ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Top K Result Retrieval in Searching the File over the Encrypted Data in Cloud

C.Saranya[1], G.Radha[2], R.Subash[3]

M.E Scholar, Department of CSE, Ranganathan Engineering College, Coimbatore, India[1, 2].

Assistant Professor, Department of CSE, Ranganathan Engineering College, Coimbatore, India[3].

ABSTRACT: In cloud computing, data owners may share their outsourced data with a number of users, who might want to only retrieve the data files they are interested in. One of the most popular ways to do so is through keyword-based retrieval. We propose a new searchable encryption scheme, in which novel technologies in cryptography community, including ECC encryption and the vector space model. In the proposed scheme, the data owner encrypts the searchable index with kNN. When the cloud server receives a query consisting of multikeywords, it computes the scores from the encrypted index stored on cloud and then returns the encrypted scores of files to the data user. Next, the data user decrypts the scores and picks out the top-k highest- scoring files' identifers to request to the cloud server. The retrieval takes a two-round communication between the cloud server and the data user. The scheme, the privacy-preserving multi-keyword ranked search over encrypted data in cloud computing scheme, in which ranking is done at the user side while scoring calculation is done at the server side.Thorough analysis investigating privacy and efficiency guarantees ofproposed schemes is given. Experiments on the real-world data set further show proposed schemes indeed introduce lowoverhead on computation and communication.
.

KEYWORDS: Cloud computing, searchable encryption, privacy-preserving, keyword search, ranked search, Two-Round Searchable Encryption Scheme

I. INTRODUCTION

Cloud computing [1], a critical pattern for advanced data service, has became a necessaryfeasibility for data users to outsource data. Controversies on privacy, however, have beenincessantly presented as outsourcing of sensitive information including emails, health historyand personal photos is explosively expanding. Reports of data loss and privacy breaches incloud computing systems appear from time to time [2][3].The main threat on data privacy roots in the cloud itself [4]. When users outsource theirprivate data onto the cloud, the cloud service providers are able to control and monitor the dataand the communication between users and the cloud at will, lawfully or unlawfully,. Instancessuch as the secret NSA program, working with AT&T and Verizon, which recorded over 10million phone calls between American citizens, cause uncertainty among privacy advocates,and the greater powers it gives to telecommunication companies to monitor user activity [5].To ensure privacy, users usually encrypt the data before outsourcing it onto cloud, which bringsgreat challenges to effective data utilization. However, even if the encrypted data utilizationis possible, users still need to communicate with the cloud and allow the cloud operates on theencrypted data, which potentially causes leakage of sensitive information.Furthermore, in cloud computing, data owners may share their outsourced data with anumber of users, who might want to only retrieve the data files they are interested in. One ofthe most popular ways to do so is through keyword-based retrieval. Keyword-based retrieval isa typical data service and widely applied in plaintext scenarios, in which users retrieve relevantfiles in a file set based on keywords. However, it turns out to be a difficult task in ciphertextscenario due to limited operations on encrypted data. Besides, in order to improve feasibilityand save on the expense in the cloud paradigm, it is preferred to get the retrieval result withthe most relevant files that match users' interest instead of all the files, which indicates thatthe files should be ranked in the order of relevance by users' interest and only the files with thehighest relevances are sent back to users.A series of searchable symmetric encryption schemes have been proposed to enable search onciphertext. Traditional SSE schemes [6, 7] enable users to securely retrieve the ciphertext, butthese schemes support only boolean keyword search, i.e., whether a keyword exists in a file ornot, without considering the difference of relevance with the queried keyword of these files in theresult. To improve security without sacrificing efficiency, schemes presented in [8] showthat they

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

support top-k single keyword retrieval under various scenarios. Authors [9, 10]made attempts to solve the problem of top-k multi-keyword over encrypted cloud data. Theseschemes, however, suffer from two problems-boolean representations and how to strike a balancebetween security and efficiency. In the former, files are ranked only by the number of retrievedkeywords, which impairs search accuracy. In the latter, security is implicitly compromised totradeoff for efficiency, which is particularly undesirable in security-oriented applications.Preventing the cloud from involving in ranking and entrusting all the work to the user is anatural way to avoid information leakage. However, the limited computational power on theuser side and the high computational overhead precludes information security. The issue ofsecure multi-keyword top-k retrieval over encrypted cloud data thus is: how to make the clouddo more work during the process of retrieval without information leakage.In this paper, we introduce the concepts of similarity relevance and scheme robustness toformulate the privacy issue in searchable encryption schemes, and then solve the insecurityproblem by proposing a two-round searchable encryption (TRSE) scheme. Novel technologiesin the cryptography community and information retrieval community are employed, includinghomomorphic encryption and vector space model. In the proposed scheme, the majority ofcomputing work is done on the cloud while the user takes part in ranking, which guarantees topkmulti-keyword retrieval over encrypted cloud data with high security and practical efficiency.Our contributions can be summarized as follows:1) propose the concepts of similarity relevance and scheme robustness. We thus performthe first attempt to formulate the privacy issue in searchable encryption, and we show server sideranking based on order-preserving encryption (OPE) inevitably violates data privacy.2) propose a two-round searchable encryption (TRSE) scheme, which fulfills the securemulti-keyword top-k retrieval over encrypted cloud data. Specifically, for the first time weemploy relevance score to support multi-keyword top-k retrieval.3) Thorough analysis on security demonstrates the proposed scheme guarantees high dataprivacy. Furthermore, performance analysis and experimental results show that our scheme isefficient for practical utilization.The rest of this paper is organized as follows. We provide scenario and related backgroundin Section 2. In Section 3, we present the detailed description of the proposed searchableencryption scheme. In Section 4 we discuss proposed scheme and the security analysis and performance analysis are given in Section 5. Section 6 concludes this paper.

II. RELATED WORK

Ning Caoy et al. [11] has proposed method which allow users to securely search complete encrypted data through keywords, these method support only Boolean search, without capturing any relevant data. This approach suffers from two main drawbacks when directly applied in the context of Cloud Computing. First one, users, who do not necessarily have preknowledge of the encrypted cloud data, have to post process every got file in order to find ones most matching their interest;another drawback, invariably getting all files containing the queried keyword further incurs unnecessary network traffic, when retrieve more than one files.However, it only supports single keyword search. Where anyone with public key can write to the data stored on server but only authorized users with private key can search. Public key solutions are usually very computationally expensive however.Cong Wang et al [12] discuss the major disadvantage of above mentioned techniques gets the better of in ranked keyword search. This system enables data users to find the most related information rapidly, rather than burdensome sorting through every match in the content collection. Ranked search can also elegantly eliminate unnecessary network traffic by sending back only the most relevant data. For privacy protection, such ranking function, however, should not leak any keyword relevant information. Another One, to improve search result accuracy as well as enhance user searching experience, it is also essential for such ranking system to support multiple keywords search.Deepa P et al [13] has discussed this technique; conjunction of keywords is implemented for searching. The conjunctive keyword search mechanism will retrieve most efficient and relevance of data files. The conjunctive keyword search automatically creates ranked results so that the searching is efficient and flexible. This technique uses the wildcard based method and gram based method for constructing fuzzy keyword sets and symbol based trie- traverse scheme for generating a multi way tree to store the fuzzy keyword sets generated. This reduces the storage overhead. The Edit distance concept used for quantifies the keyword similarity. Kiruthigapriya Sengoden et al. [14], have proposed concept based searching techniques return a list of files that not only contain the exact search terms, but also search words are conceptually related to the topic, which provides a wider search scope capability. So the combination of both keyword searches along with concept search produce the relevant search result which greatly improve the efficiency of search. Jin Li et al[15] have proposed this method, It enhances system usability when searching input exactly matches. Keywords are measured using edit distance and fuzzy keyword sets are making. Straight forward and wild card based are the two approaches are dealt with edit distance .In straight forward approach

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

edit distance are calculated where all the forms of keywords are to be listed .Based on this indexing is built .Trapdoor are shared between user and the owner While retrieving file user computes the trapdoor based on the request, server matches with index table and return all potential identifiers. Reza Curtmola et al [16] presented a Searchable symmetric encryption (SSE) allows a party to outsource the storage of its data to another party (a server). SSE schemes enable users to securely retrieve the cipher text, but these method support only Boolean keyword search, i.e., whether a keyword subsists in a file or not, without regarding the difference of relevance with the queried keyword of these files in the result. To improve security without sacrificing efficiency, schemes presented in [17], [18] show that they support top-k single keyword retrieval under various scenarios in a secret manner, while maintaining the ability to selectively search complete it. So there is a need of new work to overcome these drawbacks.

III. PROPOSED METHODOLOGY

The proposed system is for searching the data from the encrypted data.The data gets encrypted by data owner with the keyword and stored in cloud.The user search for the data, the system will search for the results from the encrypted data.The relevance scoring and ranking methods are used for providing the accurate top k results. Data encryption protects data security to some extent,but at the cost of compromised efficiency. Searchable encryption scheme allows retrieval of encrypted data over cloud. In this project, we focus on addressing data privacy issues using Searchable encryption scheme. For the first time, we formulate the privacy issue from the aspect of similarity relevance and scheme robustness. To eliminate the leakage, we propose a two-round searchable encryption (TRSE) scheme that supports top-k multi keyword retrieval. In TRSE, we employ a vector space model and homomorphic encryption. The vector space model helps to provide sufficient search accuracy, and the homomorphic encryption enables users to involve in the ranking while the majority of computing work is done on the server side by operations only on ciphertext. As a result, information leakage can be eliminated and data security is ensured. The architecture diagram is given in Fig.1.

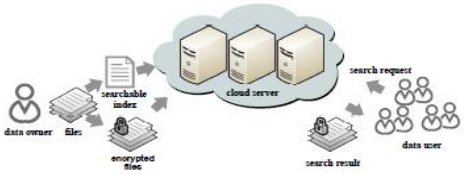

Fig.1. Architecture Diagram

In this work, a two-round searchable encryption (TRSE) scheme proposed that supports top-k multi-keyword retrieval. In TRSE, we employ a vector space model and homomorphic encryption. The vector space model helps to provide sufficient search accuracy, and the homomorphic encryption enables users to involve in the ranking while the majority of computing work is done on the server side by operations only on ciphertext. As a result, information leakage can be eliminated and data security is ensured. Thorough security and performance analysis show that the proposed scheme guarantees high security and practical efficiency. The proposed scheme is illustrated if Fig.2.

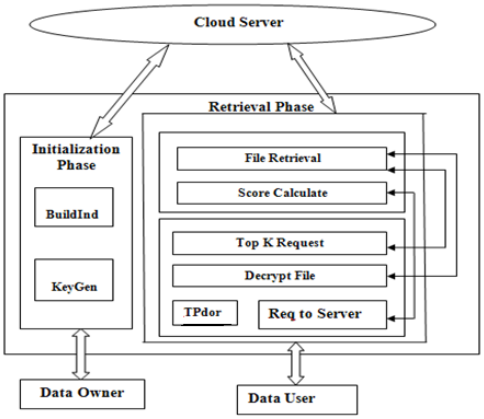

Fig.2.Proposed Scheme Architecture Diagram

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

1.1. Data owner

A cloud computing system hosting data service, as illustrated in Figure 1 in which three different entities are involved: Cloud server, Data owner and Data user. The cloud server hosts thirdparty data storage and retrieve services. Since data may contain sensitive information, the cloud servers cannot be fully entrusted in protecting data. For this reason, outsourced files must be encrypted. Any kind of information leakage that would affect data privacy is regarded as unacceptable.

1.2. Encryption

To alleviate the computational burden on user side, computing work should be at the server side, need an encryption scheme to guarantee the operability and security at the same time on server side. Homomorphic encryption allows specific types of computations to be carried out on the corresponding ciphertext. The result is the ciphertext of the result of the same operations performed on the plaintext. That is, homomorphic encryption allows computation of ciphertext without knowing anything about the plaintext to get the correct encrypted result.

1.3. Searchable indexing

The data owner has a collection of n files $C = \{f_1, f_2, \ldots, f_n\}$ to outsource onto the cloud server in encrypted form and expects the cloud server to provide keyword retrieval service to data owner himself or other authorized users. To achieve this, the data owner needs to build a searchable index I from a collection of l keywords $W = \{w_1, w_2, \ldots, w_l\}$ extracted out of C, and then outsources both the encrypted index I and encrypted files onto the cloud server. The authorized data user at first generates a query REQ . For privacy consideration, which keywords the data user has searched must be concealed. Thus, the data user encrypts the query and sends it to the cloud server that returns the relevant files to the data user. Afterward, the data user can decrypt and make use of the file In this scheme, the data owner encrypts the searchable index with homo-morphic encryption. When the cloud server receives a query consisting of multi-keywords, it computes the scores from the encrypted index stored on cloud and then returns the encrypted scores of files to the data user. Next, the data user decrypts the scores and picks out the top-k highest scoring files, identifiers to request to the cloud server. The retrieval takes a two-round communication between the cloud server and the data user, thus, name the scheme the TRSE scheme, in which ranking is done at the user side while scoring calculation is done at the server side.As shown in Algorithm 1.

Algorithm 1: TOPKSELECT (Source,k)
Input:
List source to be selected
Number k
Initialization:
Set topk←ϕ; topkid←ϕ;
Iteration:
For all item ∈ source do
INSERT (topk,(item,itemindex))
End ofr
For all tuple ∈ topk do
Topkid.append(tuple[1])
End for
Output: topkid

1.4. Multi-keyword Search

This module is used to help the user to get the accurate result based on the multiple keyword concepts. The users can enter the multiple words query, the server is going to split that query into a single word after search that word file in our database. Finally, display the matched word list from the database and the user gets the file from that list. The data user is authorized to process multi-keyword retrieval over the outsourced data. Thus the data user encrypts the query and sends it to the cloud server that returns the relevant files to the data user. Afterwards, the data user can decrypt and make use of the files.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

1.5. Relevance Scoring

Some of the multi-keyword SSE schemes support only Boolean queries, i.e., a file either matches or does not match a query. Considering the large number of data users and documents in the cloud, it is necessary to allow multi-keyword in the search query and return documents in the order of their relevancy with the queried keywords. Scoring is a natural way to weight the relevance. Based on the relevance score, files can then be ranked in either ascending or dissenting manner. Several models have been proposed to score and rank files in IR community. Among these schemes, adopt the most widely used one(tf-idf) weighting. The (tf-idf)weighting involves two attributes: Term frequency and inverse document frequency. Term frequency denotes the number of occurrences of term t in file f. Document frequency refers to the number of files that contains term t, and the inverse document frequency is defined as: $idf = log\left(\frac{N}{df}\right)$.Where N denotes the total number of files. By introducing the IDF factor, the weights of terms that occur very frequently in the collection are diminished and the weights of terms that occur rarely are increased.

1.6. Vector Space Model

While (tf-idf) depicts the weight of asingle keyword on a file, employ the vector space model to score a file on multi-keyword. The vector space model is an algebraic model for representing a file as a vector. Each dimension of the vector corresponds to a separate term, i.e., if a term occurs in the file, its value in the vector is nonzero, otherwise is zero. The vector space model supports multi-term and non-binary presentation. Moreover, it allows computing a continuous degree of similarity between queries and files, and then ranking files according to their relevance. It meets needs of top-k retrieval. A query is also represented as a vector ~ q, while each dimension of the vector is assigned with 0 or 1 according to whether this term is queried. Given the scores, files can be ranked in order and, therefore, the most relevant files can be found.As given in Algorithm 2.

Algorithm 2: INSERT(topk,(item, itemindex))
Input:
List topk to store the top-k scoring item
Tuple (item,itemindex)
Iteration:
If len(topk)<k then
Insert (item, itemindex) into topk in nondecreasing order of item
Else
For all element ∈ topk do
If item<element[0] then
Continue
Else
Discard topk[0], insert(item,itemindex) into topk in nondecreasing order of item
Endif
End for
endif

1.7. TRSE Design

Existing SSE schemes employ server-side ranking based on OPE to improve the efficiency of retrieval over encrypted cloud data. However, server-side ranking based on OPE violates the privacy of sensitive information, which is considered uncompromisable in the security oriented third party cloud computing scenario, i.e., security cannot be tradeoff for efficiency. To achieve data privacy, ranking has to be left to the user side. Traditional user-side schemes, however, load heavy computational burden and high communication overhead on the user side, due to the interaction between the server and the user including searchable index return and ranking score calculation. Thus, the user-side ranking schemes are challenged by practical use. A more serversiding scheme might be a better solution to privacy issues. We propose a new searchable encryption scheme, in which novel technologies in cryptography community and IR community are employed, including homoorphic encryption and the vector space model. In the proposed scheme,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

the data owner encrypts the searchable index with homomorphic encryption. When the cloud serverreceives a query consisting of multi keywords, it computes the scores from the encrypted index stored on cloud and then returns the encrypted scores of files to the data user. Next, the data user decrypts the scores and picks out the top-k highest scoring files' identifiers to request to the cloud server. The retrieval takes a two-round communication between the cloud server and the data user. We, thus, name the scheme the TRSE scheme, in which ranking is done at the user side while scoring calculation is done at the server side.

1.8. Framework of TRSE

The framework of TRSE includes four algorithms: Setup, IndexBuild, TrapdoorGen; ScoreCalculate, and Rank. Setup(λ):The data owner generates thesecret key and public keys for the homomorphic is encryption scheme. The security parameter λ taken as the input, the output is a secret key SK and a public key set PK .
IndexBuild (C,PK): The data owner builds the secure searchable index from the file collection C. Technologies from IR community like stemming are employed to build searchable index I from C, and then I is encrypted into I' with PK , output the secure searchable index I'.

TrapdoorGen (REQ, PK).The data user generates secure trapdoor from his request. Vector T' is built from user's multi-keyword request REQ and then encrypted into secure trapdoor T' with public key from PK, output the secure trapdoor T'. Score Calculate (T', I'). When receives secure trapdoor T', the cloud server computes the scores of each files in I' with T' and returns the encrypted result vector V back to the data user. Rank (V, SK,K) .The data user decrypts the vector V with secret key SK and then requests and gets the files with top-k scores. Note that Ỹ is only involved in the Setup algorithm, and the Setup algorithm needs to be processed only once by the data owner, ¥ thus, is a constant integer for one individual application instance. The whole framework can be divided into two phases: Initialization and Retrieval. The Initialization phase includes Setup and Index Build. The Setup stage involves the secure initialization, while the Index Build stage involves operations on plaintext. For security concerns, the vast majority of work should only be done by the data owner. Moreover, for convenience of retrieve, we modify the original vector space model by adding each vector V_i a head node idi at the first dimension of V_i to store the identifier of f_i. In this way, the correspondence between scores and files is established.

1.9. Log file generation

A log file will be generated at the server for each action done by any user (both owner and data user) for any file. This information can be used by the cloud admin to know about the issues happened while uploading, encrypting or downloading the files. This information can also be used by data owner to know the statistics about his files downloads.The Retrieval phase involves TrapdoorGen, Score Calculate, and Rank, in which the data user and the cloud server are involved. As a result of the limited computing power on the user side, the computing work should be left to server side as much as possible. Meanwhile, the confidentiality privacy of sensitive information cannot be violated.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

In this section, a thorough experimentalevaluation of the proposed technique demonstratedon a real-world dataset: the Enron Email Data Set [35]. We randomly selectdifferent number of e-mails to build data set. The wholeexperiment system is implemented by C language on aLinux Server with Intel Xeon Processor 2.93 GHz. Thepublic utility routines by Numerical Recipes are employedto compute the inverse of matrix. The performance of ourtechnique is evaluated regarding the efficiency of existingMRSE schemes, as well as the tradeoff betweensearch precision, privacy and computation time cost for k-word retrieval.

1.10. Precision Result Comparison

Fig. 3 shows that the precision comparison results between proposed TRSE, MRSE and SSE. From the results, it is well know thatproposed schemeobtain high precision indicating the good purity ofretrieved documents.However, user's rank privacy may have been partiallyleaked to the cloud server in MRSE and SSE methods

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

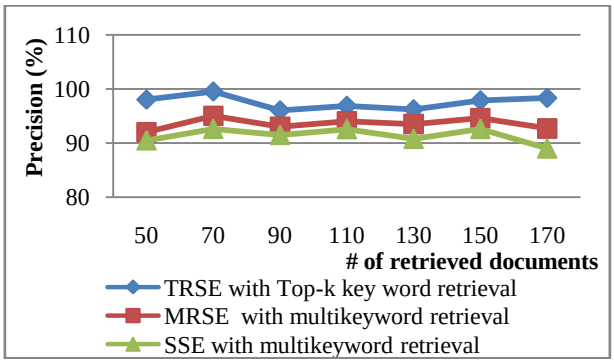

Fig.3. Precision Comparison

. The access pattern is defined as thesequence of ranked search results. Here, the search resultshighly protected, and thus rank order of retrieved documents effectively retrieved in proposed method.

1.11. Privacy Guarantee Comparison

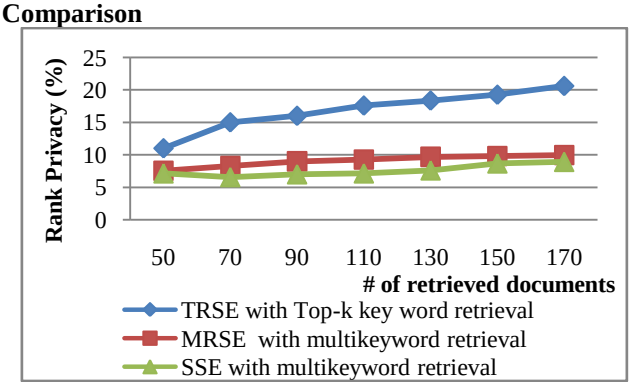

Fig.4. Precision Comparison

Fig. 4 shows the rank privacy between proposed TRSE, MRSE and SSE.From the figure, it is well known that the proposed method leads tohigher precision of search result but lower rank privacyguarantee. This schemeprovides a balance parameter for data users to satisfy theirdifferent requirements on precision and rank privacy.

Computation Time Comparison

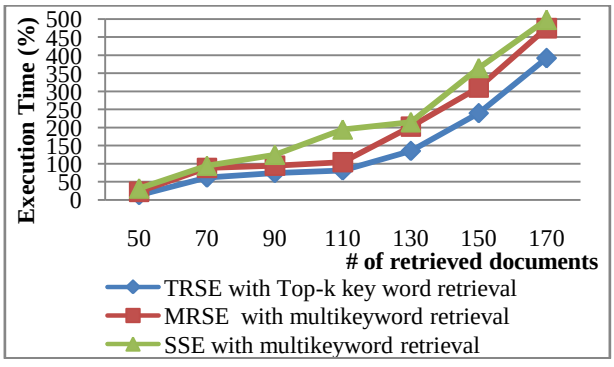

Fig.5. Computation time cost for k-word retrieval

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

V. CONCLUSION AND FUTURE WORK

In this paper, we motivate and solve the problem of secure multi-keyword top-k retrieval over encrypted cloud data. We define similarity relevance and scheme robustness .Based on OPE invisibly leaking sensitive information, we devise aserver-side ranking SSE scheme. We then propose a TRSE scheme employing the fully homomorphic encryption, which fulfills the security requirements of multi-keyword top-k retrieval over the encrypted cloud data. By security analysis, we show that the proposed scheme guarantees data privacy. According to the efficiency evaluation of the proposed scheme over a real data set, extensive experimental results demonstrate that our scheme ensures practical efficiency. The system is designed to solve the problem of supporting efficient ranked keyword search for achieving effective utilization of remotely stored encrypted data in Cloud Computing.

REFERENCES

1. M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and M. Zaharia. "A view of cloud computing," Communication of the ACM 53 (4): 50 58, 2010.
2. M. Arrington, "Gmail disaster: Reports of mass email deletions," http://www.techcrunch.com/2006/12/28/gmail-disasterreports-of-mass-email-deletions/, December 2006.
3. Amazon.com, "Amazon s3 availability event: July 20, 2008," http://status.aws.amazon.com/s3-20080720.html, 2008.
4. Cloud Security Alliance, "Top threats to cloud computing," http://www.cloudsecurity alliance.org, 2010.
5. C. Leslie, "NSA has massive database of Americans' phone calls," http://usatoday30.usatoday.com/news/washington/2006-05-10/.
6. D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. of IEEE Symposium on Security and Privacy, 2000.
7. D. Boneh, G. Crescenzo, R. Ostrovsky and G. Persiano, "Public-key encryption with keyword Search," in Proc. of Eurocrypt, 2004
8. A. Swaminathan, Y. Mao, G.-M. Su, H. Gou, A. L. Varna, S. He, M. Wu, and D. W. Oard, "Confidentiality-preserving rank-ordered search," in Proc. of the Workshop on Storage Security and Survivability, 2007.
9. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multikeyword ranked search over encrypted cloud data," in Proc. of IEEE INFOCOM, 2011.
10. H. Hu, J. Xu, C. Ren and B. Choi, "Processing private queries over untrusted data cloud through privacy homomorphism," in Proc. of ICDE, 2011.
11. Ning Caoy, Cong Wangz, Ming Liy, Kui Renz, and Wenjing Louy" Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data" INFOCOM, 2011 Proceedings IEEE.
12. Cong Wang†, Ning Cao‡, Jin Li†, Kui Ren†, and Wenjing Lou"Secure Ranked Keyword Search over Encrypted Cloud Data" Distribute d Computing System, 2010 IEE 30th international conference.
13. Deepa P L, S Vinoth Kumar, Dr S Karthik" searching techniques in encrypted Cloud data" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 8, October 2012
14. Kiruthigapriya Sengoden, Swaraj Paul "Improving the Efficiency of Ranked keyword Search over Cloud Data" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 3, March 2013
15. Jin Li†, Qian Wang† , Cong Wang†, Ning Cao‡ , Kui Ren† , and Wenjing Lou‡ "Fuzzy Keyword Search over En crypted Data in Cloud Computing" INFOCOM,2010 Proceedings IEEE.
16. Reza Curtmola† Juan Garay‡ Seny Kamara§ Rafail Ostrovsky" Searchable Symmetric Encryption:Improved Definitions and Efficient Constructions" CCS '06 Proceedings of the 13th ACM conference on Computer and communications security.
17. P. Naresh K. Pavan kumar D. K. Shareef "Implementation Of Secure Ranked Keyword Search By Using RSSE" International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 2 Issue 3, March – 2013.
18. Alexandra Boldyreva, Nathan Chenette_ Adam O'Neilly" Order-Preserving Encryption Revisited: Improved Security Analysis and Alternative Solutions"CRYPTO'11 Proceedings of the 31st annual onference on Advances in cryptology.

BIOGRAPHY

C.Saranya received Bachelor of Technology degree in Information Technology from the Anna University Chennai in 2010.Where she is Currently pursuing Master of Engineering degree in Computer Science and Engineering in Anna University Chennai.

G.Radha received Bachelor of Engineering degree in Computer Science and Engineering from the Anna University Chennai in 2013.Where she is Currently Pursuing Master of Engineering Degree in Computer Science and Engineeringin Anna University Chennai.

Mr.R.Subash received Bachelor of Technology degree in Information Technology from the Anna University Chennai in 2009.Where he also received Master of Engineering degree in Computer Science and Engineering in Anna University Chennai in 2012.He is currently working as a Assistant Professor in Ranganathan Engineering College,Coimbatore.