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 12, Issue 4, April 2023

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 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204101 |

Secure Data Encryption Techniques Using ABE In Cloud Computing

Madhura Maruti Burud, Pratiksha Anil Patil, Prajakta Ananda Kamble, Mrs. Nutan V. Patil

Department of Computer Science and Engineering, NMCOE College of Engineering, DBATU University, Lonere, India

ABSTRACT*:* An overview of cloud computing, cloud file services, their usability, and storage is given by this project. Storage optimization is also considered by the de-duplication analysis of current data de-duplication techniques, processes and implementations for the benefit of cloud service providers and cloud users. The project also proposes an effective method for detecting and eliminating duplicates by measuring the digest of files using file checksum algorithms, which takes less time than other methods pre-implemented.This suggested method is to delete duplicate data, but according to that duplication search, the user has allocated some privilege and each user has its unique token.Using the hybrid cloud model, cloud deduplication is accomplished.This proposed technique is more reliable and uses less cloud resources. It has also shown that, relative to the standard deduplication technique, the proposed scheme has limited overhead in duplicate elimination. Content level deduplication as well as file level deduplication of file data is reviewed through the cloud in this document

KEYWORDS*:* Cloud computing, Checksum algorithm, Deduplication

I. INTRODUCTION

Cloud Computing is an emerging technology that has transformed the IT Business model of a computer. Apps and data are required for centralized data centers where, on a per-payment basis, a broad user community can access information. This poses a security risk to the database. Confidentiality of data that requires care may be violated. So before sending it to a cloud server, it is important to encrypt the data. This makes data usage a daunting task. Typical search methods include Boolean encrypted data search, which does not work if there is a large number of users and a large number of data files stored in the cloud. They also cause two major problems; one is the background processing that users have to do to get the required documentation and the other is the unfavorable network traffic where all the files associated with the keywords are restored. Proposed application of standard keywords that solve these

As a growing processing model, cloud computing attracts many organizations to seriously consider cloud computing in terms of cost effectiveness, flexibility, and cost-effectiveness management. Often, organizations assign their computer functions to enhance their knowledge in the cloud. Aside from the incredible benefits that the cloud offers, security and comfort considerations prevent companies from exploiting those benefits. If the information is extremely fragile, the information needs to be encrypted before it can be released to the cloud. However, when information is secure, no matter what the actual security plan, performing any information mining operations becomes complicated without removing the encryption. In addition, the cloud can also access useful and soft information about real information products by monitoring information access styles even if the information is encrypted.

Objectives:

To increase the storage utilization
To remove the duplicate copies of data and improve the reliability
To reduce network bandwidth for cloud storage providers
To develop algorithms of Role Base Access Control (RBAC) for secure data access

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

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204101 |

II.RELATED WORK

.

J. Li et.al, worked on this system in which [1] improving the kNN secure process, MRSF can retrieve the most accurate ciphertext text. Alternatively, by using a polynomial-based access method, it can effectively filter users' search rights. With regard to the confidentiality of exported data and the confidentiality of references and tokens, the official security analysis indicates that the MRSF is secure. In addition, a detaied study shows that the MRSF gains greater search accuracy and more efficiency compared to current schemes.

H. Huang et.al, worked on this system in which [2] Embrace the Doc2Vec model to gain a search scheme calculated by semantic-aware keywords. The Doc2Vec model uses a broad representation of words and documents with a limited vector size while being trained on a database with a few hundred million words. Distributed document submissions are extracted as a document vector of Doc2Vec and used as a search index. The query keywords are also excluded as a query feature vector, and secure in-product product functionality is adopted to achieve semantic search that maintains privacy with query query vector and index. Our program can support a flexible update to a document set in the Doc2Vec model. Real-world data analysis shows that a vector of fixed length feature can improve time and space efficiency in semantic information research.

G. Yang et.al, worked on this system in which [3] Retrieving required files for encrypted cloud becomes a problem that requires searching for encrypted data. In this paper, we propose a more efficient keyword search program over cloud-encrypted data using the B + data structure tree. To improve query efficiency, we are building a B + tree index structure based on a set of data sets, which can improve the index structure and provide an effective and faster correlation between query and cloud data. Specifically, for the privacy concerns of data query, we use an advanced KNN-based algorithm to encrypt sensitive data; The searchable encryption of this program achieves the accuracy of multiple query queries on encrypted cloud data and returns the highest possible high-quality results. Extensive test results in real-life data sets indicate that the proposed method can significantly reduce index retention and improve recovery efficiency.

G. SamrinA et.al, worked on this system in which [4] a secure keyword-level search method is used to provide more privacy and efficiency, with accessible functions such as reviews, deletion, inserting words. These functions are used to retrieve files from the cloud server with minimal retrieval time. Data owners collect a lot of data and store it on cloud servers for future purposes; later users use that data. Data owners are only allowed to loginto the cloud server after they have been successfully authorized and allowed to create their own web pages. To store and retrieve data from the cloud server, the Blowfish algorithm is commonly used to encrypt and decrypt. Lower line search time and efficiency increase.

X. Dai et.al, worked on this system in which [5] a novel searchable continuous encryption system based on the Latent Dirichlet Allocation (LDA) title model. Documents are moderated by LDA, and the concept of topics is used to generate a matrix for the relationship of the document title and the subject matter vectors in question. The matrix is used as an indicator of the proposed system. The function of a secure internal product is adopted to encrypt the index and veggies of the query title, which provides an accurate number of subject link points between the encrypted index and the trapdoors departments. To improve the efficiency of our basic system, we use a special complete binary tree and use the algorithm "Deeply Greedy Search". Our test results show the effectiveness of our system.

W. Kang et.al, worked on this system in which [6] a conjunctive multi-keyword ranked secure search scheme for multiple data owners. To guarantee data security and system flexibility in the multiple data owners environment, we design an ingenious secure query scheme that allows each data owner to adopt randomly chosen temporary keys to build secure indexes for different data files. An authorized data user does not need to know these temporary keys of constructing indexes and can instead randomly choose another temporary query keys to encrypt query keywords, while the cloud server can correctly perform keywords matching over encrypted data files. To rank the query results of a conjunctive multi-keyword query, the cloud server computes the similarity scores between the query and its query results according to encrypted relevance scores of keywords without obtaining any sensitive information. Extensive experiments demonstrate the correctness and practicality of the proposed scheme.

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

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204101 |

C. Chen et.al, worked on this system in which [7] discussed hierarchical approach clusters the documents based on the minimum relevance threshold, and then partitions the resulting clusters into sub-clusters until the constraint on the maximum size of cluster is reached. In the search phase, this approach can reach a linear computational complexity against an exponential size increase of document collection. In order to verify the authenticity of search results, a structure called minimum hash sub-tree is designed in this approach. System also investigated ciphertext search in the scenario of cloud storage. System explore the problem of maintaining the semantic relationship between different plain documents over the related encrypted documents and give the design method to enhance the performance of the semantic search.
J. Shao et.al, worked on this system in which [8] focus on cloud-aided frequent itemset mining solution, which is used to build an association rule mining solution. Here outsourced databases that allow multiple data owners to efficiently share their data securely without compromising on data privacy and leak less information about the raw data than most existing solutions. In comparison to the only known solution achieving a similar privacy level as this proposed solutions, the performance of this proposed solutions is three to five orders of magnitude higher.

B. K. Samanthula et.al, worked on this system in which [9] k-NN protocol protects the confidentiality of the data, user's input query, and data access patterns. To the best of this knowledge, this work is the first to develop a secure k-NN classifier over encrypted data under the standard semi-honest model. In this system, author focus on solving the classification problem over encrypted data. In particular, propose a secure k-NN classifier over encrypted data in the cloud. The proposed protocol protects the confidentiality of data, privacy of user's input query, and hides the data access patterns.
M. S. Dumbre Anita et.al, worked on this system in which [10] a protocol of finding frequent item in accountable computing (AC) framework which enables two parties to conduct collaborative computation on their transactional databases to find out the common frequent items without disclosing their private data to the other party. Their scheme was proposed in a secure two-party computation model against malicious adversaries. System also analyzes the implementation details of AC-framework and identifies some security weaknesses in their scheme. Furthermore, system clarifies the security requirements for the AC-framework and presents an augmented solution to enhance security. System also analyzes the search efficiency and security under two popular threat models.

III.METHODOLOGY

In this study we suggest an effective multi-key search system and a data sharing scheme with multiple data owners' settings. It means that any user in the group can search and share data with others within the group through a reliable cloud. The performance of the protocol was also tested by the system under different parameter settings. With the support of the Vector Base Cosine Similarity (VCS) method, such downtime items can be removed. PBE With MD5 And DES Encrypted Search Process and Encrypted Data using ElGamal Algorithm also provides an accurate search method instead of line-based search. In particular, it makes new use of cryptographic primitives to protect data and file sharing.

In a cloud-based group data sharing to access Internal Access Control, private keys are generated for every user to provide access to files and maintain data security, the secret keys of the group members need to be updated after the removal of any group members. Also to prevent malicious members from accessing data to prevent group file uploads will be introduced in the group name. Data encryption will be stored using encryption when uploading data to the cloud. For a successful data recovery process, here use high quality search for multiple keywords. Provides search result to end user as the most important k-document in the rated form as output. The silent system can be used to share group data and multi-key search searches on a cloud computer with high security and efficiency. On this machine instead of one data owner a multi-owner system is established.

In this case we checked the location of most owners in front of the groups. All team members of a particular group have rights to share and receive data up to that group. Members may be disqualified by a group manager from the corresponding group when members leave the group or move to a different group. Members are also dismissed for their unauthorized action. The system structure of the proposed program is given in the figure. It gives an overview of the whole process. The proposed model provides secure access control and privacy to members, ensuring that each member of the public uses the cloud service anonymously.

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

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204101 |

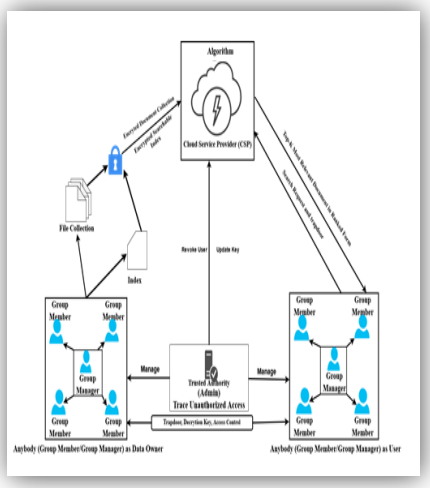

Fig. Proposed System Architecture

IV.CONCLUSION AND FUTURE SCOPE

In this work, the system provides a fast data recovery mechanism for the encrypted generation. The efficiency of the protocol was also assessed by the system under different parameter settings. A functionality that complies with the system's prevention of data. With the support of the Vector Base Cosine Similarity (VCS) method, such runtime objects can be removed. The Encrypted index search technique also offers an accurate search mechanism rather than a linear base search. Finally, Framework has tested the heterogeneous public cloud environment with outcomes assessment in the cloud environment, which has also met the targets. The framework also discusses the additional goals of privacy and security, such as Function Base Access Control (RBAC). There are still some safety barriers; future changes should be moved forward.

Ranked search greatly enhances system usability by enabling search result relevance ranking instead of sending undifferentiated results, and further ensures the file retrieval accuracy.

Specifically, we explore the statistical measure approach, i.e. relevance score, from information retrieval to build a secure searchable index, and develop a one-to-many order-preserving mapping technique to properly protect those sensitive score information.

The resulting design is able to facilitate efficient server-side ranking without losing keyword privacy.

Thorough analysis shows that our proposed solution enjoys “asstrong-as-possible” security guarantee compared to previous searchable encryption schemes, while correctly realizing the goal of ranked keyword search.

Extensive experimental results demonstrate the efficiency of the proposed solution.

Ranked key word search: For efficient searching process the process use the mechanism of Topic detection and tracking . The search time includes fetching the posting list in the index, decrypting, and rank ordering each entry.

Security guarantee: For providing the security in the cloud server, this process uses the privilege method

REFERENCES

[1] J. Li, J. Ma, Y. Miao, Y. Ruikang, X. Liu, and K.-K. R. Choo, “Practical Multi-keyword Ranked Search with Access Control over Encrypted Cloud Data,” *IEEE Transactions on Cloud Computing*, pp. 1–1,Sep. 2020, doi: 10.1109/tcc.2020.3024226.

[2] X. Dai, H. Dai, G. Yang, X. Yi, and H. Huang, “An Efficient and Dynamic Semantic-Aware Multikeyword Ranked Search Scheme over Encrypted Cloud Data,” *IEEE Access*, vol. 7, pp. 142855– 142865, 2019, doi: 10.1109/ACCESS.2019.2944476

[3] J. Xu, X. Huang, G. Yang, and Y. Wu, “An Efficient Multi-keyword top-k Search Scheme over Encrypted Cloud Data.

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

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204101 |

[4] G. SamrinA, "EFFICIENT PRIVACY-PRESERVING KEYWORD SEARCH METHOD FOR RETRIEVING DATA FROM CLOUD.",2017 International Conference on Innovations in information Embedded and Communication Systems (ICIIECS)

[5] X. Dai, H. Dai, C. Rong, G. Yang, and F. Xiao, "Enhanced Semantic-Aware Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data," *IEEE Transactions on Cloud Computing*, 2020, doi:10.1109/TCC.2020.3047921.

[6] R. Li, Z. Xu, W. Kang, K. C. Yow, and C. Z. Xu, "Efficient multi-keyword ranked query over encrypted data in cloud computing," *Future Generation Computer Systems*, vol. 30, no. 1, pp. 179– 190, 2014, doi: 10.1016/j.future.2013.06.029.

[7] C. Chen *et al.*, "An Efficient Privacy-Preserving Ranked Keyword Search Method," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 4, pp. 951–963, Apr. 2016, doi: 10.1109/TPDS.2015.2425407.

[8] L. Li, R. Lu, K. K. R. Choo, A. Datta, and J. Shao, "Privacy-Preserving-Outsourced Association Rule Mining on Vertically Partitioned Databases," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1847–1861, Aug. 2016, doi: 10.1109/TIFS.2016.2561241.

[9] B. K. Samanthula, Y. Elmehdwi, and W. Jiang, "K-nearest neighbor classification over semantically secure encrypted relational data," *IEEE Transactions on Knowledge and Data Engineering*, vol. 27,no. 5, pp. 1261–1273, May 2015, doi: 10.1109/TKDE.2014.2364027.

[10] M. S. Dumbre Anita and M. D. Rokade, "An Efficient and Privacy-Preserving Multi Keyword Ranked Search and Deduplication over Encrypted Data," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 10, no. 6, 2021, doi: 10.15680/IJIRSET.2021.1006430.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

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