IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 2, April 2025

Impact Factor: 7.67

Practical Multi-Keyword Ranked Search With Access Control Over Encrypted Cloud Data

Ms.. K. T. Gomathi[1], Saribali Chandana[2], Potha Poojitha[3], Muniraju Pavan[4], Mallela Dharma Teja[5]

Assistant Professor, Department of Computer Science and Engineering[1]

Students, Department of Computer Science and Engineering[2,3,4,5]

Siddartha Institute of Science and Technology, Puttur, A.P., India

sistkcse.gomathi@gmail.com, saribalachandanareddy@gmail.com, poojithapothap@gmail.com

mpavan5525@gmail.com, mallelladharmateja@gmail.com

Abstract: *With the explosive growth of data volume in the cloud computing environment, data owners are increasingly inclined to store their data on the cloud. Although data outsourcing reduces computation and storage costs for them, it inevitably brings new security and privacy concerns, as the data owners lose direct control of sensitive data. Meanwhile, most of the existing ranked keyword search schemes mainly focus on enriching search efficiency or functionality, but lack of providing efficient access control and formal security analysis simultaneously. To address these limitations, In this Project propose an efficient and privacy-preserving Multi-keyword Ranked Search scheme with Fine-grained access control (MRSF). MRSF can realize highly accurate ciphertext retrieval by combining coordinate matching with Term Frequency-Inverse Document Frequency (TF-IDF) and improving the secure k NN method. Besides, it can effectively refine users' search privileges by utilizing the polynomial-based access strategy.*

Keywords: Ranked Search, Document Frequency, Data owners, Cipher-text ,Encrypted Search, Cloud Computing, Access Control, Multi-Keyword Search, Ranked Search, Secure Indexing, Attribute-Based Encryption (ABE), Privacy Preservation, Trapdoor Generation, Searchable Encryption

I. INTRODUCTION

The increasing reliance on cloud storage has spurred substantial research into searchable encryption and access control mechanisms to safeguard data privacy. Early approaches, such as those by Song et al. [1], introduced the concept of searching over encrypted data, but were limited to single keyword queries and lacked ranking capabilities. As user demands evolved, so did the need for more practical search schemes that could support complex queries without exposing sensitive data.

To address this, the concept of Multi-Keyword Ranked Search (MKRS) over encrypted data was proposed. Cao et al. [2] introduced a secure and efficient ranked search model based on the vector space model and TF-IDF weighting, which significantly improved search accuracy. However, this method assumed a semi-trusted cloud server and did not consider fine-grained access control, leaving room for unauthorized access in multi-user environments.

Further enhancements were made with the introduction of Boolean keyword search and conjunctive keyword search, which improved flexibility but often increased system complexity and query latency. The work by Sun et al. [3] incorporated access policies, yet lacked scalability in real-world scenarios due to high overhead in policy evaluation.

The integration of Attribute-Based Encryption (ABE) into search systems offered a promising direction. In particular, the scheme proposed by Yu et al. [4] utilized ABE for access control, enabling only authorized users to decrypt the search results. While secure, this method struggled with query efficiency and ranked relevance.

Recent works have focused on balancing efficiency, data privacy, and access control. Wang et al. [5] developed a privacy-preserving keyword search with ranked output, yet it still required heavy computation on the user side. Other schemes attempted to outsource more computation to the cloud but risked leaking search patterns or access structures.

DOI: 10.48175/IJARSCT-24943

In summary, existing solutions tend to excel in one aspect—search accuracy, security, or access control—but often compromise the others. This motivates the need for a practical scheme that simultaneously supports multi-keyword ranked search and fine-grained access control over encrypted cloud data, without sacrificing efficiency or privacy.

II. CLOUD COMPUTING

Cloud computing has emerged as a transformative paradigm that enables on-demand access to a shared pool of configurable computing resources, including servers, storage, applications, and services. It offers significant benefits such as scalability, cost-efficiency, and flexibility, making it widely adopted across both enterprise and personal environments. However, outsourcing data to the cloud introduces serious security and privacy concerns, especially when dealing with sensitive information.

To address these concerns, various security mechanisms have been proposed. Encryption is the most common method to protect data confidentiality in the cloud. While effective in preventing unauthorized access, traditional encryption schemes hinder the ability to perform efficient search and retrieval operations. This limitation led to the development of searchable encryption (SE), which allows encrypted data to be queried without revealing its contents to the cloud service provider.

In parallel, researchers have also explored privacy-preserving access control methods to restrict data availability to authorized users. Techniques such as Attribute-Based Encryption (ABE) and Role-Based Access Control (RBAC) are commonly employed to enforce these policies. However, integrating access control with searchable encryption while maintaining performance remains an active area of research.

Recent advancements in cloud security aim to strike a balance between usability and privacy. The focus has shifted towards creating systems that support multi-keyword search, ranking of results, and fine-grained access control, all while preserving the confidentiality of both the data and the search queries. These developments form the foundation for the proposed system in this work

III. PROPOSED SHYSTEM

This paper presents a secure and efficient system that enables multi-keyword ranked search over encrypted cloud data while enforcing fine-grained access control. The system involves three main entities: a data owner, a cloud server, and a data user. The data owner extracts keywords from each document, calculates their TF-IDF scores, and generates encrypted index vectors using a k-Nearest Neighbor-based encryption scheme. These encrypted indexes, along with the encrypted documents, are uploaded to the cloud server.

To ensure only authorized users can access the data, symmetric keys used for file encryption are protected using Attribute-Based Encryption (ABE). Data users generate encrypted queries known as trapdoors based on their search keywords and submit them to the cloud server. The server performs similarity computations between the trapdoor and the encrypted indexes, returning the top-k most relevant documents without learning their contents or the search query.

The proposed system ensures data confidentiality, hides access patterns, and protects user queries, all while delivering relevant search results. It balances security and usability, supporting practical cloud applications where users need to search over sensitive data while complying with strict access control policies.

The global financial ecosystem handles vast sums of money daily while catering to billions of individuals worldwide. However, this massive system faces several persistent challenges, including high operational costs due to multiple intermediaries, delays in transactions, excessive paperwork, and inefficiencies in data management. Traditional trade financing methods often lead to disruptions in operations, making liquidity management difficult for businesses.

Blockchain technology presents a transformative solution by enabling seamless, secure, and decentralized financial transactions. It simplifies cross-border trade and enhances transparency in financial operations, reducing reliance on intermediaries like regulators and stock exchanges. This decentralization not only lowers costs but also streamlines processes, making financial transactions more efficient and secure.

DOI: 10.48175/IJARSCT-24943

IV. SYSTEM ARCHITECTURE

The architecture of the proposed system is composed of three key entities: the Data Owner, the Cloud Server, and the Data User. Each plays a critical role in ensuring secure, efficient, and privacy-preserving access to cloud-stored data.

The Data Owner is responsible for preparing and uploading encrypted documents to the cloud. Prior to uploading, each document is analyzed to extract keywords, which are then used to create a secure searchable index. The index is encrypted using a modified k-Nearest Neighbor (kNN) encryption technique to enable similarity-based matching while preserving keyword privacy. Additionally, documents are encrypted using symmetric encryption, and the keys are protected using Attribute-Based Encryption (ABE) to enforce fine-grained access control.

The Cloud Server stores both encrypted documents and their corresponding encrypted indexes. It is considered semi-trusted—it performs search operations but should not learn the content of documents or search queries. Upon receiving an encrypted search query (trapdoor) from a Data User, the server computes similarity scores between the trapdoor and stored indexes, then returns the most relevant results.

V. IMPLEMENTATION

The implementation phase plays a pivotal role in demonstrating the practical viability of the proposed system. In this project, we have developed a secure and efficient search mechanism that allows users to retrieve encrypted cloud data using multiple keywords while preserving both privacy and access control.

The system is built using Java for the backend logic, while MySQL handles the data storage layer. The user interface is designed using HTML, CSS, and JavaScript, offering a simple and responsive experience. We also make use of JSP (JavaServer Pages) and Servlets to handle server-side processes and manage user requests.

The core functionality of the system revolves around enabling users to store data on the cloud in an encrypted format and perform keyword-based searches without revealing the actual data or the search terms to the cloud server. When a user uploads a file, it is first encrypted using AES (Advanced Encryption Standard) before being sent to the cloud. Simultaneously, a secure index is created using keywords extracted from the file content. These keywords are then encrypted and stored separately, ensuring that the cloud server cannot infer sensitive information.

To support multi-keyword search, the system generates a trapdoor based on the user's search query. This trapdoor is constructed in such a way that it can match encrypted keywords in the index without revealing the actual query. When a search is performed, the cloud server uses the trapdoor to compare against its encrypted index and returns a list of matching files, ranked by relevance. The relevance score is calculated based on keyword frequency and other predefined metrics.

Access control is another crucial aspect of the implementation. Only authorized users are permitted to perform searches or download files. This is achieved by assigning unique credentials to each user and validating them before granting access to any operations. Unauthorized access is strictly denied, and all user activities are logged for monitoring purposes.

The implementation was tested using a set of sample documents to evaluate the correctness, efficiency, and security of the search mechanism. The system successfully demonstrated the ability to retrieve relevant files based on multiple keyword queries while maintaining the confidentiality of both the data and the search inputs.

VI. RESULT

The primary objective of the system was to ensure secure, multi-keyword ranked search over encrypted cloud data while maintaining strict access control. After implementing the system, we conducted a series of tests to evaluate its functionality, performance, and security under realistic conditions.

To begin with, we uploaded a diverse set of documents to the cloud server. These documents contained varying content and keyword density, enabling us to assess how effectively the system could handle different types of search queries. Each file was encrypted before storage, and a corresponding secure index was generated for keyword-based retrieval.

When users performed multi-keyword searches, the system successfully generated encrypted trapdoors for each query. These trapdoors allowed the cloud server to search the encrypted index without revealing either the keywords or the file contents. The search results were returned in a ranked format, based on keyword relevance and occurrence frequency.

In all test cases, the most relevant documents consistently appeared at the top of the results, demonstrating the system's ability to rank accurately.

In terms of access control, the system reliably restricted unauthorized users from accessing either the search functionality or stored files. Attempts to bypass authentication were effectively blocked, confirming that the access control mechanisms were robust and correctly implemented.

Performance-wise, the search process remained efficient even as the number of files increased. Although the ranking computation added a slight overhead, it did not noticeably affect response time. The system maintained reasonable speed and scalability, making it suitable for practical deployment in environments with moderate to large data volumes.

Additionally, the encryption and indexing processes performed during file upload did not significantly delay the operation, making it feasible for real-world use where quick file uploads are essential.

In summary, the results confirmed that the system meets its goals: it provides secure, efficient, and accurate multi-keyword search functionality, upholds user privacy, and enforces access control without compromising usability or performance.

VII. CONCLUSION AND FUTURE WORK

This project presents a practical solution for enabling secure, multi-keyword ranked search over encrypted data stored in the cloud, while simultaneously enforcing strict access control policies. By combining symmetric encryption techniques with an efficient searchable indexing mechanism, the system allows users to retrieve relevant information without compromising data confidentiality or query privacy. The implementation demonstrates that it is feasible to support advanced search capabilities—such as multi-keyword queries and relevance-based ranking—even in a privacy-preserving environment. In addition, the system enforces user authentication effectively, ensuring that only authorized individuals can access the data or perform search operations.

Experimental results confirm that the system is reliable, scalable, and accurate. It maintains acceptable performance levels even as the volume of data increases, and the search results consistently reflect the relevance of keyword matches. The encryption and indexing processes also perform efficiently, making the solution suitable for real-world use cases where privacy and speed are critical.

Although the core objectives have been successfully met, there is still room for further improvement. Future work can focus on supporting fuzzy or semantic search, enabling users to retrieve data even when exact keywords are not known. Enhancing the system to support dynamic updates, such as adding or deleting documents and keywords without re-indexing the entire dataset, would increase its flexibility. Additionally, exploring lightweight cryptographic alternatives could improve performance on resource-constrained devices. Integration with decentralized storage solutions and the use of intelligent ranking algorithms that adapt to user behavior are also promising directions that could make the system more secure, transparent, and user-friendly. Overall, this work serves as a solid foundation for future advancements in privacy-preserving search over encrypted cloud data.

VIII. SIGNIFICANCE OF CLOUD COMPUTING

Cloud computing has become a cornerstone of modern digital infrastructure, offering scalable, flexible, and cost-effective solutions for data storage and processing. Its significance in this project lies in the ability to offload data to remote servers while maintaining ubiquitous access from any location. For organizations and individuals dealing with large volumes of data, the cloud eliminates the need for expensive local hardware and provides virtually unlimited storage capacity. Furthermore, cloud services enable collaboration, remote access, and real-time data sharing across geographically distributed teams. In the context of this project, cloud technology not only acts as a convenient storage platform but also challenges the traditional notions of data security and privacy. Since data is managed by third-party providers, ensuring confidentiality and controlled access becomes a critical concern. This project addresses those concerns by integrating searchable encryption and access control mechanisms, thereby allowing users to benefit from the convenience and power of the cloud without compromising sensitive information. The cloud's scalability also means that the proposed system can be easily extended to accommodate growing data needs and user bases, making it a highly practical solution for real-world deployment.Cloud computing plays a transformative role in modern information

DOI: 10.48175/IJARSCT-24943

systems by offering on-demand access to a shared pool of configurable computing resources, including networks, servers, storage, applications, and services. One of its most significant advantages is the scalability it provides—organizations can easily scale resources up or down based on demand without having to invest heavily in physical infrastructure. This dynamic resource allocation not only reduces capital expenditure but also optimizes operational efficiency.

In the context of data management and security, cloud computing enables the storage and retrieval of vast amounts of data from remote servers, making it accessible to users regardless of geographic location. This is particularly beneficial in collaborative environments, academic research, healthcare systems, and enterprise-level applications where real-time data access is crucial. Moreover, cloud platforms offer automated backup, disaster recovery, and high availability, ensuring business continuity and data durability.

However, the very features that make cloud computing powerful—such as remote access and multi-tenancy—also raise serious concerns regarding data privacy, integrity, and unauthorized access. This project leverages the advantages of cloud computing while addressing these concerns through the implementation of searchable encryption and access control mechanisms, allowing users to securely search encrypted data without revealing sensitive information to the cloud provider.

Additionally, cloud computing supports cost-effective deployment of large-scale applications, making it ideal for startups and academic projects that require high computing power but operate under tight budgets. The elasticity and flexibility of cloud services allow researchers and developers to test, deploy, and iterate solutions quickly. Cloud platforms like AWS, Microsoft Azure, and Google Cloud further offer APIs and machine learning tools that enhance the capability of systems developed on top of them.

IX. FUTURE ENHANCEMENT

While the current system achieves its intended goals of enabling secure, multi-keyword ranked search with access control over encrypted cloud data, there are several opportunities for further enhancement. One promising direction is the integration of fuzzy search capabilities, allowing the system to tolerate typographical errors or partial keyword matches, thereby improving user experience. Additionally, implementing semantic search—where the system understands the contextual meaning of queries—could significantly enhance result accuracy. Another area for improvement lies in supporting dynamic data operations, such as updating or deleting files and keywords without the need to rebuild the entire index. To cater to users on resource-constrained devices, future versions of the system could explore the use of lightweight cryptographic techniques that reduce computational overhead without compromising security. Moreover, incorporating machine learning-based ranking algorithms could personalize search results based on user behavior or preferences. Finally, integrating the system with decentralized or blockchain-based cloud platforms could further strengthen data integrity, auditability, and transparency, making the solution more robust for critical applications such as healthcare, legal, or government data management.In conclusion, this project demonstrates a secure, efficient, and practical solution for privacy-preserving, multi-keyword ranked search over encrypted cloud data with effective access control.he system successfully balances security, usability, and scalability, laying a strong foundation for secure cloud-based data retrieval. With future enhancements, including semantic search, dynamic updates, and decentralized storage integration, this solution has the potential to significantly improve real-world cloud data security systems across various industries such as healthcare, finance, and education, where data confidentiality and intelligent retrieval are crucial.

REFERENCES

[1] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, “Secure ranked keyword search over encrypted cloud data,” in *Proc. IEEE 30th Int. Conf. Distributed Computing Systems (ICDCS)*, 2010, pp. 253–262.

[2] D. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in *Proc. IEEE Symposium on Security and Privacy*, 2000, pp. 44–55.

[3] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy-preserving multi-keyword ranked search over encrypted cloud data,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 1, pp. 222–233, Jan. 2014.

DOI: 10.48175/IJARSCT-24943

[4] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: Improved definitions and efficient constructions,” in *Proc. ACM Conference on Computer and Communications Security*, 2006, pp. 79–88.

[5] S. Kamara and K. Lauter, “Cryptographic cloud storage,” in *Proc. Int. Conf. Financial Cryptography and Data Security*, 2010, pp. 136–149.

[6] Amazon Web Services, “AWS Security Best Practices,” [Online]. Available: https://aws.amazon.com/security/

[7] M. Armbrust et al., “A view of cloud computing,” *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[8] P. Mell and T. Grance, “The NIST Definition of Cloud Computing,” National Institute of Standards and Technology, 2011.

[9] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, “Fuzzy keyword search over encrypted data in cloud computing,” in *Proc. IEEE INFOCOM*, 2010, pp. 1–5.

[10] B. Wang, S. Yu, W. Lou, and Y. T. Hou, “Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud,” in *Proc. IEEE INFOCOM*, 2014, pp. 2112–2120.

[11] Y. Tang, D. Liu, and P. P. Lee, “Secure Logging as a Service—Delegating Log Management to the Cloud,” *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 2, pp. 148–162, Mar.-Apr. 2016.

[12] M. Naveed, M. Prabhakaran, and C. A. Gunter, “Dynamic searchable encryption via blind storage,” in *IEEE Symposium on Security and Privacy*, 2014, pp. 639–654.

[13] K. Yang, X. Jia, and K. Ren, “Secure and verifiable policy update outsourcing for big data access control in the cloud,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 12, pp. 3461–3470, Dec. 2015.

[14] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” in *Proc. IEEE INFOCOM*, 2010, pp. 534–542.

[15] C. Gentry, “A Fully Homomorphic Encryption Scheme,” Ph.D. dissertation, Stanford University, 2009.

[16] H. Liang, L. Xiong, and J. Liu, “Searchable encryption with access control for multi-owner data sharing in cloud computing,” in *Proc. ACM SAC*, 2015, pp. 1691–1696.

[17] M. Blaze, G. Bleumer, and M. Strauss, “Divertible protocols and atomic proxy cryptography,” in *Advances in Cryptology—EUROCRYPT’98*, 1998, pp. 127–144.

[18] D. Boneh, G. Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in *Advances in Cryptology—EUROCRYPT 2004*, pp. 506

DOI: 10.48175/IJARSCT-24943