# PROTECTION SAVING POSITIONED MULTI KEYWORD SCAN FOR MULTIPLE DATA OWNERS IN CLOUD COMPUTING

**DR. M. CHANDRA SEKHAR**, Associate Professor, Department of CSE, Nalla Malla Reddy Engg. College, Hyderabad.

**DEEPU JIMMYJOEL LAZARUS**, Research Scholar, Associate Professor, Department of Computer Science & Technology, Sri Krishnadevaraya University, Anantapur.

**DR.G.A. RAMACHANDRA**, Associate Professor, Department of Computer Science & Technology, Sri Krishnadevaraya University, Anantapur.

## ABSTRACT

*With the coming of cloud computing, it has turned out to be progressively prevalent for data owners to outsource their information to open cloud servers while permitting information clients to recover this information. For protection concerns, secure inquiries over scrambled cloud information have spurred a few research works under the single proprietor model. Notwithstanding, most cloud servers by and by don't simply serve one proprietor; rather, they bolster various proprietors to share the advantages brought by distributed computing. In this paper, we propose plans to manage Privacy safeguarding Ranked Multi-keyword Search in a Multi-proprietor demonstrate (PRMSM). To empower cloud servers to perform secure inquiry without knowing the genuine information of both keywords and trapdoors, we deliberately build a novel secure inquiry convention. To rank the indexed lists and safeguard the security of pertinence scores amongst watchwords and records, we propose a novel Additive Order and Privacy Preserving Function family. To keep the aggressors from listening in mystery keys and putting on a show to be legitimate information clients submitting looks, we propose a novel element mystery key era convention and another information client verification convention. Besides, PRMSM underpins proficient information client denial. Broad analyses on genuine datasets affirm the viability and proficiency of PRMSM.*

***Keywords:*** *Cloud Computing, Ranked Multi key word Search, Privacy Preserving*

## 1. INTRODUCTION

Cloud computing is a subversive technology that is changing the way IT hardware and software are designed and purchased. As a new model of computing, cloud computing provides abundant benefits including easy access, decreased costs, quick deployment and flexible resource management, etc. Enterprises of all sizes can leverage the cloud to increase innovation and collaboration. Despite the abundant benefits of cloud computing, for privacy concerns, individuals and enterprise users are reluctant to outsource their sensitive data, including emails, personal health records and government confidential files, to the cloud. This is because once sensitive data are outsourced to a remote cloud; the corresponding data owners lose direct control of these data. Cloud service providers (CSPs) would promise to ensure owners' data security using mechanisms like virtualization and firewalls. However, these mechanisms do not protect owners' data privacy from the CSP itself, since the CSP possesses full control of cloud hardware, software, and owners' data. Encryption on sensitive data before outsourcing can preserve data privacy against CSP. However, data encryption makes the

traditional data utilization service based on plaintext keyword search a very challenging problem. A trivial solution to this problem is to download all the encrypted data and decrypt them locally. However, this method is obviously impractical because it will cause a huge amount of communication overhead. Therefore, developing a secure search service over encrypted cloud data is of paramount importance. Secure search over encrypted data has recently attracted the interest of many researchers. Song et al. first define and solve the problem of secure search over encrypted data. They propose the conception of searchable encryption, which is a cryptographic primitive that enables users to perform a keyword-based search on an encrypted dataset, just as on a plaintext dataset. Searchable encryption is further developed. However, these schemes are concerned mostly with single or Boolean keyword search. Extending these techniques for ranked multi keyword search will incur heavy computation and storage costs. Secure search over encrypted cloud data is first defined by Wang et al. and further developed. These researches not only reduce the computation and storage cost for secure keyword search over encrypted cloud data, but also enrich the category of search function, including secure ranked multi-keyword search, fuzzy keyword search, and similarity search. However, all these schemes are limited to the single-owner model. As a matter of fact, most cloud servers in practice do not just serve one data owner; instead, they often support multiple data owners to share the benefits brought by cloud computing. For example, to assist the government in making satisfactory policies on health care service, or to help medical institutions conduct useful research, some volunteer patients would agree to share their health data on the cloud. To preserve their privacy, they will encrypt their own health data with their secret keys. In this scenario, only the authorized organizations can perform a secure search over this encrypted data contributed by multiple data owners. Such a Personal Health Record sharing system, where multiple data owners are involved, can be found at mymedwall.com. Compared with the single-owner scheme, developing a full-fledged multi-owner scheme will have many new challenging problems. First, in the single owner scheme, the data owner has to stay online to generate trapdoors (encrypted keywords) for data users. However, when a huge amount of data owners are involved, asking them to stay online simultaneously to generate trapdoors would seriously affect the flexibility and usability of the search system. Second, since none of us would be willing to share our secret keys with others, different data owners would prefer to use their own secret keys to encrypt their secret data. Consequently, it is very challenging to perform a secure, convenient, and efficient search over the data encrypted with different secret keys. Third, when multiple data owners are involved, we should ensure efficient user enrollment and revocation mechanisms, so that our system enjoys excellent security and scalability. In this paper, we propose PRMSM, a privacy preserving ranked multi-keyword search protocol in a multi-owner cloud model. To enable cloud servers to perform secure search without knowing the actual value of

both keywords and trapdoors, we systematically construct a novel secure search protocol. As a result, different data owners use different keys to encrypt their files and keywords. Authenticated data users can issue a query without knowing secret keys of these different data owners. To rank the search results and preserve the privacy of relevance scores between keywords and files, we propose a new additive order and privacy preserving function family, which helps the cloud server, return the most relevant search results to data users without revealing any sensitive information. To prevent the attackers from eavesdropping secret keys and pretending to be legal data users submitting searches, we propose a novel dynamic secret key generation protocol and a new data user authentication protocol.

**Objective of the Project**

With the advent of cloud computing, it has become increasingly popular for data owners to outsource their data to public cloud servers while allowing data users to retrieve this data. For privacy concerns, secure searches over encrypted cloud data have motivated several research works under the single owner model. However, most cloud servers in practice do not just serve one owner; instead, they support multiple owners to share the benefits brought by cloud computing. In this paper, we propose schemes to deal with Privacy preserving Ranked Multi-keyword Search in a Multi-owner model (PRMSM). To enable cloud servers to perform secure search without knowing the actual data of both keywords and trapdoors, we systematically construct a novel secure search protocol. To rank the search results and preserve the privacy of relevance scores between keywords and files, we propose a novel Additive Order and Privacy Preserving Function family. To prevent the attackers from eavesdropping secret keys and pretending to be legal data users submitting searches, we propose a novel dynamic secret key generation protocol and a new data user authentication protocol.

## 2. LITERATURE SURVEY

### 2.1 High-Performance Cloud Computing: A View of Scientific Applications

Scientific computing often requires the availability of a massive number of computers for performing large scale experiments. Traditionally, these needs have been addressed by using high-performance computing solutions and installed facilities such as clusters and super computers, which are difficult to setup, maintain, and operate. Cloud computing provides scientists with a completely new model of utilizing the computing infrastructure. Compute resources, storage resources, as well as applications, can be dynamically provisioned (and integrated within the existing infrastructure) on a pay per use basis. These resources can be released when they are no more needed. Such services are often offered within the context of a Service Level Agreement (SLA), which ensure the desired Quality of Service (QOS). Aneka, an enterprise Cloud computing solution, harnesses the power of compute resources by relying on private and public Clouds and delivers to users the desired QOS. Its flexible and service based infrastructure supports multiple programming paradigms that make Aneka address a variety of

different scenarios: from finance applications to computational science.

We have discussed the potential opportunities and the current state-of-the-art of high-performance scientific computing on public clouds. The adoption of Cloud computing as a technology and a paradigm for the new era of computing has definitely become popular and appealing within the enterprise and service providers. It has also widely spread among end users, which more and more host their personal data to the cloud. For what concerns scientific computing, this trend is still at an early stage. Science computing Grids such as Open Science Grid and EGEE already provide a large scale infrastructure, a set of well-established methods and tools, and huge community of users.

### 2.2 Privacy-Preserving Public Auditing for Secure Cloud Storage

The cloud storage has a lot of problems about the security and data Integrity. So we need to prevent the all problems. In cloud storage users can remotely store their data and enjoy the on-demand high quality applications and services from shared resources, without the burden of local data storage and maintenance. Users are not able to check his data again and again from the cloud storage it is secure or not. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public audit ability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently.

In this paper, we propose a privacy-preserving public auditing system for data storage security in Cloud Computing. We utilize the homomorphism linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy preserving public auditing protocol into a multi-user setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency.

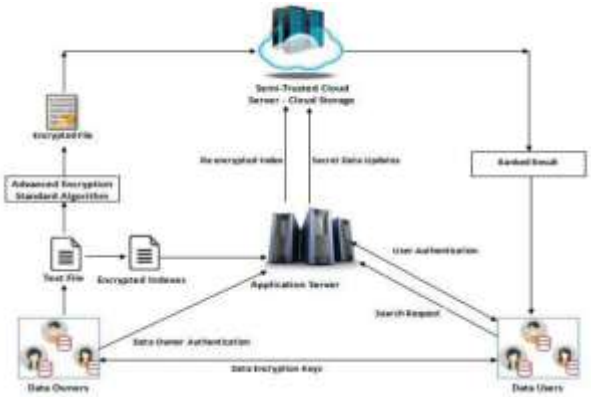

**Figure 1 : System Architecture**

### 2.3 Secure Conjunctive Keyword Search over Encrypted Data

We study the setting in which a user stores encrypted documents (e.g. e-mails) on an untrusted server. In order to retrieve documents satisfying a certain search criterion, the user gives the server a capability that allows the server to identify exactly those documents. Work in this area has largely focused on search criteria consisting of a single keyword. If the user is actually interested in documents containing each of several keywords (conjunctive keyword search) the user must either give the server capabilities for each of the keywords individually and rely on an intersection calculation (by either the server or the user) to determine the correct set of documents, or alternatively, the user may store additional information on the server to facilitate such searches. Neither solution is desirable; the former enables the server to learn which documents match each individual keyword of the conjunctive search and the latter results in exponential storage if the user allows for searches on every set of keywords. We define a security model for conjunctive keyword search over encrypted data and present the first schemes for conducting such searches securely. We propose first a scheme for which the communication cost is linear in the number of documents, but that cost can be incurred "offline" before the conjunctive query is asked. The security of this scheme relies on the Decisional Diffie-Hellman (DDH) assumption. We propose a second scheme whose communication cost is on the order of the number of keyword fields and whose security relies on a new hardness assumption.

We've presented two protocols for conjunctive search for which it is provably hard for the server to distinguish between the encrypted keywords of documents of its own choosing. Our protocols allow secure conjunctive search with small capabilities. Our work only partially solves the problem of secure Boolean search on encrypted data. In particular, a complete solution requires the ability to do disjunctive keyword search securely, both across and within keyword fields.

### 2.4 Adaptively Secure Computationally Efficient Searchable Symmetric Encryption

Searchable encryption is a technique that allows a client to store documents on a server in encrypted form. Stored documents can be retrieved selectively while revealing as little information as possible to the server. In the symmetric searchable encryption domain, the storage and the retrieval are performed by the same client. Most conventional searchable encryption schemes suffer from two disadvantages. First, searching the stored documents takes time linear in the size of the database, and/or uses heavy arithmetic operations. Secondly, the existing schemes do not consider adaptive attackers; a search-query will reveal information even about documents stored in the future. If they do consider this, it is at a significant cost to updates. In this paper we propose a novel symmetric searchable encryption scheme that offers searching at constant time in the number of unique keywords stored on the server. We present

two variants of the basic scheme which differ in the efficiency of search and update. We show how each scheme could be used in a personal health record system.

We propose a novel searchable encryption scheme which has searching time logarithmic in the number of unique keywords stored on the server while it is efficiently updatable. We propose two variants of the approach which differ in the efficiency of the Search and the Meta data Storage algorithms. We now present a general assessment of the two schemes proposed. The first scheme is more efficient in terms of computation for the Search algorithm, but requires two rounds of communication between the server and the client for each search. Moreover, a large bandwidth for the Meta data Storage algorithm is required. The second scheme enables the client to invoke the Meta data Storage with a minimum bandwidth and high efficiency. However, the Search algorithm is efficient under the condition that the Meta data Storage and the Search algorithms are interleaved, and the maximum number of times the database is updated.

**2.5 Efficient Keyword Search Scheme in Encrypted Cloud Computing Environment**

With the increasing popularity of cloud computing, more and more sensitive or private information has been outsourced onto the cloud server. For protecting data privacy, sensitive data usually has to be encrypted before outsourcing, which makes traditional search techniques based on plaintext useless. In response to the search over encrypted data, searchable encryption is a good solution in Information Security. However, most of existing searchable encryption schemes only support exact keyword search. That means they don't support searching for different variants of the query word, which is a significant drawback and greatly affects data usability and user experience. Recently, a fuzzy keyword search scheme proposed by some researchers aims at addressing the problems of minor typos and format inconsistence but couldn't solve the problem above. In this paper, we formalize the problem of semantic keyword-based search over encrypted cloud data while preserving privacy. Semantic keyword-based search will greatly improves the user experience by returning all the documents containing semantically close keywords related to the query word. In our solution, we use the stemming algorithm to construct stem set, which reduces the dimension of index. And the symbol-based tried is also adopted in index construction to improve the search efficiency. Through rigorous privacy analysis and experiment on real dataset, our scheme is secure and efficient.

In the paper, we discuss and address the problem of querying different variants of a keyword. Combining with the stemming algorithm, we propose a semantic keyword-based search scheme over encrypted cloud data. Given a query word, data users can find all the documents containing the semantically close keywords or different variants through our scheme, which tackles the limitation of exact keyword search. Through rigorous privacy analysis and

experimental study on real dataset, our scheme is quite secure and practical

**2.6 Efficient Fuzzy Search Engine with B -Tree Search Mechanism**

Search engines play a vital role in day to day life on internet. People use search engines to find content on internet. Cloud computing is the computing concept in which data is stored and accessed with the help of a third party server called as cloud. Data is not stored locally on our machines and the software's and information are provided to user if user demands for it. Search queries are the most important part in searching data on internet. A search query consists of one or more than one keywords. A search query is searched from the database for exact match, and the traditional searchable schemes do not tolerate minor typos and format inconsistencies, which happen quite frequently. This drawback makes the existing techniques unsuitable and they offer very low efficiency. In this paper, we will for the first time formulate the problem of effective fuzzy search by introducing tree search methodologies. we will explore the benefits of B trees in search mechanism and use them to have an efficient keyword search. We have taken into consideration the security analysis strictly so as to get a secure and privacy-preserving system.

In this paper, we presented a complete architecture of fuzzy keyword search scheme. Through the results, we suggest that Dictionary-based Fuzzy Keyword Search is an efficient method to make fuzzy keyword search scheme. Time taken by Dictionary–based fuzzy keyword search is much less than the time taken by any other method. For searching the keyword, we have explored the benefits of B Trees and our proposed system is secure and privacy-preserving, therefore, it correctly realize the function of Fuzzy keyword search. This solution has features like: 1. Text to speech search is there, so, the user can recheck the data which he has entered, 2. History of the user is provided, so that he can check the history. This searching technique works well on every data set such as database table entry, data matrix, column, etc.

**2.7 Survey on Searchable Public-key Cipher Texts for Privacy Preserving Keyword Search**

The Public Key Encryption along with Keyword Search allows one to search the data that is in encrypted form with a keyword without showing any information. This paper gives the detail study on searchable Public-Key Cipher texts with Hidden Structures (SPCHS) that fasten the keyword search without sacrificing the security of encrypted keywords. In SPCHS, the keyword cipher texts is structured by hidden relation and by using a trapdoor function used in cryptography to keywords to disclose minimum information to search algorithm. In SPCHS Schema, cipher texts have hidden star like structure. The SPCHS construction is based on IBKEM i.e. Identity Based Keyword Encapsulation Management that splits the computation in two parts first that perform heavy computation and other cipher text produced by light computation. The generic SPCHS construction is built with IBE i.e. Identity Based Encryption and Collision-free fully identity malleability IBKEM.

Public Key Encryption along with Keyword Search (PEKS) scheme allows one to search the encrypted data with a keyword without revealing any information. Thus the searchable public key cipher text with hidden structure for keyword search (SPCHS)makes search as fast as possible without sacrificing its semantic security .To increase search performance in PKES without sacrificing semantic security ,the cipher text are designed with hidden relation. If keyword searchable have hidden star like structure then search for cipher texts containing keywords can be fasten.

**2.8 Protecting Your Right: Attribute-based Keyword Search with Fine-grained Owner-enforced Search Authorization in the Cloud**

Search over encrypted data is a critically important enabling technique in cloud computing, where encryption-before out sourcing is a fundamental solution to protecting user data privacy in the un trusted cloud server environment. Many secure search schemes have been focusing on the single-contributor scenario, where the outsourced dataset or the secure searchable index of the dataset are encrypted and managed by a single owner, typically based on symmetric cryptography. In this paper, we focus on a different yet more challenging scenario where the outsourced dataset can be contributed from multiple owners and are searchable by multiple users, i.e. multi-user multi contributor case. Inspired by attribute-based encryption (ABE), we present the first attribute-based keyword search scheme with efficient user revocation (ABKS-UR) that enables scalable fine-grained (i.e. file-level) search authorization. Our scheme allows multiple owners to encrypt and outsource their data to the cloud server independently. Users can generate their own search capabilities without relying on an always online trusted authority. Fine-grained search authorization is also implemented by the owner-enforced access policy on the index of each file. Further, by incorporating proxy re-encryption and lazy re encryption techniques, we are able to delegate heavy system update workload during user revocation to the resourceful semi trusted cloud server. We formalize the security definition and prove the proposed ABKS-UR scheme selectively secure against chosen-keyword attack. Finally, performance evaluation shows the efficiency of our scheme.

In this paper, we design the first attribute-based keyword search scheme in the cloud environment, which enables scalable and fine-grained owner-enforced encrypted data search supporting multiple data owners and data users. Compared with existing public key authorized keyword search scheme, our scheme could achieve system scalability and fine-graininess at the same time. Different from search scheme with predicate encryption, our scheme enables a flexible authorized keyword search over arbitrarily-structured data. In addition, by using proxy re-encryption and lazy re encryption techniques, the proposed scheme is better suited to the cloud outsourcing model and enjoys efficient user revocation. Moreover, we formally prove the proposed scheme semantically secure in the selective model.

### 2.9 Efficient Information Retrieval for Ranked Query (EIRQ) In a Cost Effective of Cloud

Cloud computing as an emerging technology trend is expected to reshape the advances in information technology. In a cost efficient cloud environment, a user can tolerate a certain degree of delay while retrieving information from the cloud to reduce costs. In this paper, we address two fundamental issues in such an environment: privacy and efficiency. We first review a private keyword-based file retrieval scheme that was originally proposed by Ostrovsky. Their scheme allows a user to retrieve files of interest from an un trusted server without leaking any information. The main drawback is that it will cause a heavy querying overhead incurred on the cloud, and thus goes against the original intention of cost efficiency. In this paper, we present a scheme, termed efficient information retrieval for ranked query (EIRQ), based on an aggregation and distribution layer (ADL), to reduce querying overhead incurred on the cloud. In EIRQ, queries are classified into multiple ranks, where a higher ranked query can retrieve a higher percentage of matched files. A user can retrieve files on demand by choosing queries of different ranks.

In this paper, we proposed three EIRQ schemes based on an ADL to provide differential query services while protecting user privacy. By using our schemes, a user can retrieve different percentages of matched files by specifying queries of different ranks. By further reducing the communication cost incurred on the cloud, the EIRQ schemes make the private searching technique more applicable to a cost-efficient cloud environment. However, in the EIRQ schemes, we simply determine the rank of each file by the highest rank of queries it matches.

### 2.10Adaptive Indexing over Encrypted Numeric Data

Today, outsourcing query processing tasks to remote cloud servers becomes a viable option; such outsourcing calls for encrypting data stored at the server so as to render it secure against eavesdropping adversaries and/or an honest-but-curious server itself. At the same time, to be efficiently managed, outsourced data should be indexed, and even adaptively so, as a side-effect of query processing. Computationally heavy encryption schemes render such outsourcing unattractive; an alternative, Order-Preserving Encryption Scheme (OPES), intentionally preserves and reveals the order in the data, hence is unattractive from the security viewpoint. In this paper, we propose and analyze a scheme for lightweight and index able encryption, based on linear-algebra operations. Our scheme provides higher security than OPES and allows for range and point queries to be efficiently evaluated over encrypted numeric data, with decryption performed at the client side. We implement a prototype that performs incremental, query-triggered adaptive indexing over encrypted numeric data based on this scheme, without leaking order information in advance, and without prohibitive overhead, as our extensive experimental study demonstrates.

This paper presents a novel, lightweight, linear-algebra-based encryption scheme that allows for (i) range query processing over

encrypted numeric data outsourced in the cloud, and thereby for (ii) incremental, adaptive indexing whereby only data that are queried by trusted clients get indexed. Our scheme represents numerical values as short vectors, and relies on simple linear-algebra operations for encryption and decryption; it allows neither the actual data values nor their order to be disclosed. While the structure of the index may reveal order in the long-term, the index may reveal order in the long-term, this only happens after crucial indexing operations have been performed; furthermore, we propose an additional obfuscation component in our scheme, which deliberately introduces ambiguity in our construction by allowing two variant interpretations of each encrypted value vector. We propose that our scheme assures the security needed in time-critical operations such as high-frequency trading and financial transaction processing over the cloud.

**2.11 Optimal Average-Complexity Ideal-Security Order-Preserving Encryption**

Order-preserving encryption enables performing many classes of queries – including range queries – on encrypted databases. Popa et al. recently presented an ideal-secure order-preserving encryption (or encoding) scheme, but their cost of insertions (encryption) is very high. In this paper we present an also ideal-secure, but significantly more efficient order preserving encryption scheme. Our scheme is inspired by Reed's referenced work on the average height of random binary search trees. We show that our scheme improves the average communication complexity from O ($^{n}$log(n)) to $O_{(n)}$ under uniform distribution. Our scheme also integrates efficiently with adjustable encryption as used in Crypt DB. In our experiments for database inserts we achieve a performance increase of up to 81% in LANs and 95% in WANs.

We present a novel order-preserving encryption scheme. It has optimal average communication complexity of O(n) and is provably ideal-secure. We have shown in our database benchmark that it significantly – with a performance gain of up to 95% – outperforms previous work. Further experimental results indicate that our scheme works well with real world data sets and has a higher diffusion between plaintexts and cipher texts than previous work. Our scheme also efficiently integrates with adjustable encryption. Hence, it is currently the best suited scheme for outsourced, encrypted databases based on order-preserving encryption.

**3.0 Existing System**

Cloud service providers (CSPs) would promise to ensure owners' data security using mechanisms like virtualization and firewalls. However, these mechanisms do not protect owners' data privacy from the CSP itself, since the CSP possesses full control of cloud hardware, software, and owners' data. Encryption on sensitive data before outsourcing can preserve data privacy against CSP. However, data encryption makes the traditional data utilization service based on plaintext keyword search a very challenging problem. A trivial solution to this problem is to download all the encrypted data and decrypt them locally. However, this method is obviously

impractical because it will cause a huge amount of communication overhead. Therefore, developing a secure search service over encrypted cloud data is of paramount importance.

**Disadvantages:**

1. Single keyword search without ranking
2. Boolean keyword search without ranking
3. Single-keyword search with ranking
4. Do not get relevant data

### 3.1 Proposed System

We propose PRMSM, a privacy preserving ranked multi-keyword search protocol in a multi-owner cloud model. To enable cloud servers to perform secure search without knowing the actual value of both keywords and trapdoors, we systematically construct a novel secure search protocol. As a result, different data owners use different keys to encrypt their files and keywords. Authenticated data users can issue a query without knowing secret keys of these different data owners. To rank the search results and preserve the privacy of relevance scores between keywords and files

#### 3.1.1 Advantages:

- Prevents attackers from eavesdropping secret keys and pretending to be illegal data users performing searches, but also enables data user authentication and revocation.
- Allows data owners to encrypt keywords with self-chosen keys and allows authenticated data users to query without knowing these keys.
- Allows data owners to protect the privacy of relevance scores using different functions according to their preference, while still permitting the cloud server to rank the data files accurately.

## 4. CONCLUSION

In this paper, we explore the problem of secure multi-keyword search for multiple data owners and multiple data users in the cloud computing environment. Different from prior works, our schemes enable authenticated data users to achieve secure, convenient, and efficient searches over multiple data owners' data. To efficiently authenticate data users and detect attackers who steal the secret key and perform illegal searches, we propose a novel dynamic secret key generation protocol and a new data user authentication protocol. To enable the cloud server to perform secure search among multiple owners' data encrypted with different secret keys, we systematically construct a novel secure search protocol. To rank the search results and preserve the privacy of relevance scores between keywords and files, we propose a novel Additive Order and Privacy Preserving Function family. Moreover, we show that our approach is computationally efficient, even for large data and keyword sets.

## 5. BIBLIOGRAPHY

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Communication

of the ACM, vol. 53, no. 4, pp. 50–58, 2010.

[2] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013.

[3] D.Song, D.Wagner, and A.Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE International Symposium on Security and Privacy (S&P'00), Nagoya, Japan, Jan. 2000, pp. 44–55.

[4] E. Goh. (2003) Secure indexes. [Online]. Available: http://eprint.iacr.org/

[5] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. ACM CCS'06, VA, USA, Oct. 2006, pp. 79–88.

[6] D. B. et al., "Public key encryption with keyword search secure against keyword guessing attacks without random oracle," EUROCRYPT, vol. 43, pp. 506–522, 2004.

[7] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Proc. Applied Cryptography and Network Security (ACNS'04), Yellow Mountain, China, Jun. 2004, pp. 31–45.

[8] L. Ballard, S. Kamara, and F. Monrose, "Achieving efficient conjunctive keyword searches over encrypted data," in Proc. Information and Communications Security (ICICS'05), Beijing, China, Dec. 2005, pp. 414–426.

[9] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. IEEE Distributed Computing Systems (ICDCS'10), Genoa, Italy, Jun. 2010, pp. 253–262.

[10] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacypreserving multi-keyword ranked search over encrypted cloud data," in Proc. IEEE INFOCOM'11, Shanghai, China, Apr. 2011, pp. 829–837.