ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Respecting Independent Query Services and Specified Systematic In Clouds Computing

T.Swathi
M.Tech Student
Sri Vatsavai Krishnam Raju College of Engineering and Technology,
Bhimavaram, AP.

Dr.Penmetsa Vamsi Krishna Raja, M.Tech
Principal
Sri Vatsavai Krishnam Raju College of Engineering and Technology,
Bhimavaram, AP.

Abstract:
The needs of Cloud computing is increasing due to massive increase of user access to the cloud databases. The more number of users are trying to access the cloud databases to fulfill their storage requirements In the existing work the EIRQ scheme is proposed to provide a differential query services with the user privacy It works based on the ranking of users query. In this method the communication cost is also reduced by retrieving only the required contents to the users based on users ranking Based on this ranking Private keyword based file retrieval scheme was anticipated it is necessary to protect the user privacy while querying the data in the cloud environment, different techniques are developed by researchers to provide privacy, but the computational and bandwidth costs increased which are unacceptable to the users This entity introduces retrieval of files with low bandwidth and low computational and communication cost. In order to audit the effectiveness of our blueprints.

Index Terms: ***Cloud Computing, AES algorithm, Page ranking, file filter, Aggregation, matrix, Ostrovsky, EIRQ, user privacy.***

1. INTRODUCTION

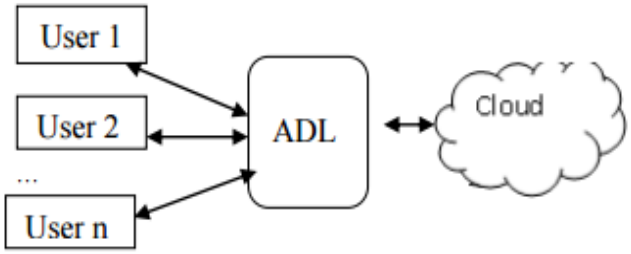
Cloud computing as an emanate technology to imperative information technology process in future. Many organizations choose to out-source their data for sharing in cloud [1] An organization supports the cloud services and authorizes its staff to share files in the cloud, its typical in cloud application. Each file is related by set of keywords The staff as authorized users for retrieving files They can retrieve files of their interests by querying the cloud with certain keywords the key problem is that user privacy The main drawback is because of altering of all the queries from different users.[2] Security is one of the major issues in cloud computing. So it is necessary to protect the user privacy while querying the data in the cloud environment different techniques are developed by researchers to provide privacy in this scenario the issue that is to be addressed is Security User privacy must be protected in addition to querying of cloud [3] This process edges to substantial query overhead from distinct users. An avant-garde solution would be to make a rank matrix that intensifies the user privacy than the erstwhile methods. EIRQ scheme address the issues of privacy, aggregation, computational cost and bandwidth wastage Ranked and security model user to take the different files from the cloud in the case number of query and data is encrypted The work [8], take supports single-keyword searches security files and queries different Preserving Symmetric Encryption (OPSE) [9] and utilizes keyword frequency and rank results The user send query time to process process the cloud is over headed queries in the many users

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

different organization in the process communication and computation is different methods.[4].

2. RELATED WORK

In this scheme alphanumeric message is converting into a purely numeric message, which is broken into blocks, mi, such that, for each i, 0 < mi < n, for a predetermined value, n. in this the term plaintext is used to refer to a message that is numeric that is not encrypted [5] while the term cipher text is used to refer to plaintexts, that is not dencrypted. One property in particular, the addition of plaintexts through multiplication of cipher texts, it is looked at in terms of its potential application to a form of electronic voting, in order to illustrate the system‟s potential. Unlike RSA cryptosystem, Paillier cryptosystem results in a non-zero cipher text for a plaintext message of value Private keyword based searching allows a server to filter out streaming data without compromising user privacy In existing work an efficient decoding [2] method is used to recovery the files and crash in a buffer position. Security searching schemes is support searching for keywords two sets of keywords. In query searching use Disjunctive normal forms (DNF) of keywords the existing scheme model [6] keywords the existing scheme model [6]



3. OVERVIEW

Private searching was proposed by Ostrovsky allows user [6], the customer is publicized for different transactions such as bandwidth, CPU eternity, and so on. To make private searching pertinent in a cloud habitat, our prior work designed a cooperate private searching protocol This paper presents a novel computational problem, called as Composite Residuosity [7] Class Problem, and its applications to public-key cryptography. It presents a new trapdoor mechanism and three encryption schemes a trapdoor permutation and two homomorphism probabilistic encryption schemes. These are computationally compared with RSA.

ARCHITECTURE

The searching protocol is like a proxy [4] server called in aggregation and different layer) is placed inside the organization. This ADL is set of mediator among the cloud The functioning is aggregation and distribution The ADL reduces the computation cost [8].

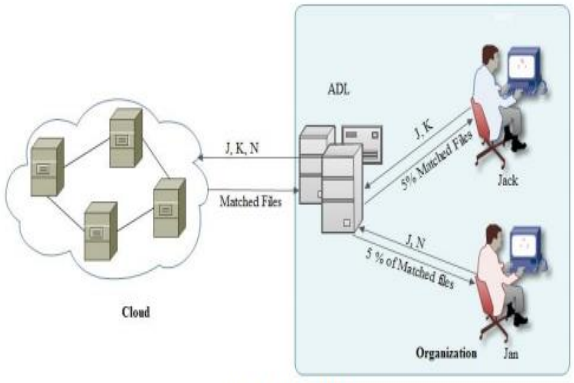


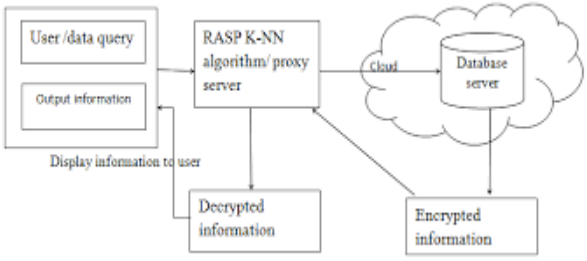
Fig. 2 EIRQ Model

This scheme is very query overhead as well as every time accesses the broadband connection. This process is more costly to accessing files at every query Issues in Ostrovsky [9] it does not lower the costs incurred by the customers of the cloud.

4. Proposed System:

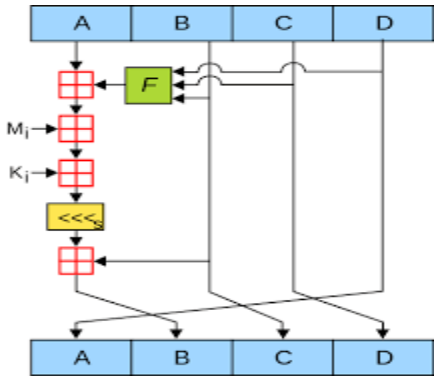
In the existing work the EIRQ scheme is proposed to provide a differential query services with the user privacy it works based on the ranking of users query [10]. In this method the communication cost is also reduced by retrieving only the required contents to the users based on users ranking Based on this ranking the files will be retrieved to the users This is impelled by the phenomenon that beneath certain cases, there are a pile of files corresponding a user's query, but the user is concerned in only a definite percentage of matched files Efficient [3] the sends queries in cloud and process is sends results to users number of files is matched users query the user want files only they interested on certain percentage of files

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal



A. MD5- (Message-Digest algorithm)

The input message is broken up into chunks of 512-bit blocks. The message is padded so that its length is divisible by 512. In this sender use the public key of the receiver to encrypt the message and receiver use its private key to decrypt the message [11].



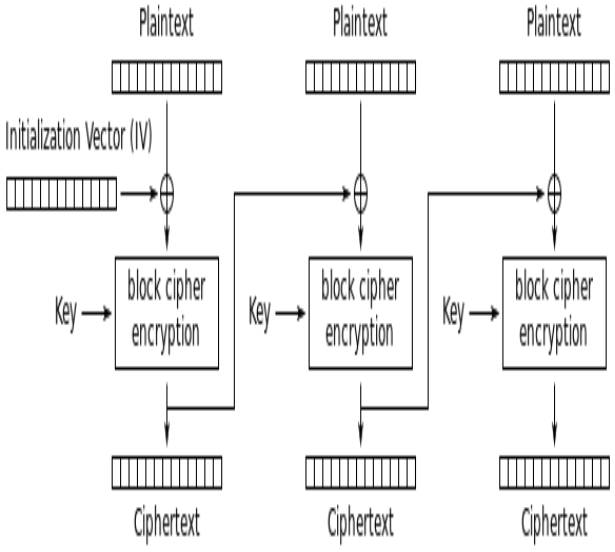

```
void callback(state, markFd, markOffset, reqFd, reqOffset) {
1:   struct access_entry accesses[BATCH_SIZE];
2:   int accepted, full, n = 0;
3:   int mode = PF_SET;
4:   tileInfo_t *tile = getTileInfo(reqFd, reqOffset);
5:   imageInfo_t *img = tile->imageInfo;

6:   for (; !lastTile(tile); tile = nextTile(tile, img->accessOrder) ) {
7:       accesses[n].page_offset = tile->swap_offset;
8:       accesses[n].fd = img->swap_file;
9:       accesses[n++].marked = 0;
10:      if (n == BATCH_SIZE) {
11:          accepted = request_prefetching(state->client,
                 accesses, n, mode);
12:          full = (accepted < n);
13:          mode = PF_APPEND;
14:          n = 0;
15:          if (full)
16:              break;
17:  }   }
18:  request_prefetching(state->client, accesses, n,
         mode | PF_DONE);
}
```

B. AES- (Advanced Encryption Standard)

In cryptography, the Advanced Encryption Standard (AES) is a symmetric-key encryption standard. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. AES algorithm ensures that the hash code is encrypted in a highly secure manner. AES has a fixed block size of 128 bits and uses a key size of 128 in this paper. Its algorithm is as follows: 1. Key Expansion - 2.

Initial Round - 3.Add Round Key - 4.Rounds - 5.Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table. 6. Shift Rows—a transposition step where each row of the state is shifted cyclically a certain number of steps. 7. Mix Columns [12] a mixing operation which operates on the columns of the state, combining the four bytes in each column 8. Add Round Key—each byte of the state 9) 17 combined with the round key; each round key is derived from the cipher key using a key schedule. 9. Final Round (no Mix Columns) 10. Sub Bytes 11. Shift Rows 12. Add Round Key



Cipher Block Chaining (CBC) mode encryption

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Encryption with RC6-$w/r/b$

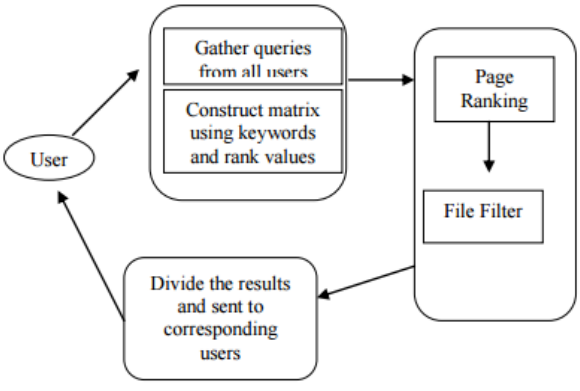
Input: Plaintext stored in four w-bit input registers A, B, C, D
Number r of rounds
w-bit round keys $S[0, \ldots, 2r+3]$

Output: Ciphertext stored in A, B, C, D

Procedure:
$B = B + S[0]$
$D = D + S[1]$
for $i = 1$ to r do
{
$t = (B \times (2B+1)) \lll \lg w$
$u = (D \times (2D+1)) \lll \lg w$
$A = ((A \oplus t) \lll u) + S[2i]$
$C = ((C \oplus u) \lll t) + S[2i+1]$
$(A, B, C, D) = (B, C, D, A)$
}
$A = A + S[2r+2]$
$C = C + S[2r+3]$

C. SCHEME DESCRIPTION

In this section, the EIRQ scheme described in three schemes.1) EIRQ Efficient,2) EIRQ Simple and 3) EIRQ privacy scheme[13] .By comparing all the scheme the EIRQ Efficient scheme provide less communication cost we should determine which matched files will be returned and which will not. In this paper, we simply fix the probability of a file being produces queries selecting it[14].

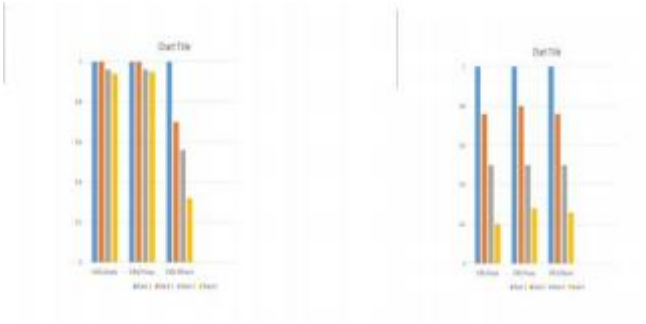


5. RESULT AND DISCUSSION

The results are observed on the file survival [4] rate and computation cost. These schemes is tested the Amazon Elastic Compute Cloud (EC2) to test the file survival rate and computation cost.[15] File survival rate is observed in the clouds with distinct knowledge retrieval schemes. File durability rates give the mobility of retrieving the in demand file for a user using Ostrovsky scheme and our model.

Protocol	Parameter		
	Security and privacy	*Computational Cost*	*Bandwidth Cost*
Otrovsky	Yes	No	No
COPS protocol	Yes	Yes, to some extent	Yes, to some extent
EIRQ	Yes	Yes	Yes

Schemes under the Ostrovsky scheme Throughput of Ostrovsky Scheme is not satisfied by using Parameter Settings [16].



6. CONCLUSION

In business organizations, cloud provides many advantages but few cons are user privacy, security and efficiency. By using query services that provides a bridge between empty set and the desired result set for the users privacy is an important issue in the cloud computing when requesting for an contents stored in the cloud storage. It will become burden for cloud service providers for handling the differential query service from the users we present different Techniques for searching over outsourced encrypted data. This study concludes fast search access and does not leak information to untrusted authorities We have also shown the comparison of these algorithms which is useful for better understanding of these algorithms in terms of different parameters

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

7. Future Work

In the future we can consider alternative implementations for the file content filters in addition to authority flow ranking. In addition to that better security mechanism can also be implemented in order to provide a better satisfaction level for the cloud users who intend to share their sensitive information to the cloud service providers This kind of ranking i.e. ranking of files depends upon highest rank of queries leaves few bottlenecks, a sophisticated ranking system can be developed by providing attributes to each file

8. REFERENCES

[1] P. Mell and T. Grance, ‘‘The NIST Definition of Cloud Computing (Draft),’’ in NIST Special Publication. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2011.

[2]. Boneh.D,Crescenzo.D,Ostrovsky.R,and Persiano.G,(2004) Public- Key with Keyword Search,‟ Proc. Int‟l Conf. Theory and Applications of Cryptographic Techniques.

[3]. Cao.N,Wang.C, Ren.M Li, K. and Lou.W,(2011),,Privacy-Preserving Multi keyword Ranked Search over Encrypted Cloud Data,‟ Proc. IEEE INFOCOM.

[4]. Coron.J.S,Mandal.A, Naccache.D and Tibouchi.M, (2011) „Fully Homomorphic Encryption over the Integers with Shorter Public Keys,‟ CRYPTO ‟11: Proc. 31st Ann. Conf. Advances in Cryptology.

[5]. Curtmola.R, Garay.J.A, Kamara.S, and Ostrovsky.R, (2006) „Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions,‟Proc. ACM 13th Conf. Computer and Comm. Security.

[6] Cong Wang, Ning Cao, Kui Ren, and Wenjing Lou, ”Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, SYSTEMS, VOL. 23, NO. 8.

[7] Qin Liu, Chiu C. Tan, Jie Wu, and Guojun Wang, “Towards Differential Query Services in cost-Efficient clouds” IEEE Transactions on Parallel and Distributed Systems,Volume:25,Issue:6,Issue Date :June.2014

[8] Hore, S. Mehrotra, and G. Tsudik, “A privacy-preserving index for range queries,” in Proceedings of Very Large Databases Conference (VLDB), 2004.

[9]C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, “Secure ranked keyword search over encrypted cloud data,” in Proceedings of IEEE International Conference on Distributed Computing Systems (ICDCS), 2010

[10] Ning Cao, Cong Wang , Li, Ming , Kui Ren, Wenjing Lou, “Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data” INFOCOM, 2011 Proceedings IEEE April 2011..

[11] W. Wong, D. Cheung, B. Kao, and N.Mamoulis, “Secure knn computation on encrypted databases,” in Proc. of ACM SIGMOD, 2009.

[12] Qin Liu, Chiu C. Tan, Jie Wu and Fellow (2013) “Towards Differential Query Services in Cost-Efficient Clouds” IEEE Transactions On Parallel and Distributed Systems, vol. 20, no.10, pp-1-11.

[13] Qin Liu, Chiu C. Tan, Jie Wu, and Guojun Wang, “Efficient Information Retrieval for Ranked Queries in Cost Effective Cloud Environment”, IEEE INFOCOM, 2012.

[14] Qin Liu, Chiu C. Tan, Jie Wu, and Guojun Wang, “Towards Differential Query Services in Cost Efficient Clouds” IEEE Transactions on Parallel and Distributed Systems, 2013.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[15] Qin Liu, Chiu C. Tan, Jie Wu, and Guojun Wang, "Cooperative Private Search in Clouds", Journal of Parallel and Distributed Computing, 2012.

[16] Wikipedia: http://en.wikipedia.org/wiki/ Efficient Information Retrieval for Ranked Queries.

Author Details

T.Swathi is one of the author received B.Tech(C.S.E) Degree from JNTU Kakinada in 2012.She is Studying M.Tech in Sri Vathsava Krishnam Raju Institute of Engineering and Technology, Bhimavaram, AP.

Dr.Penmetsa Vamsi Raja, He did his PhD from JNTU Kakinada AP. He received M.Tech Post Graduation degree in C.S.T department from Andhra University, Visakhapatnam, A.P. He is presently working as Principal in Sri Vatsavayi Krishnam Raju College of Engineering & Technology Bhimavaram AP. He has authored more than 20 relevant publications in journals and Conferences. His Research areas include Computer Networks, Network Security, Cloud Computing, Big Data, Data Mining and Software Engineering.