IJARETY

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 12, Issue 3, May-June 2025

Impact Factor: 8.152

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

www.ijarety.in editor.ijarety@gmail.com

International Journal of Advanced Research in Education and TechnologY(IJARETY)

4-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203052

Secure and Verifiable Searchable Encryption for Cloud Data Warehouse

P. Chandra Sekhar[1], Nandala Vishal[2], Mohammed Asif [3], Mohammed Asaduddin[4]

Assistant Professor, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana, India[1]

Student, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana, India[2,3,4]

ABSTRACT: Ensuring Offering the security of sensitive data has become more crucial with the increasing deployment of Cloud Data Warehouse (CDW) platforms for storage and large-scale data analysis. Organizations prefer to encrypt their warehouse data before outsourcing it to the cloud to ensure data confidentiality. Encryption, however, restricts the use of legacy tools to enable useful queries. In this paper, we present an efficient and secure searchable encryption scheme for encrypted CDW platforms. Our scheme employs bitmapping techniques, inverted index data structures, and partial homomorphic encryption (PHE) to enable efficient and private search over encrypted data. We employ blockchain and smart contract techniques for decentralized verification, index updates, and secure query evaluation to further achieve search result accuracy and reliability without involving a third-party auditor. Experimental results confirm the efficiency of our scheme by estimating data security and search performance enhancement over existing practices. Apart from this, our design achieves scalability and responsiveness in real CDW deployments. The proposed technique fills the gap between data secrecy and useful query usability, thus enabling secure cloud-based analytics

KEYWORDS: Searchable Encryption, Verifiable Search, Cloud Data Warehouse (CDW), Secure Query Evaluation Data Privacy, Encrypted Data Retrieval, Encryption, Decryption.

I. INTRODUCTION

A multidimensional schema containing a great deal of sensitive data is stored in a data warehouse (DW). Firm availability and resilience are provided by the cloud data warehouse (CDW). Before being sent to the cloud, data is encrypted. Using cube-based or multidimensional OLAP (MOLAP) with pre-computed data cubes, the DW uses various dimensions and facts. Users receive encrypted results when they submit routine queries on encrypted DWs. Most queries cannot be decrypted, but authorized users with a key can. By extracting, encrypting, and uploading the keywords of data cubes to the cloud, where they can be safely shared, SE techniques make a large number of queries possible. The cloud uses stored keywords to match a search query. Methods offer solutions for multi-keyword searches, such as rank and range searches based on standard or inverted indexes, which speed up searches by taking more keyword inputs than standard methods. By mapping encrypted data keywords, the majority of studies optimize inverted indexes for keyword searches. However, for a variety of reasons, existing SE schemes have difficulty searching over encrypted DWs. Boolean searches linking keywords with indexing, rather than just multiple keyword SE, are used in cubes of more than one dimension. Because of the complex data types involved, encrypted DWs cannot be supported by current SE schemes, which rely on particular indexing structures and document arrays. Boolean expressions are used to support cloud-based encrypted data cubes that are outsourced. Partially Homomorphic Encryption (PHE) is the foundation of our suggested Searchable Encryption (SE) scheme, which encrypts keywords and uses three primary indexing techniques—B+Tree, inverted index, bitmapping functions, etc. In addition, we implemented and deployed smart contracts for search permission and result verification using blockchain technology. For cloud data warehouses, we recommend a fine-grained, secure, cryptographic-based access control system with effective and verifiable searchable encryption. Boolean expressions in the search query over encrypted data cubes that are outsourced to the cloud are also supported by our recently introduced searchable encryption.

II. LITERATURE REVIEW

H. Yin et. al (2023) 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.

X. Liu et. al (2023) 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.

S. Guo et. al (2023) 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. By combining secure search functionality with dynamic data updates and result ranking, the scheme aims to provide both privacy and performance, addressing the challenges of maintaining secure, searchable data in a constantly changing cloud environment. The project will focus on developing encryption protocols, updating mechanisms, and performance evaluation for secure cloud storage and search capabilities.

B. Chen et. al (2023) 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 scheme also ensures that only authorized users can perform searches, protecting patient privacy while maintaining the ability to access critical health information. 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.

L. Chen et.al (2023) The CASE-SSE (Context-aware Semantically Extensible Searchable Symmetric Encryption) project focuses on developing a sophisticated encryption scheme that enables efficient, context-aware searches over encrypted data stored in the cloud. In this system, symmetric encryption is used to secure sensitive data, while allowing users to perform search queries on the encrypted data without exposing it to unauthorized parties. The context-aware feature enhances search capabilities by tailoring the search process based on the specific context of the query, such as user roles or data categories, improving both search accuracy and security. Additionally, the semantically extensible aspect allows the system to dynamically adapt to evolving data types and query patterns, ensuring scalability and flexibility for cloud environments with diverse datasets. This scheme will enable secure, searchable cloud storage, where users can perform effective queries while preserving data privacy, with the flexibility to handle a variety of semantic contexts and maintain extensibility for future changes in data and access requirements. The project will involve developing encryption protocols, context-aware mechanisms, and performance evaluations to balance security, efficiency, and scalability in cloud-based data management.

Y . Yang et.al (2023) The Dual Traceable Distributed Attribute-Based Searchable Encryption (DT-DABSE) and Ownership Transfer project focuses on enhancing the security and flexibility of searchable encryption in distributed cloud environments, particularly for attribute-based access control systems. In this scheme, sensitive data is encrypted with an attribute-based encryption model, allowing authorized users to perform keyword searches over the encrypted data without exposing it. The dual traceability feature ensures that both the search queries and the data access can be traced to prevent malicious activities, thus ensuring accountability and transparency in the system. Additionally, the project introduces an ownership transfer mechanism, enabling the secure transfer of data ownership between users while maintaining the integrity and confidentiality of the encrypted data.

III. EXISTING SYSTEM

Cloud data warehouse (CDW) solutions have been offered by numerous cloud service providers to provide immense storage and unlimited accessibility service to business users. Sensitive data warehouse (DW) data in the form of dimension and fact data is typically encrypted before outsourcing to the cloud. The query over encrypted DW is not practically supported by any analytical query tools. The Searchable Encryption (SE) approach is concrete for enabling the keyword searches over the encrypted data. Although numerous SE schemes have suggested their own specific searching techniques based on indexing structure over searchable encryption methods, no schemes are available for supporting Boolean expression queries, which are essential for the search conditions over the DW schema.

Existing System Disadvantages:

- Implementing a CDW can be intricate.
- Needing sophisticated coding systems and algorithms.
- Facilitate effective data collection and dissemination.

Proposed System

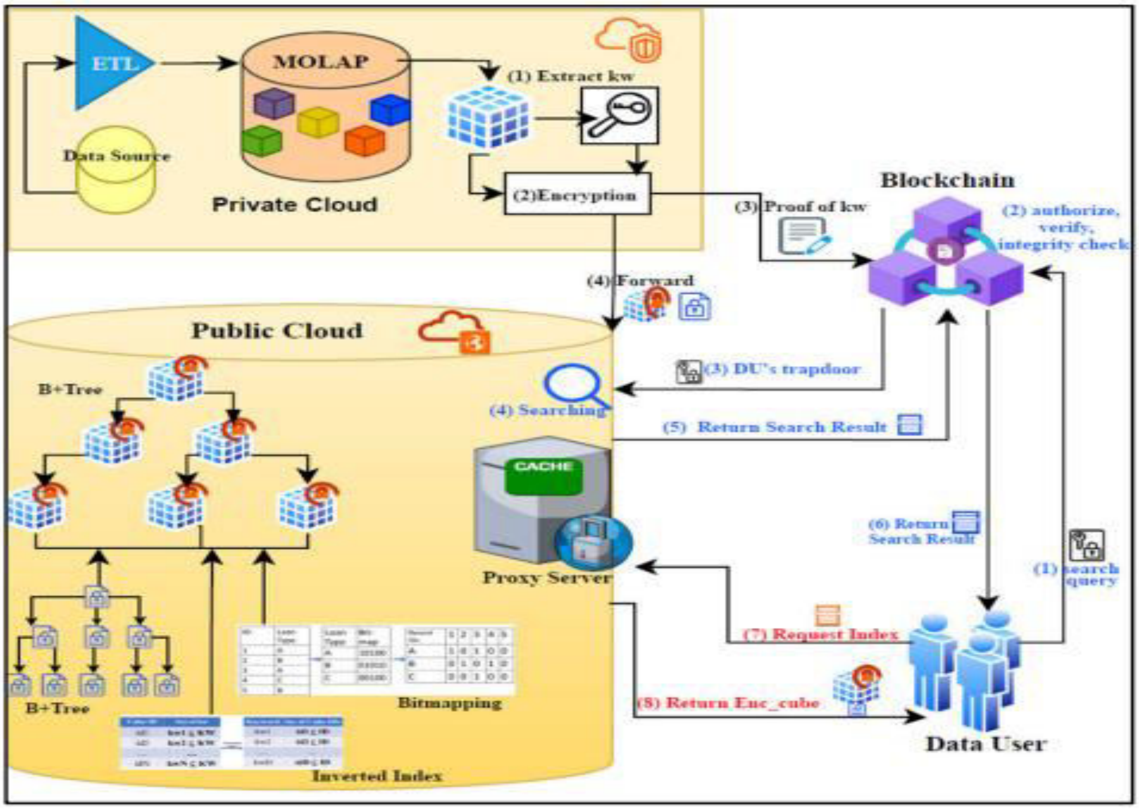
We propose a secure and verifiable searchable encryption scheme with Boolean expression support for CDW. The technical framework of our proposed scheme is to combine Partial Homomorphic Encryption (PHE), B+Tree and Inverted Index, and bitmapping functions to provide privacy-preserving SE and high-performance search capability appropriate for encrypted DW. To ensure the scalability without the involvement of a third party to assist the verification of search results, we utilized blockchain and smart contracts to enable automated authentication, search indices storage, and trapdoor generation. For the experiment, we conducted comparative experiments to show that our scheme is superior and more efficient than the related works.

PROPOSED SYSTEM ADVANTAGES

- PHE is capable of carrying out particular tasks effectively
- Adapting it to situations where these operations are regularly required.
- Sensitive data can be processed without exposing it to potentially untrusted parties.

IV.SYSTEM ARCHITECTURE

In order to promote efficiency and security, the system architecture for the suggested secure and verifiable searchable encryption method in a cloud data warehouse (CDW) is created in this project. The three primary parts of the architecture are the database, the cloud, the users, and the data owner. Partially Homomorphic Encryption (PHE) is used by the data owner to encrypt the data before uploading it to the database, where it is kept safe. The architecture uses sophisticated indexing methods, such as bitmap functions, inverted index, and B+Tree, to facilitate effective searching. After obtaining the necessary access rights, authorized users can submit search queries to the cloud. They can also request search permissions. In order to return encrypted results, the cloud uses the indexing structures to process these queries against the encrypted data. Furthermore, the architecture incorporates blockchain technology to control search permissions and use smart contracts to ensure the accuracy of search results. This multi-layered strategy guarantees the protection of sensitive data while enabling authorized users to safely and effectively execute sophisticated analytical queries.



V. METHODOLOGY

Searchable encryption (SE) allows for searching on encrypted data without revealing data or queries to a cloud provider. When applied to cloud data warehouses, it is harder because of the velocity, variety, and volume of data, together with complex query support and scalability needs. The following are methodologies categorized for designing secure and verifiable searchable encryption systems with cloud data warehouses:

1. **AES** is a widely employed symmetric block cipher algorithm that enables safe encryption and decryption of data using the same secret key. It is the standard encryption algorithm employed by the U.S. government and is utilized internationally to protect confidential data.
2. **PEKS** is the abbreviation of Public Key Encryption with Keyword Search. It enables a given keyword to be searched within encrypted documents on a distrustful cloud server in such a manner that both the search query and the content remain secret.

MODULES:

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

Here, the data owner assumes the central role to manage and secure the sensitive data stored in the Cloud Data Warehouse (CDW). The data owner imports the data cubes consisting of the multidimensional and fact data into the cloud for the very first time after encrypting them with Partially Homomorphic Encryption (PHE). The data owner protects the encrypted data from unauthorized users by defining access controls and securely distributing encryption keys.

3.User

The user is a valid user who accesses the Cloud Data Warehouse (CDW) to perform searches on the encrypted data cubes. Access is given to the users according to the access control policies set by the data owner, and they are provided with the decryption keys necessary to retrieve the query results. When a search query is submitted, the user provides the corresponding keywords or Boolean expressions to search over the encrypted data cubes in the cloud.

4.Cloud

The cloud is the processing and storage center of the Cloud Data Warehouse (CDW) whose sensitive data cubes are encrypted and stored. The encrypted data are stored in the cloud and the search queries entered by authorized users are processed without exposing any sensitive data. The search operations are done by the cloud on the encrypted data cubes using the searchable encryption (SE) algorithms and provides the results encryptically, which can be decrypted only by users having the respective keys.

5.Upload

Uploading in the solution context presented herein means the process of moving securely encrypted data from a data warehouse (DW) to the cloud. The data, such as sensitive dimension and fact data in the form of cubes, is encrypted initially through techniques like Partially Homomorphic Encryption (PHE) such that it is not revealed when stored and fetched in the cloud. Keywords derived from such encrypted cubes are also encrypted and uploaded to the cloud storage.

6.Search

Uploading in the solution proposed herein is the upload of safely encrypted data from a data warehouse (DW) to the cloud. The sensitive dimension and fact data organized in the form of cubes is first encrypted using techniques such as Partially Homomorphic Encryption (PHE) such that it is not revealed while being accessed and stored in the cloud. Keywords generated from such encrypted cubes are also encrypted and uploaded to the cloud storage.

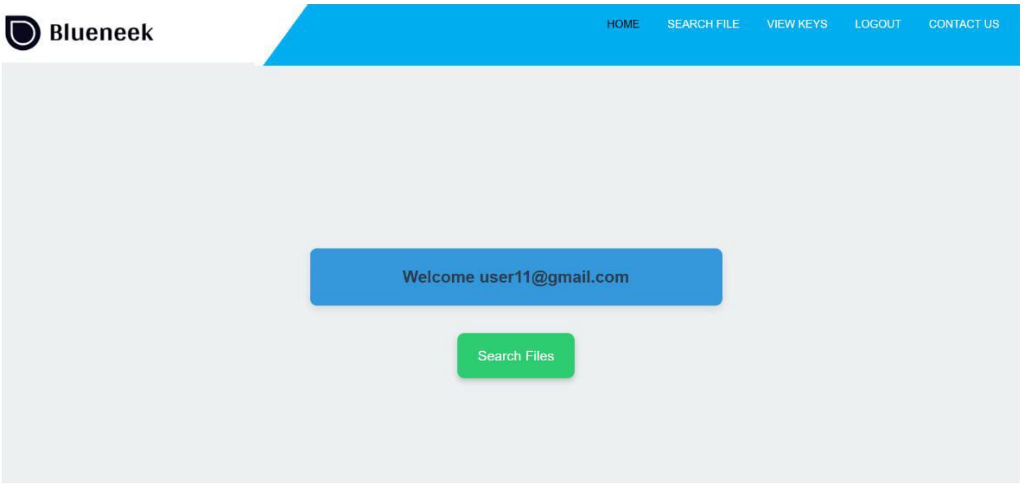
IMPLEMENTATION

1. **AES (Advanced Encryption Standard)** is the most widely used symmetric block cipher algorithm globally. AES is hardware- and software-friendly, but very secure and fast. he most popular symmetric key encryption algorithm worldwide is called AES (Advanced Encryption Standard). It works well with both software and hardware implementations and is safe.The same key is used for both encryption and decryption in symmetric encryption. The sender and the recipient must keep the key confidential.

2. **PHE**

In order to enable privacy-preserving SE with effective search performance appropriate for encrypted DW, the technical construct of the suggested scheme is based on the combination of Partial Homomorphic Encryption (PHE), Inverted Index, and bitmapping functions. We used blockchain and smart contracts to automate authentication, search index retention, and trapdoor generation in order to improve scalability without needing a third party to support the verification of search results. Partially Homomorphic Encryption (PHE) is the foundation of our suggested SE scheme, which guarantees keyword security and important indexing methods, such as bitmapping functions and inverted index. For keyword security, it combines Partially Homomorphic Encryption (PHE), guaranteeing that the information is kept private while being searched.

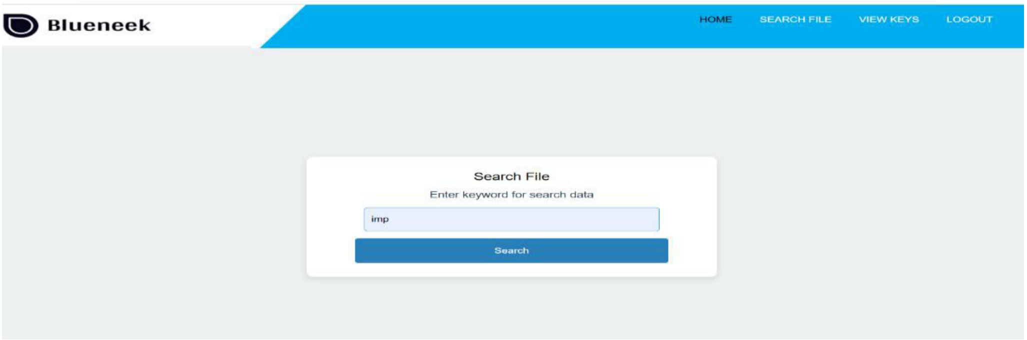
VI. EXPERIMENTAL RESULT



Welcome user11@gmail.com

Fig 1: Home Page

DOI:10.15680/IJARETY.2025.1203052



Search File

Enter keyword for search data

imp

Fig 2: Search File Page

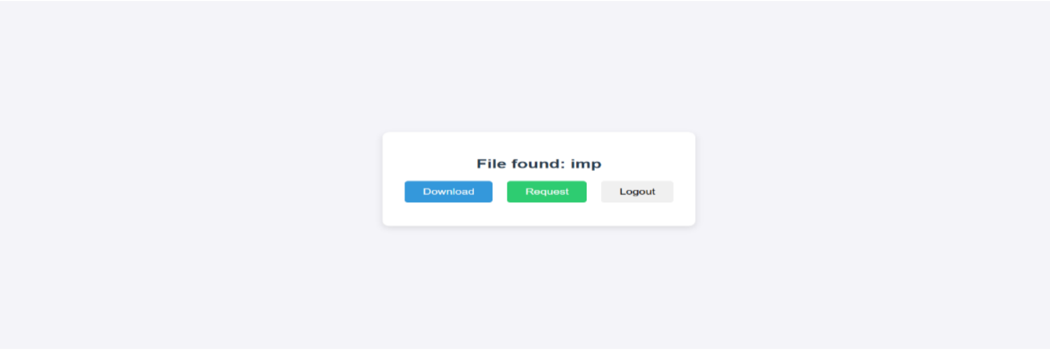
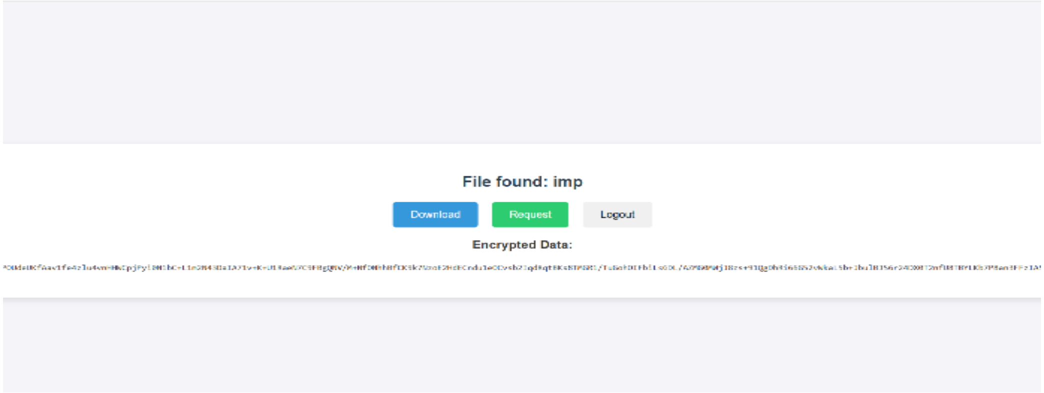

File found: imp

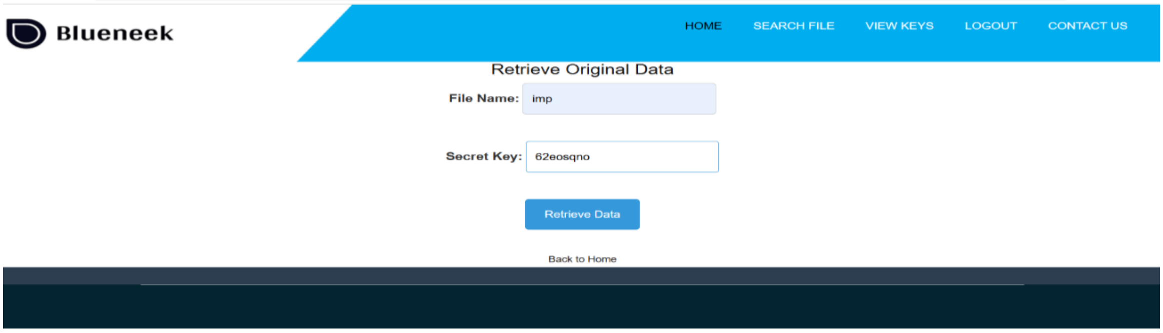
Fig 3: File Found Page


File found: imp

Encrypted Data:

[illegible]

Fig 4: Encrypted Data File Page



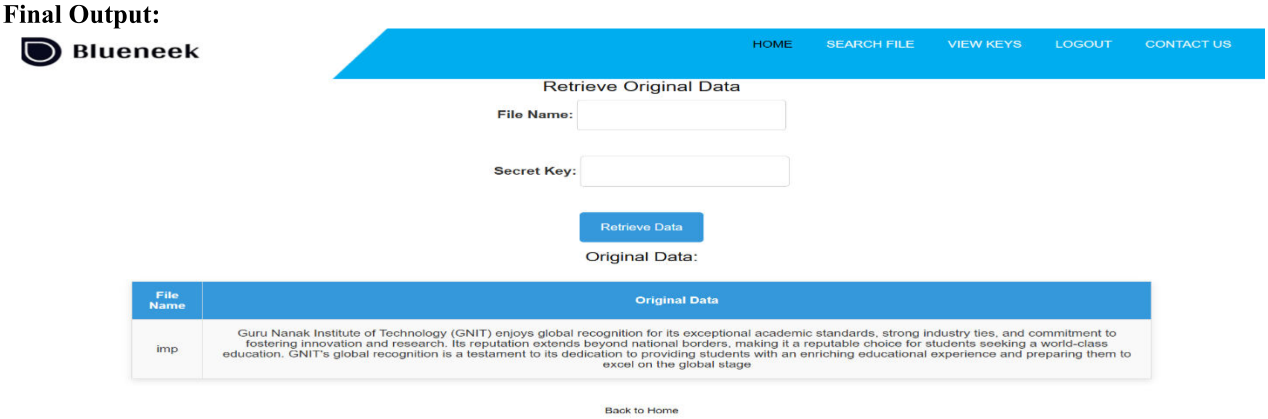
Retrieve Original Data

File Name: imp

Secret Key: 62eosqno

Fig 5: Decryption

Final Output:



Retrieve Original Data

File Name:

Secret Key:

Original Data:

File Name	Original Data
imp	Guru Nanak Institute of Technology (GNIT) enjoys global recognition for its exceptional academic standards, strong industry ties, and commitment to fostering innovation and research. Its reputation extends beyond national borders, making it a reputable choice for students seeking a world-class education. GNIT's global recognition is a testament to its dedication to providing students with an enriching educational experience and preparing them to excel on the global stage

Fig 6: Retrieved Original Data

VII. CONCLUSION

With support for more than encrypted data cubes in a cloud-based data warehouse, we have demonstrated in this project a versatile, secure, and verifiable searchable encryption scheme. Our approach, which combines B+Tree, inverted index, and partial homomorphic encryption, offers both security and search performance. Furthermore, we utilized blockchain technology to expedite the automation of user authentication, search permission verification, and search result validation procedures. Scalability and immutability are guaranteed by the way these tasks are carried out. Notably, we have used a variety of search function types, including bitmapping functions, B+Trees, and inverted indexes, to accommodate different data types that are appropriate for searching over multidimensional data. Our tests have shown that our plan can save a great deal of time and money. Additionally, the system can support multiple concurrent OLAP query requests with a reasonable system throughput.

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] T.Kishore Babu, Raja Kiran Kolati, Pathipati Chandrasekhar, Nimmagadda MuraliKrishna, Sriharaha Vikruthi, B. Rajeswari Computer-Assisted Leukemia Detection and Classification using Machine Learning “2024 International Conference on Expert Clouds and Applications (ICOECA)”,2024.

[6] International Research Journal of Modernization in Engineering Technology and Science(irjmets) ,AUTHORIZED SEARCHABLE FRAMEWORK FOR E-HEALTHCARE SYSTEM, P.Chandra Sekhar*1, Kammala Vinay*2, Mogulla Ragender*3, Gouri Rohith*4

[7] International Journal of Scientific Research in Engineering and Management (IJSREM),EFPB: Efficient Fair Payment Based on Blockchain for Outsourcing Services in Cloud Computing Pathipati Chandra Sekhar1 Assistant Professor, Guru Nanak Institute of Technology, Department of CSE, Hyderabad. K.Suresh Babu2Assistant Professor, PACE Institute of Technology and Sciences, Department of CSE,Ongole

[8] International Research Journal of Modernization in Engineering Technology and Science, FASHION RECOMMENDATION SYSTEM USING SOCIAL MEDIA WEBSITE, P.Chandra Sekhar*1, Sania Mahereen*2, S. Ram Prasad*3, S. Farhan Akther*4

[9] International Research Journal of Modernization in Engineering Technology and Science,USING MICROSERVICES PLANNING FOR ADDITIONAL CREATED HELP PARTAKING IN IOT EDGE CONDITIONS P.Chandra Sekhar*1, G.Sravani*2, Ch.Deekshitha*3, G.Nandini*4

DOI:10.15680/IJARETY.2025.1203052

[10] International Journal of Scientific Research in Engineering and Management (IJSREM),A Review of Machine Learning Strategies for Enhancing Efficiency and Innovation in Real-World Engineering Applications,Mrs. Palagati Anusha1, Mr. S. Sujith Kumar2, Mr. Chandrasekhar Pathipati3

[11] Y. Wang, S.-F. Sun, J. Wang, J. K. Liu, and X. Chen, ''Achieving searchable encryption scheme with search pattern hidden,'' IEEE Trans. Services Comput., vol. 15, no. 2, pp. 1012–1025, Mar. 2022, doi:10.1109/TSC.2020.2973139.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

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

[19] 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.

[20] 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.

[21] 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.

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

[23] 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.

[24] 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.

[25] 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.

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com