Iran University of Science &Technology
INTERNATIONAL CONFERENCE ON COMBINATORICS, CRYPTOGRAPHY AND COMPUTATION

Proceedings of the 2nd International Conference on Combinatorics, Cryptography and Computation (I4C2017)

Keyword-based Search over Encrypted Cloud Data: A Review

Maryam Hozhabr, Hamid Haj Seyyed Javadi
Department of computer engineering, South Tehran Branch, Islamic Azad University, Tehran, Iran, Department of mathematics and computer science, Shahed University, Tehran, Iran
m.hozhabr2015@gmail.com; h.s.javadi@shahed.ac.ir

ABSTRACT
Cloud computing provides an efficient and scalable computing infrastructure to process and store a large volume of data which motivates data owners to outsource their data to cloud servers. One of the most important issues in data outsourcing is how to protect sensitive data. To guarantee data privacy, data owner encrypts their sensitive data before uploading to the cloud. Thus, enabling keyword-based search over encrypted data is a very challenging task. Recently, searchable encryption schemes have been presented to execute keyword-based search over encrypted data. Searchable encryption allows the cloud server search over encrypted data securely without decryption them. We introduce relevant concepts and review state-of-the-art approaches.
Keywords: Cloud computing; Data outsourcing; Searchable encryption; Encrypted-Data Search;

1 INTRODUCTION

Cloud computing has been the hottest word in the IT area. It provides services in a pay-per-use model to users who can access the network. Similarly cloud storage provides users on-demand storage service, such as Dropbox, Amazon Simple Storage Services (S3), and Google Drive. Using these services, users can upload their data to the cloud storage server, and access their online data over the network regardless of when and where they are. For business users, rather than building their own data center, the company can leverage cloud storage service to store their data to the cloud storage server (Han et al., 2016),".Data security is a main concern of data owners when they outsource their data to cloud servers .The security of data is important not only for using of cloud computing, but also for development of application in other areas like internet of things (IoT) and big data. Cloud computing and IoT are dependent. IoT can use unlimited resources of cloud computing to recover its limitation (e.g. storage, energy, processing).
Cloud computing and big data are conjoined. Big data utilizes distributed storage technology based on cloud computing rather than local storage attached to a computer or electronic device. Big data evaluation is driven by fast-growing cloud-based applications developed using virtualized technologies. Therefore, cloud computing not only provides facilities for the computation and processing of big data but also serves as a service model (Hashem et al., 2015). Data owners are not able to control the outsourced data to cloud servers, hence privacy of sensitive data can be protected through encryption. One of challenges of data encryption is operations cannot be directly applied to the encrypted data therefore cloud provider cannot perform search operations over the encrypted data. Fully homomorphic encryption (zhao et al., 2014) proposed for retrieval of the encrypted data.
Fully homomorphic encryption is a powerful idea and undoubtedly has a role to play in cloud computing. In principle, it means that the cloud provider can run the correspondent of any program the client wishes, while not obtaining access either to the argument data or the result data (Ryan., 2016). Fully homomorphic encryption includes two basic homomorphism types. They are the multiply homomorphic encryption algorithm and additively homomorphic encryption algorithm. However they have high computation overhead. Searchable encryption is proposed to execute

keyword search on encrypted data. Searchable encryption system must meet some security properties. It is an encryption system, hence it should guarantee the data privacy, i.e. ciphertext does not reveal any private information of the data plaintext (Han et al., 2016). We survey keyword-based searching techniques for the retrieval of encrypted cloud data. This paper summarizes as follows: In session2, we outline architecture for search over encrypted cloud data and problem statement. Session 3 describes the literature survey and Session 4 concludes the paper.

2 ARCHITECTURE FOR SEARCH OVER ENCRYPTED CLOUD DATA AND PROBLEM STATEMENT

2.1 Architecture for search over encrypted cloud data

In (Cao et al., 2014), (Xia et al., 2016), (Li et al., 2016), (Wang et al., 2014), (Song et al., 2017), (Chen et al., 2016), (Sun et al., 2013) are considered the cloud storage has three different entities: the data owner, the cloud server and data users.

Data owner has a large collection of documents and he wants to outsource them to the cloud server. The documents should be encrypted before outsourcing because of protecting data privacy. First data owner creates a searchable index from the extracted keywords set of documents for improving efficiency search. Second the data owner encrypts collection of documents and searchable index, then uploads both of encrypted documents and secure index to the cloud server.

Data users are authorized to access the documents of the data owner. The authorized data user generates an encrypted query request (trapdoor) with query keywords by search control mechanism to fetch encrypted documents from the cloud server. The access control mechanism is applied to manage decryption for data users.

Cloud server stores the encrypted documents and the index. When a data user sends an encrypted query request to the cloud server, it executes keyword-based search over the index to find the documents which contain the query keywords. Finally, it sends related documents to the data user.

Communications should be protected between data users and cloud. Security of communication between data users and the cloud can be provided by the SSL standard protocol.

SSL is built into every browser, so no special client software is required. In addition as cloud services are mostly accessed through browsers, SSL has many benefits for client to host communications (Zissis et al., 2012).

The process of keyword-based search consists of four steps as follows:

- **Key Generation algorithm** takes a security parameter as input and then returns the secret keys as outputs.
- **Build index algorithm** builds a searchable index based on the extracted keywords set of documents which are encrypted with secret keys and then are outsourced to the cloud server.
- **Create Trapdoor algorithm** generates trapdoor by encrypting keywords of data user interested in the extracted keywords of documents as the input with secret keys.
- **Search algorithm** receives a Trapdoor, it performs the search on the index and returns the related encrypted documents.

2.2 Threat Model

In the exiting proposed works on secure cloud data search Cao et al., 2014), (Xia et al., 2016), (Li et al., 2016), (Wang et al., 2014), (Song et al., 2017), (Sun et al., 2013), (Wang et al., 2012) are considered the honest-but-curious model. The cloud server honestly executes search instructions in the designated protocol. Meanwhile, it is curious to infer encrypted documents, message received during the protocol and index to acquire more information. Based on what information the cloud server knows they have considered two threat model.

Known Cipher Text Model: In this model, the cloud server only knows the encrypted document collection, the searchable index which is outsourced by the data owner and the encrypted query requests are sent to the cloud server by the authorized data users.

Known Background Model*:* This model is stronger security threat. The cloud server knows more knowledge and utilize related statistical information to identify keywords.

2.3 Security requirements

Data privacy: The cloud server cannot get the plaintext of stored documents in the cloud server when data privacy is guaranteed. Data owner can employ traditional symmetric key cryptography to encrypt data before uploading to the cloud server, and prevent cloud server from curiosity in outsourced documents.
Confidentiality of index and trapdoor: keywords from documents are stored in the index and trapdoor, therefore they should not to be identified by the cloud server.
Trapdoor Unlinkability: The cloud server should not be able to distinguish two search requests are generated for the same search request.
Keyword privacy: The cloud server must not be able to discern keywords in the trapdoor and index by analyzing statistical information.
Verification of query results: The cloud server might be untrusted, hence verification of query results is an important element. Verification of query results includes three aspects:

1. Correct: if the computation involves only genuine data.
2. Complete: if the computation has been performed on the whole data collection and includes all resources satisfying the computation**.**
3. Fresh: if the computation has been performed on the most recent version of the data (vimercati et al., 2015).

2.4 Access control

Access control mechanisms are an indispensable security component of data outsourcing to the cloud server which the data owner limits a user's access to a subset of the data. Access controls comprising authentication and authorization, are the main means to control the dissemination of information. Typically, a principal is authenticated, and perhaps associated with various roles. Authorization to access data is then carried out at policy enforcement points in the application to grant or deny access to system objects by principals (in roles), (Pasquier et al., 2016). Models of secure data access are often classified into Mandatory Access Control (MAC) or Discretionary Access Control (DAC) systems. MAC systems: MAC systems differ as security policy is defined for the entire system, typically by administrators and achieves protection by associating *security labels* with data, in order to track and limit data propagation. DAC systems: Traditional and common models such as Access Control Lists (ACLs), capability systems and Role-Based Access Control (RBAC) are DAC systems, meaning that the owner of the data can modify access permissions DAC systems achieve protection by controlling access to resources (Bacon et al., 2014). A data owner can perform the selective restriction of access to his or her data outsourced to the cloud. Some users can be authorized by the owner to access the data, while others cannot access it without permission. Further, it is desirable to enforce fine-grained access control to the outsourced data; that is, different users should be granted different access privileges with regard to different data pieces. The access authorization must be controlled only by the owner in untrusted cloud environments (Tang et al., 2016).

3 LITERATURE SURVEY

3.1 Single keyword Search

A data user can search a certain keyword in single keyword search, On the other hand single keyword search allows a user gives a trapdoor for a keyword. Single keyword search for the first time is proposed by using symmetric encryption without index by (song et al., 2000). Every document is divided into some words with fixed length and each of them encrypted separately. The search time is depended on with size of data collection linearly. Update operations are supported in their scheme. This scheme is inefficient because the server has to perform a linear scan through all the documents on every query request. (Goh., 2003) first proposed a scheme bloom filter based index which supports dynamic operations. Their scheme has high efficiency, with O(1) search time per file however it has false positive problem. (Curtmola et al.,2006) proposed two schemes (SSE-1 and SSE-2) which are secure respectively against chosen-keyword attacks (CKA1) and against adaptive chosen-keyword attacks (CKA2) using inverted index. Their scheme supports static search. Inverted index is a kind of indexing structure that contains a list of mappings from the set of keywords to the corresponding set of files containing the keyword in the file collection

uploaded in the cloud server. For Ranked keyword search scheme, the task of determining the files that are most relevant is typically done by assigning a numerical score, which can be pre-compiled, to each file based on some ranking function (Raghavendra et al., 2016).(Karma et al., 2012) constructed an encrypted inverted index to perform dynamic operation efficiently. The total search time depended on the prevalence of words in files. (Wang et al., 2010) first proposed a secure ranked keyword search over encrypted cloud data. They have used keyword frequency for ranking results and order-preserving encryption.

Ranked search can enable quick search of the most relevant data. Sending back only the top-*k* most relevant documents can effectively decrease network traffic (Xia et al., 2016). Documents and queries are encrypted with a one-to-many OPSE (Order Preserving Symmetric Encryption) scheme. Their method has high efficient. (Cash et al., 2014) designed and implemented dynamic symmetric searchable encryption schemes. Their scheme support single-keyword searches. Their scheme ignore rank mechanism. (Ananthi et al., 2011) presented a secure ranked keyword search scheme. However when cloud server knows some background information, cloud server can deduce the actual value of some keywords.

(Boneh et al.,2004) proposed first public-key searchable encryption with supporting multi user model. The Public key encryption is expensive computationally and violate keyword privacy. The search time is O(1) in this scheme. Table1 shows comparison of Single keyword search schemes.

Table1 comparison of single keyword search schemes

Scheme	Dynamic	Search Time
song et al., 2000	Yes	The search time is linear to the size of the data collection
Goh., 2003	Yes	The search time is O (n), n is the cardinality of the document collection
Curtmola et al.,2006	No	O(number of documents containing keyword w)
Karma et al., 2012	Yes	O (number of documents containing keyword w)* log (number of documents.)
Wang et al., 2010	NO	The overall search time cost is almost as efficient as on unencrypted data
Cash et al., 2014	Yes	If the size of the result set is constant, then query time is largely independent of the size of the database and for result sets where the size is proportional to the database size, the cost is linear in the database size
Ananthi et al., 2011	No	The query time is dominated by the number of documents in dataset and is linear with the number of documents

3.2 Multi-keyword Boolean Search

Multi-keyword boolean search allows the users to input multiple query keywords to request suitable documents. Among these works, Disjunctive keyword search returns undifferentiated results, which means it returns every document that contains a subset of the specific keywords, even only one keyword of interest. Conjunctive keyword search returns "all-or-nothing", which means it only returns those documents in which all the keywords specified by the search query appear (Cao et al.,2014). Conjunctive keyword search schemes (Golle et al.,2004), (Ballardet al.,2005), (Brinkman.,2007), (Hwang et al.,2007), (Boneh et al.,2007) have been proposed over encrypted data. These methods have large overhead. Predicate search schemes (Shen et al.,2009), (Katz al.,2008), (Lewoko.,2010),are presented to support both conjunctive and disjunctive keyword search. The cost is linear with the number of query keywords in (Golle et al.,2004), (Boneh et al.,2007).Predicate encryption is a new paradigm for public-key encryption generalizing, among other things, identity-based encryption(Brinkman.,2007). (Shen et al., 2009) proposed a symmetric key predicate encryption scheme which supports inner product queries. They proved that their scheme can achieve both plaintext privacy and predicate privacy. (Katz et al.,2008) constructed a predicate encryption scheme supporting polynomial evaluation, disjunctions and inner products that is attribute-hiding and a public-key based encryption. (Lewko et al., 2010) presented two fully secure functional encryption schemes, a fully secure Attribute-

Based Encryption (ABE) scheme and a fully secure (attributed-hiding) predicate encryption (PE) scheme for inner-product predicated and proved the security. These multi keyword search schemes cannot support ranked search.

3.3 Multi Keyword Search

Multi-keyword search provides the capability of searching on encrypted documents with a set of keywords.
(Cao et al., 2014) proposed the first multi-keyword ranked search over encrypted cloud data using ‘‘Coordinate matching’’ technique. They have used inner product values to rank query results. The secure KNN scheme (Wang., 2009) is applied to encrypt but the search time of their scheme is linear with cardinality of document collection and the cloud server has to traverse all the indexes of the document collection for each query. The importance of the different keywords does not consider in their scheme, and thus the query results cannot be accurate. (Xia et al., 2016) proposed a secure and dynamic multi-keyword ranked search scheme and suggest tree-based index structure. They used the vector space model (TF×IDF) in the construction of index and generating query. A “Greedy Depth-first Search” algorithm is proposed to obtain high search efficiency. This scheme can achieve sub linear search time because of tree-based index. (Chen et al., 2016) proposed hierarchical clustering method. All documents are divided into subcategories. The vector space model is used and every document is represented by a vector. Users can execute search based on the novel dynamic K-means. Their approach can achieve a linear computational complexity against an exponential size increasing of document collection. (Sun et al., 2013) proposed privacy-preserving multi-keyword text search. The search index built based on term frequency and the vector space model with cosine similarity measure to achieve higher search result accuracy. To improve the search efficiency, a tree-based index structure is used and every node value is a vector of term frequency related. Various adaption methods for multi-dimensional (MD) algorithm are proposed in their scheme. However the relevance between documents is ignored in index building process. (Li et al., 2016) proposed enabling fine-grained multi-keyword Search. The preference factors and the relevance scores is introduced for the precise search and personalized user experiment. The vector space model (TF×IDF) is used for relevance scores measurement and the classified sub-dictionaries technique is employed to achieve better efficiency on index building, trapdoor generating and query. Their scheme can support complicated logic search the mixed “AND”, “OR” and “NO” operations of keywords. (Wang et al., 2014) proposed a novel multi keyword fuzzy search scheme by exploiting the locality-sensitive hashing technique. This scheme is based bloom filter and has eliminated the need of a predefined dictionary. Their scheme can tolerate keyword spelling error. However, their scheme does not consider the relevance between the original keyword and the files, which may cases some incorrect ranking. (Zhang et al., 2016) proposed multi-keyword search for multiple data owners. They presented a novel "Additive Order Preserving Function" to rank search results, a novel dynamic secret key generation protocol and a new data user authentication protocol. In this work, different data owners use different secret keys to encrypt their keywords and authenticated data users can generate their trapdoors without knowing these secret keys but their scheme is not dynamic. (Li et al., 2014) proposed a flexible multi-keyword query scheme, called MKQE. The documents with higher access frequencies and users’ access history have higher rankings in the matching result set. MKQE can reduce the maintenance overhead during the keyword dictionary expansion. (Orenic et al., 2013) proposed an efficient privacy-preserving search method over encrypted cloud data that utilizes minhash functions. They utilized a ranking method based on term frequencies and inverse document frequencies (tf-idf) of keywords. However, their scheme cannot provide exact ranking and the server computation is more. (Yu et al., 2013) proposed a two-round searchable encryption (TRSE) scheme that supports top-k multi-keyword retrieval. They employ a vector space model and homomorphic encryption. The key size is too large in their scheme and the communication aerial is very high, when the encrypted trapdoor's size is too large. Their scheme does not make effective searchable index update. (Chen et al.,2014) proposed an efficient and privacy-preserving semantic multi-keyword ranked search over encrypted cloud data. They utilize the “Latent Semantic Analysis” to reveal relationship between terms and documents. They employ secure “k-nearest neighbor (k-NN)” to achieve secure search functionality. Their method is better than the original Multi-keyword Ranked Search over Encrypted Cloud Data (MRSE) scheme. (Orenic et al., 2012) proposed a practical privacy-preserving ranked keyword search scheme based on Private Information Retrieval (PIR) that allows multi-keyword queries with ranking capability. Their scheme increases the security of the search scheme while satisfying efficient computation and communication requirements. Their scheme is not dynamic. Comparison of Multi keyword search schemes is shown in table2.

Table2 comparison of multi keyword search schemes

Scheme	Dynamic	Search Time
Cao et al., 2014	No	linear with cardinality of document collection
Xia et al., 2016	Yes	Sub linear
Chen et al., 2016	No	Linear computational complexity against an exponential size increasing of document collection.
Sun et al., 2013	No	better-than-linear search efficiency
Li et al., 2016	NO	greatly affected by the size of dictionary and the number of documents, and almost has no relation to the number of query keywords
Wang et al., 2014	NO	Linear with the size of file set and the number of keywords in the query has little impact
Zhang et al., 2016	No	For different size of queried keywords with the same size of data set and for different size of keyword dictionary with the same size of queried keywords is linear. For different size of data set with the same size of queried keywords do not increase
Li et al., 2014	No	-
Orenic et al., 2013	No	independent from the number of documents
Yu et al., 2013	Yes	Selecting the top-k files independent to the number of queried keywords and dependent to K and number of files
Chen et al.,2014	No	better than the original MRSE scheme
Orenic et al., 2012	NO	linear in the number of documents

3.4 Verifiable Search

Methods verification of query results can be divided into two main classes: deterministic and probabilistic (Vimercati., 2015).Deterministic approaches are based on the definition of authenticated data structures, which are structures built over specific attributes (e.g., Merkle hash trees or signature chaining schemes. Merkle hash tree and cryptographic signature techniques are used to construct authenticated tree structure upon which end users can verify the correctness and completeness of the query results (Chen et al., 2016). Merkle hash tree and cryptographic signature to create a verifiable MDB-tree are applied by (Sun et al., 2013) but results have less precision. (Chen et al., 2016) designed a structure called minimum hash sub-tree to verify the authentication of search results by applying the Merkle hash tree and cryptographic signature. (Jain et al., 2013) provided correctness and completeness verification of query results in the presence of access control policies with modifying the Merkle B-tree. Their scheme allowed easy change in access control policies under the lazy revocation model. (Pang et al., 2008) presented the first work for verifying the query results generated by text search engines. They employ Merkle hash tree based authenticated structure to enable verification over the query results. They ignored the search privacy preserving capabilities. (Lu., 2012) Proposed provably secure techniques to provide truly efficient and flexible search over encrypted data. Their scheme can achieve logarithmic search over encrypted data. (Sun et al., 2014) presented a verifiable privacy-preserving multi-keyword text search (MTS) scheme with similarity-based ranking. They applied hash and signature techniques. (Kurosawa et al., 2012) construct a (verifiable) SSE scheme that is universal composability (UC) with single keyword and supported linear search time. (Wang et al., 2012) proposed the ranked keyword search scheme that considers the relevance score of a keywords. They used the hash chain to verify the single keyword search result. However, their scheme does not support dynamic operations. (Stefanov et al., 2014) proposed a dynamic encrypted data search scheme with small privacy leakage and supports both updates and searches in sublinear time in the worst case, maintaining a data structure of linear size at the same time. (Sun et al. 2015) proposed an efficient verifiable conjunctive keyword search scheme over large dynamic encrypted cloud data. Their scheme allowed file to be updated without affecting the effective conjunctive keyword search operation. The verification complexity of our scheme is o (t+ρ), where ρ is number of files in the final search result and n is file collection size

Probabilistic approaches can detect an integrity violation for any query but with only probabilistic guarantees (vimercati et al., 2015) (e.g., (vimercati., 2014),(Wang., 2008)). Comparison of Verifiable search schemes is shown in table3.

Table3 comparison of verifiable search schemes

Scheme	**Dynamic**	**Query Type**
Chen et al., 2016	No	Multi-Keyword Search
Sun et al., 2013	No	Text Search
Jain et al., 2013	Yes	Range
Pang et al., 2008	No	Text search
Lu., 2012	Yes	Range
Sun et al., 2014	No	Conjunctive
Kurosawa et al., 2012	No	Single
Wang et al., 2012	No	Single
Stefanov et al. 2015	Yes	Single
Sun et al. 2015	Yes	Conjunctive

4 CONCLUSION

Security risks are the main concern about the deployment of cloud computing. In this paper, we have surveyed searchable encryption techniques for keyword-based search over encrypted data, which is an important challenging problem in cloud security. Searchable encryption provides a secure and efficient mechanism to retrieval of encrypted data over the cloud. The existing works, consider some of important issues to search on encrypted data such as security, efficiency, result ranking and dynamic update operations. We describe security requirements and recent progress in current solutions. Our future work is improving the efficiency and security of search.

REFERENCES

Han, F., Qin, J., & Hu, J. (2016). Secure searches in the cloud: a survey. Future Generation Computer Systems, 62, 66-75.

Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Khan, S. U. (2015). The rise of "big data" on cloud computing: Review and open research issues. Information Systems, 47, 98-115.

Zhao, F., Li, C., & Liu, C. F. (2014, February). A cloud computing security solution based on fully homomorphic encryption. In Advanced Communication Technology (ICACT), 2014 16th International Conference on (pp. 485-488). IEEE.

Ryan, M. D. (2013). Cloud computing security: The scientific challenge, and a survey of solutions. *Journal of Systems and Software*, 86(9), 2263-2268.

Cao, N., Wang, C., Li, M., Ren, K., & Lou, W. (2014). Privacy-preserving multi-keyword ranked search over encrypted cloud data. *IEEE Transactions on parallel and distributed systems*, 25(1), 222-233.

Xia, Z., Wang, X., Sun, X., & Wang, Q. (2016). A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. *IEEE Transactions on Parallel and Distributed Systems*, 27(2), 340-352.

Li, H., Yang, Y., Luan, T. H., Liang, X., Zhou, L., & Shen, X. S. (2016). Enabling fine-grained multi-keyword search supporting classified sub- dictionaries over encrypted cloud data. *IEEE Transactions on Dependable and Secure Computing*, 13(3), 312-325.

Wang, B., Yu, S., Lou, W., & Hou, Y. T. (2014, April). Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud. In I*NFOCOM*, 2014 Proceedings IEEE (pp. 2112-2120). IEEE.

Song, W., Wang, B., Wang, Q., Peng, Z., Lou, W., & Cui, Y. (2017). A privacy-preserved full-text retrieval algorithm over encrypted data for cloud storage applications. *Journal of Parallel and Distributed Computing*, 99, 14-27.

Chen, C., Zhu, X., Shen, P., Hu, J., Guo, S., Tari, Z., & Zomaya, A. Y. (2016). An efficient privacy-preserving ranked keyword search method. *IEEE Transactions on Parallel and Distributed Systems*, 27(4), 951-963.

Sun, W., Wang, B., Cao, N., Li, M., Lou, W., Hou, Y. T., & Li, H. (2013, May). Privacy-preserving multi- keyword text search in the cloud supporting similarity-based ranking. In *Proceedings of the 8th ACM SIGSAC symposium on Information*, *computer and communications security* (pp. 71-82). ACM.

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation computer systems*, 28(3), 583-592.

Wang, C., Cao, N., Ren, K., & Lou, W. (2012). Enabling secure and efficient ranked keyword search over outsourced cloud data. *IEEE Transactions on parallel and distributed systems*, 23(8), 1467-1479.

di Vimercati, S. D. C., Foresti, S., & Samarati, P. (2015, December). Data security issues in cloud scenarios. In *International Conference on Information Systems Security* (pp. 3-10). Springer International Publishing.

Pasquier, T., Bacon, J., Singh, J., & Eyers, D. (2016, June). Data-centric access control for cloud computing. In *Proceedings of the 21st ACM on Symposium on Access Control Models and Technologies* (pp. 81-88). ACM.

Bacon, J., Eyers, D., Pasquier, T. F. M., Singh, J., Papagiannis, I., & Pietzuch, P. (2014). *Information flow control for secure cloud computing. IEEE Transactions on Network and Service Management*, 11(1), 76-89.

Tang, J., Cui, Y., Li, Q., Ren, K., Liu, J., & Buyya, R. (2016). Ensuring security and privacy preservation for cloud data services. *ACM Computing Surveys (CSUR)*, *49*(1), 13.

Song, D. X., Wagner, D., & Perrig, A. (2000). Practical techniques for searches on encrypted data. In *Security and Privacy*, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on (pp. 44-55). IEEE.

Goh, E. J. (2003). Secure indexes. IACR Cryptology ePrint Archive, 2003, 216.

R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky, Searchable symmetric encryption: improved definitions and efficient constructions, in: Proceedings of the 13th ACM Conference on Computer and Communications Security, ACM, 2006, pp. 79–88

Raghavendra, S., Reddy, C. S., Geeta, C. M., Buyya, R., Venugopal, K. R., Iyengar, S. S., & Patnaik, L. M. (2016). Survey on Data Storage and Retrieval Techniques over Encrypted Cloud Data. *International Journal of Computer Science and Information Security*, *14*(9), 718.

Kamara, S., Papamanthou, C., & Roeder, T. (2012, October). Dynamic searchable symmetric encryption. In Proceedings of the 2012 ACM conference on Computer and communications security (pp. 965-976). ACM.

Wang, C., Cao, N., Li, J., Ren, K., & Lou, W. (2010, June). Secure ranked keyword search over encrypted cloud data. In *Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on* (pp. 253-262). IEEE.

Cash, D., Jaeger, J., Jarecki, S., Jutla, C. S., Krawczyk, H., Rosu, M. C., & Steiner, M. (2014, February). Dynamic Searchable Encryption in Very-Large Databases: Data Structures and Implementation. In *NDSS* (Vol. 14, pp. 23-26).

Ananthi, S., Sendil, M. S., & Karthik, S. (2011). Privacy preserving keyword search over encrypted cloud data. *Advances in Computing and Communications*, 480-487.

Boneh, D., Di Crescenzo, G., Ostrovsky, R., & Persiano, G. (2004, May). Public key encryption with keyword search. In International Conference on the Theory and Applications of Cryptographic Techniques (pp. 506-522). Springer Berlin Heidelberg.

Golle, P., Staddon, J., & Waters, B. (2004, June). Secure conjunctive keyword search over encrypted data. In *International Conference on Applied Cryptography and Network Security* (pp. 31-45). Springer Berlin Heidelberg.

Ballard, L., Kamara, S., & Monrose, F. (2005, December). Achieving efficient conjunctive keyword searches over encrypted data. In *International Conference on Information and Communications Security* (pp. 414-426). Springer Berlin Heidelberg.

Brinkman, R. (2007). *Searching in encrypted data*. University of Twente.

Hwang, Y. H., & Lee, P. J. (2007, July). Public key encryption with conjunctive keyword search and its extension to a multi-user system. In *International Conference on Pairing-Based Cryptography* (pp. 2-22). Springer Berlin Heidelberg.

Boneh, D., & Waters, B. (2007, February). Conjunctive, subset, and range queries on encrypted data. In *Theory of Cryptography Conference* (pp. 535-554). Springer Berlin Heidelberg.

Shen, E., Shi, E., & Waters, B. (2009, March). Predicate privacy in encryption systems. In *Theory of Cryptography Conference* (pp. 457-473). Springer Berlin Heidelberg.

Katz, J., Sahai, A., & Waters, B. (2008, April). Predicate encryption supporting disjunctions, polynomial equations, and inner products. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 146-162). Springer Berlin Heidelberg.

Lewko, A., Okamoto, T., Sahai, A., Takashima, K., & Waters, B. (2010, May). Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 62-91). Springer Berlin Heidelberg.

Wong, W. K., Cheung, D. W. L., Kao, B., & Mamoulis, N. (2009, June). Secure knn computation on encrypted databases. In *Proceedings of the 2009 ACM SIGMOD International Conference on Management of data* (pp. 139-152). ACM.

Zhang, W., Lin, Y., Xiao, S., Wu, J., & Zhou, S. (2016). Privacy preserving ranked multi-keyword search for multiple data owners in cloud computing. *IEEE Transactions on Computers*, *65*(5), 1566-1577.

Li, R., Xu, Z., Kang, W., Yow, K. C., & Xu, C. Z. (2014). Efficient multi-keyword ranked query over encrypted data in cloud computing. *Future Generation Computer Systems*, *30*, 179-190.

Orencik, C., Kantarcioglu, M., & Savas, E. (2013, June). A practical and secure multi-keyword search method over encrypted cloud data. In *Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on* (pp. 390-397). IEEE.

Yu, J., Lu, P., Zhu, Y., Xue, G., & Li, M. (2013). Toward secure multikeyword top-k retrieval over encrypted cloud data. *IEEE transactions on dependable and secure computing*, *10*(4), 239-250.

Chen, L., Sun, X., Xia, Z., & Liu, Q. (2014). An efficient and privacy-preserving semantic multi-keyword ranked search over encrypted cloud data. *International Journal of Security and Its Applications*, *8*(2), 323-332.

Örencik, C., & Savaş, E. (2012, March). Efficient and secure ranked multi-keyword search on encrypted cloud data. In *Proceedings of the 2012 Joint EDBT/ICDT Workshops* (pp. 186-195). ACM.

Jain, R., & Prabhakar, S. (2013, July). Access control and query verification for untrusted databases. In *IFIP Annual Conference on Data and Applications Security and Privacy* (pp. 211-225). Springer Berlin Heidelberg.

Pang, H., & Mouratidis, K. (2008). Authenticating the query results of text search engines. *Proceedings of the VLDB Endowment*, *1*(1), 126-137.

Lu, Y. (2012, February). Privacy-preserving Logarithmic-time Search on Encrypted Data in Cloud. In *NDSS*.

Sun, W., Wang, B., Cao, N., Li, M., Lou, W., Hou, Y. T., & Li, H. (2014). Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking. IEEE Transactions on Parallel and Distributed Systems, 25(11), 3025-3035.

Kurosawa, K., & Ohtaki, Y. (2012, February). UC-Secure Searchable Symmetric Encryption. In *Financial Cryptography* (Vol. 7397, pp. 285-298).

Stefanov, E., Papamanthou, C., & Shi, E. (2014, February). Practical Dynamic Searchable Encryption with Small Leakage. In *NDSS* (Vol. 14, pp. 23-26).

Sun, W., Liu, X., Lou, W., Hou, Y. T., & Li, H. (2015, April). Catch you if you lie to me: Efficient verifiable conjunctive keyword search over large dynamic encrypted cloud data. In *Computer Communications (INFOCOM), 2015 IEEE Conference on* (pp. 2110-2118). IEEE.

di Vimercati, S. D. C., Foresti, S., Jajodia, S., Livraga, G., Paraboschi, S., & Samarati, P. (2014, October). Integrity for distributed queries. In *Communications and Network Security (CNS), 2014 IEEE Conference on* (pp. 364-372). IEEE.

Wang, H., Yin, J., Perng, C. S., & Yu, P. S. (2008, October). Dual encryption for query integrity assurance. In *Proceedings of the 17th ACM conference on Information and knowledge management* (pp. 863-872). ACM.