Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 16, Issue. 1: 2025
ISSN : **1906-9685**

An Encrypted Searchable Approach that is Both Secure and Verifiable Using Boolean Expressions as Support

Mr. B. AMARNATH REDDY[1],AMBAVARAPU SIREESHA[2]

1.Assistant Professor, #2 Pursuing M.C.A Department of Master of Computer Application

QIS COLLEGE OF ENGINEERING & TECHNOLOGY

Vengamukkapalem(V), Ongole, Prakasam dist., Andhra Pradesh- 523272

Abstract

Cloud Data Warehouse (CDW) platforms provide extensive storage and accessibility for business users, but protecting sensitive data warehouse (DW) content, such as dimension and fact data, requires encryption before outsourcing to the cloud. Traditional encryption methods hinder direct querying, creating challenges for efficient search operations. To address this, a Boolean Keyword Searchable Encryption (BKSE) approach using Partial Homomorphic Encryption (PHE) is proposed, enabling secure storage and query processing on encrypted data. The system utilizes a Binary Tree (BTREE) and Inverted Index for efficient data organization, supporting Boolean expressions like AND and OR for precise search results. A Bit Mapping Function maps and executes user queries, while Blockchain-based Ethereum Smart Contracts ensure tamper-proof data storage and authentication. Additionally, the HMAC authentication code secures the transmission of search results, preventing tampering. Processing efficiency is enhanced through a multi-VM packet routing technique, which splits and distributes query responses across virtual machines. Validated on a bank dataset, this approach ensures robust data confidentiality, integrity, and efficient search capabilities, offering an advanced solution for secure and verifiable querying in cloud-based data warehouses.

INTRODUCTION:

A data warehouse (DW) functions as a store for diverse sensitive or strategic data, where

aggregated results are obtained from a multidimensional framework and involve much greater data volumes. The cloud data warehouse (CDW) serves as a promising platform that provides substantial resource resilience and accessibility for enterprises. Due to the cloud's transparency but inquisitiveness, data encryption methods are typically used prior to outsourcing data to the cloud. The data warehouse is built on a multidimensional model that materializes numerous dimensions and information. A prevalent data warehouse type endorsed by several online analytical processing (OLAP) applications is the cube-based or multidimensional OLAP (MOLAP) model. In MOLAP, the data warehouse has many data cubes, with each cube representing a pre-computed perspective on the dimension and fact data. To facilitate analytical queries on an encrypted data warehouse, the user must execute a standard query, with the cube results delivered in an encrypted format. Subsequently, authorized users with a key can decrypt and retrieve the unencrypted query result. Consequently, this renders it unfeasible for several query outcomes. Searchable encryption (SE) methods are effective for facilitating numerous queries efficiently. SE is a technique that involves extracting keywords from a data cube, encrypting them, and subsequently uploading them to the cloud. Keywords are sent between data proprietors and data consumers within the secure channel. Upon the initiation of a search query, the search function will be executed by the cloud to identify a corresponding term from the user's request that matches those stored in the cloud.

LITERATURE SURVEY

1. An Attribute-Based Searchable Encryption Scheme for Cloud-Assisted IIoT:

https://ieeexplore.ieee.org/abstract/document/10039049

ABSTRACT: The searchable encryption (SE) is a particular case of structured encryption, which has been intensively researched in the secure cloud storage system. By constructing a structured secure index, such as encrypted multimaps (EMMs), encrypted inverted index (EII), etc., SE can achieve efficient keyword search over the encrypted data set. However, existing SE constructions do not take search permissions into consideration, resulting in the lack of a mechanism of the data access control, which may not be suitable for Industrial Internet of Things

(IIoT) applications, since an integrated industrial system contains all kinds of data with rigorous access permissions. In this article, we construct an attribute-based SE (ABSE) construction for a cloud-assisted IIoT application scenario. By designing the novel access policy-based structured secure index and the attribute-based search token, our construction achieves fine-grained keyword search privilege control over encrypted IIoT data as well as the same search complexity as the traditional SE. To the best of our knowledge, this is the first ABSE construction. We provide the correctness and security proofs for our construction. Experimental evaluation results in a real-world data set show the correctness and the practical search efficiency of the proposed ABSE.

2. A Pairing-Free Certificateless Searchable Public Key Encryption Scheme for Industrial Internet of Things:

https://ieeexplore.ieee.org/abstract/document/10147303

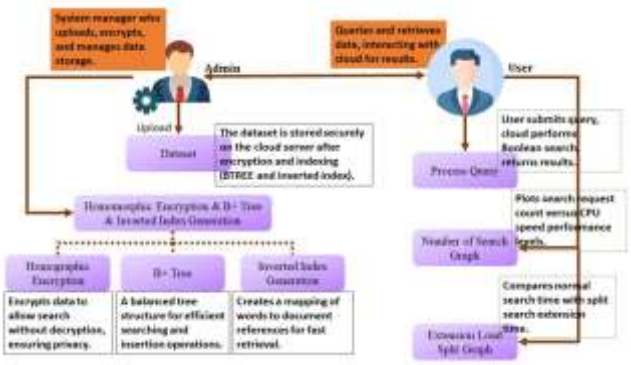
ABSTRACT: The Industrial Internet of Things (IIoT) collects a large amount of data through various types of sensors and intelligently processes this data using cloud computing, which is flexible, efficient, and cost-effective. Since IIoT data is stored on the cloud service provider's server, the data must be encrypted to protect the user's privacy. However, the encrypted data faces the search problem, which is usually solved by Public Key Encryption with Keyword Search (PEKS). In addition, most existing PEKS schemes are vulnerable to Inside Keyword Guessing Attacks (IKGA). Recently, some certificateless public key authenticated encryption with keyword search (CLPEKS) schemes have been proposed, which not only avoid the problems of certificate management and key escrow but can also resist IKGA. However, most of them rely on the expensive bilinear pairing. To overcome these problems, in this paper we propose a pairing-free CLPEKS scheme. The security of the proposed scheme is proved in the random oracle model. The analysis results show that the proposed scheme has better overall performance in terms of computational cost, communication cost and security properties.

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

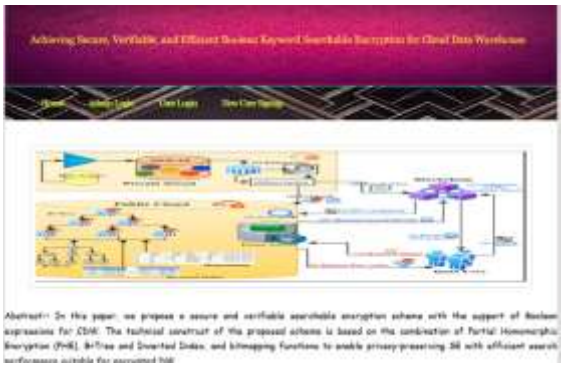
https://ieeexplore.ieee.org/abstract/document/10147833

ABSTRACT: At present, three problems exist in searchable encryption in cloud storage services: firstly, most traditional searchable encryption schemes only support single-keyword search while fail to perform Boolean searches; even if a few schemes support Boolean searching, the storage efficiency is also unsatisfactory. Secondly, most existing schemes do not support dynamic keyword updates, so the update efficiency is low. Thirdly, most existing schemes cannot meet all demands of users, to perform rankable searching over search files according to the importance of keywords. To solve these problems, a rankable Boolean searchable encryption scheme supporting dynamic updates in a cloud environment (RBDC) is proposed. By using Paillier and GM encryption algorithms, secure indices supporting dynamic updating are established. Based on applicable knowledge gleaned from cryptography and set theory, the indices of keyword intersections and the intersection search trapdoors are constructed to achieve multi-keyword Boolean search. With assistance of the SCP, score indices of each file are constructed according to the TF-IDF index, which allow ranking of files. Security analysis proofs that our scheme can ensure security in the known ciphertext model and the known background model. Experimental results prove that the scheme improves the search efficiency and the index storage efficiency.

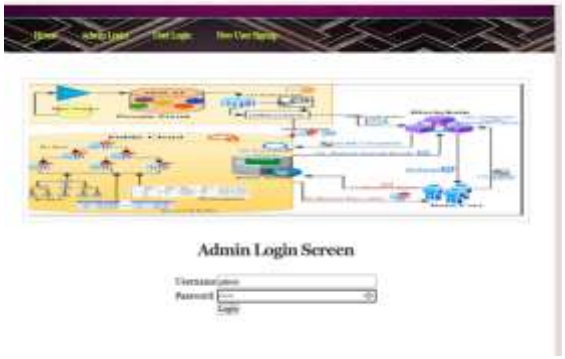
System Architecture:



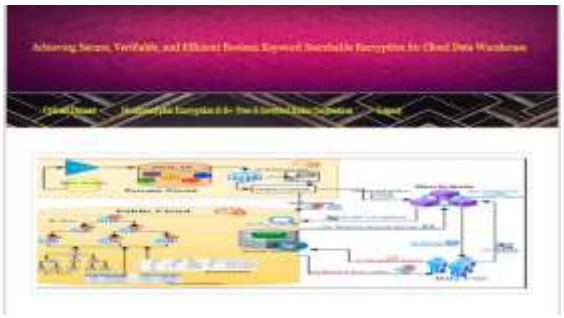
RESULTS



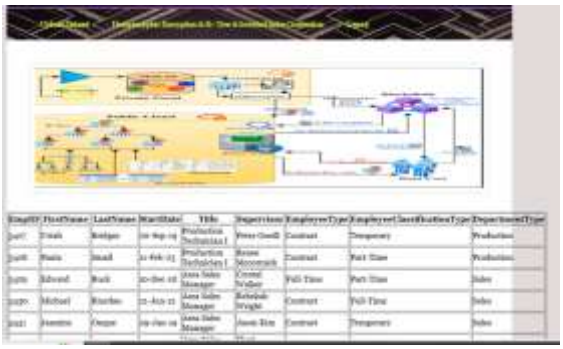
Home Screen



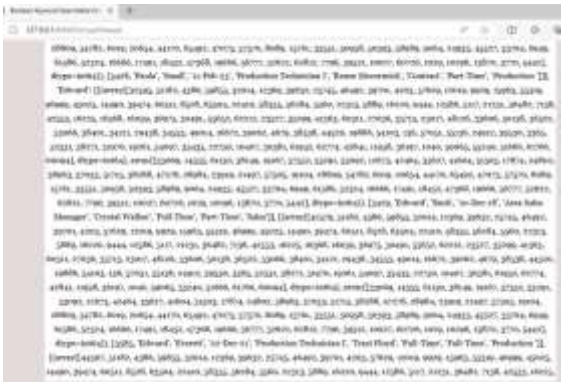
Admin Login



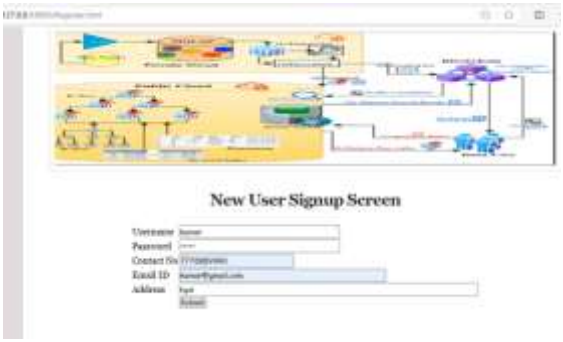
Upload Datasets



In above screen dataset loaded and now click on 'Homomorphic Encryption & B+ Tree & Inverted Index Generation' link to encrypt dataset and then generate BTREE + and get below output



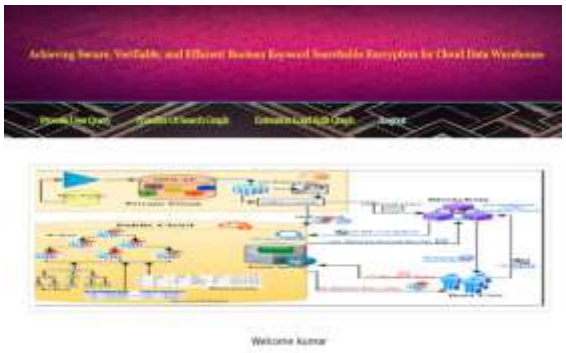
In above screen can see encrypted data stored inside BTREE and now logout and sign up new user



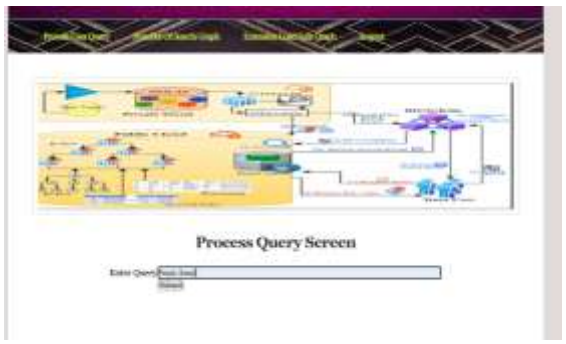
In above screen user is entering sign up details and then press button to get below output

In above screen user sign up details saved in Blockchain and in red colour text displaying all log obtained from Blockchain and this

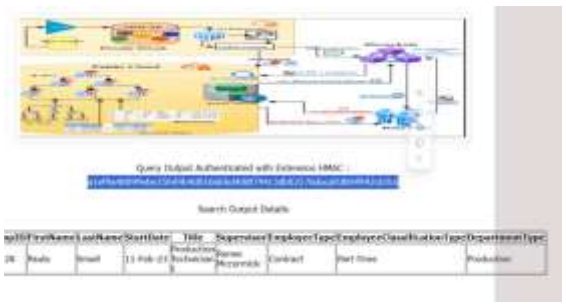
log contains details like Block No, Transaction No, hash code and many other details. Now click on 'User Login' link to get below page



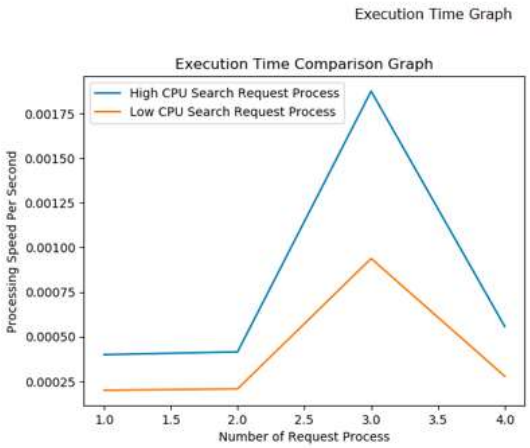
Home Screen



In above screen I entered some query to search detail of given person name and then press button to get below page



In above screen in blue colour text can see HMAC Extension1 authenticated code which will alert user about query result authentication and in tabular format can see the search result. Similarly you can search any details from dataset



In above graph x-axis represents 'Number of Search' and y-axis represents processing speed time and orange line represents LOW CPU which has less sped and blue line represents HIGH CPU which has more speed and now click on 'Extension Load Split Graph' link to get below graph

CONCLUSION AND FUTURE ENHANCEMENT

The Boolean Keyword Searchable Encryption (BKSE) approach addresses critical challenges in querying encrypted data within Cloud Data Warehouses

(CDWs). By integrating Partial Homomorphic Encryption (PHE) for secure storage and search operations, along with a Binary Tree (BTREE) and Inverted Index for efficient data organization, the system ensures precise and rapid query execution. The inclusion of Boolean expressions like AND and OR further enhances query accuracy, while the Bit Mapping Function facilitates seamless execution of user queries. Blockchain-based Ethereum Smart Contracts, built with Solidity, add a layer of trust and tamper-proof authentication, ensuring data integrity. The HMAC authentication code guarantees the secure transmission of search results, safeguarding against unauthorized alterations. Processing efficiency is significantly boosted by leveraging a multi-VM packet routing mechanism that optimally distributes query handling across virtual machines. Demonstrated on a bank dataset, the system effectively balances security, performance, and functionality, offering an advanced solution for secure and efficient querying in encrypted cloud environments. This development represents a significant advancement in ensuring confidentiality and integrity while maintaining practical usability for sensitive data operations.

Future Scope:

The future scope of this system lies in enhancing scalability and performance for large-scale cloud data warehouses. Integrating advanced machine learning algorithms for dynamic query optimization and incorporating multi-cloud environments for distributed storage could further improve efficiency. Additionally, adopting privacy-preserving techniques such as Zero-Knowledge Proofs (ZKPs) could further enhance security. The system could also be extended to handle real-time data processing, allowing for faster updates and query execution, making it adaptable to a broader range of industries and use cases.

REFERENCES

[1] H. Yin, W. Zhang, H. Deng, Z. Qin, and K. Li, ‘‘An attribute based searchable encryption scheme for cloud-assisted IIoT,’’ IEEE Internet Things J., vol. 10, no. 12, pp. 11014–11023, Jun. 2023, doi: 10.1109/JIOT.2023.3242964.

[2] X. Liu, H. Dong, N. Kumari, and J. Kar, ‘‘A pairing-free certificateless searchable public key encryption scheme for industrial Inter net of Things,’’ IEEE Access, vol. 11,

pp. 58754–58764, 2023, doi: 10.1109/ACCESS.2023.3285114.

[3] S. Guo, H. Geng, L. Su, S. He, and X. Zhang, ‘‘A rankable Boolean searchable encryption scheme supporting dynamic updates in a cloud environment,’’ IEEE Access, vol. 11, pp. 63475–63486, 2023, doi: 10.1109/ACCESS.2023.3284904.

[4] B. Chen, T. Xiang, D. He, H. Li, and K. R. Choo, ‘‘BPVSE: Publicly verifiable searchable encryption for cloud-assisted electronic health records,’’ IEEE Trans. Inf. Forensics Security, vol. 18, pp. 3171–3184, 2023, doi: 10.1109/TIFS.2023.3275750.

[5] L. Chen, Y. Xue, Y. Mu, L. Zeng, F. Rezaeibagha, and R. H. Deng, ‘‘CASE-SSE: Context-aware semantically extensible searchable symmetric encryption for encrypted cloud data,’’ IEEE Trans. Services Comput., vol. 16, no. 2, pp. 1011–1022, Mar. 2023, doi: 10.1109/TSC.2022. 3162266.

[6] X. Li, Q. Tong, J. Zhao, Y. Miao, S. Ma, J. Weng, J. Ma, and K. R. Choo, ‘‘VRFMS: Verifiable ranked fuzzy multi-keyword search over encrypted data,’’ IEEE Trans. Services Comput., vol. 16, no. 1, pp. 698–710, Jan. 2023, doi: 10.1109/TSC.2021.3140092.

[7] Q. Zhang, S. Wang, D. Zhang, J. Sun, and Y. Zhang, ‘‘Authorized data secure access scheme with specified time and relevance ranked keyword search for industrial cloud platforms,’’ IEEE Syst. J., vol. 16, no. 2, pp. 2879–2890, Jun. 2022, doi: 10.1109/JSYST.2021. 3093623.

[8] X. Wang, J. Ma, X. Liu, Y. Miao, Y. Liu, and R. H. Deng, ‘‘For ward/backward and content private DSSE for spatial keyword queries,’’ IEEE Trans. Dependable Secure Comput., vol. 20, no. 4, pp. 3358–3370, Jul. 2023, doi: 10.1109/TDSC.2022.3205670.

[9] J. Fu, N. Wang, B. Cui, and B. K. Bhargava, ‘‘A practical framework for secure document retrieval in encrypted cloud file systems,’’ IEEE Trans. Parallel Distrib. Syst., vol. 33, no. 5, pp. 1246–1261, May 2022, doi: 10.1109/TPDS.2021.3107752.

[10] F. Li, J. Ma, Y. Miao, Z. Liu, K. R. Choo, X. Liu, and R. H. Deng, ‘‘Towards efficient verifiable Boolean search over encrypted cloud data,’’ IEEE Trans. Cloud Comput., vol. 11, no. 1, pp. 839–853, Jan. 2023, doi: 10.1109/TCC.2021.3118692.

[11] R. Zhou, X. Zhang, X. Wang, G. Yang, H.-N. Dai, and M. Liu, ‘‘Device oriented

keyword-searchable encryption scheme for cloud-assisted industrial IoT,'' IEEE Internet Things J., vol. 9, no. 18, pp. 17098–17109, Sep. 2022, doi: 10.1109/JIOT.2021.3124807.

[12] L. Xue, ''DSAS: A secure data sharing and authorized search able framework for e-Healthcare system,'' IEEE Access, vol. 10, pp. 30779–30791, 2022, doi: 10.1109/ACCESS.2022.3153120.

[13] Y. Yang, R. H. Deng, W. Guo, H. Cheng, X. Luo, X. Zheng, and C. Rong, ''Dual traceable distributed attribute-based searchable encryption and ownership transfer,'' IEEE Trans. Cloud Comput., vol. 11, no. 1, pp. 247–262, Jan. 2023, doi: 10.1109/TCC.2021.3090519.

[14] P. Zhang, Y. Chui, H. Liu, Z. Yang, D. Wu, and R. Wang, ''Efficient and privacy-preserving search over edge–cloud collaborative entity in IoT,'' IEEE Internet Things J., vol. 10, no. 4, pp. 3192–3205, Feb. 2023, doi: 10.1109/JIOT.2021.3132910.

[15] J. Liu, Y. Li, R. Sun, Q. Pei, N. Zhang, M. Dong, and V. C. M. Leung, ''EMK-ABSE: Efficient multikeyword attribute-based searchable encryption scheme through cloud-edge coordination,'' IEEE Internet Things J., vol. 9, no. 19, pp. 18650–18662, Oct. 2022, doi: 10.1109/JIOT.2022.3163340.

[16] Q. Liu, Y. Tian, J. Wu, T. Peng, and G. Wang, ''Enabling verifiable and dynamic ranked search over outsourced data,'' IEEE Trans. Services Com put., vol. 15, no. 1, pp. 69–82, Jan. 2022, doi: 10.1109/TSC.2019.2922177.

[17] G. Liu, G. Yang, S. Bai, H. Wang, and Y. Xiang, ''FASE: A fast and accurate privacy-preserving multi-keyword top-k retrieval scheme over encrypted cloud data,'' IEEE Trans. Services Comput., vol. 15, no. 4, pp. 1855–1867, Jul. 2022, doi: 10.1109/TSC.2020.3023393.

[18] M. Zeng, H. Qian, J. Chen, and K. Zhang, ''Forward secure public key encryption with keyword search for outsourced cloud storage,'' IEEE Trans. Cloud Comput., vol. 10, no. 1, pp. 426–438, Jan. 2022, doi: 10.1109/TCC.2019.2944367.

[19] Z.-Y. Liu, Y.-F. Tseng, R. Tso, Y.-C. Chen, and M. Mambo, ''Identity certifying authority-aided identity-based searchable encryption framework in cloud systems,'' IEEE Syst. J., vol. 16, no. 3, pp. 4629–4640,

Sep. 2022, doi: 10.1109/JSYST.2021.3103909.

[20] P. Chaudhari and M. L. Das, ‘‘KeySea: Keyword-based search with receiver anonymity in attribute-based searchable encryption,’’ IEEE Trans. Services Comput., vol. 15, no. 2, pp. 1036–1044, Mar. 2022, doi: 10.1109/TSC.2020.2973570.

Author1:

Mr. B. Amarnath Reddy is an Assistant Professor in the Department of Master of Computer Applications at QIS College of Engineering and Technology, Ongole, Andhra Pradesh. He earned his M.Tech from Vellore Institute of Technology(VIT), Vellore. His research interests include Machine Learning,Programming Languages. He is committed to advancing research and fostering innovation while mentoring students to excel in both academic and professional pursuits.