International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

# Verifiable and Multi-Keyword Searchable Attribute-Based Encryption Scheme for Cloud Storage

**P Mamatha [1],Pagudala Chandana[2], Paduru Janitha[3],R Kaushik Reddy[4], Ranga[5]**
[2,3,4,5] UG Scholars, Department of CSE, **AVN Institute of Engineering and Technology,**Hyderabad, Telangana, India.
[1] Assistant Professor, Department of CSE, **AVN Institute of Engineering and Technology**, Hyderabad, Telangana, India.

## Abstract:

In attribute-based searchable encryption (ABSE) scheme, data owners can encrypt their data with access policy for security consideration, and encrypt keywords to obtain keyword index for privacy keyword search, and data users can search interesting keyword on keyword indexes by keyword search trapdoor. However, many existing searchable encryption schemes only support single keyword search and most of the existing attribute-based encryption (ABE) schemes have high computational costs at user client. These problems significantly limit the application of attribute-based searchable encryption schemes in practice. In this paper, we propose a verifiable and multi-keyword searchable attribute-based encryption (VMKS-ABE) scheme for cloud storage, in our new scheme, multi-keyword can be searched and the search privacy is protected. That is, the cloud server can search the multi-keyword with keyword search trapdoor but it does not know any information about the keywords searched. In the proposed scheme, many computing tasks are outsourced to the cloud proxy server, which greatly reduces the computing burden at the user client. Besides, the scheme also supports the verification of the correctness of the outsourced private key. The proposed scheme is proved secure that the keyword index is indistinguishable under the adaptive keyword attacks in the general group model, and the ciphertext is selective secure under selective plaintext attacks in the random oracle model. The security and experimental results show that our scheme is suitable for practicability.

## INTRODUCTION

With the development of cloud computing, many of information can be shared through computer networks. The cloud server(CS)can provide users with a variety of services, such as outsourcing commission calculations and data storage. Users can store their large amounts of data to the CS and share data with other users. For the purpose of the security of storage data and user's privacy, data is usually stored in encrypted form in CS. However, under this environment users will encounter a difficulty problem of how to search keywordin ciphertext. Searchable Encryption(SE) is a cryptographic technology that has been developed for many years, which supports users' keyword search in ciphertext. In the meanwhile, it can save a lot of network and computational overhead for user, and take advantage of the huge computing power of CS.

The SE technology mainly solves the problem of how to use the server to complete the search for interesting keywords when the data is encrypted and stored in CS, but CS is not completely trusted. How to improve the efficiency of keyword search while reducing local computing load is still a problem to be solved. Most of existing schemes support single-keyword search. Single-keyword search waste network bandwidth and computing resources, as this search method returns a large number of results, this means that the search result is not accurate. That is, when a data user uses multi- keyword search, the cloud server will return relatively few number of files containing these multi-keyword, thus the search result is much more accurate than when a data user uses one keyword search. In order to solve this problem, multi-keyword search is proposed.

Most of existing attribute-based encryption (ABE) schemes have high computational costs at user client. These problems greatly limit the applications of ABE schemes in practice. To solve the problems of network bandwidth waste and high computational cost, we propose a verifiable and multi-keyword searchable attribute-based encryption (VMKS-ABE) scheme for cloud storage, in which many computing tasks are outsourced to cloud proxy server to reduce local computing burden, the scheme also supports the verification of the correctness of out sourced private keys. In our new scheme multi-keyword can be searched and the search privacy is protected, which can greatly improve the accuracy of keyword search.

## A. RELATED WORK

### 1) SEARCHABLE ENCRYPTION

Song et al. first proposed the concept of searchable encryption(SE),which provides a basic method for searching on encrypted cloud data. Dong et al. [2] used RSA public key encryption algorithm and proxy encryption technology to implement a SE scheme in a multi-user environment. Li and Xu proposed ABSE scheme based on the attribute encryptional gorithm, and proved that the scheme can achieve indistinguishable safety against chosen keyword plaintext attacks under the selective model of attribute set. Subsequently, many experts and scholars published their solutions about the problem of how to conduct secure keyword search in encrypted data.To encrypt the data, and enable users who have corresponding access rights to search encrypted data. Sun et al. [7], and Dong et al. [8] constructed ABSE schemes to implement fine-grained access control and search for encrypted data. Attribute-based keyword search has been focused extensively because it canimpleent flexible access policy. Notably, the computation cost and communication cost in existing ABSE schemes are linear with the number of required attributes. Ye et al. [9] constructed ABSE with constant-size cipher texts schemes, the schemes realizes a constant calculation cost and the cipher text size remains unchanged. Moreover, because data destruction and improper operation, the CS may return error search answers. Consequently, it is very significant to ensure the correctness of returned answers in semi-trusted cloud environment. Under these circumstances, Chai and Gong [10] proposed the first keyword search scheme that can provide verifiable search capabilities.

### 2)ATTRIBUTE-BASEDENCRYPTION(ABE)

The concept of ABE was proposed by SahaiandWaters[11]. ABE can be classified into two types: one is the key-policy attribute-based encryption (KP-ABE) [12]; the other is the ciphertext-policy attribute-based encryption (CP-ABE) [13].

In the CP-ABE schemes, the ciphertext is related to an access policy, and private key of each user is related to the attribute set of the user. Users can decrypt a ciphertext only if his/her attribute set satisfies the access policy of the ciphertext. In the KP-ABE schemes, the attribute set and access policy are opposite to those described in the CP-ABE scheme. In the decryption process, only if a user's attributes set satisfies the access policy, the use can do decryption correctly. After attribute-based encryption schemes were proposed, there are many research works about ABE, such as CP-ABE schemes [14], [15], ABE schemes with hidden-policy[16]–[18],hierarchical attribute-based encryption schemes [19], [20], multi-authorization center ABE schemes [21] and traceable ABE schemes [22], [23]. However, in the above ABE schemes, the number of operations in the decryption process is associated with the complexity of access policy, and the user's computing power is limited. Therefore, how to decrease the user's computational load becomes an urgent problem to be solved. Green et al. [15] provided an ABE scheme in which partial decryption operations are outsourced to the CS. Wang et al. [24] proposed an adaptive security outsourcing CP-ABE scheme. But, they only considered the requirements of decryption outsourcing. Rui et al. [25] proposed a fully outsourced ciphertext policy ABE scheme that for the first time achieves outsourced key generation, encryption and decryption simultaneously. However, although CS has strong computing power, it is not completely trustworthy. CS is usually regarded as honest but curious. To ensure that CS can perform the ciphertext conversion process correctly, Lai et al. [26] proposed a verifiable outsourced ABE scheme that can verify the correctness of decryption. Their scheme adds additional information to the ciphertext and this information is used for verification. To decrease the length of encrypted ciphertext, Mao et al. [27]presented a new verifiable ABE scheme based on thes cheme proposed by Laietal.[26].Instead of encrypting the random message independently, the scheme [27] concatenates random message with original message before encrypting them. This greatly reduces the size of the original ciphertext, decreases the communication cost of the solution. Li et al. [28] proposed a new outsourced ABE scheme which supports both secure outsourced key-issuing and decryption. In 2016, Wang et al. [29] introduced the concept of verifiable outsourcing, that is, key generation center, data owner and data user can outsource their computational tasks to corresponding service providers to reduce local loads. The above schemes mainly focuses on verifiability of outsourced decryption for the authorized users. In 2017, Li et al. [30] proposed an ABE solution with verifiable out sourced decryption (referredtoasfullverifiabilityofoutsourceddecryption), which can simultaneously check the correctness of conversion passwords of authorized users and unauthorized users.

## LITERATURAL SURVEY

**Title**: **Practical techniques for searches on encrypted data.**

**Author**: D. X. Song, D. Wanger, and A. Perrig.

It is desirable to store data on data storage servers such as mail servers and file servers in encrypted form to reduce security and privacy risks. But this usually implies that one has to sacrifice functionality for security. For example, if a client wishes to retrieve only documents containing certain words, it was not previously known how to let the data storage server perform the search and answer the query, without loss of data confidentiality. We describe our cryptographic schemes for the problem of searching on encrypted data and provide proofs of security for the resulting crypto systems. Our techniques have a number of crucial advantages. They are provably secure: they provide provable secrecy for encryption, in the sense that the untrusted server cannot learn anything about the plaintext when only given the ciphertext; they provide query isolation for searches, meaning that the untrusted server cannot learn anything more about the plaintext than the search result; they provide controlled searching, so that the untrusted server cannot search for an arbitrary word without the user's authorization; they also support hidden queries, so that the user may ask the untrusted server to search for a secret word without revealing the word to the server. The algorithms presented are simple, fast (for a document of length n, the encryption and search algorithms only need O(n) stream cipher and block cipher operations), and introduce almost no space and communication overhead, and hence are practical to use today.

**Title: Shared and searchable encrypted data for untrusted servers.**

**Author**: C. Dong, G. Russello, and N. Dulay.

Current security mechanisms are not suitable for organisations that outsource their data management to untrusted servers. Encrypting and decrypting sensitive data at the client side is the normal approach in this situation but has high communication and computation overheads if only a subset of the data is required, for example, selecting records in a database table based on a keyword search. New cryptographic schemes have been proposed that support encrypted queries over encrypted data. But they all depend on a single set of secret keys, which implies single user access or sharing keys among multiple users, with key revocation requiring costly data re-encryption. In this paper, we propose an encryption scheme where each authorised user in the system has his own keys to encrypt and decrypt data. The scheme supports keyword search which enables the server to return only the encrypted data that satisfies an encrypted query without decrypting it. We provide a concrete construction of the scheme and give formal proofs of its security. We also report on the results of our implementation.

**Title**: **Attribute-based public encryption with keyword search.**

**Author**: S. Li and M. Xu, .

Public key encryption with keyword search applies only to the certain circumstances that keyword ciphertext can only be retrieved by a specific user and only supports single-keyword matching. In the existing searchable encryption schemes, either the communication mode is one-to-one, or only single-keyword search is supported. This paper proposes a searchable encryption that is based on attributes and supports multi-keyword search. The proposed scheme allows keyword ciphertext to be inquired correctly by multiple users if and only if the users defined by a series of attributes satisfy the access structure. This can realize the multi-user information query. In particular, the keyword of the user query does not need to match the keyword ciphertext exactly. The keywords in the ciphertext simply determine whether the keyword belongs to the set of keywords which are used for encryption. Extensive analysis indicates that the proposed scheme is secure and efficient.

Title: **Searchablesymmetric encryption: Improved definitions and efficient constructions.**

**Author:** R.Curtmola,J.Garay,S.Kamara,andR.Ostrovsky.

Searchable symmetric encryption (SSE) allows a party to outsource the storage of his data to another party in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research and several security definitions and constructions have been proposed. In this paper we begin by reviewing existing notions of security and propose new and stronger security definitions. We then present two constructions that we show secure under our new definitions. Interestingly, in addition to satisfying stronger security guarantees, our constructions are more efficient than all previous constructions. Further, prior work on SSE only considered the setting where only the owner of the data is capable of submitting search queries. We consider the natural extension where an arbitrary group of parties other than the owner can submit search queries. We formally define SSE in this multi-user setting, and present an efficient construction.

**Title: Deterministic and efficiently searchable encryption**

**Author**:M. Bellare, A. Boldyreva, and A. O'Neill.

We present as-strong-as-possible definitions of privacy, and constructions achieving them, for public-key encryption schemes where the encryption algorithm is deterministic. We obtain as a consequence database encryption methods that permit fast (i.e. sub-linear, and in fact logarithmic, time) search while provably providing privacy that is as strong as possible subject to this fast search constraint. One of our constructs, called RSA-DOAEP, has the added feature of being length preserving, so that it is the first example of a public-key cipher. We generalize this to obtain a notion of efficiently-searchable encryption schemes which permit more flexible privacy to search-time trade-offs via a technique called bucketization. Our results answer muchasked questions in the database community and provide foundations for work done there.

**Existing System.**

Many existing searchable encryption schemes only support single keyword search and most of the existing attribute-based encryption(ABE) schemes have high computational costs at user client. These problems significantly limit the application of attribute-based searchable encryption schemes in practice.

**Proposed System**

we propose a verifiable and multi-keyword searchable attribute-based encryption (VMKS-ABE)scheme for cloud storage, In our news cheme, multi-keyword can be searched and the search privacy Is protected. That is, the cloud server can search the multi-keyword with keyword search trapdoor but it does not know any information about the keywords searched.

**MODULES**

1. USER
2. DATA OWNER
3. CLOUD
4. ATTRIBUTE AUTHORITY
5. CLOUD PROXY SERVER
6. OKGSP

**MODULE DESCRIPTION**

1. **User**

   Here user is one of the module should register with the application, the user should be authorized by the cloud

   Here the user can perform the following actions such as request search key, view files, search based on multi key word, request for download permission, downloaded files and logout.

2. **Data Owner**

   Here owner is one of the module should register with the application, the owner should be authorized by the cloud

   Here the owner can perform the following actions such as upload files, view uploaded files, view my profile, view search transaction and logout.

3. **Attribute Authority**

   Here the attribute authority can directly login with the application and the attribute authority performs the operations like view permitted files to the cloud, send current time files to proxy, view waiting files and logout.

4. **Cloud Proxy Server**

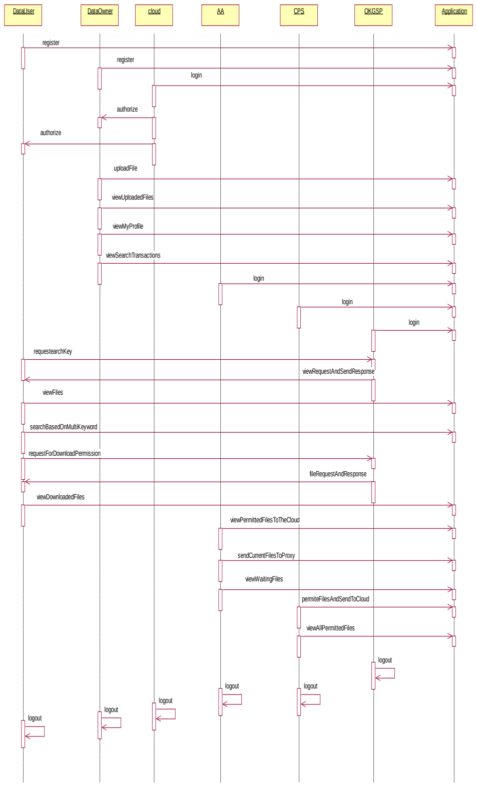
   Here the Cloud Proxy Server can directly login with the application and the Cloud Proxy Server performs the operations like permit files and send to cloud, view all permitted files and logout.

5. **Cloud**

   Here the cloud can also login with the application and the cloud can have the rights to authorize the users as well as owners, and also the cloud can perform view files, view all transactions.

6. **OKGSP**

   Okgsp also can access his home page directly and performs some actions like view search key request, view file request.



## CONCLUSION

In this article we proposed VMKS-ABE scheme. In our scheme, we combine the verifiable of the correctness of outsourced private key with multi-keyword search based on attribute encryption. In the general group model, the security of key word index is proved. Under the random oracle model, the ciphertext is proved to be selectively secure. Since the security in the general group model is much weak than in the standard model, it is worth constructing verifiable and multi-keyword searchable scheme in the standard model.

## BIBLIOGRAPHY

[1] D. X. Song, D. Wanger, and A. Perrig, ‘‘Practical techniques for searches onencrypteddata,’’Proc.IEEESymp.Secur.Privacy,Berkeley,CA,USA, May 2000, pp. 44–55.

[2] C. Dong, G. Russello, and N. Dulay, ‘‘Shared and searchable encrypted dataforuntrustedservers,’’inDataandApplicationsSecurityXXII,Berlin, Germany: Springer, Jul. 2008, pp. 127–143.

[3] S. Li and M. Xu, ‘‘Attribute-based public encryption with keyword search,’’ Chin. J. Comput., vol. 37, no. 5, pp. 1017–1024, Jun. 2014. doi: 10.3724/SP.J.1016.2014.01017.

[4] R.Curtmola,J.Garay,S.Kamara,andR.Ostrovsky,‘‘Searchablesymmetric encryption: Improved definitions and efficient constructions,’’ J. Comput. Secur., vol. 19, no. 5, pp. 895–934, 2011.

[5] M. Bellare, A. Boldyreva, and A. O’Neill, ‘‘Deterministic and efficiently searchable encryption,’’ in Advances in Cryptology (CRYPTO). Berlin, Germany: Springer, Aug. 2007, pp. 535–552.

[6] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, ‘‘Fuzzy keyword search over encrypted data in cloud computing,’’ in Proc. IEEE INFOCOM, San Diego, CA, USA, Mar. 2010, pp. 1–5. doi: 10.1109/INFCOM.2010.5462196.

[7] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, ‘‘Protecting your right: Verifiable attribute-based keyword search with fine-grained ownerenforced search authorization in the cloud,’’ IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 4, pp. 1187–1198, Apr. 2016. doi: 10.1109/TPDS. 2014.2355202.

[8] Q. Dong, Z. Guan, and Z. Chen, ‘‘attribute-based keyword search efficiency enhancement via an online/offline approach,’’ in Proc. IEEE 21st Int. Conf. Parallel Distrib. Syst. (ICPADS), Dec. 2015, pp. 298–305.

[9] Y. Ye, J. Han, W. Susilo, T. H. Yuen, and J. Li, ‘‘ABKS-CSC: Attributebased keyword search with constant-size ciphertexts,’’ Secur. Commun. Netw., vol. 9, no. 18, pp. 5003–5015, Dec. 2016. doi: 10.1002/sec.1671.

[10] Q. Chai and G. Gong, ‘‘Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers,’’ in Proc. IEEE Int. Conf. Commun. (ICC), Jun. 2012, pp. 917–922.