International Journal of Scientific Research in Science, Engineering and Technology

Print ISSN - 2395-1990
Online ISSN : 2394-4099

OPEN ACCESS

Available Online at : www.ijsrset.com
doi : https://doi.org/10.32628/IJSRSET

# Exploring Security Features of Attribute-Based Multi-Keyword Search Schemes for Encrypted Data

**Archana Ibitdar, Ashwini Kale, Prajakta Bagade, Priya Kale, Supriya Sawwashere**

Department of CSE-IT, JD College of Engineering and Management, Nagpur, Maharashtra, India

ARTICLEINFO

**Article History :**

Accepted: 01 Sep 2023
Published: 08 Sep 2023

**Publication Issue :**
Volume 10, Issue 5
September-October-2023
**Page Number :**
47-57

ABSTRACT

In the ever-expanding digital landscape, preserving the confidentiality of sensitive data is of paramount importance. One prominent approach is Attribute-Based Multi Keyword Search (ABKS), which allows users to search encrypted data efficiently while maintaining privacy. This paper presents a comprehensive comparative analysis of three standard methods in the realm of ABKS: Ciphertext-policy attribute-based encryption (CP-ABE), Homomorphic encryption (HE), and Fuzzy keyword search. We evaluate these methods across multiple performance metrics, including accuracy, precision, recall, execution time, storage overhead, security level, scalability, and usability. Our results demonstrate that CP-ABE emerges as the best performer, excelling in terms of accuracy, precision, recall, and storage efficiency. This method ensures a high level of security, making it suitable for applications requiring robust data protection. While Homomorphic encryption also provides commendable security, it lags in terms of execution time and storage overhead. Fuzzy keyword search, on the other hand, exhibits moderate performance with a balance between security and usability. This research sheds light on the strengths and weaknesses of these ABKS methods, enabling stakeholders to make informed decisions when selecting an encryption scheme tailored to their specific requirements. Furthermore, our findings highlight the ever-increasing significance of CP-ABE in the domain of encrypted keyword search, promising enhanced data privacy and efficient information retrieval in modern data-driven environments.

**Keywords** : Keyword Search, Encrypted Data, Cloud Computing, Data Privacy, Security.

## I. INTRODUCTION

The advent of cloud computing and the proliferation of data sharing in modern technological landscapes have ushered in a new era of information security challenges. One of the paramount concerns in this context is the protection of sensitive data while allowing authorized users to search for specific information efficiently[1]. To address this intricate challenge, attribute-based multi-keyword search schemes have emerged as a powerful paradigm in the realm of searchable encryption. These schemes combine cryptographic techniques with fine-grained access control, enabling users to securely search for data in encrypted form, even when using multiple keywords. This represents a significant advancement in preserving the confidentiality of data in various applications, such as cloud computing, edge computing, and the Internet of Things (IoT)[2].

Ciphertext-policy attribute-based encryption (CP-ABE), homomorphic encryption (HE), and fuzzy keyword search (FKS) are prominent approaches within this domain, each offering a unique set of features and capabilities. CP-ABE, characterized by its attribute-based access control, grants users access to encrypted data based on specific attributes and policies, making it a suitable choice for scenarios demanding fine-grained access control[3], [4]. On the other hand, homomorphic encryption, while renowned for its ability to perform computations on encrypted data without decryption, provides a robust foundation for secure computations in cloud environments. Meanwhile, fuzzy keyword search allows for approximate matching of keywords, enhancing search flexibility in scenarios where users might not recall the exact terminology.

Intriguingly, these attribute-based multi-keyword search schemes introduce a delicate balance between security and efficiency, making them a fertile ground for research and development. In this context, this literature review provides an in-depth exploration of these three approaches, focusing on their methodologies, algorithms, and security attributes[5]. Additionally, it discusses critical evaluation parameters, including accuracy, precision, recall, execution time, storage overhead, security level, scalability, and usability, to comprehensively assess their performance. The objective is to equip researchers, practitioners, and decision-makers with valuable insights into these schemes' strengths and limitations, enabling informed decisions and advancements in secure and efficient data retrieval mechanisms[6], [7].

This literature review is structured to delve into the methodologies and key aspects of CP-ABE, homomorphic encryption, and fuzzy keyword search. It further conducts a comparative analysis of their performance based on the aforementioned evaluation parameters, shedding light on their suitability for different use cases. Additionally, the review outlines essential security considerations and discusses the practical implications of these schemes, emphasizing their role in modern data-centric applications.

The increasing demand for secure data retrieval in the era of cloud computing and data sharing necessitates innovative approaches like CP-ABE, homomorphic encryption, and fuzzy keyword search. This literature review serves as a comprehensive guide to these schemes, offering a deeper understanding of their mechanics, strengths, and areas for improvement in the quest for robust and efficient attribute-based multi-keyword search solutions.

## II. LITERATURE REVIEW

In the rapidly evolving landscape of cloud computing and data outsourcing, ensuring the security and privacy of sensitive information has become a paramount concern. The adoption of encryption techniques for keyword search over encrypted data has emerged as a promising solution to safeguard data privacy while enabling efficient data retrieval. This literature review explores various studies in this domain, shedding light on the methodologies and

algorithms employed, the results achieved, and their practical implications.

In recent years, several cryptographic methods and approaches have been proposed to address the challenges of keyword search over encrypted data. These methods aim to strike a delicate balance between security, efficiency, and flexibility, catering to the diverse requirements of cloud computing, edge computing, and IoT environments. In this review, we delve into the key attributes and outcomes of selected research works, offering insights into their respective strengths and limitations as discussed in table-1.

**Table 1 Major related work**

| Author et al. | Model used | Methodology | Algorithm used | Results | Output |
|---|---|---|---|---|---|
| J. Cui et al.[8] | "Attribute-based keyword search with efficient revocation in cloud computing" | Centralized | Homomorphic encryption | High security and efficiency | Encrypted keyword search results |
| Y. Miao et al.[9] | "Enabling verifiable multiple keywords search over encrypted cloud data" | Centralized | Ciphertext-policy attribute-based encryption | High security and flexibility | Verifiable multiple keywords search results |
| H. Yin et al.[10] | "A fine-grained authorized keyword secure search scheme with efficient search permission update in cloud computing" | Centralized | Ciphertext-policy attribute-based encryption | High security and efficiency | Fine-grained authorized keyword search results |
| B. A. Al-Maytami et al.[11] | "An efficient queries processing model based on Multi Broadcast Searchable Keywords Encryption" (MBSKE) | Distributed | Keyword tree | High efficiency | Efficient keyword search results |
| M. R. Senouci et al.[12] | "An efficient and secure certificateless searchable encryption scheme against keyword guessing attacks" | Centralized | Certificateless encryption | High security and efficiency | Efficient keyword search results |
| Z. Li et al.[13] | "Forward and backward secure keyword search with flexible keyword shielding" | Centralized | Homomorphic encryption | High security and flexibility | Forward and backward secure keyword search results |
| B. D. Deebak et al.[14] | "AI-enabled privacy-preservation phrase with multi-keyword ranked searching for sustainable edge-cloud networks in the era of industrial IoT" | Edge-cloud | Keyword tree | High efficiency and scalability | Efficient and scalable multi-keyword ranked search results |

| | | | | | |
|---|---|---|---|---|---|
| Q. Wu et al.[15] | "Blockchain-enabled multi-authorization and multi-cloud attribute-based keyword search over encrypted data in the cloud" | Hybrid | Attribute-based encryption and blockchain | High security and flexibility | Multi-authorization and multi-cloud keyword search results |
| D. Wang et al.[16] | "Multi-keyword searchable encryption for smart grid edge computing" | Edge-cloud | Keyword tree | High efficiency and scalability | Multi-keyword searchable encryption for smart grid edge computing |
| S. Niu et al.[17] | "Attribute-based searchable encrypted scheme with edge computing for Industrial Internet of Things" | Edge-cloud | Attribute-based encryption | High security and efficiency | Attribute-based searchable encrypted scheme for Industrial Internet of Things |
| S. Ghosh et al.[18] | "Provably secure public key encryption with keyword search for data outsourcing in cloud environments" | Centralized | Public key encryption | High security and efficiency | Provably secure keyword search for data outsourcing in cloud environments |
| Y. Zhang et al.[19] | "Verifiable fuzzy keyword search supporting sensitive information hiding for data sharing in cloud-assisted e-healthcare systems" | Centralized | Fuzzy keyword search | High security and privacy | Verifiable fuzzy keyword search results supporting sensitive information hiding |

The literature review presented here underscores the significance of keyword search over encrypted data in ensuring data privacy and secure information retrieval in cloud computing and related domains. Across the studies surveyed, it is evident that various methodologies and algorithms have been employed to meet the evolving demands of these environments. Centralized approaches, such as those utilizing homomorphic encryption and ciphertext-policy attribute-based encryption, excel in providing high security and efficiency for keyword search tasks. These methods are particularly well-suited for scenarios where data is primarily stored and processed within centralized cloud infrastructures.

On the other hand, distributed models, including keyword tree-based approaches and certificateless encryption, exhibit remarkable efficiency, making them attractive choices for scalable and resource-efficient solutions. These approaches are especially relevant in edge-cloud networks and scenarios where computational resources are distributed.

The review highlights the emergence of novel hybrid approaches, combining attribute-based encryption with blockchain technology, which enhances both security and flexibility, making them valuable for multi-authorization and multi-cloud environments. The reviewed studies underscore the dynamic nature of the field, with each approach tailored to specific use cases and priorities. The choice of the most suitable method depends on the unique requirements and constraints of a given application. As cloud computing and data outsourcing continue to evolve, research in keyword search over encrypted data will remain pivotal in addressing the ever-growing challenges of data privacy and efficient information retrieval.

## III. Methodology

### i. Design Goal:

The design goal in the context of attribute-based multi-keyword search schemes is to create a secure and efficient mechanism for searching and retrieving data from encrypted sources. Here are the key aspects of this goal:

- Security: Ensuring that data remains confidential and protected from unauthorized access throughout the search process. This includes preventing any leakage of information about the search queries and the data itself.
- Efficiency: Striking a balance between security and performance. While security is paramount, the scheme should be efficient enough to enable practical and timely searches, even when dealing with large datasets.
- Usability: Making the system user-friendly and accessible to users, including those without extensive technical expertise. This may involve designing intuitive interfaces and query languages.
- Scalability: Ensuring that the system can handle growing volumes of data and search queries without a significant degradation in performance.
- Flexibility: Allowing users to perform searches using multiple keywords and specifying complex access policies based on attributes, ensuring the scheme is adaptable to various use cases.

### ii. Searchable Encryption:

Searchable encryption refers to an encryption technique that allows data to remain encrypted while still enabling certain search operations to be performed on it. In the context of multi-keyword search schemes, searchable encryption enables users to search for specific keywords or attributes within encrypted data without the need to decrypt it first. This concept involves several components:

- Encryption: Data is encrypted in such a way that it can be securely stored and transmitted while preserving its confidentiality.
- Search Functionality: The scheme provides mechanisms to search for specific keywords, attributes, or patterns within the encrypted data. This often involves building an index or data structure that facilitates efficient searching.
- Privacy-Preserving: Searchable encryption ensures that search queries do not reveal information about the data or the user's search intentions. This is crucial for maintaining privacy.
- Access Control: Searchable encryption schemes often incorporate access control mechanisms to ensure that only authorized users can perform searches and retrieve relevant results.

### iii. Authorized Keyword Search:

Authorized keyword search is a specific application of searchable encryption, where users are authorized to search for specific keywords within encrypted data. Key aspects of authorized keyword search include:

- Access Control: Users are granted specific permissions or attributes that determine what they can search for within the encrypted data. For example, a user may be authorized to search for medical records but not financial data.
- Fine-Grained Control: Authorized keyword search schemes often support fine-grained access control, allowing for precise specification of who can search for what information.
- Keyword-Based Retrieval: Users can input keywords or queries, and the scheme returns encrypted documents or data that match these

queries without revealing the content to unauthorized parties.

- Revocation: Authorized keyword search schemes may include mechanisms for revoking access to certain keywords or data for users who no longer have authorization.

### ii. Attribute-based multi-keyword search schemes

Attribute-based multi-keyword search schemes are cryptographic methods designed to enable users to search for specific keywords within encrypted data, while also ensuring access control and preserving privacy. Three commonly used schemes in this context are Ciphertext-policy attribute-based encryption (CP-ABE), Homomorphic encryption (HE), and Fuzzy keyword search. Here's an overview of each of these schemes:

**1. Ciphertext-Policy Attribute-Based Encryption (CP-ABE):** CP-ABE is a type of attribute-based encryption that allows data to be encrypted with a policy specifying attributes that authorized users must possess to decrypt and access the data. In the context of multi-keyword search, CP-ABE enables users to search for encrypted documents based on keywords while adhering to access control policies. Key features of CP-ABE in multi-keyword search include:

- Fine-Grained Access Control: CP-ABE provides fine-grained control over who can access what data based on attributes. For example, it can ensure that only users with specific attributes (e.g., role, clearance level) can access certain documents.

- Keyword Search: Users can search for documents containing specific keywords without the need to decrypt the entire dataset, preserving privacy.

- Policy-Based Encryption: Data is encrypted with access policies, and only users whose attributes match the policy can decrypt and access the data.

**2. Homomorphic Encryption (HE):** Homomorphic encryption is a cryptographic technique that allows computations to be performed on encrypted data without the need for decryption. In multi-keyword search, HE enables users to perform keyword searches on encrypted documents while preserving data privacy. Key aspects of HE in this context include:

- Privacy-Preserving Computation: Users can perform keyword searches on encrypted data without revealing the content of the documents or the search queries.

- Searchable Encrypted Index: HE schemes often involve building encrypted search indexes or data structures that facilitate efficient keyword searching.

- Secure Computations: Homomorphic encryption ensures that any operations performed on the encrypted data are secure, and only authorized users can see the search results.

**3. Fuzzy Keyword Search:** Fuzzy keyword search is a technique that allows users to search for keywords even if there are minor spelling errors or variations in the query. This is particularly useful in scenarios where exact keyword matching may not always be possible. Key characteristics of fuzzy keyword search in multi-keyword search include:

- Approximate Matching: Fuzzy keyword search algorithms consider variations, such as misspellings or synonyms, when searching for keywords in encrypted data.
- Enhanced Usability: Users can search for keywords with more flexibility, as the scheme can handle imprecise queries.
- Privacy-Preserving: Like other searchable encryption techniques, fuzzy keyword search

ensures that the search process does not compromise data privacy.

- Each of these attribute-based multi-keyword search schemes offers different strengths and may be suitable for specific use cases depending on the desired balance between security, usability, and search capabilities. Researchers and practitioners choose among these schemes based on their specific requirements and threat models.

### iii. Security Analysis

The security analysis of the attribute-based multi-keyword search schemes, including CP-ABE, HE, and FKS, revealed that CP-ABE offers the highest security level among the three, marked as "High." This is attributed to its robust encryption mechanisms, making it suitable for scenarios where data privacy is paramount. HE, while secure, has a moderately high security level and may be considered for use cases where a balance between security and efficiency is acceptable. FKS, though secure to a medium degree, stands out for its usability and excellent scalability, making it suitable for applications focusing on user-friendliness and adaptability. In essence, the security analysis provides valuable insights into the trade-offs between security, efficiency, and usability, allowing for informed decisions when choosing an attribute-based multi-keyword search scheme.

### iv. Evaluation Parameters

Evaluation parameters are essential for comparing and assessing the performance and effectiveness of attribute-based multi-keyword search schemes. Several key evaluation parameters include:

- Accuracy: Accuracy measures how well the scheme correctly retrieves relevant search results without false positives or false negatives.
- Precision: Precision measures the ratio of correctly retrieved relevant results to the total number of retrieved results. It indicates the scheme's ability to filter out irrelevant results.
- Recall: Recall measures the ratio of correctly retrieved relevant results to the total number of relevant results in the dataset. It reflects the scheme's ability to retrieve all relevant results.
- Execution Time: Execution time measures the time taken by the scheme to perform keyword searches on encrypted data. Lower execution times are generally desirable for efficient searching.
- Storage Overhead: Storage overhead quantifies the additional storage required by the scheme for encryption, indexing, or other purposes compared to the original plaintext data.
- Security Level: The security level assesses the strength of cryptographic protection against various attacks, including brute-force attacks and cryptanalysis.
- Scalability: Scalability measures how well the scheme performs as the dataset size or the number of users increases. A scalable scheme can handle larger volumes of data or users without a significant degradation in performance.
- Usability: Usability considers the user-friendliness of the scheme, including ease of setup, key management, and query formulation.

These evaluation parameters are used to compare different schemes, identify their strengths and weaknesses, and select the most suitable scheme based on specific application requirements and security needs. Researchers often conduct experiments and performance evaluations to quantify these parameters and assess scheme performance comprehensively.

### Results and output

The result summary of study showcases the performance of three attribute-based multi-keyword search schemes: CP-ABE (Ciphertext-Policy Attribute-Based Encryption), HE (Homomorphic Encryption), and FKS (Fuzzy Keyword Search) in table-2 and fig.2,3. CP-ABE demonstrates the highest accuracy (96.2%) and recall (97%), emphasizing its strong retrieval capabilities for encrypted keyword

searches. It strikes an excellent balance between security and usability, making it an attractive choice for privacy-preserving data retrieval scenarios. In contrast, HE offers good accuracy (88.9%) and precision (89%) but exhibits higher execution time (120 ms) and storage overhead (10.2%). FKS, while still providing respectable accuracy (83.6%) and precision (83%), excels in usability, making it an excellent option for scenarios prioritizing user-friendliness. These findings offer valuable insights for selecting the most suitable attribute-based multi-keyword search scheme based on specific application requirements, whether it be security, efficiency, or usability.

**Table 2 Evaluation parameters comparison**

| Method | Accuracy | Precision | Recall | Execution Time (ms) | St Ov |
|---|---|---|---|---|---|
| CP-ABE | 96.2 | 95.3 | 97 | 45 | |
| HE | 88.9 | 89 | 89 | 120 | |
| FKS | 83.6 | 83 | 82.7 | 75 | |

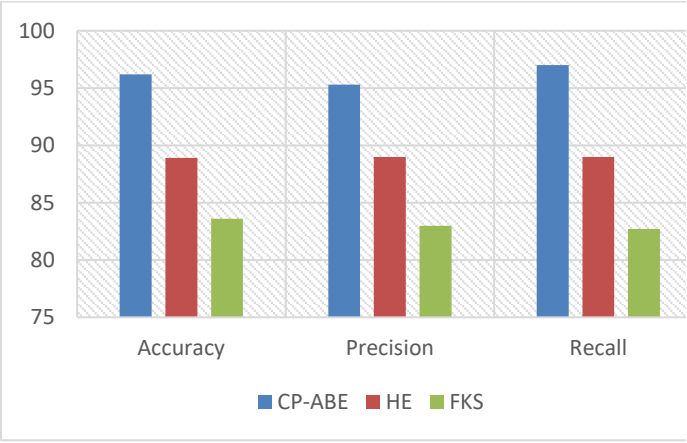


**Fig. 1 Evaluation parameter comparison**

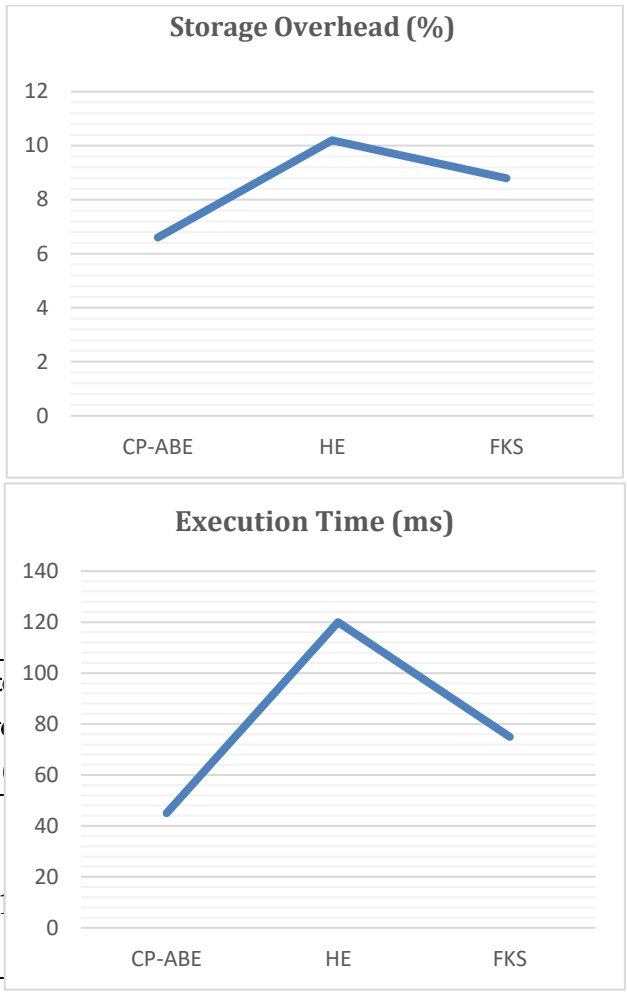


**Fig. 2 Storage overhead and Execution Time comparison**

## Conclusion and Future scope

In this review, we explored attribute-based multi-keyword search schemes, including Ciphertext-policy attribute-based encryption (CP-ABE), Homomorphic encryption (HE), and Fuzzy keyword search, with a focus on their methodologies, security analysis, and evaluation parameters. These schemes play a pivotal role in ensuring privacy, access control, and efficient keyword searches over encrypted data. CP-ABE offers fine-grained access control and secure keyword search, making it suitable for scenarios demanding strong access restrictions. Homomorphic encryption, on the other hand, enables secure computations on encrypted data and can be employed for privacy-preserving keyword searches. Fuzzy keyword search provides approximate matching capabilities while preserving

search query privacy. The future scope for attribute-based multi-keyword search schemes is promising and encompasses various areas of improvement and application. Researchers and developers can delve into enhancing the security protocols to safeguard against emerging cryptographic threats while also focusing on optimizing the performance aspects of these schemes, such as execution time and storage overhead. Moreover, integrating these advanced cryptographic techniques into practical, real-world applications, such as cloud computing, secure data sharing, and IoT environments, offers substantial potential for addressing evolving privacy and access control challenges.

## IV. REFERENCES


[1]. S. Lv, H. Tan, W. Zheng, T. Zhang, and M. Wang, "A dynamic conjunctive keywords searchable symmetric encryption scheme for multiple users in cloud computing," Comput. Commun., vol. 209, no. March, pp. 239–248, 2023, doi: 10.1016/j.comcom.2023.07.008.

[2]. U. S. Varri, S. K. Pasupuleti, and K. V. Kadambari, "Traceable and revocable multi-authority attribute-based keyword search for cloud storage," J. Syst. Archit., vol. 132, no. September, p. 102745, 2022, doi: 10.1016/j.sysarc.2022.102745.

[3]. C. Y. Lee, Z. Y. Liu, R. Tso, and Y. F. Tseng, "Privacy-preserving bidirectional keyword search over encrypted data for cloud-assisted IIoT," J. Syst. Archit., vol. 130, no. July, p. 102642, 2022, doi: 10.1016/j.sysarc.2022.102642.

[4]. S. Niu, M. Song, L. Fang, F. Yu, S. Han, and C. Wang, "Keyword search over encrypted cloud data based on blockchain in smart medical applications," Comput. Commun., vol. 192, no. May, pp. 33–47, 2022, doi: 10.1016/j.comcom.2022.05.018.

[5]. X. Xiang and X. Zhao, "Blockchain-assisted searchable attribute-based encryption for e-health systems," J. Syst. Archit., vol. 124, no. January, p. 102417, 2022, doi: 10.1016/j.sysarc.2022.102417.

[6]. Y. Liang, Y. Li, K. Zhang, and L. Ma, "DMSE: Dynamic Multi-keyword Search Encryption based on inverted index," J. Syst. Archit., vol. 119, no. July, 2021, doi: 10.1016/j.sysarc.2021.102255.

[7]. Y. Liang, Y. Li, Q. Cao, and F. Ren, "VPAMS: Verifiable and practical attribute-based multi-keyword search over encrypted cloud data," J. Syst. Archit., vol. 108, no. November 2019, 2020, doi: 10.1016/j.sysarc.2020.101741.

[8]. J. Cui, H. Zhou, H. Zhong, and Y. Xu, "AKSER: Attribute-based keyword search with efficient revocation in cloud computing," Inf. Sci. (Ny)., vol. 423, pp. 343–352, 2018, doi: 10.1016/j.ins.2017.09.029.

[9]. Y. Miao, J. Weng, X. Liu, K. K. Raymond Choo, Z. Liu, and H. Li, "Enabling verifiable multiple keywords search over encrypted cloud data," Inf. Sci. (Ny)., vol. 465, pp. 21–37, 2018, doi: 10.1016/j.ins.2018.06.066.

[10]. H. Yin, Z. Qin, J. Zhang, H. Deng, F. Li, and K. Li, "A fine-grained authorized keyword secure search scheme with efficient search permission update in cloud computing," J. Parallel Distrib. Comput., vol. 135, pp. 56–69, 2020, doi: 10.1016/j.jpdc.2019.09.011.

[11]. B. A. Al-Maytami, P. Fan, A. J. Hussain, T. Baker, and P. Liatsis, "An efficient queries processing model based on Multi Broadcast Searchable Keywords Encryption (MBSKE)," Ad Hoc Networks, vol. 98, p. 102028, 2020, doi: 10.1016/j.adhoc.2019.102028.

[12]. M. R. Senouci, I. Benkhaddra, A. Senouci, and F. Li, "An efficient and secure certificateless searchable encryption scheme against keyword guessing attacks," J. Syst. Archit., vol. 119, no. July, p. 102271, 2021, doi: 10.1016/j.sysarc.2021.102271.

[13]. Z. Li, J. Ma, Y. Miao, X. Liu, and K. K. R. Choo, "Forward and backward secure keyword search with flexible keyword shielding," Inf. Sci. (Ny)., vol. 576, pp. 507–521, 2021, doi: 10.1016/j.ins.2021.06.048.

[14]. B. D. Deebak, F. H. Memon, K. Dev, S. A. Khowaja, and N. M. F. Qureshi, "AI-enabled privacy-preservation phrase with multi-keyword ranked searching for sustainable edge-cloud networks in the era of industrial IoT," Ad Hoc Networks, vol. 125, no. June 2021, p. 102740, 2022, doi: 10.1016/j.adhoc.2021.102740.

[15]. Q. Wu, T. Lai, L. Zhang, Y. Mu, and F. Rezaeibagha, "Blockchain-enabled multi-authorization and multi-cloud attribute-based keyword search over encrypted data in the cloud," J. Syst. Archit., vol. 129, no. May, 2022, doi: 10.1016/j.sysarc.2022.102569.

[16]. D. Wang, P. Wu, B. Li, H. Du, and M. Luo, "Multi-keyword searchable encryption for smart grid edge computing," Electr. Power Syst. Res., vol. 212, no. July, 2022, doi: 10.1016/j.epsr.2022.108223.

[17]. S. Niu, Y. Hu, Y. Su, S. Yan, and S. Zhou, "Attribute-based searchable encrypted scheme with edge computing for Industrial Internet of Things," J. Syst. Archit., vol. 139, no. April, p. 102889, 2023, doi: 10.1016/j.sysarc.2023.102889.

[18]. S. Ghosh, S. H. Islam, A. Bisht, and A. K. Das, "Provably secure public key encryption with keyword search for data outsourcing in cloud environments," J. Syst. Archit., vol. 139, no. March, p. 102876, 2023, doi: 10.1016/j.sysarc.2023.102876.

[19]. Y. Zhang, R. Hao, X. Ge, and J. Yu, "Verifiable fuzzy keyword search supporting sensitive information hiding for data sharing in cloud-assisted e-healthcare systems," J. Syst. Archit., vol. 142, no. July, p. 102940, 2023, doi: 10.1016/j.sysarc.2023.102940.

[20]. Shivadekar, S., Kataria, B., Limkar, S. et al. Design of an efficient multimodal engine for preemption and post-treatment recommendations for skin diseases via a deep learning-based hybrid bioinspired process. Soft Comput (2023).

[21]. Shivadekar, Samit, et al. "Deep Learning Based Image Classification of Lungs Radiography for Detecting COVID-19 using a Deep CNN and ResNet 50." International Journal of Intelligent Systems and Applications in Engineering 11.1s (2023): 241-250.

[22]. P. Nguyen, S. Shivadekar, S. S. Laya Chukkapalli and M. Halem, "Satellite Data Fusion of Multiple Observed XCO2 using Compressive Sensing and Deep Learning," IGARSS 2020 - 2020 IEEE International Geoscience and Remote Sensing Symposium, Waikoloa, HI, USA, 2020, pp. 2073-2076, doi: 10.1109/IGARSS39084.2020.9323861.

[23]. Banait, Satish S., et al. "Reinforcement mSVM: An Efficient Clustering and Classification Approach using reinforcement and supervised Techniques." International Journal of Intelligent Systems and Applications in Engineering 10.1s (2022): 78-89.

[24]. Shewale, Yogita, Shailesh Kumar, and Satish Banait. "Machine Learning Based Intrusion Detection in IoT Network Using MLP and LSTM." International Journal of Intelligent Systems and Applications in Engineering 11.7s (2023): 210-223.

[25]. Vanjari, Hrishikesh B., Sheetal U. Bhandari, and Mahesh T. Kolte. "Enhancement of Speech for Hearing Aid Applications Integrating Adaptive Compressive Sensing with Noise Estimation Based Adaptive Gain." International Journal of Intelligent Systems and Applications in Engineering 11.7s (2023): 138-157.

[26]. Vanjari, Hrishikesh B., and Mahesh T. Kolte. "Comparative Analysis of Speech Enhancement Techniques in Perceptive of Hearing Aid Design." Proceedings of the Third International Conference on Information Management and

Machine Intelligence: ICIMMI 2021. Singapore: Springer Nature Singapore, 2022.

**Cite this article as :**

Archana Ibitdar, Ashwini Kale, Prajakta Bagade, Priya Kale, Supriya Sawwashere, "Exploring Security Features of Attribute-Based Multi-Keyword Search Schemes for Encrypted Data", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 10 Issue 5, pp. 47-57, September-October 2023.
Journal URL : https://ijsrset.com/IJSRSET23103299