A Rankable Boolean Searchable Encryption Scheme Supporting Dynamic Updates in a Cloud Environment

Mrs.M.Swathi, Assistant professor, Department of CSE, Narayana Engineering College, Gudur.

D.Sanjana Reddy, Department of CSE, Narayana Engineering College, Gudur.

Abstract: *In today's digital world, cloud storage has become a practical solution for storing important documents and records. Cloud computing provides services like computation, software, data access, and storage without needing users to understand the physical systems behind them. This allows individuals and organizations to store data remotely and access high-quality applications without managing local hardware and software. Despite these benefits, cloud storage introduces new security risks regarding data integrity. Users must trust cloud service providers to secure their valuable information, making security a critical concern. Cloud storage reduces costs related to software and maintenance, offering better performance and scalability. However, this increased reliance on internet-based services also heightens vulnerability to security breaches, deterring some organizations from adopting cloud solutions. Innovations like rankable Boolean searchable encryption schemes address these security challenges by enabling users to search encrypted data and retrieve relevant results. While cloud storage offers significant advantages, ensuring data security remains crucial as the digital landscape evolves.*

I.INTRODUCTION

Cloud computing is the next generation of internet technology, offering a range of services like computing power, infrastructure, applications, and business processes on demand. It allows users to access data and resources from any location at any time, reducing infrastructure costs, enhancing scalability, and eliminating maintenance needs.

The rise of cloud computing has accelerated data production and transfer, ushering in the era of big data. Many users and enterprises outsource data storage and computations to cloud servers, saving on storage costs and system maintenance. However, frequent security incidents have raised concerns about data confidentiality, prompting the use of data encryption.

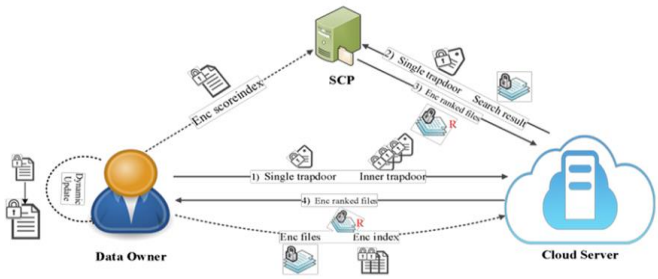
While encryption ensures data security, it complicates practical functions like keyword searches. Searchable encryption addresses this by allowing encrypted data to be searched using keywords. This concept, proposed by Goldreich and Ostrovsky, enables secure searches without exposing data.

The goal of a rankable Boolean searchable encryption scheme with dynamic updates in a cloud environment is to enable secure, efficient searches of encrypted cloud data. Users can store data in encrypted form and search it without decrypting, ensuring both security and usability.

II. METHODS AND RELATED WORK

In the existing system, users rely on conventional file management methods that lack robust security features necessary to protect sensitive digital assets. These methods involve manual file handling, such as storing files on local devices, sending files via email or unsecured file-sharing platforms, and managing access permissions through basic user credentials. The convenience of unsecured or consumer-grade file-sharing platforms often comes at the expense of robust encryption, access controls, and audit trails, leaving data susceptible to breaches and unauthorized access. Misconfigured sharing settings can inadvertently expose sensitive files.

THE RBDC SCHEME



RBDC Model: The RBDC scheme involves three entities: the Data Owner, Cloud Server, and SCP (Search Control Proxy) In the model of the RBDC scheme, the offline transmission phase, indicated by dotted lines, is executed first. During this phase, the Data Owner transfers encrypted files and encrypted keyword indices to a Cloud Server, while encrypted score indices are transferred to the SCP.

1. The Data Owner transfers the search trapdoor to a Cloud Server and initiates the Search Request.
2. After searching, the Cloud Server transfers the search results and search trapdoor to the SCP.
3. After ranking search results by score indices, the SCP transfers the ranked encrypted files to a Cloud Server.
4. The Cloud Server transfers the ranked encrypted files to the Data Owner, completing the RBDC scheme.

Data Owner: The Data Owner is responsible for key generation throughout the search process and for generating encrypted files using a symmetric encryption algorithm, thereby initiating the search. It is tasked with generating keyword sets corresponding to file sets and producing inverted indices based on these sets. These inverted indices are encrypted and uploaded to a Cloud Server, which handles the generation of keyword indices. To support Boolean search, the indices comprise two components: single keyword indices and indices of keyword intersections. For a rankable search, the Data Owner must generate a forward score index for each file. Additionally, the Data Owner generates trapdoors corresponding to each keyword to be searched. Furthermore, when returning search results, the Data

Owner decrypts the data to obtain the searched files. If the keyword set changes (additions, deletions, or modifications), dynamic updating of the keyword set is necessary.

Cloud Server: A Cloud Server primarily receives encrypted indices transferred from the Data Owner. It also accepts Search Requests from trusted users along with corresponding search trapdoors and conducts searches. Additionally, a Cloud Server receives Search Requests sent by the Data Owner and the file set ranked by SCP.

SCP (Search Control Proxy): SCP is primarily responsible for receiving encrypted score indices in the scheme. It receives encrypted character strings transferred by a Cloud Server to search and rank keywords and returns corresponding document tags.

Security Threats: Security threats in two models, namely, the known ciphertext model and the known background model are considered in the RBDC scheme. The Data Owner and SCP are considered as completely trusted entities in the scheme, while any Cloud Server is curious but honest. The Cloud Server honestly stores all data documents belonging to the Data Owner according to the specified protocol of algorithms while it is curious about the stored data. That is, the Cloud Server tends to obtain all data and metadata pertaining to the Data Owner by inferring or analyzing enciphered data and search trapdoors.

Security and Performance analysis

The security and performance of the RBDC scheme are analyzed herein. The scheme is compared with existing schemes from two perspectives: performance and function. Finally, the search efficiency and the index storage efficiency are assessed

In the known ciphertext model, attackers can establish a linear equation through the known ciphertexts, thus calculating the true values of encrypted indices and search trapdoors. Considering encrypted indices, the two parts sEIndex and iEIndex of the encrypted indices EIndex are both known to a Cloud Server, while the values of sub-indices corresponding to each keyword therein are unknown. sEIndex and iEIndex are separately encrypted using the random vector random vector vi ∈ V, random number r ∈ R, and GM and Paillier encryption algorithms, thus constructing a linear equation set:

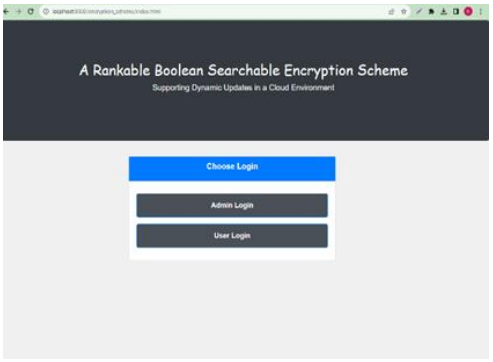
$$\begin{cases} \sum_{i=1}^{|\mathcal{W}|} \left(\boldsymbol{v}_i \cdot Enc_{\mathrm{GM}}\left(ID_i\right) \cdot Enc_{\mathrm{PL}}\left(ID_i\right)\right) + \boldsymbol{v}_r \cdot r = \boldsymbol{sE\tilde{I}ndex}, \\ \sum_{j=i+1}^{|\mathcal{W}|} \left(\boldsymbol{v}_i \cdot Enc_{\mathrm{GM}}\left(ID_{i\cap j}\right) \cdot Enc_{\mathrm{PL}}\left(ID_{i\cap j}\right)\right) \\ \qquad + \boldsymbol{v}_r \cdot r = \boldsymbol{iE\tilde{I}ndex}, \end{cases}$$

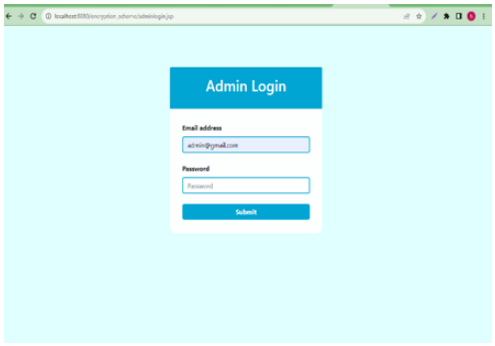
III.RESULTS AND DISCUSSIONS

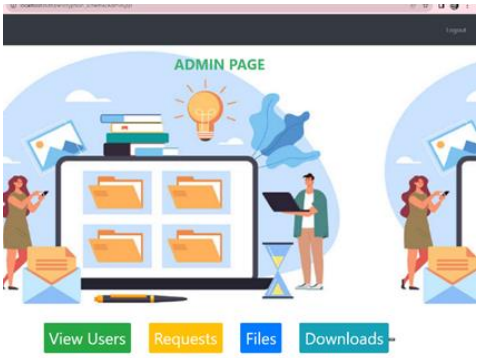
Scheme	Boolean	Ranking	Dynamic update	Search efficiency	Storage efficiency
MRSE	×	√	√	$O\left(\lvert W'\rvert^2 \lvert D\rvert\right)$	$O\left(strg\left(\sum_w \#DB(w)\right)\right)$
OXT	√	×	×	$O\left(\lvert W'\rvert^2 M\right)$	$O\left(strg\left(\sum_w \#DB(w)\right)+\sum_w strg\left(\sum_{v\in co(w)} \#DB(w)\cap DB(v)\right)\right)$
IBE	√	×	×	$O\left(\lvert W'\rvert^2 M\right)$	$O\left(strg\left(\sum_w \#DB(w)\right)+\sum_w strg\left(\sum_{\substack{v\in co(w)\\ T_{w,v}>p}} \#DB(w)\cap DB(v)\right)\right)$
RBDC	√	√	√	$O\left(\lvert W'\rvert^2\right)$	$O\left(strg\left(\#\boldsymbol{SEIndex}\right)+strg\left(\lvert W-1\rvert\#\boldsymbol{iEIndex}\right)\right)$

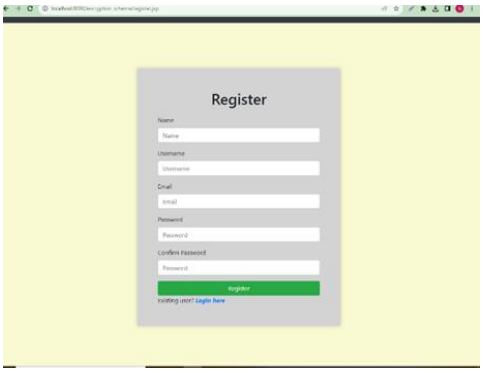
Comparison of RBDC with other schemes is facilitated by referring to the data in TABLE 1: M represents the length of the longest inverted indices generated by MRSE [4] and OXT [5]. #DB (w) denotes the length of inverted indices generated by schemes MRSE, OXT, and IBE [6];strg refers to the storage space of indices. From the perspective of functions of schemes, RBDC supports multi-keyword Boolean search compared with IBE. Compared with MRSE and OXT, RBDC can rank searched files. RBDC supports dynamic update of keyword indices in comparison with MRSE, OXT, and IBE. Regarding the performance of schemes, the time complexity of schemes is assessed at first. The keyword set to be searched is assumed to be W = w1,w2, . . . ,wq . At first, the single-keyword search trapdoor of each keyword is taken to have multiplication and power operations with the single-keyword indices, and the search efficiency is O (|W|). Then, the search trapdoor itwq for intersections of keywords w1,w2, . . . ,wq−1 is taken to have multiplication and power operations with the index iEIndex of keyword intersections and the search efficiency is O |W| 2 . Then, the time efficiency of the search algorithm in RBDC is O |W| 2 . Compared with MRSE and OXT that also support Boolean searching, RBDC improves the efficiency of the search algorithm. The time complexity of the search algorithm of RBDC is lower than that of IBE mainly because IBE only supports single-keyword search functions intersections. RBDC further improves the index storage efficiency; because the single-keyword index sEIndex is a vector element, the storage efficiency of the scheme is O (strg (#sEIndex)). As the index iEIndex of keyword intersections is a dictionary containing (|W| − 1) vector elements, its storage efficiency is O (strg (|W − 1| #iEIndex)).

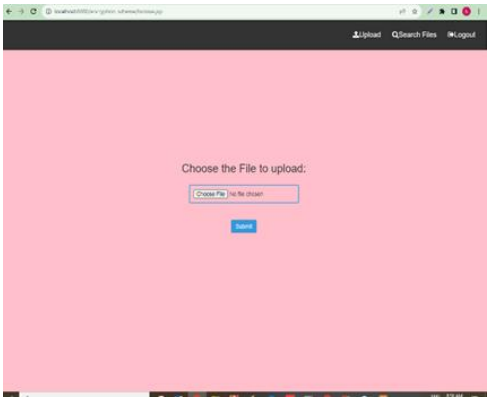
Snapshots:

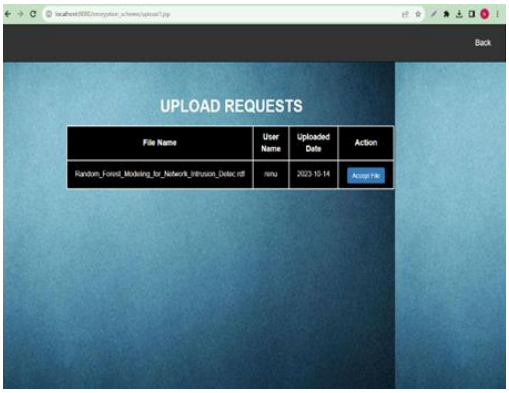












IV.CONCLUSION

To solve the problem whereby most existing searchable encryption schemes do not support multi-keyword Boolean searching, the RBDC scheme is proposed. Based on traditional searchable encryption schemes, the scheme generates encrypted secure indices with high search efficiency and high storage efficiency using GM and Paillier encryption algorithms. Encrypted indices of single keywords and keyword intersections are then constructed according to the tenets of set theory to achieve multi-keyword Boolean searches. TF-IDF is used to construct the forward score indices, and the searched files are ranked by virtue of the third-party entity SCP. Meanwhile, the method also can dynamically update multiple keywords and improve the efficiency thereof. Thereafter, security analysis shows that

the algorithm can counter two different types of security threat. Finally, the superiority of the RBDC scheme has been verified through function and performance analysis and comparison with other searchable encryption schemes.

V.REFERENCES

[1] O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious RAMs," J. ACM, vol. 43, no. 3, pp. 431-473, 1996.

[2] H.-A. Park, J. W. Byun, and D. H. Lee, "Secure index search for groups," in Proc. 2nd Int. Conf. Trust, Privacy Secur. Digital Bus., Piscataway, NJ, USA, 2005, pp. 128-140.

[3] S. Tahir, S. Ruj, A. Sajjad, and M. Rajarajan, "Fuzzy keywords enabled ranked searchable encryption scheme for a public cloud environment," Comput. Commun., vol. 133, pp. 102-114, Jan. 2019.

[4] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 222-233, Jan. 2014.

[5] Y. Zhang, Y. Zhao, Y. Wang, and Y. Li, "Searchable public-key encryption supporting simple Boolean keywords search," IEICE Trans. Fundamentals Electron., Commun. Comput. Sci., vol. E103A, no. 1, pp. 114-124, 2020.

[6] S. Kamara and T. Moataz, "Boolean searchable symmetric encryption with worst-case sub-linear complexity," in Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn., Cham, Switzerland: Springer 2017, pp. 94-124.