International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

SECURE AND VERIFIABLE SEARCHABLE ENCRYPTION FOR CLOUD DATA WAREHOUSES

K. VIJAYA LAXMI [1], ANKIREDDY RAKESH REDDY[2], ABHISHEK NUCHU[3], BODDUPALLY VAMSHI[4], CHEEDALLA SRIJAN[5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— With the growing reliance on Cloud Data Warehouse (CDW) platforms for large-scale data storage and analytics, ensuring the security of sensitive information has become increasingly important. To protect data privacy, organizations often encrypt their warehouse data before outsourcing it to the cloud. However, this encryption limits the ability to perform meaningful queries using conventional tools. In this work, we introduce a secure and efficient searchable encryption scheme specifically designed for encrypted CDW environments. Our approach employs Partial Homomorphic Encryption (PHE), Inverted Index structures, and bitmapping techniques to enable fast and privacy preserving search over encrypted datasets. To further ensure the integrity and trustworthiness of search results without involving a third-party auditor, we integrate blockchain and smart contract mechanisms for decentralized verification, index management, and secure query handling. Experimental results validate the effectiveness of our solution, showing improvements in both search performance and data security compared to existing methods. In addition, our design ensures scalability and adaptability in real-world CDW scenarios. The proposed scheme bridges the gap between data privacy and practical query usability, making it a viable solution for secure cloud-based analytics.

Index Terms – Cloud Data Warehouse (CDW), searchable encryption, Partial Homomorphic Encryption (PHE), blockchain, smart contracts, encrypted data

search, inverted index, bitmap indexing, cloud security, privacy-preserving search, secure cloud analytics, data integrity, encrypted query processing.

I. INTRODUCTION

Typically, a data warehouse (DW) serves as the repository for a wide array of sensitive or strategic data, where the aggregated outcomes are derived from a multidimensional framework and feature significantly larger data volumes. The cloud data warehouse (CDW) represents a promising platform that offers high resource resilience and accessibility for businesses. Since the cloud is honest but curious, data encryption techniques are generally applied before outsourcing the data to the cloud. Since the data warehouse is constructed based on multidimensional model where multiple dimensions and facts are materialized. One of the common DW models supported by many online analytical processing (OLAP) tools is cube-based or multidimensional OLAP(MOLAP). In MOLAP DW consists of a number of data cubes, where each cube represents the pre computed view of the dimension and fact data. To support analytical queries over encrypted DW, the user needs to make a normal query, while the cube result should be returned in an encrypted format. Then, authorized users with a key can decrypt and access the plain query result. However, this makes it impractical for multiple query results. Searchable encryption (SE) techniques are viable for supporting multiple queries in an efficient manner. SE is a method in which keywords are extracted from a data cube, encrypted and uploaded to the cloud. Keywords are shared between data owners and data users in the secure channel. Once a search query is made, the search function will be performed by cloud to find a matching keyword from the data user's request with the ones stored on the cloud. Some studies have proposed a solution to support multiple keyword searches, such as multi-keyword rank searches and range searches with the search structure of a normal index, an inverted index, or a Tree index.

II. RELATED WORK

A. An attribute-based searchable encryption scheme for cloud-assisted IIoT

Attribute-based searchable encryption (ABSE) scheme tailored for Cloud assisted Industrial Internet of Things (IIoT) environments. In IIoT, vast amounts of sensitive data are generated by connected devices such as sensors, machines, and control systems. This data is typically stored

in the cloud for accessibility, but ensuring its security while maintaining efficient searchability is a significant challenge. The proposed scheme uses attribute-based encryption to encrypt data based on user-defined attributes, allowing authorized users to search encrypted data based on specific attributes without revealing any sensitive information. This scheme is designed to offer fine-grained access control, where search capabilities are determined by the attributes associated with the data, providing flexibility and enhanced privacy. By integrating this with cloud storage, the system enables secure and efficient querying of encrypted data generated by IIoT devices, ensuring both confidentiality and scalability.

The scheme aims to address the dual challenges of securing sensitive IIoT data and providing fast, scalable search capabilities without compromising privacy. This project will involve the development of encryption protocols, search algorithms, and the integration of cloud services to support secure data management in the IIoT ecosystem.

B. A pairing-free certificateless searchable public key encryption scheme for industrial Internet of Things

The project aims to develop a pairing-free certificateless searchable public key encryption (CL-SPE) scheme specifically designed for the Industrial Internet of Things (IIoT). In IIoT environments, large-scale networks of interconnected devices generate massive amounts of sensitive data that need to be securely stored and queried. Traditional encryption schemes often require complex pairing operations or certification authorities, which can introduce overhead and potential bottlenecks, especially in resource-constrained IIoT devices.

This project proposes a certificateless encryption approach, eliminating the need for a certificate authority while still providing secure, efficient, and searchable public key encryption for IIoT systems. The proposed scheme will support efficient searching over encrypted data without requiring pairing-based cryptographic operations, reducing computational complexity and improving performance on low-power devices.

By combining security with the ability to perform searches on encrypted data, the scheme will ensure data confidentiality, access control, and scalability within the IIoT ecosystem. The project will focus on developing encryption protocols that facilitate secure querying and integrating them with IIoT devices and cloud systems,

ensuring that both performance and security requirements are met for industrial applications.

C. A rankable Boolean searchable encryption scheme supporting dynamic updates in a cloud Environment

A Rankable Boolean searchable encryption (RBSE) scheme that supports dynamic updates in a cloud environment. In cloud computing, data security and privacy are critical concerns, particularly when dealing with sensitive information that needs to remain confidential while still being searchable. Traditional searchable encryption schemes often struggle with efficiently supporting Boolean queries, especially as the dataset evolves with dynamic updates such as additions, deletions, or modifications.

This project proposes a rankable Boolean searchable encryption method that allows users to perform Boolean queries on encrypted data in the cloud, with the added capability of ranking the search results based on relevance or other criteria. Additionally, the system will support dynamic updates, ensuring that as data changes, the encrypted indexes and search structures remain consistent and efficient. The project will focus on developing encryption protocols, updating mechanisms, and performance evaluation for secure cloud storage and search capabilities.

D. BPVSE: Publicly verifiable searchable encryption for cloud-assisted electronic health records

The BPVSE (Publicly Verifiable Searchable Encryption) project focuses on developing a secure, publicly verifiable encryption scheme designed for cloud-assisted electronic health records (EHRs).

As healthcare data is highly sensitive, securing electronic health records while enabling efficient search capabilities is a critical challenge. The proposed BPVSE scheme ensures that healthcare providers and other authorized entities can search over encrypted EHR data stored in the cloud without compromising privacy.

By integrating public verifiability, the system allows third parties, such as auditors or healthcare regulators, to independently verify the correctness of search results, without accessing the underlying sensitive data. This approach combines the benefits of searchable encryption with a verification mechanism to ensure data integrity and accountability.

The project will focus on designing secure search protocols, ensuring the efficiency of search operations, and providing a

framework for verification in cloud-based healthcare systems.

III. PROPOSED METHODOLOGY

In this paper, we propose a secure and verifiable searchable encryption scheme with the support of Boolean expressions for CDW. The technical construct of the proposed scheme is based on the combination of Partial Homomorphic Encryption (PHE), B+Tree and Inverted Index, and bitmapping functions to enable privacy-preserving SE with efficient search performance suitable for encrypted DW. To enhance the scalability without requiring a third party to support the verification of search results, we employed blockchain and smart contracts to automate authentication, search index retention, and trapdoor generation. For the evaluation, we conducted comparative experiments to show that our scheme is more proficient and effective than related works.

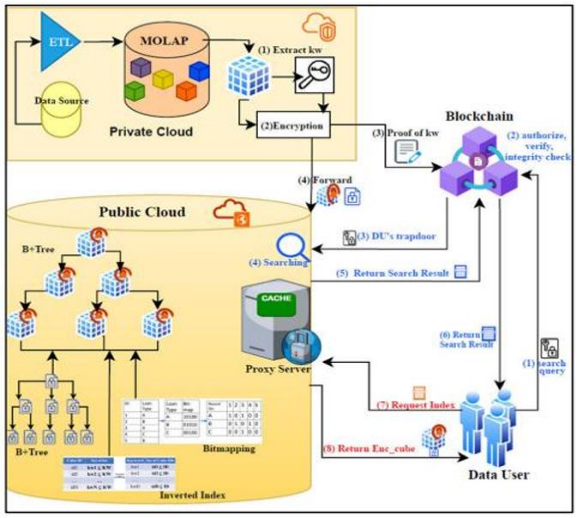
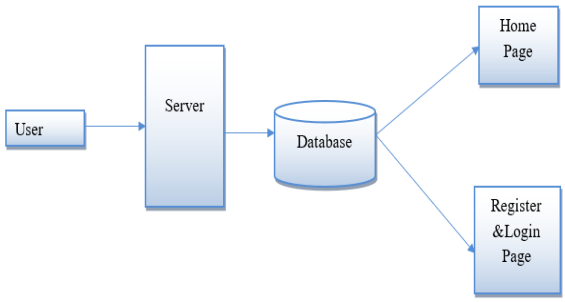


Fig. 1: System Overview

1. User Interface Design

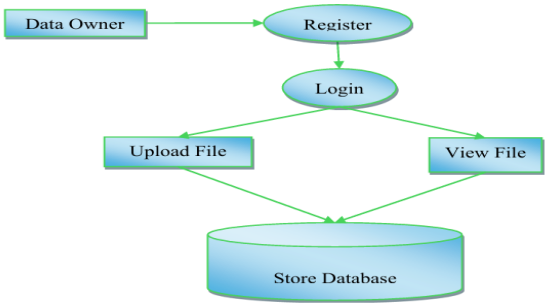
In this module we design the windows for the project. These windows are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server.

If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page.



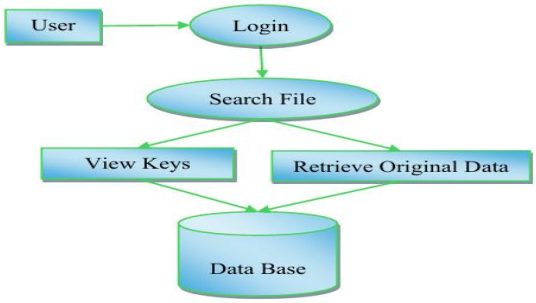
2. Data Owner

In this context, the data owner plays a crucial role in managing and securing the sensitive data stored in the Cloud Data Warehouse (CDW). The data owner is responsible for initially uploading the data cubes, which contain the multidimensional and fact data, to the cloud after encrypting them using Partially Homomorphic Encryption (PHE). The data owner ensures that only authorized users can access the encrypted data by defining access policies and sharing encryption keys securely.



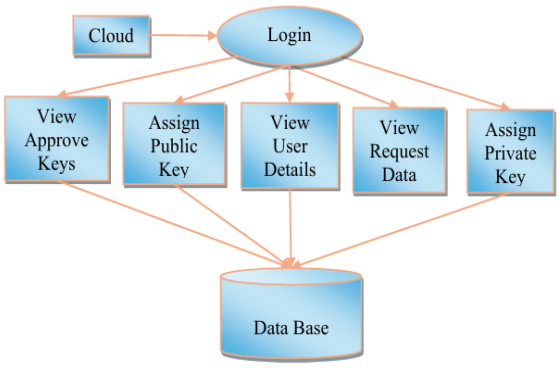
3. User

The user is an authorized individual who interacts with the Cloud Data Warehouse (CDW) to perform searches over the encrypted data cubes. Users are granted access based on the access control policies defined by the data owner, and they are provided with the necessary decryption keys to retrieve the query results. When a user submits a search query, they provide the relevant keywords or Boolean expressions to search through the encrypted data cubes stored in the cloud.



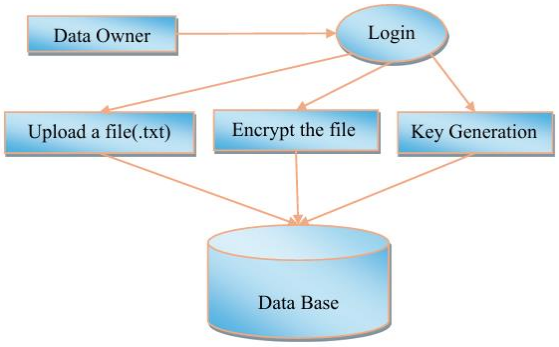
4. Cloud

The cloud acts as the storage and processing platform for the Cloud Data Warehouse (CDW), where the sensitive data cubes are stored in an encrypted format. The cloud is responsible for hosting the encrypted data and executing search queries submitted by authorized users without revealing any sensitive information. It performs the search operations over the encrypted data cubes using the searchable encryption (SE) techniques and returns the results in encrypted form, which can only be decrypted by users who possess the appropriate keys.

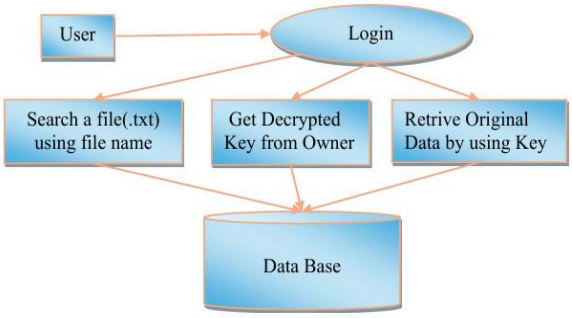


5. Upload

Uploading in the context of the proposed solution refers to the process of securely transferring encrypted data from a data warehouse (DW) to the cloud. The data, which includes sensitive dimension and fact data organized into cubes, is first encrypted using techniques like Partially Homomorphic Encryption (PHE) to ensure that it remains confidential during storage and access in the cloud. Keywords extracted from these encrypted cubes are also encrypted and then uploaded to the cloud storage.



6. Search Uploading in the context of the proposed solution refers to the process of securely transferring encrypted data from a data warehouse (DW) to the cloud. The data, which includes sensitive dimension and fact data organized into cubes, is first encrypted using techniques like Partially Homomorphic Encryption (PHE) to ensure that it remains confidential during storage and access in the cloud. Keywords extracted from these encrypted cubes are also encrypted and then uploaded to the cloud storage.



IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results show that the proposed searchable encryption scheme enables efficient and privacy-preserving search over encrypted Cloud Data Warehouse (CDW) data. By integrating Partial Homomorphic Encryption (PHE), inverted indexing, and bitmap techniques, the system achieves faster search performance while maintaining data confidentiality. The use of blockchain and smart contracts ensures secure and decentralized verification of

search results without requiring a third-party auditor.

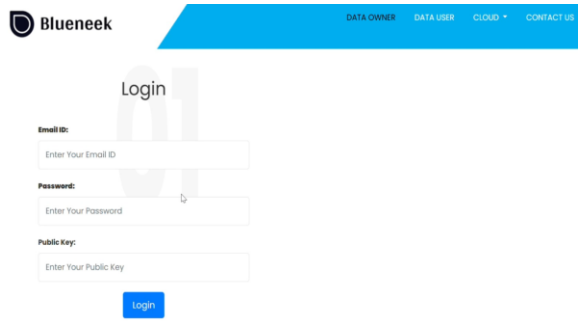


Fig. 2: Login

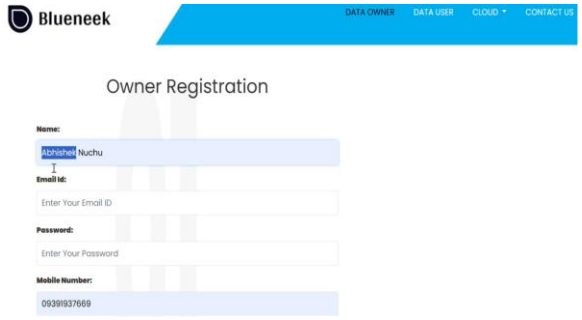


Fig. 3: Owner Registration

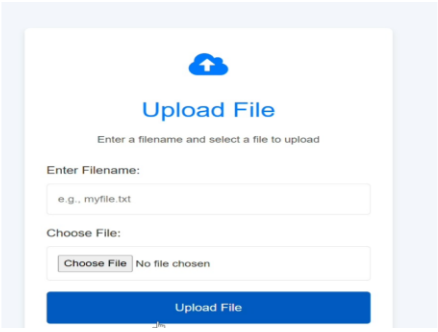


Fig. 4: Upload File

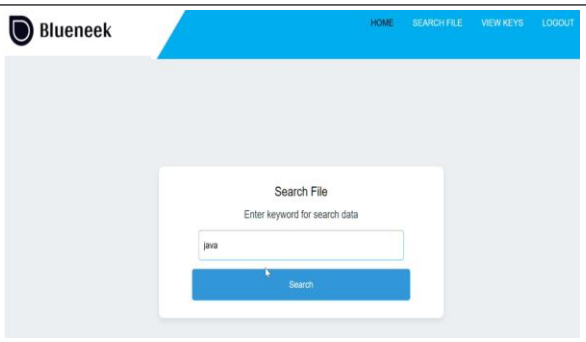


Fig. 5: Search File

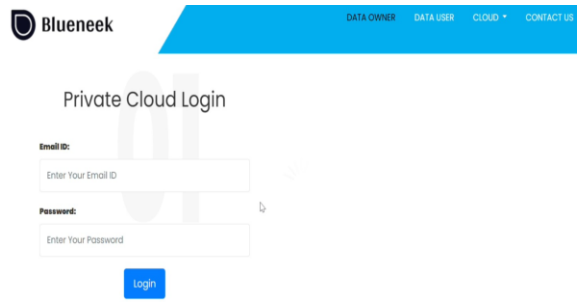


Fig. 6: Private Cloud Login

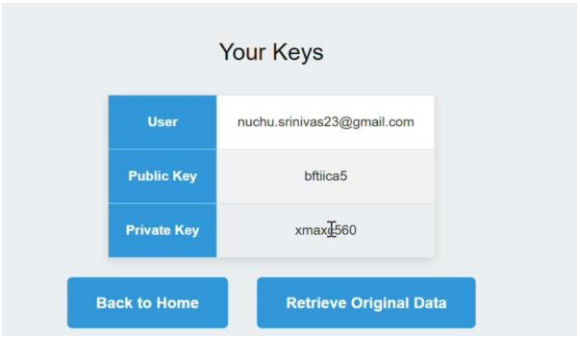


Fig. 7: Keys

V. CONCLUSION

In this paper, we have presented a flexible, verifiable, and secure searchable encryption scheme with support for boolean expression over encrypted data cubes within a cloudbased data warehouse. Our scheme enjoys both security and search performance

based on the integration of partial homomorphic encryption, inverted index, and B+Tree. In addition, we leveraged blockchain technology to streamline the automation of search permission verification, user authentication, and search result validation processes.

These tasks are executed in a manner that ensures scalability and immutability. Notably, we have utilized various search function types to suit different data types applicable for searching over multi dimentional data, such as inverted indexes, B+Trees, and bitmapping functions. Another key advantage of our proposed B+Tree indexing scheme is to reduce the search space. Our experiments have demonstrated that our scheme can significantly save time and resources. The system can also provide reasonable system throughput for supporting multiple concurrent OLAP query requests.

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 Internet 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] Y. Zheng, R. Lu, J. Shao, F. Yin, and H. Zhu, ‘‘Achieving practical symmetric searchable encryption with search pattern privacy over cloud,’’IEEE Trans. Services Comput., vol. 15, no. 3, pp. 1358–1370, May 2022,doi: 10.1109/TSC.2020.2992303.

[5] Maturi, S. Y. -(2024). Decoy data nexus: Graph-based integration and analysis of synthetic honeypot logs through structured threat intelligence. International Journal of Computational and Experimental Science and Engineering (IJCESEN), 10(4), 4255–4261. https://doi.org/10.22399/ijcesen.5010.

[6] J. Li, X. Lin, Y. Zhang, and J. Han, ‘‘KSF-OABE: Outsourced attribute-based

encryption with keyword search function for cloud storage,'' IEEE Trans. Services Comput., vol. 10, no. 5, pp. 715–725, Sep. 2017, doi:10.1109/TSC.2016.2542813.

[7] Pavan Kumar Adabala. (2026). Smart Retail Fuel Systems: IoT-Enabled Solutions for Loss Prevention and Environmental Safety. Computer Fraud and Security, 868–875. https://doi.org/10.52710/cfs.995.

[8] Bhagwat, V. B. (2026). Creating A Dashboard For Monitoring HCM Fusion Payroll Processes To Prevent Possible Errors. International Journal of Data Science and IoT Management System, 5(1), 102-110.

[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] Shashank A. (2025). Metadata-driven data integration framework: Automating enterprise data integration through declarative approaches. European Modern Studies Journal, 9(4), 9.

[11] Boyapati, P. K. Building a centralized data operations hub for healthcare enterprise integration. IJSAT-Int. J. Sci. Technol. 16 (2). https://doi.org/10.71097/IJSAT.v16.i2.3219

AUTHORS Profile



Ms. K. VIJAYA LAXMI received her B. Tech degree in Computer Science & Engineering from JNTUH, Hyderabad in 2015 and her M. Tech degree in Computer Science from JNTUH, Hyderabad in 2017. She is currently pursuing her Ph.D. degree in Computer Science & Engineering from Guru Nanak University, Hyderabad. She has been dedicated to the teaching field for the last 7 years. Her research area is Deep Learning. At present, she is working as an Assistant Professor in the CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



Mr. ANKIREDDY RAKESH REDDY pursuing B.Tech degree in Computer Science and Engineering at Guru

Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. ABHISHEK NUCHU pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. BODDUPALLY VAMSHI pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. CHEEDALLA SRIJAN pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.