iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IV **Month of publication:** April 2018

DOI: http://doi.org/10.22214/ijraset.2018.4608

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

Illustration on Secure and Efficient Multi-keyword Ranked Search on Encrypted Cloud Data

Sai Anusha Kancharla[1], P. Venkateswara Rao[2], N. C. Sindhu Priya[3], P. Anusha[4], M.Madhavi[5]
[1, 3, 4, 5,] *Computer Science & Engineering (Student), Narayana Engineering College, Gudur*
[2]*Computer Science & Engineering (Professor), Narayana Engineering College, Gudur*

Abstract: More and more business people today store and share their data by using the public cloud services because of its promising economical benefits, ease and flexibility in the data sharing. However, there can be malicious data users who misuses the sensitive data shared by the data owners. To avoid this we have to encrypt the data before outsourcing it into the cloud. There are so many techniques proposed to perform efficient search on the encrypted data in the cloud and out of them the ranked multi-keyword search have acquired more attention. In this paper, we propose a model where an efficient search is performed on the encrypted information stored in the cloud by providing the ranks to the keywords. We have encrypted the information by using RSA algorithm and we implement an efficient searching technique by matching the coordinates.
Keywords: RSA Algorithm, cloud computing, multi-keyword search, Privacy preserving

I. INTRODUCTION

Cloud computing is a way in which our data is processed outside our system i.e., in the servers located in some remote area. There are various types of services offered by different cloud providers like SaaS-where a software application can be used without installing it in our pc, PaaS-where one can work on different platform from our system and IaaS-where one can use hardware components like storage devices and processors which are located remotely. The Cloud services provide ease and flexibility in working at a low cost. The pay-as-you-go model of the cloud services have made a comprehensive change in cloud computing. The users of cloud services have increased extensively within a very small period of time. The cloud storage is the most used service over the other services provided by the cloud service providers. Many of the business people depend on the cloud services to store and share their information. As the business data contains sensitive information in it, it can be misused by some of the malicious users in the cloud. So, to avoid this misuse of the sensitive information such as the business' data the data must have to be encrypted before it is outsourced into the cloud storage and also the encrypted data should be searchable so it can be searched by the data users. To make the search more efficient, many different techniques have been proposed. Out of these the multi-keyword ranked search has drawn more contemplation. In this paper, we propose a model where an efficient search is performed on the encrypted information stored in the cloud by providing the ranks to the keywords. We have encrypted the information by using RSA algorithm and we implement an efficient searching technique by matching the coordinates. We have observed different privacy issues in the techniques proposed earlier to this and identified a few Privacy requisites. For searching on the cloud data we use the multi keyword ranked search by matching coordinates with queries using some threat designs.

II. LITERATURE SURVEY

The searchable encryption techniques, different methodologies proposed to search the encoded information in a cloud and their limitations are reviewed. The searchable encryption scheme is a technique in which the data is encoded and some search terms which are used to retrieve that data are associated with it, so that, the data can be searched without its contents being known. Song et al. [1] is the one who proposed the idea of searchable encryption for the first time where each and every word of the data is encrypted independently. The computational overhead is very high for this scheme as to search a document each and every word in that document must be scanned. So, they later proposed search by the index where for large information it would be easy to search, but there is no scheme provided for the update of the information as it worked well only on read-only data. The secured index architecture was proposed by Goh [2], which allows the search to performed quick if the trapdoor is present in the index structure of the document. The trapdoor is generated by the secret key and so it ensures secure and privacy of the information. In the paper, Secure and privacy preserving keyword searching for cloud storage services, Qin Liu [3] proposed a SPKS scheme by analyzing cloud storage characteristics in which the CSP participates in the decipherment and returns only the files that contain those keywords.

©IJRASET (UGC Approved Journal): All Rights are Reserved

The secure ranked keyword search scheme over the encrypted cloud is proposed by Wang [4], which gave more efficient search results by using the ranking mechanism of the keyword and the ranking of keyword is based on some criteria like frequency etc. Wang [5] have also conducted experiments to show the inefficiency of SSE [6] mechanism. After that some single keyword ranked [7] searches were proposed to reduce the computational overhead due to the encryption and decryption mechanisms. But they do not provide the relevant search results for the user. Yu J [8] proposed a two round searchable encryption (TRSE) with a multi-keyword top-k retrieval scheme. They have employed a homomorphic encryption and a vector space model where all the operations are performed on ciphertext in server side and provides a search accuracy. An attribute based keyword search scheme is proposed by Wenhai Sun[9] with user revocation (ABKS-UR) where the users can encrypt their files on their own without depending on the third party authorization, but the trapdoor generation takes more time in this mechanism. The multi-keyword ranked search techniques were proposed which boosted the retrieval of the most relevant search results. A secure multi keyword search scheme is proposed by Zhihua Xia [10], which also provides the dynamic update and delete operations on the encrypted documents in the cloud. The keywords were ranked by using the TF_IDF method, the index tree was encrypted by using the secure K- nearest neighbour algorithm and greedy depth first search mechanism was used.

III. PROBLEM STATEMENT

The problem statement is to implement the Multi-keyword ranked search more efficiently by preserving the privacy so that the cloud server cannot have knowledge about the additional data about the encrypted user information in the cloud server.

IV. METHODOLOGY

A. *System Architecture*

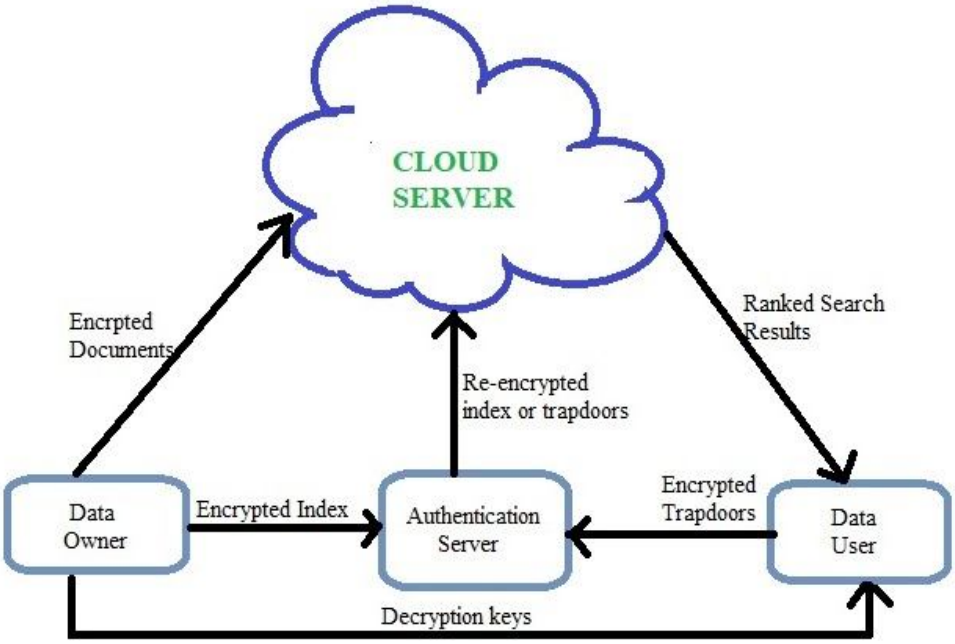


Fig. 1 System Architecture

There are four modules in this Secure and efficient Multi-keyword ranked search:

1) The Owner of the data is the one who encrypts and outsources that encrypted information into the semi-trusted cloud server and also generates the decryption keys to decrypt the files and send them to the corresponding data user.
2) The authorised data user who generates the trapdoors to search and access the files in the cloud server. The user can only access the data when the user possess the correct decryption key.
3) The cloud server and the encryption module is the entity which possess the information in its database about the files and data users and from where the documents are retrieved from.
4) The rank search module allows the data user to search in the cloud by using the multiple keywords with coordinate matching and retrieves the more relevant results.

©IJRASET (UGC Approved Journal): All Rights are Reserved

B. Encryption Using RSA Algorithm

The RSA algorithm is the first public key block cipher encryption scheme which is used in encrypting the data, digital signatures and diffusion of the secret key. Two keys are generated in this encryption mechanism one is the public key and the other is private key. If some information is encoded by using the private key of the data user then it can only be decrypted by using the public key of that user. RSA makes use of an expression with exponentials. Plaintext is encrypted in blocks, the block size must be less than or equal to $\log_2(n) + 1$, *where* $0 \leq n \leq 1024$

1) Key Generation

a) Select two prime numbers i, j
b) Calculate their product as n=i*j
c) Find the Euler's totient value of n as Ø(n)= (i-1)(j-1)
d) Now, select an integer e such that gcd(Ø(n),e)=1, 1<e< Ø(n)
e) Calculate d= e^{-1} mod(Ø(n))
f) The Public Key is {e,n} and the private key is {d,n}

2) Encryption And Decryption

A message M (where 0≤M≤n) is encrypted using equation:
$C = P^e \bmod n$,where {e,n} is public key
To decrypt cipher text
$P = C^d \bmod n$, where {d,n} is private key

C. Trapdoors

The trapdoor generation characteristic should be a randomized one as a substitute of being deterministic. The generation of trapdoors incurs a vector splitting operation and two multiplication of a (m×m) matrix (m being the whole quantity of keywords), for that reason the time complexity is $O(m^2)$. The cloud servers need to not be in a position to deduce the relationship of any given trapdoors, e.g., to be aware of whether or not two trapdoors are created with the aid of the equal quit user search request. Otherwise the deterministic trapdoor technology would give benefit to the cloud server to accumulate frequencies of different search requests involving one-of-a-kind keyword(s), which might also similarly violate the keyword privacy requirement.

D. Threat Models

The cloud server is semi-trusted and it may know some of the information about the data contained in it. Based on this we refer to two threat models, the known cipher text model and the known background model. In the first model the cloud server may know about the encrypted data files in it and about the searchable encrypted index, where as the second threat model is that the cloud server may know the information like some statistical information about the encrypted data files which may lead to disclosure of the keywords used by the user in the trapdoors through the help of reverse-engineering.

E. Coordinate Matching

It is the mechanism in which perform an intermediate similarity check of the keywords used in the query generated by the user and that present in the document which ensure more relevant results in the ranking order.

V. RESULTS

In a cloud server there can be any number of data owners and users who have registered persons to access the cloud storage services. These registered users and owners are to be authenticated and activated by the authorization server. The owner can encrypt and outsource the data into the server which is re-encrypted by the authentication server and is placed into the cloud. The data user searches by using different keywords using trapdoors and a set of results in a ranked order are displayed. The data user can request the access to the files and it s sent to the corresponding data owner. The data owner transfers the key generated to the user. Only by using the correct key the user can access the document.

VI. CONCLUSION

In this paper, we have explored different ranking search models and privacy concerns of the data members of the cloud. In this paper, it was implemented the secure RSA Algorithm for the data encryption decryption and key generation. The authentication server re-encrypts the data making it more secure and also it activates and authenticated the data owners and the users providing a sound security for the data in the cloud. As the future enhancement look forward to solve the data integrity concerns.

©IJRASET (UGC Approved Journal): All Rights are Reserved

REFERENCES

[1] Song D, Wagner D, Perrig A. Practical techniques for searches on encrypted data. In: Proceedings of the IEEE symposium on security and privacy. California; 2000

[2] Goh, E.-J. "Secure indexes, Cryptology ePrint Archive", http://eprint.iacr.org/. 2003/216, 200

[3] Qin Liuy, Guojun Wangyz, and Jie Wuz, "Secure and privacy preserving keyword searching for storage services", ELSEVIER Journal of Network and computer Applications, March 201

[4] C. Wang, N. Cao, J. Li, K. Ren, W. J. Lou, "Secure Ranked Keyword Search over Encrypted Cloud Data", 30th International Conference on Distributed Computing Systems, pp. 253-262, 2010

[5] Wang C, Cao N, Ren K, Lou W. Enabling secure and efficient ranked keyword search over outsourced cloud data. IEEE Trans Parallel Distrib Syst 2012;23 (8):1467–7

[6] M. Kuzu, M. S. Islam, and M. Kantarcioglu, "Efficient similarity search over encrypted data," in Data Engineering (ICDE), 2012 IEEE 28th International Conference on. IEEE, 2012, pp. 1156–1167

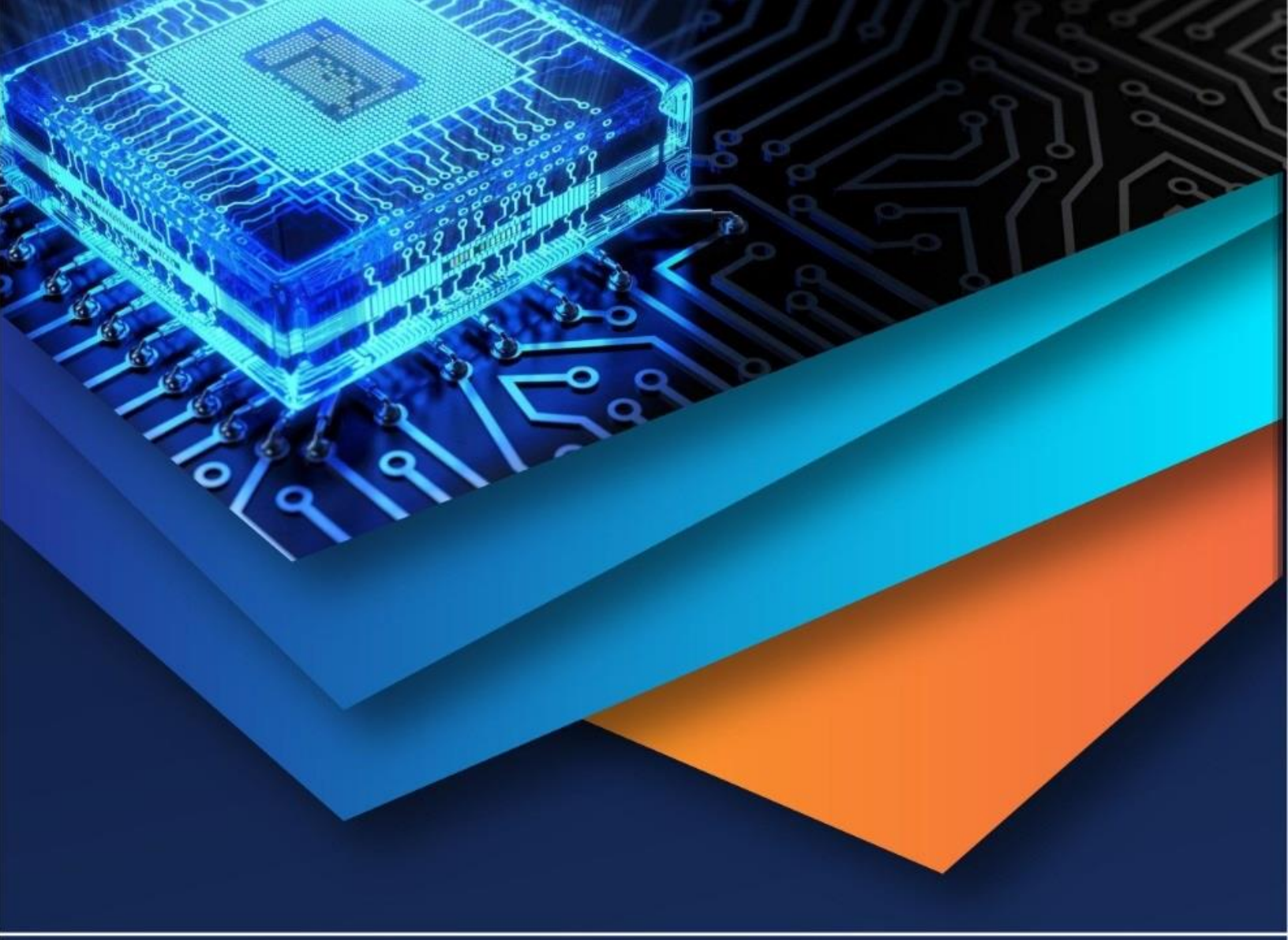
[7] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in INFOCOM, 2010 Proceedings IEEE. IEEE, 2010, pp. 1–5.

[8] Jiadi Yu, Peng Lu, "Toward Secure Multikeyword Top k Retrieval over Encrypted Cloud Data", IEEE Journal of Theoretical and Applied Information Technology 10th August 2014. Vol. 66 No.1 ISSN: 1992-8645 E-ISSN: 1817-3195 6

[9] Wenhai Sun et al., "Protecting Your Right: Attribute-based Keyword Search with Fine grained Owner-enforced Search Authorization in the Cloud", IEEE INFOCOM 2014, Toronto, Canada, April 27 - May 2, 2014

[10] Zhihua Xia, "A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data", IEEE Transactions On Parallel And Distributed Systems, VOL: PP NO: 99 YEAR 2015

©IJRASET (UGC Approved Journal): All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)