International Journal of Innovative Computing, Information and Control
Volume **11**, Number **4**, August **2015**

ICIC International ©2015 ISSN 1349-4198
pp. 1257–1267

AN EFFECTIVE SEARCH OF CLOUD DATA USING ABC BASED CRYPTOGRAPHY AND MULTIPLE KEYWORD SEMANTICS

P. Senthil Kumari[1] and A. R. Nadira Banu Kamal[2]

[1]Department of Master of Computer Applications
[2]Department of Computer Science
Thassim Beevi Abdul Kader College for Women
Kilakarai, Tamil Nadu, India
{ senthilmathimca; nadirakamal }@gmail.com

Received October 2014; revised February 2015

Abstract. *Cloud computing enables the organizations to outsource their information and data by providing a service model known as IaaS (Infrastructure as a Service). In a public cloud, the cloud service provider manages the infrastructure and it is situated in the provider's control. The documents are encrypted before outsourcing in order to protect the privacy of sensitive data. When the number of encrypted documents is exponentially increased, the search service and retrieval becomes critical. The process of retrieving files consisting of queried keyword leads to unnecessary network traffic. In this paper, a secure scheme with multi keyword search is proposed for encrypted cloud data. A searchable index is generated for the data that has to be outsourced to the cloud. Encryption of data is performed using Association Based Cryptography (ABC). The encrypted data is wrapped with index and then outsourced. The searched result is ranked by the cloud server according to Robust Searchable Symmetric Encryption (RSSE) ranking criteria in order to enhance the document retrieval accuracy. This approach provides high security by using ABC. The experimental results show that the method provides efficient integrity verification for the transferred data and achieves minimum overhead for both communication and computation.*

Keywords: Data outsourcing, Encryption, Index generation, Multiple keyword semantics, Association Based Cryptography (ABC), Search query

1. **Introduction.** Cloud computing refers to a variety of computing concepts that include a large number of computers connected through a real-time communication network such as Internet. The cloud refers to software, infrastructure and platforms that are sold "as a service", i.e., remotely through the Internet. Usually, the seller contains actual energy-consuming servers that host products and services from a remote location. The end-users can log on to the network without installing anything. The main models of cloud computing service are known as Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Hardware as a Service (HaaS) and Everything as a Service (EaaS).

The providers of IaaS offer computers-virtual or physical machines and other resources. IaaS clouds also offer additional resources like raw (block) and file-based storage, load balancers, virtual machine disk image library, firewalls, IP addresses, software bundles, and Virtual Local Area Networks (VLANs). These cloud services can be offered in a public, hybrid or private network. The cloud computing contains a client server running at a remote location. End users use a web browser, mobile app or thin client to access cloud-based applications. The user's data and business software are stored on servers at remote location. It motivates both enterprises and individuals to outsource their local

complex data management system into the cloud, mainly when the usage of their data is rapidly increasing. The data is encrypted before outsourcing to commercial public cloud by the data owners to protect data sensitive data from unsolicited accesses in cloud.

Exploring efficient and privacy-preserving search service over the encrypted cloud data is very significant. In order to meet efficient data retrieval, a large number of documents demand cloud server to execute result relevance ranking. This ranked search prevents unnecessary network traffic by sending back only the relevant data and also enables data users to determine most relevant data quickly. Single keyword search usually yields coarse result [1]. It is necessary for the ranking system to support multiple keyword search in order to enhance search result accuracy and user searching experience. To retrieve relevant data, data users tend to provide a set of keywords to indicate their search interest. The use of multi-keyword semantics in the encrypted cloud data search system is a challenging task due to inherent security and privacy obstacles that include different strict requirements such as index privacy, data privacy, keyword privacy and many others.

This paper introduces a novel Association Based Cryptography (ABC) and multiple keywork semantics approach for secure search of the cloud data. The secure cloud data hosting service involves three different entities such as data owner, data user, and cloud server. Data owner has a collection of data documents to be outsourced to cloud. The outsourcing of data are in the encrypted form. Before outsourcing the data, the encrypted searchable index is formulated from the document. Then, the owner outsources the index and encrypted document collection to the cloud server. In order to search the document with the given keywords, an authorized user obtains a corresponding doucument through the search query. Cloud server is responsible to search the index and return the corresponding set of encrypted documents. The major advantages of the proposed ABC results are as follows,

- High security in cloud data and provide effective integrity verification for data transferred.
- Retrieve the results with lesser memory consumption and lesser latency.
- It can provide effective and security and privacy applications.

The remaining part of the paper is organized as follows. Section 2 involves the works related to the techniques for searching data in the cloud environment. Section 3 involves the description of the proposed approach including ABC based data encryption and use of multiple keyword semantics for searching cloud data. Section 4 involves performance analysis of the proposed approach with existing approach RSA. Section 5 includes conclusion and future enhancement.

2. **Related Work.** A practical privacy-preserving ranked keyword search scheme depending on Private Information Retrieval (PIR) was proposed [2]. It allows multi-keyword queries with ranking capability. The approach enhances the security of keyword search scheme and also satisfies effective communication and computation requirements. The approach consists of three steps:

- Index generation
- Trapdoor generation
- Query generation

The symmetric-key encryption technique is used for document encryption. The blinded encryption method is used to access the contents of retrieved documents without revealing to other parties. The testing is performed on a real dataset to compare the performance with other ranking approaches utilized in plain datasets. The Privacy-Preserving Query

over encrypted Graph-structured data in cloud computing (PPGQ) [3] uses "filtering-and-verification" principle to prune the possible negative data graphs. A feature-based index is prebuilt in order to provide feature-related data about encrypted data graph. The filtering procedure is carried out by choosing an effective inner product as the pruning tool. A secure inner product computation method meets the challenge of supporting graph query without any privacy breaches. The approach accomplishes privacy requirements under the well-known background threat model. The approaches lower overhead on communication and computation. The fuzzy keyword search over the encrypted cloud data [4] maintains keyword privacy and increases system usability. The approach returns matching files when the searching inputs match predefined keywords. When the exact match fails, the closest matching files depending on the keyword similarity semantics are returned. Two advanced approaches (i.e., gram-based and wildcard-based techniques) are designed to construct the storage-effective fuzzy keyword sets. The edit distance is used to quantify the keywords similarity.

A new symbol-based trie-traverse searching scheme is used to build a multi-way tree structure. The symbols that are transformed from the resulted fuzzy keyword sets are also used. The search scheme [5] provides privacy protection and rank-ordered search capability with minimum overhead. Initially, documents and search indexes are encrypted by the data owner and stored onto the cloud server. The approach preserves data privacy and retains good retrieval performance. Practical Keyword Index Search (PKIS) approach on cloud datacenter [6] consists of two schemes of efficiency and group search. The keyword index search privacy and group search secrecy are analyzed. A secure group search is supported by the approach without re-encrypting all documents under the group-key update. The scheme provides realistic, practical and secure solutions over the encrypted DB. A similarity index that ensures data privacy [7] is suitable for search systems outsourced in a cloud. The existing effective metric indexes are exploited that depend on a fixed set of reference points. The approach is implemented as a security extension of an existing method (M-Index). The evaluation of standard range and nearest neighbors' queries in an approximate and precise manner is supported by this encrypted M-Index.

The performance of the encrypted M-Index method is tested on three real data sets. A Secure Anonymous Database Search (SADS) system [8] provides exact keyword match capability. SADS allows effective execution of exact-match queries over distributed encrypted databases in controlled manner. A general framework built on cryptographic and privacy-preserving guarantees of SADS primitive is proposed. It is used in private secure search systems. The integrity of data storage is ensured in cloud computing [9] by allowing TPA (Third Party Auditing) on behalf of cloud client in order to validate the integrity of dynamic data. The involvement of client is eliminated by TPA. The approach ensures remote data integrity and also supports dynamic data operations. A secure cloud storage service [10] is built on top of a public cloud infrastructure. Non-standard and recent cryptographic primitives are combined. A light-weight solution [11] was used to preserve the access pattern privacy in un-trusted clouds. The approach incurs minimum communication and computational overhead when compared with the existing state-of-the-art solutions. The method requires less storage space at the cloud user. The scheme also hides the data access pattern efficiently in a long run after a number of accesses have been made.

An effective and Secure Data Sharing (SDS) framework [12] uses proxy re-encryption and homomorphic encryption schemes. The leakage of unauthorized data is prevented by these two schemes when a revoked user rejoins the system. The underlying SDS framework is modified. The information leakage during collision between revoked user and cloud service provider is prevented by a new solution based on data distribution approach. The

performance of the approach is tested on Amazon EC2. An effective quasi-identifier index based approach [13] is used to assure privacy preservation and accomplish high data utility over distributed and incremental data sets on cloud. The quasi-identifiers that represent groups of anonymized data are indexed in order to enhance the efficiency. The similar quasi-identifier groups are placed on the same node by the locality-sensitive hash function. The generalization or specialization process is elaborated during the occurrence of data updates. The experimental results show that the approach enhances the effectiveness of privacy preservation on large-volume incremental data sets. The searching method [14] enhances the effectiveness of ranked keyword search.

An efficient Ranked Searchable Symmetric Encryption is designed by using one-to-many order preserving mapping function. The keyword based and concept based searching approaches are combined. The method has the ability to classify and search large collections of unstructured information on conceptual basis. This searching method is reliable and provide more relevant results than the conventional searches. A new security architecture for cloud computing platform [15] performs the information hiding and ensures secure communication system. The approach performs information and data exchange by using asynchronous key system and Advanced Encryption Standard (AES) based file encryption system. Onetime password system is used for the user authentication process. Rivest-Shamir-Adleman (RSA) system is used for secure communication. Message Digest (MD5) hashing is used for information hiding. In the proposed system, an intruder cannot get data and upload files easily because it is significant to take control over all the servers. As there is priority for operation of individual servers, decision making is easy for each server, i.e., user authentication, file access. This structure can be applied with main cloud computing features, e.g., SaaS, PaaS and IaaS.

A ranked keyword based searching approach [16] allows the users to search over encrypted data. The information from the cloud is provided in ranked order to the user. The method determines exact matching copy of the file in an arranged order by considering essential elements such as keyword frequency. The approach deployed privacy enabled data hosting scheme. The server side ranking is performed with no loss of data by downloading and viewing the searched data. The method solves the inefficiency of secured searching. A scalable multi-keyword search [17] against searchable encrypted data uses multiple keywords in the search query. The documents are returned in order of their relevance to these keywords. The retrieved results for a given keyword search query are displayed in an effective order by using a scalable ROR (Relevance Oriented Ranking). The experimental results show that the approach achieves effective retrieval and display of data. The Ranked Semantic keyword Search (RSS) approach [18] allows the design of semantic extension. The approach not only returns exact matched files but also the files consisting of terms that are semantically related to the query keyword. A piece of file metadata is generated by the data owner for each file. The file collection and encrypted metadata set are uploaded to the cloud server.

After receiving a query request, the keywords that are semantically related to the query keyword are determined by the cloud server. Then the files are retrieved by using both the extensional words and query keyword. Total relevance score is used to retrieve the result files in order. The security analysis showed that the approach is secure and privacy-preserving under the previous SSE (Searchable Symmetric Encryption) security definition. Public-key Encryption with Multi-Keyword Search (PEMKS) approach [19] consists of a receiver which query subset keywords of all keywords that are embedded in the ciphertext. A Two-Round Searchable Encryption (TRSE) scheme [20] is used to eliminate the leakage of data. The approach supports top-k multi-keyword retrieval. Homomorphic encryption and vector space model are employed in the TRSE method. Sufficient search accuracy

is provided by the vector space model. Majority of the computing work is performed on the server side by operations on ciphertext. The approach eliminates data leakage and ensures data security. The fuzzy multi-keyword search approach [21] uses co-occurrence probabilities in order to determine additional multi-keywords which can be associated with the published encrypted data items. The approach has smaller storage cost when there is increase in the size of data files collection.

3. **Proposed Work.** This section describes the proposed effective search of confidential data in cloud computing. The flow of the proposed method is shown in Figure 1. A cloud data hosting service consists of three different entities.

- Data owner (DO)
- Data user (DU)
- Cloud server (CS)

Data owner is the actual owner of the database. The data owner collects and generates the information in the database. It consists of collection of data documents $D = (F_1, F_2, \ldots, F_n)$ to be outsourced to the cloud.

Data users are the members in the group who are entitled to access the information of the database.

Cloud server is the professional entity to deliver the information services to the authorized users. It often needs that the server is unaware to content of the database it maintains, the search terms in queries and the corresponding documents retrieved.

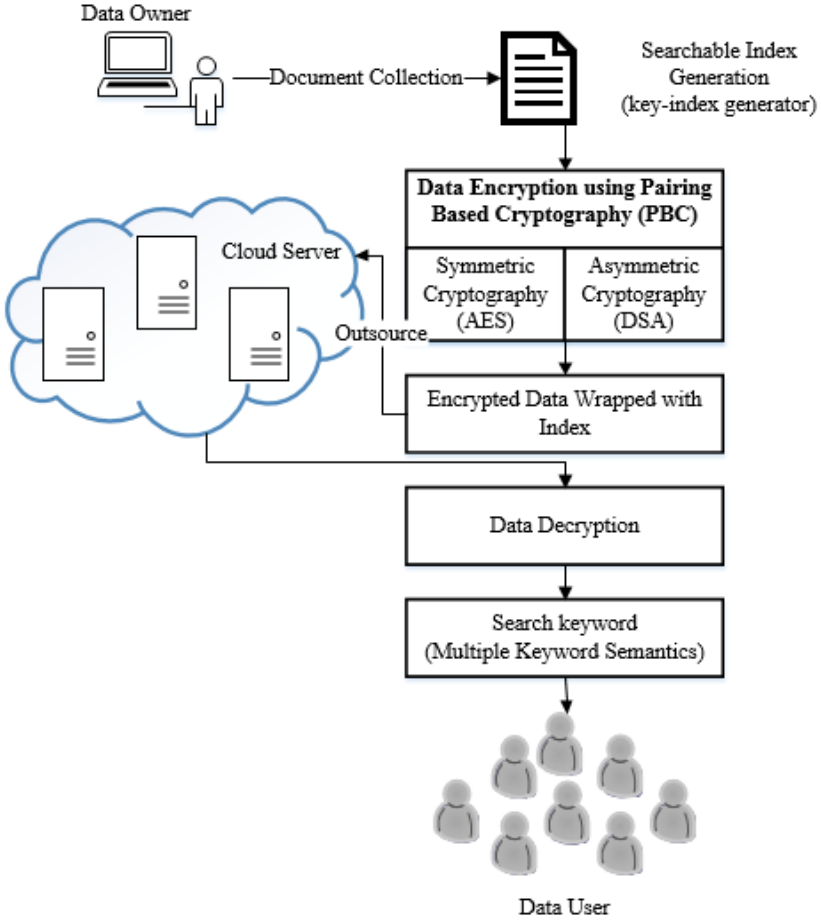

FIGURE 1. Flow of the proposed method

The pseudocode for the secure searching method over the cloud data is shown below.

Steps for secure searching method over cloud data
Step 1: Scan the collection of data files $D = (F_1, F_2, \ldots, F_n)$
Step 2: Extract distinct keywords $K = (k_1, k_2, \ldots, k_n)$ from the file collection D
Step 3: Construct the searchable index I from the set of keywords K
Step 4: Encrypt the document collection using ABC
a. Symmetric cryptography using AES
b. Assymetric cryptography using DSA
Step 5: Outsource index I and encrypted file collection D on the cloud server (CS)
Step 6: Retrieve the search query Q from the data user (DU)
Step 7: CS performs multi keyword search over the encrypted file collection D
Step 8: Relevant documents returned to DU

3.1. **Generation of index.** The data is outsourced on the cloud server in the encrypted form. For effective data utilization, the searching capability should be enabled over the encrypted form. So, a searchable index I is built from a set of n distinct keywords $K = (k_1, k_2, \ldots, k_n)$ extracted from the document collection D before encryption. Searchable index prevents server from performing association attack.

3.2. **Encryption of data.** In order to protect data privacy and act against unsolicited accesses, data encryption is performed before outsourcing. Data encryption also provides end-to-end data confidentiality assurance in the cloud. In the proposed approach, the data to be outsourced to the cloud is encrypted by using Association Based Cryptography (ABC). ABC is the use of association between elements of two cryptographic groups to a third group to generate cryptographic systems. If the same group is utilized for the first two groups, then the association is known as symmetric. Both symmetric and asymmetric based cryptography are used in the approach. The proposed method uses Advanced Encryption Standard (AES) algorithm for symmetric cryptography and Digital Signature Algorithm (DSA) for asymmetric cryptography. AES is a symmetric key algorithm, i.e., the same key is used for data encryption and decryption.

We are using AES algrotihm for data encryption and DSA algorithm for key generation. AES has key size of 128, 192, or 256 bits. The key size utilized for the AES cipher denotes the number of repetitions of transformation rounds which convert the plaintext (input) into ciphertext (final output). The AES algorithm protects the data up to secret level, i.e., a cryptographic algorithm consisting of two separate keys (a private and a public key). In DSA, the public key is used to encrypt the plaintext and the private key is used to decrypt the ciphertext.

3.3. **Data outsourcing.** The encrypted data is wrapped with the searchable index I and then outsourced on the cloud server. The authorization between the data owner and users is appropriately performed. Data owners share the outsourced data with a large number of users who want to retrieve only particular data files that they are interested in.

This is achieved with through keyword-based search. The authorized data user requests document from the cloud by sending a search query. The users who request data from the cloud, first get access and detail of requested query from owner. With the help of those details, the request is forwarded to cloud. The approach supports multiple keyword semantics, i.e., the document collection is searched for multiple keywords through the search query. Depending on the multi keyword semantics, an effective principle of similarity is selected between search query and the data index. The proposed approach achieves secure multi keyword search for the encrypted cloud data. The query is not sent

as what the data user requested. Instead, the query is subject to mathematical operation and sent through the network. So, the keyword query that is sent to the cloud is secured. After receiving the search query from the data users, cloud server searches the index and returns the corresponding set of encrypted documents. The cloud server sends back the documents that are most relevant to the search query.

3.4. **Robust Searchable Symmetric Encryption (RSSE) ranking.** The cloud server performs the ranking of the search result according to RSSE ranking criteria in order to enhance the document retrieval accuracy.

During the document retrieval, the ranking function computes relevance scores of matching files to a given search request. TF×IDF rule is used to evaluate the relevance score in the information retrieval process. TF (Term Frequency) denotes the number of times a given keyword is presented within a file. IDF (Inverse Document Frequency) is generated by dividing the number of files in the document collection by the number of files containing the keyword or term.

The determination of IDF is shown in Equation (1)

$$\text{IDF} = \frac{N}{N(k)} \tag{1}$$

where, N = total number of files in the document collection, $N(k)$ = number of files containing the term.

In order to rank the documents, a ranking procedure is required which assigns relevancy scores to each document matching to a given search query. The relevancy score of a document is calculated as the number representing the highest level search index that the query index matches. The relevance score is calculated as follows in Equation (2)

$$Score(S, F_e) = \sum\nolimits_{k \in S} \frac{1}{|F_e|}.(1 + \ln f_{e,k}).\ln\left(1 + \frac{N}{f_k}\right) \tag{2}$$

where S = searched keywords, $f_{e,k}$ = TF of keyword k in file F_e, f_k = number of files that contain keyword k, N = total number of files in the document collection, $|F_e|$ = length of file F_e, obtained by counting number of indexed terms.

The accurate ranking of the search results can be performed depending on the term frequency and file length information contained within single file as follows,

$$Score(k, F_e) = \frac{1}{|F_e|}.(1 + \ln f_{e,k}) \tag{3}$$

The term frequency is defined as the number of times a keyword appears in the document. Based on the score, the highest relevance factor pages appear at the top of the retrieved results.

4. **Performance Analysis.** In this section, the performance of the proposed cloud data outsourcing using Association Based Cryptography is discussed. The proposed encryption algorithms DSA and AES are compared with RSA algorithm. The performance of the proposed approach is compared with the existing algorithm RSA in terms of data encryption time, memory usage, time delay, and optimum relevancy scores.

4.1. **Key generation time.** We are using the DSA algorithm for key generation, because it is more secure and less susceptible to attacks. Moreover, it supports larger key sizes than the RSA algorithm. Figure 2 shows the comparison of key generation time of the proposed Digital Signature Algorithm (DSA) and RSA (cryptosystems). The analysis showed that the DSA consumes lesser key generation time than RSA.

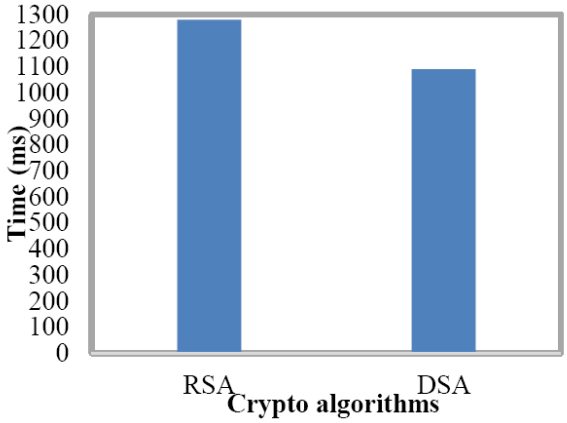

FIGURE 2. Key generation time of RSA and DSA

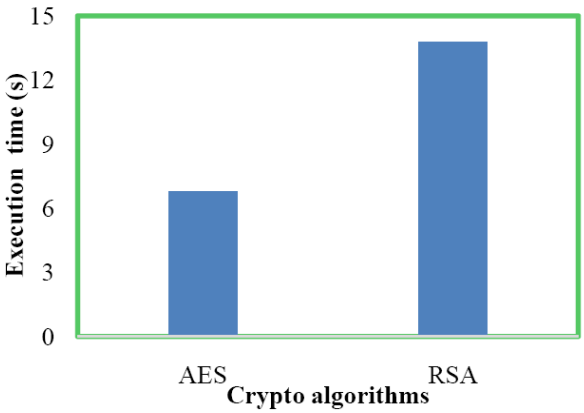

FIGURE 3. Data encryption time consumption of AES and RSA

4.2. **Data encryption time.** The data encryption time consumption of the proposed AES algorithm is compared with RSA. The result is shown in Figure 3. The analysis shows that AES consumes less data encryption time when compared with RSA.

4.3. **Processing memory for encryption.** The memory usage for encryption of the proposed AES algorithm is compared with RSA. AES algorithm requires lesser memory for implementation, which makes it suitable for restricted space environments. Still, no differential and linear cryptanalysis attacks have been yet proved on AES. Figure 4 shows the analysis of the proposed method with the existing RSA algorithm. It shows that AES consumes less processing memory for encryption when compared with RSA.

4.4. **Latency.** Latency is the response time to retrieve the results with the encryption of AES algorithm and existing RSA. The resultant values of the proposed AES algorithm is compared with RSA. Figure 5 shows that the AES algorithm achieves less time delay when compared with RSA.

4.5. **Relevance score.** Query execution in the cloud server consists of computing and ranking similarity scores for all the documents in the database. The relevance score is computed to list the top searched documents. The relevancy score comparison of multi keyword search (MKR) and single keyword search (SKR) is shown in Figure 6. The results show that the multi keyword search achieves optimal relevancy score when compared with single keyword search.

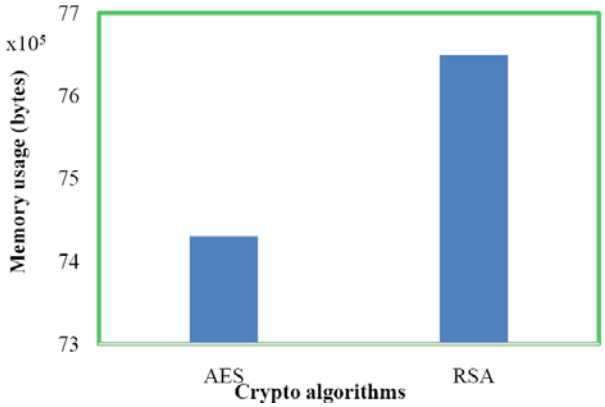

FIGURE 4. Processing memory consumption of AES and RSA

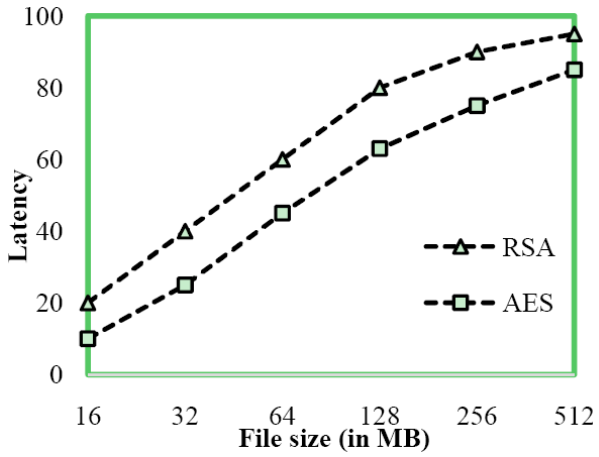

FIGURE 5. Time delay of AES and RSA

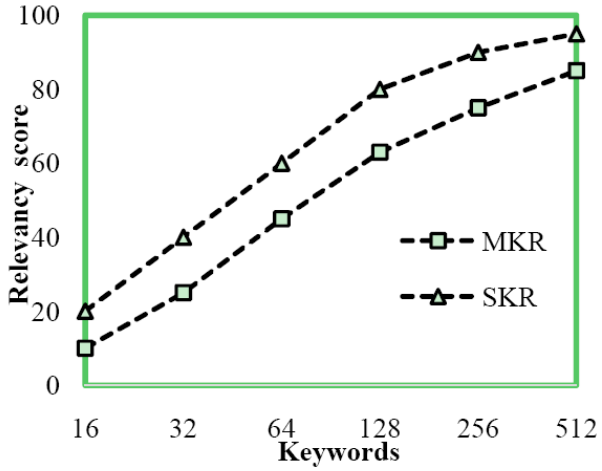

FIGURE 6. Relevance score comparison of multi keyword and single keyword search

Various experiments are conducted for analyzing the time consumption. Table 1 summarises the time consumption (in milliseconds) for building searchable index for different data sizes and for different number of keywords. The proposed method takes only fewer milliseconds to build the searchable index.

TABLE 1. Time consumption for building searchable index

Data Size (Kb)	No. of Keywords	Time for Building Index (Ms)
40	26	1.33
60	37	1.86
80	53	2.03
90	62	2.33

The proposed method proves to be efficient to return the highly relevant documents corresponding to the submitted multiple search keywords.

5. **Conclusion and Future Work.** An approach for effective search of confidential data in cloud computing is proposed. The documents are encrypted by using Association Based Cryptography (ABC) and wrapped with the searchable index. Then the encrypted data from the data owners is outsourced on the cloud server. The approach allows multi keyword search for the encrypted cloud data. The approach achieves high security by using ABC. Effective integrity verification is provided for the transferred data. The proposed method achieves low overhead for computation and communication. The proposed method is analyzed against key generation time, data encryption time consumption, memory usage, latency and relevancy score. The experimental results and response time when compared with the existing show that the proposed method achieves optimized memory and relevance score, minimum data encryption time consumption RSA. The proposed approach works well in private cloud and it is suitable for private cloud applications.

As future work, the method can be enhanced to work in multi user environment, i.e., in public cloud. The approach can be combined with attribute based cryptography and bilinear mapping to enhance the data security. By enhancing the key generation, the data security is also enhanced.

REFERENCES

[1] C. Wang, N. Cao, K. Ren and W. Lou, Enabling secure and efficient ranked keyword search over outsourced cloud data, *IEEE Trans. Parallel and Distributed Systems*, vol.23, no.8, 2012.

[2] C. Öencik and E. Savaş, Efficient and secure ranked multi-keyword search on encrypted cloud data, *Proc. of the 2012 Joint EDBT/ICDT Workshops*, pp.186-195, 2012.

[3] N. Cao, Z. Yang, C. Wang, K. Ren and W. Lou, Privacy-preserving query over encrypted graph-structured data in cloud computing, *2011 the 31st International Conference on Distributed Computing Systems (ICDCS)*, pp.393-402, 2011.

[4] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren and W. Lou, Fuzzy keyword search over encrypted data in cloud computing, *INFOCOM, 2010 Proc. of IEEE*, pp.1-5, 2010.

[5] S. Ananthi, M. S. Sendil and S. Karthik, Privacy preserving keyword search over encrypted cloud data, *Advances in Computing and Communications*, pp.480-487, 2011.

[6] H.-A. Park, J. H. Park and D. H. Lee, PKIS: Practical keyword index search on cloud data center, *EURASIP Journal on Wireless Communications and Networking*, pp.1-16, 2011.

[7] S. Kozak, D. Novak and P. Zezula, Secure metric-based index for similarity cloud, *Secure Data Management*, pp.130-147, 2012.

[8] M. Raykova, A. Cui, B. Liu, B. Vo, T. Malkin, S. M. Bellovin and S. J. Stolfo, *Usable Secure Private Search*, Department of Computer Science, Columbia University, New York, NY, USA, 2011.

[9] Q. Wang, C. Wang, K. Ren, W. Lou and J. Li, Enabling public auditability and data dynamics for storage security in cloud computing, *IEEE Trans. Parallel and Distributed Systems*, vol.22, pp.847-859, 2011.

[10] S. Kamara and K. Lauter, Cryptographic cloud storage, *Financial Cryptography and Data Security*, pp.136-149, 2010.

[11] K. Yang, J. Zhang, W. Zhang and D. Qiao, A light-weight solution to preservation of access pattern privacy in un-trusted clouds, *Computer Security – ESORICS 2011*, pp.528-547, 2011.

[12] B. K. Samanthula, Y. Elmehdwi, G. Howser and S. Madria, A secure data sharing and query processing framework via federation of cloud computing, *Information Systems*, 2013.

[13] X. Zhang, C. Liu, S. Nepal and J. Chen, An efficient quasi-identifier index based approach for privacy preservation over incremental data sets on cloud, *Journal of Computer and System Sciences*, vol.79, no.5, pp.542-555, 2013.

[14] K. Sengoden and S. Paul, Improving the efficiency of ranked keyword search over cloud data, *International Journal of Advanced Research in Computer Engineering & Technology*, vol.2, pp.0881-0883, 2013.

[15] K. W. Nafi, T. S. Kar, S. A. Hoque and M. M. A. Hashem, A newer user authentication, file encryption and distributed server based cloud computing security architecture, *International Journal of Advanced Computer Science and Applications*, vol.3, no.10, pp.181-186, 2013.

[16] G. Shynu P., M. Jose and M. M. Chacko, An efficient and secure searching model for outsourced cloud data, *International Journal of Advanced Research in Computer Science*, vol.4, no.9, p.198, 2013.

[17] S. Chinna, A. S. Kumar, D. Priyanka and B. S. Kumar, A scalable multi keyword search and relevance oriented ranking for searchable network encrypted data in cloud storage systems, *International Journal of Innovative Research in Computer and Communication Engineering*, vol.1, no.2, 2013.

[18] X. Sun, Y. Zhu, Z. Xia, J. Wang and L. Chen, Secure keyword-based ranked semantic search over encrypted cloud data, *Advanced Science and Technology Letters*, vol.31, pp.271-283, 2013.

[19] C. Hu, P. He and P. Liu, Public key encryption with multi-keyword search, *Network Computing and Information Security*, pp.568-576, 2012.

[20] J. Yu, P. Lu, Y. Zhu, G. Xue and M. Li, Toward secure multikeyword top-k retrieval over encrypted cloud data, *IEEE Trans. Dependable and Secure Computing*, vol.10, no.4, 2013.

[21] P. Kalidas and R. Chandrasekaran, Searchable encryption and fuzzy keyword search in cloud computing technology, *International Journal of Advanced Research in Computer Science and Software Engineering*, vol.3, no.7, 2013.