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.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

An Efficient Retrieval of Encrypted Data In Cloud Computing

N.Nandhini[1] and P.G Kathiravan[2]

II Year M.Tech. IT Student, V.S.B Engineering College, Karur, Tamil Nadu, India[1]

Assistant Professor/IT, V.S.B Engineering College, Karur, Tamil Nadu, India[2]

ABSTRACT— The arrival of cloud computing the new pattern for data outsourcing and high quality data service is great flexibility and economic saving. However fear about the sensitive information on cloud to be protecting the data privacy problems sensitive information has to be encrypted before outsourcing, which creates the effective data utilization services a very big challenging task. Symmetric Searchable Encryption (SSE) technique allows to retrieval of encrypted data on cloud, but it leaks the data privacy. Secure server –side ranking based on the order-preserving Encryption (OPE) it include the similarity relevance and robustness. But OPE also unavoidable of data privacy. To eliminate server side ranking introduce the Two-Round Searchable Encryption (TRSE) it include the vector space model and homomorphic encryption. Vector space model used for user retrieve file accurately and homomorphic encryption used for ranking involve in the user side it done by server side operation on cipher text. The TRSE also leakage the privacy and it generated the small number of keys so unauthorized user easily hack the sensitive information so to avoid this problem propose the blowfish algorithm it generate the large number keys. We propose scheme is high security guarantee and more efficiently retrieve the over encrypted data.

KEYWORDS— Cloud computing, Data privacy, Relevance scoring, Homomorphic encryption, Vector space model, Blow fish algorithm.

I. INTRODUCTION

Cloud computing is an large-scale distributed computing paradigm driven by reconfigurable computing resources can be rapidly provisioned and released with minimal management effort in the data centers[1].Increasing the outsourcing data user continuously presented sensitive information like government records, personal health records and photos etc., So data privacy[6] and data loss will be increase. When users outsource their private onto cloud, the cloud service provider able to monitor the communication between the users and cloud at will trust or untrusted. The cloud server leaks the data information to unauthorized users or even be hacked. To assure the secrecy, users usually encrypting the data before Outsourcing it onto cloud; it brings the adult challenges to effective data utilization. Data owners also share their data to outsource cloud with a number of users, who might want to retrieve the files in a given during session. Keyword based retrieval is an most popular method for searching the plaintext scenario, which users to retrieve relevant files based on keywords, but it is very difficult to retrieve the files in cipher text. Improve the efficiency and feasibility of cloud paradigm introduces the relevant result files, which indicates the files should be ranked in order to relevance by users' interest and highest relevance send to the users.

Searchable Symmetric Encryption (SSE)[22],[23] method is used for retrieve the file in encrypted data to enable search on cipher text. It support only Boolean-keyword search, it performing the AND,OR and NOT operations. In this search

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.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

method retrieve only limited number of files and also it leaks the privacy of keywords. To improve the search efficiency[9],[10],[24] introducing the server-side ranking based on the Order Preserving Encryption (OPE) to develop a one-to-many order mapping technique to protect that sensitive weight information, while providing the efficient ranked search functionalities. Order preserving encryption is that fixing the range size requires pre-knowledge on the duplicates among all the plaintexts. However, such extra sensitive information to be leakage. To improve security without sacrificing efficiency, that support top-k single keyword retrieval. To find the optimal and relevant set of k documents from a collection of documents based on the user's query. Single keyword top-k in this method retrieve only limited number of documents based on user query. So this is not suitable for pay-as-pay cloud environment.[25],[26]

Introduce the multi keyword top-k retrieval method over encrypted cloud data, thus how to make the cloud do most work during the procedure of retrieval without leakage of information. The concepts of resemblance relevance and scheme robustness to formulate the privacy issues in searchable encryption and avoid the security problem. The Two round searchable encryption (TRSE), which fulfills the secure multi keyword top-k retrieval over encrypted data.

II. DESIGN GOALS

2.1 Scenario

Cloud computing system hosting data service, Fig.2.1 which three different entities involved Cloud server, Data users and Data owner. Cloud server legion third party data storage and retrieve services. The data may be containing sensitive information; the cloud server cannot fully trustworthy for protecting the data. So all the outsource files must be encrypted.

Data owner has a collection of files C= { $f_1,f_2,f_3..f_n$} before outsource onto the cloud server all files to be encrypted format and anticipate the cloud server to provide the keywords both data users and data owner. The data owner make a searchable index I from collective keywords W={$w_1,w_2,w_3..w_n$} and also both encrypted searchable index I' and encrypted files onto cloud server.

A data user is an authorized user to retrieve the using multi keyword. Data user generating the query REQ={$(w'_1,w'_2,..w'_s)|w'_i \in W, 1 \leq i \leq s \leq l$}.For privacy concern data user concealed into query. Data user encrypt the query send it to the cloud server .The cloud server return to the relevant files afterwards the data user decrypts the files.

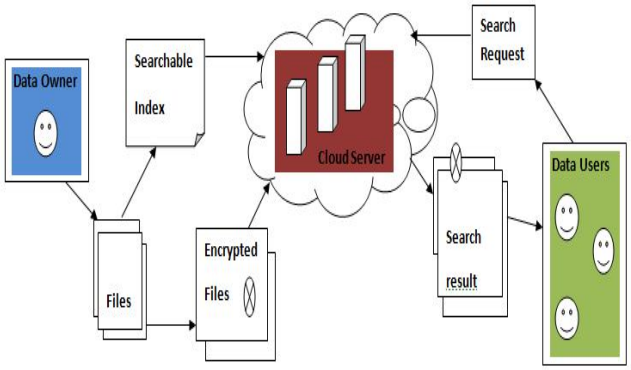

Fig 2.1: Scenario retrieval of encrypted cloud data.

2.2 Relevance Scoring

Scoring is a natural way to weighting the relevance, it is used for the multi keyword in the search query and returns documents in the order of their relevancy with queried keywords. Based on the relevance score files can be stored in either ascending or descending order.

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.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Many models to be developed to score and rank files in IR Community. Relevance score using one of the most term is tf-idf , it involves the two entities like term frequency and inverse document frequency. Term frequency ($tf_{t,f}$) is counts the number of times each term occurs in each document i.e., term t in file f. Document frequency(df_t) refers the number of files that contain term t. Inverse document frequency(idf_t) refers to the eliminate the term which is frequently in the document set idf_t=log N/df_t where N denotes the total number of files and df_t document frequency assign the term t. The Inverse Document Frequency (IDF) factor, the weights of terms that occur very oftentimes in the collection of files and weights of term is increased.

2.3 Vector space model

The tf-idf is used for top-k single keyword retrieval method, but vector space model is used for to retrieve the multi keyword. Vector space model[19] or term model is an algebraic model for representing text documents as vectors of identifiers such as e.g index terms. In this vector space model each dimensions to a separate term. i.e. Term occurs in file means vector value is zero, otherwise non zero. It allows the similarity between the files and quires and it ranking files according to similarity relevance. Score file f on query is inner product of two vectors $score_{f,q} = \vec{v}_f \cdot \vec{q}$. given score files are ranked in order most relevant files to be found.

III. PROBLEM STATEMENT

Cloud server work may be considered as an "honest-but-curious" model i.e server learns the additional information about the data.

3.1 Statistic Leakage

All data files, indexes are in encrypted form before outsourcing onto cloud computing, but cloud server may learn the additional sensitive information through the statistical analysis. This is refers to the statistical leakage. This leakage occurs two possible ways: term distribution and inter distribution. Term distribution refers to the term t is t's score of each file i(i€c). Inter distribution is a file f is file f's frequency distribution of each term j(j€f).The statistical leakage over an access pattern and search pattern.

Distribution of information occur the similarity between the files or terms. For example user request a query "United" means the cloud server learn the co-occur of similar word is "States". This ways cloud server possible to learn the sensitive information.

3.2 K-similarity relevance

In order preserving encryption technique[9],[10] to maintain the server side ranking to use for retrieve the relevant files based on query. In that server side ranking method leaks the information. To avoid the leakage problem propose the k-similarity relevance.

k-similarity relevance the capacity of a search engine or function to retrieval the being similar to a appropriate to a user's needs. In these method based on the two terms: file sequence (FS) and term sequence (TS).

Definition 3.2.1:- File sequence(FS) is refers to the finite collection of files, usually related to each other. We denote the term vector tv_i =$\{d_1 d_2..d_n\}$ with score in non-decreasing order.

Definition 3.2.2:- Term sequence (TS) is a sequence of terms induced by sorting the file vector fv_i = $\{t_1 t_2 ..t_n\}$ with score in non-decreasing order.

For example file set 48,800files from the National science foundation (NSF) according to the statistic data in which term in non-decreasing order i.e. 160th term is "resource" FS length is 8703 the resource contain the 8703 files. The similarity relevance may be does not hidden the which term is most relevant to other term. Order-preserving similarity one-to-many mapping is still exposed. For this reason ranking can be entirely left to be cloud server. The term "resource" is the most relevant term with "resources" in the term by k=0.885 before one-to-many OPM, as shown Table.1

Term	Len	K	Len'	K'

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.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Directorate	264	0.023	264	0.283
Education	4826	0.544	3573	0.403
Human	7648	0.885	7647	0.885
Provide	1014	0.098	1014	0.098
Sciences	2480	0.226	2480	0.226

TABLE 1 Similarity relevance with" resources" before and after OPM.

3.3 Disadvantage of Existing System

1. Searchable Symmetric Encryption (SSE) to support only Boolean keyword search to retrieve the data does not satisfy the user and also leaks the privacy.

2. Order preserving Encryption (OPE) is based on the server-side ranking it violates the privacy, leaks the sensitive information i.e security cannot tradeoff efficiency.

3. OPE ranked search is a maximum communication and increase the computation overhead in server side.

IV. TWO ROUND SEARCHABLE ENCRYPTION WITH BLOWFISH ALGORITHM (TRSE)

We propose a new technique for searchable encryption scheme, IR community including the homomorphic encryption and vector space model. Data owner encrypt the searchable index using the homomorphic encryption. When data user giving request to the cloud server, it calculates scoring relevance files based on the user query. Cloud server returns to encrypted scoring files to the user. Data user securely decrypts the scoring files and takes most top-k identifiers. TRSE takes the two-round communication between data user side and cloud server.

4.1 Homomorphic encryption scheme

Homomorphic encryption [19] allows some specific types of operation carried out by cipher text. In this Homomorphic encryption to be computation on cipher text without anything knowing about the plain text. These encryptions apply the vector space model to retrieval top-k only operation done on addition and to compute from relevance score from encrypted searchable index.

A cryptosystem which supports the both addition and multiplication is refers to the fully homomorphic encryption. The being of an effective and fully homomorphic cryptosystem would have great practical significance in the outsourcing of private computations, in the circumstance of cloud computing. In this fully homomorphic encryption is used to calculate the over integers like Greatest Common Divisor (GCD) [11],[14] is providing the high security that is the list of integers l={ $I_1,I_2 \ldots I_n$} is used for multiplex the hidden integers j to find the hidden integers j. The encryption scheme can be denoting as: C=pq+2r+m, where p is an private key, q denotes the multiple parameters and r denotes the against brute force attack. pq+r is an public key.

The fully homomorphic encryptions have the following properties:

1 .keyGen(λ)

2. Encrypt (PK,m)

3. Evaluate ($C_1,C_2,..C_n$)

4. Decrypt(p,x)

KeyGen (λ): The private (secret) key SK is an odd n-bit number selected from the randomly in the interval of [2^{n-1}, 2^n].The public key PK is used for encryption the selected in the interval of {$K_0,K_1,\ldots K_T$}.

Encrypt (PK,m): Randomly choose a number R€ {1,2…T} and return the cipher text c=m+xr'+$\sum_{i€R}{}^{k}{}_{i.}$

Evaluate ($C_1,C_2,..C_n$): Perform the binary addition and multiplication to get the t cipher text C_i and done all operations return the result of integer X.

Decrypt (p,X) : The output of the m'=(x mod p) mod x.

4.2 Design of TRSE

The TRSE is a two phases: Initialization and Retrieval phase.

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.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

4.2.1 Initialization phase:

It includes two stages like setup and buildIndex. Setup stage is used for secure and authenticated data user to enter the cloud server. BuildIndex is used for to compute the operation involve in the plain text to calculate the score relevance.

Setup (λ): In this phase data owner generate the private or secret for using KeyGen(λ). In this stage easily identify the data user authorized or not.

BuildIndex (C,PK): In this Phase to build the searchable index I from collection of files C. Data owner to concern the security to encrypt the Searchable Index using the public Key(PK) to buildIndex like I'

1.Data owner generate the SK or PK is used for the access the authorized data user. Data owner matching the their Sk and data user Sk.

2. Data owner select the keywords $W=\{w_1,w_2,\ldots wn\}$ from collection of files like $C=\{f_1,f_2,\ldots f_n\}$ using the Term frequency and Inverse document frequency. Using Vector space model to calculate the score relevance of each file based on the data user query. Searchable index like $I=\{v_i|1< I <n \}$

3. Data owner encrypts the searchable index using the Pk to build the secure searchable index like $I'=\{v_i'| 1< I < N\}$.

4 .Next step to outsourced the both encrypted files and encrypted searchable index I' to the cloud server.

4.2.2 Retrieval phase

In this retrieval phase is used for data user to retrieval the documents based on the user query from cloud server. It includes the three stages like TrapdoorGen, ScoreCalculate and Rank, in this stage involve only data user and cloud server.

TrapdoorGen (REQ, PK): Data user to build the secure trapdoor from his request REQ. The vector T_w is extract from multikeyword the user request REQ. Data user encrypts the trapdoor using the public key(PK) to build the secure trapdoor like T_w'.

ScoreCalculate (T_w ',I'): When cloud server receives user query , calculate the relevance score based on the T_w' from the searchable index I' and cloud server returns the encrypted relevance files based on the REQ returns to the user.

Rank (SK,K) : Data user decrypts the top –k vector files using their secret key (SK).

The retrieval phase following steps:

1.Data user generates the collection of keywords REQ={W_1',W_2',…W_n'} and the query vector $T_w=\{m_1,m_2\ldots m_n\}$ is $m_{i=}1(1< I < l)$ if t_i € REQ or m_i =0.After encrypts the trapdoor using the public key T_w' to the cloud server.

2. For each request the cloud server to calculate the file vector the inner product p_j ' = v'$_j$[1: l] and cloud server returns the data user.

3. Data user decrypts the score files using the SK.Then TOPKSELECT algorithm is involved the top-k highest scoring files identifiers.

4. The cloud server returns the encrypted files to the data user.

The TOPKSELECT algorithm 1 to be reduced the O (n log k). The INSERT algorithm 2 used to the inserting the keywords to the index.

ALGORITHM 1 TOPKSELECT (source,k)

INPUT:

List source to be selected

Number k

INITIALIZATION:

Set topk← Φ; topkid← Φ;

ITERATION:

1. for all item € source do

2. INSERT(topk,(item, itemindex))

3.end for

4. for all tuple € topk do

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.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

5. topkid.append(tuple[1])
6. end for

OUTPUT:

Topkid

ALGORITHM 2 INSERT(topk,(item,itemidex))

INPUT:

List topk to store the top-k scoring item
Tuple (item,itemindex)

ITERATION:

1. If len (top-k) < k then
2. insert (item, itemindex) into topk in nondecreasing order of item
3. else
4. for all element € topk do
5. if item < element [0] then
6. continue
7. else
8. discard topk[0], insert (item,itemindex) into topk in nondecreasing order of item
9. end if
10. end for
11. end if

4.3 Blow fish Algorithm

Blowfish is a variable –length key 64-bit block cipher. This algorithm consists of two parts: a key expansion and a data encryption part. Key expansion converts a variable length key of at most 56 bytes into several sub keys totally 4168 keys. Data encryption occurs via 16-round, each round considers the key dependent permutation and key-dependent of substitution and four index data lookups per round.

THE SUB KEYS ARE CALCULATED USING THE BLOWFISH ALGORITHM:-

1. To set the P-array and then four S-boxes, in order, with a fixed string. This string comprise of the hexadecimal digits of pi .
2. Again cycle through the key bits upto the whole P-array has been XOR with key bits.
3. encrypted the all-zero string combining of Blowfish algorithm, using the sub keys followed by steps (1) and (2).
4. Replace P1 and P2 value with the output of step (3).
5. Encrypt the output of step (3) using the Blowfish algorithm with change the sub keys.
6. Replace P3 and P4 with the output of step (5).
7. Repeating the process, replacing all values of the P- array, and then all four S-boxes, with the output of the continuously-changing Blowfish algorithm.

V. SECURITY AND PERFORMANCE ANALYSIS OF TRSE WITH BLOWFISH ALGORITHM

5.1 security analysis of TRSE with blow fish algorithm:-

Our proposed scheme is high security it satisfy the all requirements. In this TRSE scheme do not leakage the information. The cloud server does not learn anything about the user query. Similarly cloud servers do not learn anything about the access pattern, search pattern, similarity relevance.

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.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

The first three steps do not leakage any information. The first is considered the search pattern and access pattern. For example two queries access the same query REQ1 and REQ2 $n1_i$=$n2_i$=1 in the vector trapdoor T_{w1}=T_{w2}. After that the two different query encrypted two different format using the SK. like Encrypt ($n1_i$,$R1_i$) and Encrypt($n2_i$, $R2_i$). The cloud server do not leaning the keywords of the two queries. In this scheme hidden the access pattern and search pattern.

The second step is using the homomorphic encryption scheme encrypt the searchable index to randomly selected PK.. The cloud servers do not the TF and IDF. So interterm distribution and inter distribution is secure.

The third step is random mapping order of the related terms like the Frequency Sequence (FS) like the two words randomly distributed. For example "resources" term the co-ordinate with many terms like "data", "directorate" after FHEI. The existing system "resource" term only related with "human" so easily cloud server learn the term. But TRSE many word related to the term so cloud server does not learn the user keyword easily Table 2. Shows the term "resources" related with many other terms after FHEI.

Term	Len	K	Len'	K'
Directorate	264	0.0223	3248	0.283
Education	4826	0.544	6273	0.707
Human	7648	0.885	711	0.082
Provide	1014	0.098	1132	0.109
Sciences	2480	0.226	45	0.004

TABLE 2 Similarity relevance with "resource" before and after FHEI

Consist of a variable number of iterations. For action of a small key size, it is possible to decrease the number of steps with no loss of security. Use sub keys that are pre computation and one-way hash of the key. This allows the use of extended phrases for the key without sacrificing security. Blowfish, it is a variable-length key block cipher. It is only suited for applications where the key does not change repeat, like a communicating link or an self-regulating files to be encrypted.

5.2 Performance analysis of TRSE with blowfish Algorithm

The performance analysis of TRSE is very efficient to the retrieve the data .The initialization phase Setup Stage and BuildIndex stage is very efficient. The set up stage complexity is $O(\lambda^{10})$. The BuildIndex phase to be encrypted the searchable index I'. In this encrypted index I' is increasing the search efficiency.

The retrieval phase of efficiency also increasing in the stage of TrapdoorGen, ScoreCalculate, Rank. The TrapdoorGen stage subdivided into two like ResultDecrypt and Topk. The TrapdoorGen to reduce the burden of the user side. To build the complexity of the TrapdoorGen of O(l) for multi keyword retrieval. For example, it costs 88 ms to generate a trapdoor over a file set containing 4,000 different keywords with TRSE, while the SSE scheme needs 223 ms to do the same work. The Score Calculate Stage also the cloud server calculates the inner product of the keyword for each row. The complexity of the this O(nl).The Rank stage is also performance is good compare to the previous SSE technique.

Blowfish algorithm is an 16 block encryption algorithm that not ever has been broken. The most effective way to break Blowfish is through complete search of the key space. It has been persistence tested and found to be very secure. It is highly fast due to its fetching advantage of built-in instructions on the current microprocessors for basic bit shambling operations.

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.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

VI. RELATED WORK

The searchable encryption scheme [8],[22],[23] focusing on security definitions and encryption , these support the Boolean keyword search retrieval without ranking. The create privacy-preserving top-k retrieval, including the secure index and with ranking on the OPE [10]. The proposed scheme top-k retrieval satisfies the security and efficiency.

Considering the more number of data users and documents in the cloud, it allows the multi keywords to retrieval the data. It supports the homomorphic encryption [26] technique to check the user query. Thus the SSE and OPE encryption technique to be fail retrieve the documents over encrypted cloud data.

VII. CONCLUSION

In this paper to solve the problem of security in the top-k multi keyword retrieval over encrypted cloud data. In that the existing system of SSE and OPE leaks the sensitive information of data. The TRSE scheme support the server side searchable index and support the homomorphic encryption scheme. It satisfies the security and efficiency of the encrypted cloud data. Our future is increasing the security of the server side to introduce the JAR techniques and reduced encrypted data storage on cloud computing. According to the efficiency evaluation of the proposed scheme over a real data set, extensive experimental results demonstrate that our scheme ensures practical efficiency.

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," Comm. ACM, vol. 53, no. 4, pp. 50-58,2010.
[2] M. Arrington, "Gmail Disaster: Reports of Mass Email Deletions," http://www.techcrunch.com/2006/12/28/gmail-disasterreportsof- mass-email-deletions/, Dec. 2006.
[3] Amazon.com, "Amazon s3 Availability Event: July 20, 2008," http://status.aws.amazon.com/s3-20080720.html, 2008.
[4] RAWA News, "Massive Information Leak Shakes Washington over Afghan War,"http://www.rawa.org/temp/runews/2010/08/20/massive-information-leak-shakes-washington-verafghan-war.html, 2010.
[5] AHN, "Romney Hits Obama for Security Information Leakage," http://gantdaily.com/2012/07/25/romney-hits-obama-forsecurity- information-leakage/, 2012.
[6] Cloud Security Alliance, "Top Threats to Cloud Computing," http://www.cloudsecurity alliance.org, 2010.
[7] C. Leslie, "NSA Has Massive Database of Americans' Phone Calls," http://usatoday30.usatoday.com/news/washington/ 2006-05-10/, 2013.
[8] R. Curtmola, J.A. Garay, S. Kamara, and R. Ostrovsky, "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions," Proc. ACM 13th Conf. Computer and Comm. Security(CCS), 2006.
[9] C. Wang, N. Cao, J. Li, K. Ren, and W. W. Lou, "Secure Ranked Keyword Search over Encrypted Cloud Data," Proc. IEEE 30th Int'l Conf. Distributed Computing Systems (ICDCS), 2010.
[10] S. Zerr, D. Olmedilla, W. Nejdl, and W. Siberski, "Zerber+r: Top-k Retrieval from a Confidential Index," Proc. 12th Int'l Conf. Extending Database Technology: Advances in Database Technology (EDBT), 2009.
[11] M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, "Fully Homomorphic Encryption over the Integers," Proc. 29th Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques, H. Gilbert, pp. 24-43, 2010.
[12] M. Perc, "Evolution of the Most Common English Words and Phrases over the Centuries," J. Royal Soc. Interface, 2012.
[13] O. Regev, "New Lattice-Based Cryptographic Constructions," J. ACM, vol. 51, no. 6, pp. 899-942, 2004.
[14] N. Howgrave-Graham, "Approximate Integer Common Divisors," Proc. Revised Papers from Int'l Conf. Cryptography and Lattices (CaLC' 01), pp. 51-66, 2001.
[15] "NSF Research Awards Abstracts 1990-2003," http://kdd.ics.uci. edu/databases/nsfabs/nsfawards.html, 2013.
[16] "20 Newsgroups," http://kdd.ics.uci.edu/databases/20newsgroups/20newsgroups.html, 2013.
[17] S. Gries, "Useful Statistics for Corpus Linguistics," A Mosaic of Corpus Linguistics: Selected Approaches, Aquilino Sanchez Moises Almela, eds., pp. 269-291, Peter Lang, 2010.
[18] C. Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," Proc. 41st Ann. ACM Symp. Theory of computing (STOC), pp. 169- 178, 2009.

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.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

[19] D. Dubin, "The Most Influential Paper Gerard Salton Never Wrote," Library Trends, vol. 52, no. 4, pp. 748-764, 2004.
[20] A. Cuyt, V. Brevik Petersen, B. Verdonk, H. Waadeland, and W.B. Jones, Handbook of Continued Fractions for Special Functions. Springer Verlag, 2008.
[21] T.H. Cormen, C.E. Leiserson, R.L. Rivest, and C. Stein, Introduction to Algorithms, pp. 856-887. MIT Press and McGraw-Hill, 2001.
[22] D. Song, D. Wagner, and A. Perrig, "Practical Techniques for Searches on Encrypted Data," Proc. IEEE Symp. Security and Privacy, 2000.
[23] D. Boneh, G. Crescenzo, R. Ostrovsky, and G. Persiano, "Public-Key Encryption with Keyword Search," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (Eurocrypt), 2004.
[24] 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," Proc. Workshop Storage Security and Survivability, 2007.
[25] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-Preserving Multikeyword Ranked Search over Encrypted Cloud Data," Proc.IEEE INFOCOM, 2011.
[26] H. Hu, J. Xu, C. Ren, and B. Choi, "Processing Private Queries over Untrusted Data Cloud through Privacy Homomorphism," Proc. IEEE 27th Int'l Conf. Data Eng. (ICDE), 2011.
[27] P. Golle, J. Staddon, and B. Waters, "Secure Conjunctive Keyword Search over Encrypted Data," Proc. Second Int'l Conf. Applied Cryptography and Network Security (ACNS), pp. 31-45, 2004.
[28] L. Ballard, S. Kamara, and F. Monrose, "Achieving Efficient Conjunctive Keyword Searches over Encrypted Data," Proc.Seventh Int'l Conf. Information and Communications Security (ICICS), 2005.
[29] J.-S. Coron, A. Mandal, D. Naccache, and M. Tibouchi, "Fully Homomorphic Encryption over the Integers with Shorter Public Keys," CRYPTO '11: Proc. 31st Ann. Conf. Advances in Cryptology, 2011.
[30] N. Smart and F. Vercauteren, "Fully Homomorphic Encryption with Relatively Small Key and Cipher text Sizes," Proc. 13th Int'l Conf. Practice and Theory in Public Key Cryptography (PKC), 2010.

ABOUT THE AUTHORS

Ms.N.Nandhini received B.Tech (Information Technology) from Kalaignar Karunanidhi of Technology in 2012. Now pursuing M.Tech (Information Technology) in V.S.B Engineering College Anna University, Chennai. Area of interest includes OOPS and cloud computing.

Mr.P.G.Kathiravan received M.Tech (Information Technology) from K.S.Rangasamy College of Technology (Autonomous) in 2012 Anna University, Chennai and B.Tech (Information Technology) from The Kavery Engineering College in 2010, Anna University, Chennai. He worked as Lecturer in the Department of Computer Science and Engineering & Information Technology, Government College of Technology, Coimbatore in the year (2012-13).He currently working as Assistant Professor in the Department of Information Technology in V.S.B Engineering College, Karur. He published and presented various International & National papers and attended various International & National Workshops. His area of interest includes Computer Networks, Cloud Computing, and Grid Computing.