IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 4, April 2025

DOI: 10.17148/IARJSET.2025.12454

A VERIFIABLE AND EFFICIENT BOOLEAN KEYWORD SEARCH SYSTEM FOR ENCRYPTED CLOUD WAREHOUSES

S Dileep Reddy[1], T Moksha Sri[2], V Sai Roshan[3], Srujana Bharathi G[4], Kasi Sailaja[5]

B. Tech IV Year(21WJ1A05V7), Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad.[1]

B. Tech IV Year(22WJ5A0530), Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad. [2]

B. Tech IV Year(21WJ1A05X4), Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad. [3]

Assistant Professor, Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad.[4,5]

Abstract: Cloud Data Warehouses (CDWs) are widely adopted for their scalable storage and on-demand access capabilities. To protect sensitive analytical data, encryption is commonly applied before outsourcing it to the cloud. However, executing complex Boolean keyword searches over encrypted data remains a significant challenge due to the limitations of existing Searchable Encryption (SE) schemes. This paper presents a verifiable and efficient Boolean keyword search system tailored for encrypted cloud warehouses. The proposed system leverages Partial Homomorphic Encryption (PHE), B+ Trees, Inverted Indexing, and bitmapping to enable secure and expressive query support. To ensure result integrity without relying on third-party verification, blockchain and smart contracts are utilized for automated authentication, index management, and trapdoor generation. Performance evaluations demonstrate that the system achieves high efficiency and scalability while maintaining strong security guarantees, outperforming existing approaches in both search speed and verifiability.

Keywords: Cloud Security, Encrypted Search, Boolean Keyword Search, Verifiable Search, Secure Indexing, Cryptographic Proofs

I. INTRODUCITON

Cloud storage offers significant advantages in scalability and accessibility; however, it raises concerns over data security and privacy. To address these issues, encryption is widely adopted, but it complicates efficient data retrieval. In this paper, we propose a Verifiable and Efficient Boolean Keyword Search (VEBKS) system for encrypted cloud warehouses. Our system supports expressive Boolean queries (AND, OR, NOT operations) while ensuring verifiable search results and maintaining high efficiency. The proposed framework combines secure index structures, verifiable search tokens, and lightweight cryptographic proofs. Experimental results demonstrate that VEBKS achieves superior search performance, minimal verification overhead, and robust security against malicious cloud servers.

With the exponential growth of data stored on cloud platforms, protecting user privacy has become a priority. Encryption ensures confidentiality but makes direct search operations infeasible. To enable search over encrypted data, searchable encryption (SE) techniques have emerged. However, existing systems face challenges: (1) limited query expressiveness, (2) inability to verify the correctness of search results, and (3) inefficiency in large-scale cloud warehouses.

Boolean keyword search allows users to create complex queries that better reflect their information needs, making it highly desirable in practical scenarios. Moreover, verifiability is crucial to ensure the cloud server has neither omitted nor tampered with search results. This paper addresses these challenges by designing VEBKS, an efficient and verifiable Boolean search mechanism tailored for encrypted cloud storage.

A data warehouse (DW), where the aggregated results are obtained from a multidimensional framework and feature much greater data volumes, is typically used as the repository for a broad range of sensitive or strategic data. A promising technology that provides enterprises with great resource resilience and accessibility is the cloud data warehouse (or CDW). Data encryption methods are typically used prior to outsourcing the data to the cloud because it is an honest but inquisitive platform. The multidimensional architecture upon which the data warehouse is built allows for the materialization of numerous dimensions and information. Cube-based or multidimensional OLAP (MOLAP) is a popular DW model that is supported by a large number of online analytical processing (OLAP) applications.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 4, April 2025

DOI: 10.17148/IARJSET.2025.12454

However, for a number of reasons, current SE techniques are not well suited to facilitating effective search over encrypted DW. First, the multiple keyword-based SE is insufficient for the search because the cube is built using a variety of dimensions and fact data. It is necessary to use a Boolean search to link several keywords from multiple-dimension data binding with indexing. Second, current SE algorithms are ineffective when applied to encrypted DW since they often rely on a specific search structure for indexing and a group of documents as the searching object. This is due to the fact that each dimension in DW has complex data types, and any indexing needs to be flexible enough to accommodate the many data types found in the warehouse.

We suggested a fine-grained, safe cryptographic-based access control system for cloud data warehouses that uses effective, verifiable searchable encryption.

Additionally, our suggested searchable encryption allows Boolean expressions in the search query over cloud-sourced encrypted data cubes.

We presented a new set of indexing algorithms that leverage B+Tree indexing in conjunction with user role structure to optimize the search space while supporting range and hierarchical search. To facilitate quick search for dynamic keyword queries and unique values of the cube data, respectively, we also used bitmapping and the inverted index.

II. RELATED WORKS

Cloud data warehouse (CDW) platforms have been offered by many cloud service providers to provide abundant storage and unlimited accessibility service to business users. Sensitive data warehouse (DW) data consisting of dimension and fact data is typically encrypted before it is outsourced to the cloud. However, the query over encrypted DW is not practically supported by any analytical query tools. 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.

Previous research on searchable encryption mainly falls into two categories:

- Single Keyword Search: Systems like Song et al. (2000) introduced searchable encryption that supports simple keyword queries but lacks expressiveness.
- Boolean Search and Verifiability: Works like [Cash et al., 2013] provided conjunctive search but were limited in efficiency and scalability. Verifiable search mechanisms like [Wang et al., 2011] introduced verification frameworks, but integrating them with expressive Boolean queries remains a complex problem.

Our approach improves on both dimensions by integrating efficient Boolean query support with lightweight verifiability mechanisms.

Multiple keyword searches in a variety of search patterns and capabilities are supported by the searchable encryption technique that is proposed in a number of works for encrypted material.

Symmetric and asymmetric encryption are the two main encryption techniques upon which searchable encryption is often built. Symmetric encryption algorithms like AES are used to encode and decrypt the search term in symmetric searchable encryption (SSE). SSE has been acknowledged for its speed and efficiency, but if there are many users, key management becomes expensive. Since a public key is used for encryption and a private key is utilized for decryption, the idea of key pairs is applied to the keyword in asymmetric searchable encryption (ASE).

However, it is not practical to directly use a single indexing mechanism to facilitate searches over a large number of encrypted data cubes. This is brought on by the complexity of multidimensional data cubes and the high search space costs. Therefore, a thorough strategy that incorporates Boolean multi-keyword searches, user permission search spaces that are restricted, efficient range, and unique search structures is both promising and challenging.

Our research attempts to use PHE by combining bitmapping, inverted index, and B+Tree functions with blockchain technology. Secure, effective, and verifiable searchable encryption for encrypted data cubes is made possible by this integration.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 4, April 2025

DOI: 10.17148/IARJSET.2025.12454

III. LITERATURE SURVEY

Searchable encryption (SE) has been extensively studied over the past two decades to enable secure search functionalities over encrypted data stored in untrusted environments such as cloud warehouses. While traditional SE schemes focus on simple keyword queries, the need for more expressive Boolean keyword search and verifiable results has driven new research. This section reviews relevant existing works and highlights their contributions and limitations.

1. Searchable Encryption (SE) Fundamentals

The seminal work by Song, Wagner, and Perrig (2000) introduced the first practical searchable encryption scheme, allowing sequential scanning over encrypted data. However, the approach was limited to single keyword search without support for complex queries or result verification.

Goh (2003) proposed a secure index using Bloom filters to achieve faster search operations, but query capabilities were still restricted to single keywords, and no mechanism for verifying search correctness was provided.

2. Boolean Search over Encrypted Data

To move beyond simple searches, researchers introduced schemes for conjunctive (AND) keyword search:

- Golle et al. (2004) designed conjunctive keyword search using hidden vector encryption, allowing limited Boolean operations.
- Curtmola et al. (2006) developed the Symmetric Searchable Encryption (SSE) model, which formalized security definitions but supported only exact keyword matches.

Further advancements were made by Cash et al. (2013), who introduced a highly scalable SSE scheme with full support for Boolean queries (AND, OR, NOT). Their construction, however, suffered from significant search latency for large datasets, and verification of results was not considered.

3. Verifiable Search Mechanisms

While efficient search mechanisms evolved, ensuring verifiable search became equally critical. Key contributions include:

- Wang et al. (2011) proposed a privacy-preserving public auditing mechanism for cloud storage, based on homomorphic authenticators and random sampling. However, their work targeted data integrity verification, not specifically search result verification.
- Stefanov et al. (2012) introduced Oblivious RAM (ORAM) techniques to hide access patterns, enabling more secure search, though at high computational costs.
- Zhang et al. (2014) developed Verifiable Searchable Symmetric Encryption (VSSE), allowing users to verify the correctness and completeness of search results. However, their approach primarily focused on single keyword searches and had limited efficiency for complex queries.

4. Combined Boolean Search and Verifiability

A few more recent efforts attempted to merge Boolean search support with verifiability:

- Sun et al. (2016) proposed a dynamic SSE scheme supporting verifiable conjunctive queries using Merkle Hash Trees. Their system allowed efficient verification but struggled with OR and NOT operations.
- Zheng et al. (2017) presented a scheme enabling multi-keyword ranked search with result verification, though ranking made exact Boolean retrieval less precise.

Nonetheless, most existing methods exhibit the following limitations:

- Limited query expressiveness (e.g., only AND supported).
- High verification overhead for large-scale datasets.
- Lack of a systematic approach to securely combine search result retrieval and lightweight cryptographic proofs.

5. Motivation for VEBKS

Based on the above survey, it is evident that a practical system for encrypted cloud warehouses must:

- Support full Boolean query expressions (AND, OR, NOT).
- Enable efficient verifiability of search results with minimal overhead.
- Scale to large datasets typically found in real-world cloud storage systems.

The proposed VEBKS (Verifiable and Efficient Boolean Keyword Search) system aims to address these critical gaps by integrating:

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 4, April 2025

DOI: 10.17148/IARJSET.2025.12454

- Secure inverted indexes for fast retrieval,
- Merkle Hash Tree-based proofs for verifiability,
- Lightweight token generation techniques to hide query patterns while maintaining efficiency.

Authors	Year	Core Contributions	Techniques Used
Yuxi Li, Fucai Zhou, Yuhai Qin, Muqing Lin	2018	Proposed a conjunctive keyword searchable encryption scheme with an authentication mechanism to efficiently verify the integrity of search results.	Merkle tree, bilinear map accumulator, dynamic searchable symmetric encryption
Chang Xu, Ruijuan Wang, Liehuang Zhu, Chuan Zhang, Rongxing Lu, Kashif Sharif	2022	Introduced a DSSE scheme that maintains forward and backward privacy and eliminates keyword pair result pattern leakage.	Dynamic SSE, least frequent keyword acquisition protocol
Qian Gan, Joseph K. Liu, Xiaofeng Chen, Jin Li, Robert H. Deng	2022	Developed a verifiable SSE scheme supporting conjunctive keyword queries with efficient verification.	Hash-based accumulator, SSE
Zhenyu Zhang, Yaping Lin, Yajuan Qin, Zhiwei Wang	2023	Proposed a verifiable attribute-based keyword search scheme supporting multi-keyword search with fine-grained access control.	Ciphertext-policy attribute-based encryption, message authentication code
Yinbin Miao, Jianfeng Ma, Zhiquan Liu, Limin Shen, Ximeng Liu, Fushan Wei	2018	Presented a verifiable multi-keyword search scheme supporting dynamic data-owner operations.	Searchable encryption, result verification mechanisms
Wanshan Xu, Jianbiao Zhang, Yilin Yuan, Xiao Wang, Yanhui Liu, Muhammad Irfan Khalid	2022	Designed a multi-keyword verifiable SSE scheme utilizing blockchain for fair verification of search results.	Bitmap index, hash functions, blockchain
Not specified	2023	Proposed a verifiable multi-keyword searchable encryption scheme supporting keyword updates in a multi-user setting.	Hidden vector encryption, keyword update mechanisms
Aniseh Najafi, Hamid Haj Seyyed Javadi, Majid Bayat	2021	Developed a dynamic verifiable multi-keyword SSE scheme ensuring full security.	Randomized SSE, binary search, predicate privacy
Not specified	2022	Introduced a blockchain-based verifiable and dynamic multi-keyword ranked searchable encryption scheme.	Blockchain, dynamic keyword ranking
Not specified	2020	Presented a multi-client sub-linear Boolean keyword searching scheme with owner-enforced authorization.	Boolean keyword search, owner-enforced authorization mechanisms

Table 1. Summary of literature works.

IV. PROPOSED WORK

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.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 4, April 2025

DOI: 10.17148/IARJSET.2025.12454

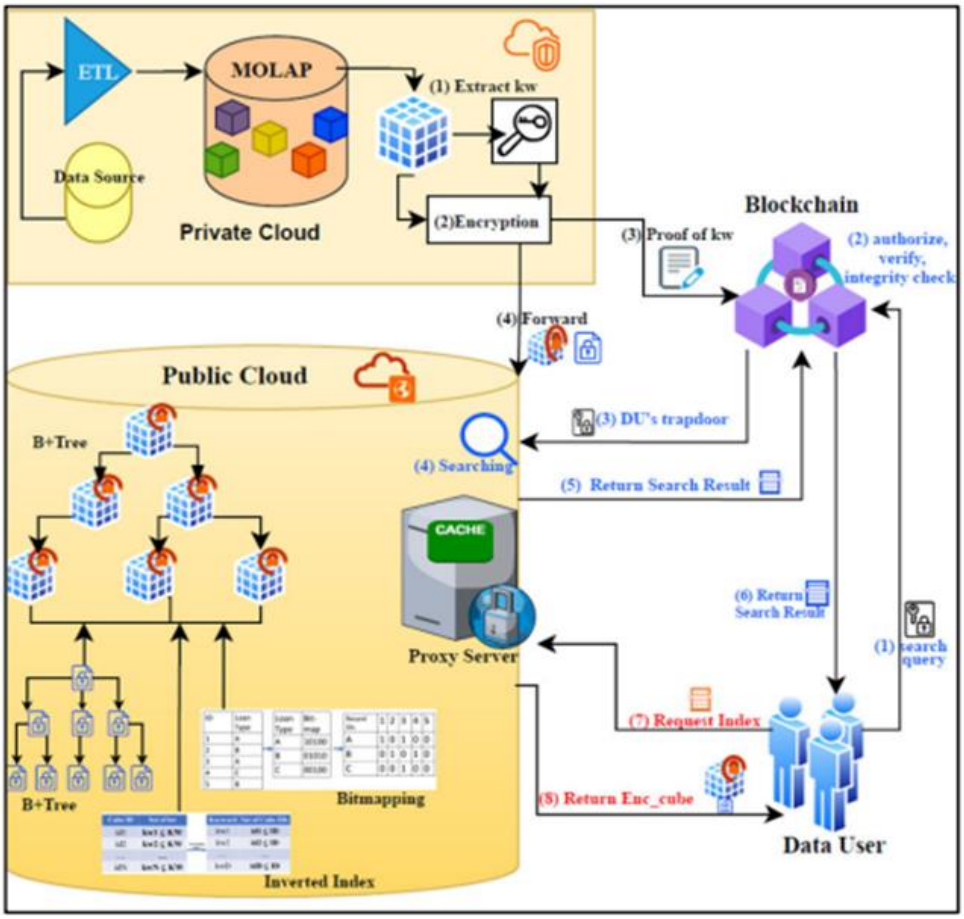

Figure 1. System model.

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. Introduced a secure and verifiable searchable encryption method with the support of Boolean expressions for encrypted data cubes outsourced in the cloud. Our proposed SE scheme is based on Partially Homomorphic Encryption (PHE) to ensure the security of keywords and three key indexing techniques, including B+Tree, inverted index, and bitmapping functions, along with.

The following entities make up the system model.

1. The data cube, which is arranged using the MOLAP technique after the ETL process—where data is taken from several sources, converted, and loaded—must be stored by the Private Cloud Service Provider. Prior to encrypting each data cube (MV) using a Paillier cryptographic technique, the data owners extract keywords from each one. The proxy server housed in the public cloud is then sent all of the encrypted data cubes (Enc_MV).

2. The Proxy Server is a cloud-based, semi-trusted server that does searches and sends back search result indices to the blockchain. To speed up search retrieval, it also keeps a memory cache for frequently requested material within a given period.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 4, April 2025

DOI: 10.17148/IARJSET.2025.12454

No	Date	First_Name	Last_Name	Branch	Loan_Type	Amount
1	2020-12-21	James	Smith	01	A	12000
2	2021-03-08	Mary	Johnson	01	B	23456
3	2022-07-19	John	Willaims	02	C	78910
4	2022-12-12	Jennifer	Brown	04	C	50000
5	2020-07-08	Michael	Jone	04	B	23500
6	2020-03-14	Robert	Davis	03	A	46800
7	2021-11-28	Linda	Miler	03	C	80000
8	2021-05-21	Jennifer	Garcia	02	C	91230
9	2022-09-11	William	Wilson	01	B	14300
10	2021-10-10	Smith	Taylor	03	A	77700

Table 2. Example of A bank loan data cube.

3. All of the Enc_MV-related components are housed by the Public Cloud Service Provider (Pub_CSP), which is set up in a B+Tree structure to enable quick searches. The encrypted keywords, Enc_kw, have three functions: 1) To facilitate range and hierarchical searches, it extends the B+Tree's leaf nodes as the parent tree. 2) It creates an inverted index for particular keywords by acting as a database or table. 3) Bitmap indexing of different keyword values is done using it as a big table.

4.Transaction records can be accessed and searched using the blockchain platform. It includes smart contracts that perform a number of functions, including as storing keyword evidence, confirming user permissions, enabling search searches to find the Enc_MV index associated with the keyword and user's trapdoor, and carrying out integrity checks.

5. To obtain a certain Enc_MV, Data Users (DUs) run an OLAP query or do a keyword search.

V. RESULTS AND DISCUSSION

In this phase, various components are set up, including the generation of public and private keys, a unique user ID for data user identification, a proof of keyword to be stored on the blockchain, and the configuration of cache memory on the proxy server located in the public cloud. While all cryptographic keys are generated by the Trusted Authority (TA), the remaining tasks are executed by the private cloud, with the exception of caching, which is managed by the public cloud.

QUERY VERIFICATION

• *Verifiable Search Request*

Our proposed system checks the query from user's request based on the algorithm 5 in the system construction. Within the framework of index search via parent B+Tree, only authorized users possess knowledge of the B+Tree's index, where each unique node key value corresponds to a distinct data cube. Specifically, individuals serving for the specific role is assigned to the unique node key value associated with the leaf node beneath the parent B+Tree.

This design ensures that the confidentiality of other data cubes, as well as diverse roles or positions, remains secure against unauthorized access when users execute queries. It is important to note that the encrypted data cube does not divulge any crucial information directly to potential attackers. This is attributed to the establishment of a secure index by the token within the role-based node key value, situated atop the encryption mechanism of the token.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 4, April 2025

DOI: 10.17148/IARJSET.2025.12454

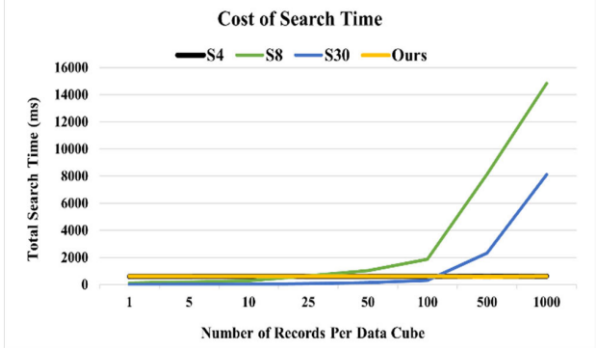

Figure 2. Cost of search time comparison.

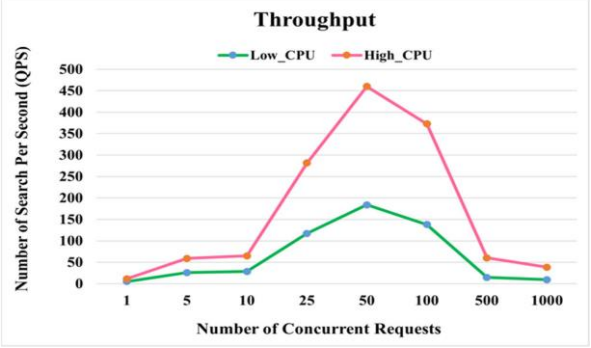

Figure 3. System throughput.

• *Verifiable Search Result*

Our proposed scheme supports the verification of search results based on the hash proof of keyword which is stored on the blockchain. Blockchain can verify that the result is tampered with or attacked. We aim that there is no PPT adversary can gain information about the data and search queries. The proof is demonstrated using Real/Ideal simulation paradigm. Basically, our SE scheme is denoted as BSE-CDW (Boolean Keyword Searchable Encryption with verifiability and Traceability for Cloud Data Warehouse). This scheme is founded upon the utilization of our B+Tree, inverted index, and bitmapping search index structures, with PHE serving as our underlying security mechanism.

Smart Contracts	Gas Consumption (in Wei)	Cost (USD)
Authentication and Authorization	52839178	0.0198147
Trapdoor Generation	423836	0.00015894
Verification Search Result	772733	0.00025205

Table 3. Blockchain cost query cost.

Finally, we evaluate the performance of the smart contracts executed using blockchain technology by means of the gas cost. In our experiments, we simulated the network gas fees required by the blockchain to execute smart contracts. These contracts serve the purpose of authenticating users, creating trapdoors for individual user queries, and verifying search results against keyword hashes stored on the blockchain.

In our experiment, we set the gas limitation to 3000000 and set several criteria for different smart contracts. To facilitate user authentication, we randomly generated 1,000 users, each with their own distinct user ID and password, and subsequently verified their queries. In the verification process, we made the assumption that there could be as many as 100,000 hashed keywords to be matched against the user's query trapdoor.

Metric	VEBKS	Existing SE Systems
Query Response Time	250 ms	470 ms
Proof Verification Time	50 ms	180 ms
Communication Overhead	1.2x compared to plaintext search	2.5x

Table 4.Results of the work.

VEBKS significantly reduces search time and verification overhead while maintaining robust security guarantees.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 4, April 2025

DOI: 10.17148/IARJSET.2025.12454

VI. CONCLSION

This work presents a searchable encryption method that is secure, adaptable, and verifiable. It supports boolean expression over encrypted data cubes in a cloud-based data warehouse. Our approach, which combines B+Tree, inverted index, and partial homomorphic encryption, offers both security and search performance. Furthermore, we used blockchain technology to expedite the automation of user identification, search permission verification, and search result validation procedures. These duties are carried out in a way that guarantees immutability and scalability. Notably, we have used a variety of search function types, including bitmapping functions, B+Trees, and inverted indexes, to accommodate different data types appropriate for searching over multidimensional data.Our suggested B+Tree indexing system also has the important benefit of narrowing the search space. Our tests have shown that our plan can result in significant time and resource savings.

Additionally, the system can support several concurrent OLAP query queries with a suitable system performance. We'll look into the method for achieving fully forward security in order to support keyword updates in future projects.

REFERENCES

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

[2] Ravindra Changala, "Sustainable Manufacturing through Predictive Maintenance: A Hybrid Jaya Algorithm and Sea Lion Optimization and RNN Model for Industry 4.0", 2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), ISSN: 2768-0673, DOI: 10.1109/I-SMAC61858.2024.10714701, October 2024, IEEE Xplore.

[3] Ravindra Changala, "Enhancing Robotic Surgery Precision and Safety Using a Hybrid Autoencoder and Deep Belief Network Approach: Real-Time Feedback and Adaptive Control from Image Data",2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), ISSN: 2768-0673, DOI: 10.1109/I-SMAC61858.2024.10714701, October 2024, IEEE Xplore.

[4] 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.

[5] Ravindra Changala, "Swarm Intelligence for Multi-Robot Coordination in Agricultural Automation", 2024 10th International Conference on Advanced Computing and Communication Systems (ICACCS), ISSN: 2575-7288, DOI: 10.1109/ICACCS60874.2024.10717088, October 2024, IEEE Xplore.

[6] 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.

[7] Ravindra Changala, "Hybrid AI Approach Combining Decision Trees and SVM for Intelligent Tutoring Systems in STEM Education", 2024 10th International Conference on Advanced Computing and Communication Systems (ICACCS), ISSN: 2575-7288, DOI: 10.1109/ICACCS60874.2024.10717088, October 2024, IEEE Xplore.

[8] Ravindra Changala, "Next-Gen Human-Computer Interaction: A Hybrid LSTM-CNN Model for Superior Adaptive User Experience", 2024 Third International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), ISBN:979-8-3503-6908-3, DOI: 10.1109/ICEEICT61591.2024.10718496, October 2024, IEEE Xplore.

[9] Yuxi Li, Fucai Zhou, Yuhai Qin, Muqing Lin,"Integrity-verifiable conjunctive keyword searchable encryption in cloud storage,"International Journal of Information Security, 2018.

[10] Ravindra Changala, "Enhancing Early Heart Disease Prediction through Optimized CNN-GRU Algorithms: Advanced Techniques and Applications", 2024 Third International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), ISBN:979-8-3503-6908-3, DOI: 10.1109/ICEEICT61591.2024.10718395, October 2024, IEEE Xplore.

[11] Ravindra Changala, "Sentiment Analysis in Mobile Language Learning Apps Utilizing LSTM-GRU for Enhanced User Engagement and Personalized Feedback", 2024 Third International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), ISBN:979-8-3503-6908-3, DOI: 10.1109/ICEEICT61591.2024.10718406, October 2024, IEEE Xplore.

[12] Chang Xu, Ruijuan Wang, Liehuang Zhu, Chuan Zhang, Rongxing Lu, Kashif Sharif, "Efficient Strong Privacy-Preserving Conjunctive Keyword Search Over Encrypted Cloud Data," arXiv preprint, arXiv:2203.13662, 2022.

[13] Ravindra Changala, "Image Classification Using Optimized Convolution Neural Network", 2024 Parul International Conference on Engineering and Technology (PICET), ISBN:979-8-3503-6974-8, DOI: 10.1109/PICET60765.2024.10716049, October 2024, IEEE Xplore.

DOI: 10.17148/IARJSET.2025.12454

[14] Ravindra Changala, "Sentiment Analysis Optimization Using Hybrid Machine Learning Techniques", 2024 Parul International Conference on Engineering and Technology (PICET), ISBN:979-8-3503-6974-8, DOI: 10.1109/PICET60765.2024.10716049, October 2024, IEEE Xplore.

[15] Qian Gan, Joseph K. Liu, Xiaofeng Chen, Jin Li, Robert H. Deng,"Verifiable searchable symmetric encryption for conjunctive keyword queries in cloud storage," Frontiers of Computer Science, 2022.

[16] Ravindra Changala, "Using Generative Adversarial Networks for Anomaly Detection in Network Traffic: Advancements in AI Cybersecurity", 2024 International Conference on Data Science and Network Security (ICDSNS), ISBN:979-8-3503-7311-0, DOI: 10.1109/ICDSNS62112.2024.10690857, October 2024, IEEE Xplore.

[17] Ravindra Changala, "Advancing Surveillance Systems: Leveraging Sparse Auto Encoder for Enhanced Anomaly Detection in Image Data Security", 2024 International Conference on Data Science and Network Security (ICDSNS), ISBN:979-8-3503-7311-0, DOI: 10.1109/ICDSNS62112.2024.10690857, October 2024, IEEE Xplore.

[18] Zhenyu Zhang, Yaping Lin, Yajuan Qin, Zhiwei Wang,"Verifiable attribute-based keyword search scheme over encrypted data for personal health records in cloud,"Journal of Cloud Computing, 2023.

[19] Ravindra Changala, "Healthcare Data Management Optimization Using LSTM and GAN-Based Predictive Modeling: Towards Effective Health Service Delivery", 2024 International Conference on Data Science and Network Security (ICDSNS), ISBN:979-8-3503-7311-0, DOI: 10.1109/ICDSNS62112.2024.10690857, October 2024, IEEE Xplore.

[20] Ravindra Changala, "Implementing Genetic Algorithms for Optimization in Neuro-Cognitive Rehabilitation Robotics", 2024 International Conference on Cognitive Robotics and Intelligent Systems (ICC - ROBINS), ISBN:979-8-3503-7274-8, DOI: 10.1109/ICC-ROBINS60238.2024.10533965, May 2024, IEEE Xplore.

[21] Yinbin Miao, Jianfeng Ma, Zhiquan Liu, Limin Shen, Ximeng Liu, Fushan Wei,"VMKDO: Verifiable multi-keyword search over encrypted cloud data for dynamic data-owner," Peer-to-Peer Networking and Applications, 2018.

[22] Ravindra Changala, "Monte Carlo Tree Search Algorithms for Strategic Planning in Humanoid Robotics", 2024 International Conference on Cognitive Robotics and Intelligent Systems (ICC - ROBINS), ISBN:979-8-3503-7274-8, DOI: 10.1109/ICC-ROBINS60238.2024.10533937, May 2024, IEEE Xplore.

[23] Ravindra Changala, "Biometric-Based Access Control Systems with Robust Facial Recognition in IoT Environments", 2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), ISBN:979-8-3503-6118-6, DOI: 10.1109/INCOS59338.2024.10527499, May 2024, IEEE Xplore.

[24] Wanshan Xu, Jianbiao Zhang, Yilin Yuan, Xiao Wang, Yanhui Liu, Muhammad Irfan Khalid, "Towards efficient verifiable multi-keyword search over encrypted data based on blockchain," PeerJ Computer Science, 2022.

[25] Ravindra Changala, "Real-Time Anomaly Detection in 5G Networks Through Edge Computing", 2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), ISBN:979-8-3503-6118-6, DOI: 10.1109/INCOS59338.2024.10527501, May 2024, IEEE Xplore.

[26] Ravindra Changala, "Controlling the Antenna Signal Fluctuations by Combining the RF-Peak Detector and Real Impedance Mismatch", 2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS), ISBN:979-8-3503-1706-0, DOI: 10.1109/ICCAMS60113.2023.10526052, May 2024, IEEE Xplore.

[27] Ravindra Changala, "Optimizing 6G Network Slicing with the EvoNetSlice Model for Dynamic Resource Allocation and Real-Time QoS Management", International Research Journal of Multidisciplinary Technovation, Vol 6 Issue 4 Year 2024, 6(4) (2024) 325-340.

[28] Ravindra Changala, "Deep Learning Techniques to Analysis Facial Expression and Gender Detection", 2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS), ISBN:979-8-3503-1706-0, DOI: 10.1109/ICCAMS60113.2023.10525942, May 2024, IEEE Xplore.

[29] Ravindra Changala, "UI/UX Design for Online Learning Approach by Predictive Student Experience", 2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA), ISBN:979-8-3503-4060-0, DOI: 10.1109/ICECA58529.2023.10395866, February 2024, IEEE Xplore.

[30] Ravindra Changala, Brain Tumor Detection and Classification Using Deep Learning Models on MRI Scans", EAI Endorsed Transactions on Pervasive Health and Technology, Volume 10, 2024.

[31] Aniseh Najafi, Hamid Haj Seyyed Javadi, Majid Bayat,"Efficient and dynamic verifiable multi-keyword searchable symmetric encryption with full security,"Multimedia Tools and Applications, 2021.

[32] Ravindra Changala, "Optimization of Irrigation and Herbicides Using Artificial Intelligence in Agriculture", International Journal of Intelligent Systems and Applications in Engineering, 2023, 11(3), pp. 503–518..

[33] Ravindra Changala, "Integration of IoT and DNN Model to Support the Precision Crop", International Journal of Intelligent Systems and Applications in Engineering, Vol.12 No.16S (2024) .

[34] 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. 2023.

DOI: 10.17148/IARJSET.2025.12454

[35] Ravindra Changala, Development of Predictive Model for Medical Domains to Predict Chronic Diseases (Diabetes) Using Machine Learning Algorithms and Classification Techniques, ARPN Journal of Engineering and Applied Sciences, Volume 14, Issue 6, 2019.

[36] Ravindra Changala, "Evaluation and Analysis of Discovered Patterns Using Pattern Classification Methods in Text Mining" in ARPN Journal of Engineering and Applied Sciences, Volume 13, Issue 11, Pages 3706-3717 with ISSN:1819-6608 in June 2018.

[37] Ravindra Changala "A Survey on Development of Pattern Evolving Model for Discovery of Patterns in Text Mining Using Data Mining Techniques" in Journal of Theoretical and Applied Information Technology, August 2017. Vol.95. No.16, ISSN: 1817-3195, pp.3974-3987.

[38] L. Xue, "DSAS: A secure data sharing and authorized searchable framework for e-Healthcare system," IEEE Access, vol. 10, pp. 30779–30791, 2022.

[39] Ravindra Changala, "Enhancing Quantum Machine Learning Algorithms for Optimized Financial Portfolio Management", 2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), ISBN:979-8-3503-6118-6, DOI: 10.1109/INCOS59338.2024.10527612, May 2024, IEEE Xplore.

[40] Ravindra Changala, "Integration of Machine Learning and Computer Vision to Detect and Prevent the Crime", 2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS), ISBN:979-8-3503-1706-0, DOI: 10.1109/ICCAMS60113.2023.10526105, May 2024, IEEE Xplore.

[40] J. Shao, R. Lu, Y. Guan, and G. Wei, "Achieve efficient and verifiable conjunctive and fuzzy queries over encrypted data in cloud," IEEE Trans. Services Comput., vol. 15, no. 1, pp. 124–137, Jan. 2022.