, ” IEEE Access, vol. 8,pp. 44 359 – 44 372, 2020. An Effective trait- Grounded Multi-Keyword Search Scheme in Encrypted Keyword Generation Attribute- grounded multiple keyword hunt(ABMKS) Yuanbo Cui, Fei Gao, The calculation cost of recoup algorithm in our scheme is less, Encrypted keyword indicator generation is time- consuming

5)Q. Zheng and S. Xu," Secure and effective evidence of storehouse with deduplication," in Proc. 2nd ACM Conf. Data Appl. Secure. sequestration, 2012,pp. 1 – 12. VeriDedup A Verifiable Cloud Data Deduplication Scheme With Integrity and Duplication Proof Xixun Yu, Hui Bai, Zheng Yan Tag-flexible Deduplication- supported Integrity Check Protocol(TDICP) VeriDedup is a secure and effective model. The operation of homomorphic markers incurs high calculation costs.

6)A. Giuseppe, R. Burns, and C.Reza, “Sustainable data ownership in untrusted business,” in,Proc. ” in Proc. 14th ACM Conf. Comput. Commun.Secur., 2007,pp. 598 – 609. A Data Deduplication Scheme Grounded on DBSCAN With Tolerable Clustering divagation Yan Teng, Hequn Xian viscosity- grounded spatial clustering of operations with noise(DBSCAN) with tolerable clustering divagation(TCD- DBSCAN) algorithm Reduces storehouse outflow and improves deduplication effectiveness Time outflow of different train size

7)G. Ateniese etal., “ Remote data checking using sustainable data possession," ACM Trans. Inf. Syst.Secur.,vol. 14,pp. 1 – 34, 2011. FASR An Effective point-apprehensive Deduplication system in Distributed Storage Systems Wenbin Yao, Mengyao Hao point-apprehensive Stateful Routing system(FASR) It reduces the system overhead The number of point lookups of FASR is slightly advanced

8)Z. Wen,J. Luo,H. Chen,J. Meng,X. Li, andJ. Li," A empirical data deduplication scheme in pall computing, ” in Proc. Int. Conf. Intell. Netw. cooperativeSyst., 2014,pp. 85 – 90. SecDedup Secure Encrypted Data Deduplication With Dynamic Power streamlining Shuguang Zhang, Hequn Xian Ciphertext policy trait- grounded encryption SecDedup can fluently and effectively perform deduplication on translated data The computational outflow on the stoner side is fairly high.

9)P. Meyer, P. Laapin, F. Tronel, and E. Anceaume, "Secure two-segment information deduplication scheme", Proc.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304069 |

IEEE International High Performance. Comput.Commun., IEEE 6th Int. Symptoms Cyberspace Safety, IEEE 11th Int. Conf. BeddedSoftw.Syst., 2014, pp. 802-809. Secure EMR bracketing and deduplication using Map ReduceA.V. Usharani and Girija will collaborate at Barracuda on KNN – Reduce, a DNA encryption and decryption algorithm. DNA algorithms provide the necessary security. As the amount of sample data increases, so does the KNN algorithm, which increases the algorithm time.

10)D. Vasilopoulos,M.€ Onen,K. Elkhiyaoui, and R.Molva," Communication locked attestations of retrievability with secure deduplication," in Process. CM Cloud ComputerSecurity.Workshop, 2016,pp. 73 – 83. empirical trait- Grounded Keyword Search Over Encrypted Cloud Data Supporting Data Deduplication Xueyan Liu, Tingting Lu Attribute-grounded keyword hunt over translated data Outsourced decryption is used to reduce the quantum of calculation caused by ABE Computational outflow occurs approaches, identifies exploration gaps, and provides perceptivity exploration, making it a precious resource for experimenters and interpreters in the field.

Yadav etal.'s paper," Managing overloaded hosts for energy- effectiveness in pall data centers," published in Cluster Computing in September 2021, proposes strategies for managing overloaded hosts to ameliorate energy effectiveness in pall data centers. The authors present an approach to stoutly conforming resource allocation to palliate host load conditions, thereby reducing energy consumption while maintaining performance situations. Their work contributes to the development of energy-effective resource operation ways in pall surroundings.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details