Privacy Preserving and Efficient Accessing Cloud Resources

K. Gopichand[1] R. Kannadasan[2] A. Anantha[3]
[1]M.Tech Student [2,3]Assistant Professor
[1,2]Department of Applied Mechanics
[1,2]SCSE, VIT University, Vellore [3]University College of Engineering, Pudhukottai.

Abstract— In recent days cloud computing is an emerging technology in terms of economy, as data owners are motivated to move their valuable data systems from local machines to commercial public cloud. But the security and sensitivity of the data should be preserved before outsourcing to public cloud. The data should be encrypted before outsourcing it in to the cloud, which needs to overcome the traditional way of data retrieval methods based on plain text keyword search. While dealing with large number of data users and files in cloud environment, it is necessary to consider efficient searching mechanism for better retrieval of data from cloud. Multi keyword query is an efficient data retrieval technique. In this proposed work we are using secure multi keyword search on encrypted cloud data and preserve the strict privacy policies. Coordinate matching and inner product similarity is used to query the keywords. Ranking of keywords is done for most frequently used search results.

Key words: Multi Keyword Query, Ranked Search, Encryption, Inner-Product Similarity

I. INTRODUCTION

Now-a-days cloud computing is recognized as an best alternative to traditional information retrieval system and has been gaining attention from every one due to its resource sharing and low maintenance cost. Cloud computing is a web based model of computing, where the shared resources, software's and data are given to PCs and different gadgets upon interest. This empowers the end users to get to the cloud computing resources whenever from any platform, for example cellphone, mobile computing platform or desktop. Clouds are huge pools of effortlessly usable and accessible virtualized resources. The information and the product applications needed by the clients are not put away all alone on their computers; rather they are stored away on remote servers which are under the control of different clients. Cloud computing is a pay-per- use design in which the infrastructure provider by means of customized "service level agreements".

As cloud computing gets to be common, more sensible data's are being stored into the cloud. For example, messages, individual health records, photograph collections, tax reports, money related exchanges and government files and so forth. The way that the data owners and cloud server are no more in the same trusted space may put the outsourced unencrypted information at risks. The cloud server may spill information data to unapproved bodies or even be hacked. To give data security, delicate information must be encoded before outsourcing to the commercial open cloud. The way of downloading all the information and decrypting them locally is impractical, because of huge amount of band width cost in cloud scale frameworks.

II. RELATED WORK

The issue of privacy-preserving keyword search is tended to by different work in writing. Related work can be broke down in two noteworthy groups: single keyword word and multi keyword search[1]. While the client can search down a single characteristic for every inquiry in the previous, that latter empowers search for a conjunction of a few catch phrases in a single query. The greater part of the protection safeguarding keyword search conventions existing in writing focus on single catchphrase query. Investigating security safeguarding and successful search over encrypted cloud data is of central significance considering the conceivably huge amount of on interest data clients & large amount of outsourced information records in the cloud, this issue is especially difficult as it is extremely hard to meet the prerequisite of performance[2], system scalability and usability. Data encryption makes powerful data utilization an exceptionally difficult undertaking given that there could be a lot of outsourced data records. Other than in the cloud computing data owners may impart their outsourced information to an extensive number of clients who may need to just retrieval certain particular information documents. They are occupied with amid a given session. A standout amongst the most prominent approaches to do as such is through keyword search technique[3] permits clients to specifically recover records of their interest. Requirement for data retrieval is the most frequently happening task in cloud by the client to the server.

Mostly cloud server performs result significance ranking with a specific end goal to make the search as faster. Such ranked search framework empowers data clients to discover the most important data rapidly, as opposed to returning undifferentiated results. Ranked search can dispense unnecessary network traffic by sending back just the most relevant information which is exceptionally attractive in the "Pay-As-You-Use"[4] cloud standard. For security reasons, such ranking operation, however, should not disclose any information related keyword. From another point of view, to enhance the search exactness and in addition to upgrade the client searching experience, it is additionally necessary for such ranking framework to help multiple keywords search, as single essential keyword look frequently yields extremely coarse results. As a typical practice demonstrated by today's web search tools[5] (e.g., Google search), data clients may have a tendency to give a set of essential keywords rather than stand out as the pointer of their search interest to recover the most significant information. Also every keyword in the search request has the capacity help narrow down the search results further. "Coordinate matching"[6] i.e., whatever number matches as would be possible to refine the outcome significance, and has been generally utilized as a part of the plaintext data recovery (IR)[2] group. Then again, how to employ it in an

encrypted cloud information search framework stays an exceptionally difficult task due to characteristic security and protection deterrents, including different strict necessities like the information protection, the record security, the keyword security, and numerous others.

III. PROPOSED WORK

For our framework, we pick the standard of coordinate matching, to recognize the similarity between search inquiry and information documents. Specially, we use internal information correspondence, i.e., the number of query keywords showing up in a record [7], to assess the similarity of that document to the search query in coordinate matching rule. Every document is connected with a double vector as a sub index where every bit represents whether relating keyword is present in the document. The search related query is likewise depicted as a binary vector where every bit implies whether comparing keywords shows up in this search demand, so the comparability could be precisely measured by internal result of query vector with data vector. However, specifically outsourcing data vector or query vector will damage record security or search protection [8]. To meet the test of supporting such multi-keyword semantic without protection, we propose an essential SMS plan utilizing secure inner product computation, which is adjusted from a protected k-nearest neighbor (KNN)[9] strategy, and afterward enhance it orderly to accomplish different security necessities in two levels of risk models.

1) Showing the issue of Secured Multi-keyword search over encrypted cloud information
2) Propose two plans taking after the guideline of coordinate matching and inner product similarity.

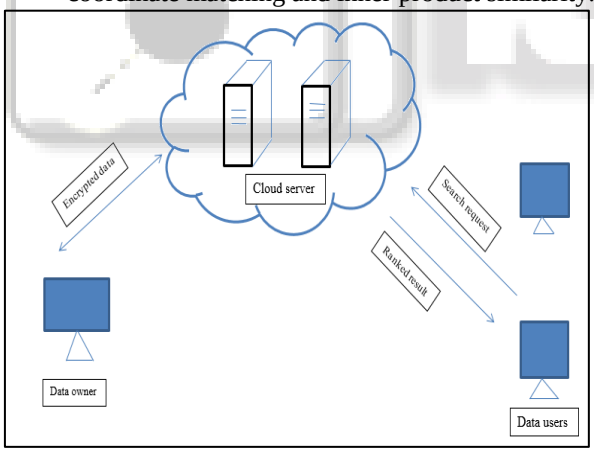

Fig. 1: Architecture of the Search over Encrypted Cloud Data

Considering three separate entities, as represented in Fig1. Data owner, Data client, and cloud server. Data owner has an accumulation of information records to be send to cloud server in the encrypted configuration. To activate the searching ability over encrypted information, data owner, before sending information, will first form an encrypted searchable index[10] and after that outsource both the list and the encrypted searchable index to cloud server. To search the file, an approved client oblige a comparing trapdoor through search components, Upon accepting from data clients, cloud server is responsible to search the file and return the relating set of encrypted files. To enhance record retrieval accurately, search result should be ranked by cloud server as per some ranking criteria[9]. Cloud server just returns back top-k files that are most apt to the search related query. In Fig1.There is another element indicated i.e. Unapproved User. In the event that unauthorized client tries to get to any information from cloud then alert will be produced as mail and message. The alert is given to the approved individual who is owner of that information.

IV. DESIGN GOALS

A. *Encryption Module:*

AES embodies three block ciphers, 128 bit, 192 bit and 256 bit. Every cipher encrypts and decrypts information in blocks of 128 bits utilizing cryptographic keys of 128-, 192- and 256-bits, individually. Symmetric or secret key ciphers utilize the same key for both encryption and decryption, so both the data owner and receiver must know the secret key utilize it. All key lengths are considered sufficient to ensure grouped data up to the "privacy" level with "Top Privacy" data requiring either 192 bit or 256 bit key lengths. AES works on a 4×4 segment significant request framework of bytes, termed the state, albeit a few variants have a bigger square size and have extra sections in the state. Most AES computations are carried out in an exceptional limited field[11]. There are 10 stages for 128-bit keys, 12 stages for 192-bit keys, and 14 stages for 256-bit keys - a stage comprises of a few transforming steps that incorporate substitution, transposition and blending of the info plaintext and change it into the last yield of cipher text.

B. *Steps in AES Algorithm:*

The encryption approach uses an arrangement of extraordinarily determined keys called round keys. These are associated, nearby distinctive operations, on a bunch of data that holds accurately one piece of information the data to be encrypted. This exhibit we call the state cluster
The accompanying steps for encrypting 128 bit block:

1) Infer the arrangement of round keys from the cipher key.
2) Initialize the state show with the piece information (plaintext).
3) Add the starting round key to the starting state show.
4) Perform nine rounds of state control.
5) Perform the tenth and last round of state control.
6) Copy the last state show out as the encrypted information.

The reason that the rounds have been recorded as "nine took after by a last tenth round" is on account of the tenth round includes a marginally diverse control from the others.

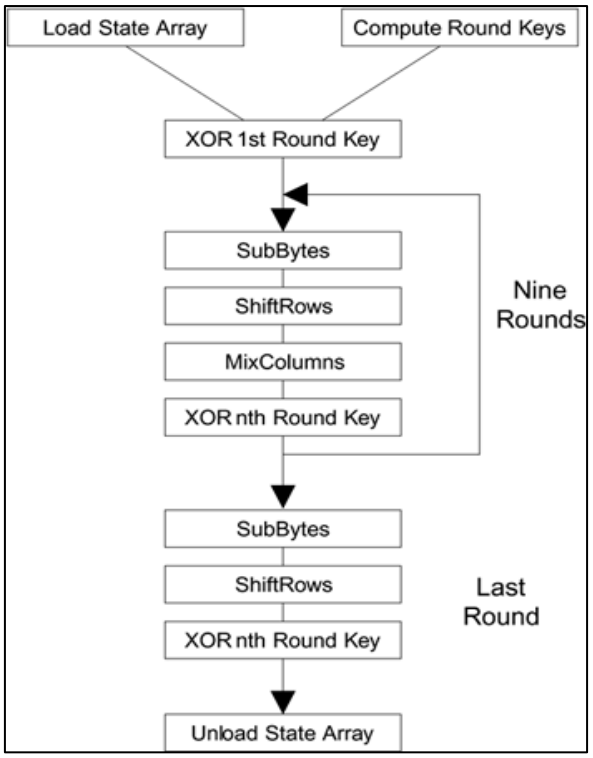

Fig. 2: Depicts AES algorithm

C. K Nearest Neighbor Algorithm:

K-nearest neighbor search distinguishes the top k nearest neighbors to the query. This method is regularly utilized in predictive analytics to estimate or order a point taking into account the accord of its neighbors[12]. K-nearest neighbor graphs are graphs in which each point is joined with its k nearest neighbors.

The fundamental thought of our algorithm: The estimation of Dmax is decreased keeping step with the progressing accurate assessment of the object similarity distance for the applicants. Towards the end of the regulated refinement, Dmax achieves the ideal query extent Ed and keeps the technique from creating a larger number of applicants than would normally be appropriate in this manner satisfying the r-optimality foundation.

V. EXPECTED RESULTS

A. Encryption and Decryption Result:

At the point when AES calculation is connected on the information then we get encoded information also that encoded information is store on the cloud. Client can get to the information in the wake of downloading and decryption document. For encryption and decryption keys are given.

B. Ranking Result:

At the point when any User demand for the information then Ranking is carried out on request for information utilizing k-closest neighbor calculation. For Ranking co-ordinate matching standard is utilized. After ranking client gets the normal result of the query.

VI. CONCLUSION

In this paper, a framework is proposed for the issue "multi-keyword ranked search over encrypted cloud" information and to create a variety of protection prerequisites. Among different multi- keyword word semantics, the efficient similarity measure is "coordinate matching", that is the same number of matches are conceivable, to adequately catch the pertinence of outsourced records to the query keywords words, and utilization "inner product similarity" to quantitatively assess such similarity measure. For meeting the test of supporting multi-keyword word search without security breaks, MRSE system is proposed utilizing secure inner product computation. Intensive investigation researching security and productivity sureties of proposed plans is given.

REFERENCES

[1] X. Sun, Y. Zhu, Z. Xia, and L. Chen, "Privacy-Preserving Keyword-based Semantic Search over Encrypted Cloud Data," vol. 8, no. 3, pp. 9–20, 2014.
[2] C. Örencik, "Efficient and Secure Ranked Multi-Keyword Search on Encrypted Cloud Data," pp. 186–195, 2012.
[3] L. Chen, X. Sun, Z. Xia, and Q. Liu, "An Efficient and Privacy-Preserving Semantic Multi-Keyword Ranked Search over Encrypted Cloud Data," vol. 8, no. 2, pp. 323–332, 2014.
[4] D. Sunny and A. George, "Synonym Based Ranked Secure Search Over Encrypted Data," vol. 4, no. 7, pp. 258–264, 2014.
[5] V. U. Kumar and D. S. Bhanu, "Retrieval Of Encrypted Cloud Data Using Multi Keyword," pp. 1–7.
[6] C. Orencik, M. Kantarcioglu, and E. Savas, "A Practical and Secure Multi-Keyword Search Method over Encrypted Cloud Data."
[7] Z. Xu, W. Kang, R. Li, K. Yow, and C. Xu, "Efficient Multi-Keyword Ranked Query on Encrypted Data in the Cloud," 2012.
[8] X. Sun, L. Zhou, Z. Fu, Z. Xia, and J. Shu, "Secure and Efficient Multi-keyword Ranked Search over Encrypted Cloud Data," vol. 48, no. Cia, pp. 141–151, 2014.
[9] A. D. Sawant and P. M. D. Ingle, "Improved Indexing and Advanced Relevance Ranking Score for Multi-Keyword Search over Encrypted Cloud Data," vol. 3, no. 7, pp. 969–973, 2014.
[10] M. Chuah and W. Hu, "Privacy-aware BedTree Based Solution for Fuzzy Multi-keyword Search over Encrypted Data."
[11] A. Kak, "Lecture 8 : AES : The Advanced Encryption Standard Lecture Notes on ' Computer and Network Security ' by Avi Kak (kak@purdue.edu) Goals : • To review the overall structure of AES . • To focus particularly on the four steps used in each round of AES : • ," no. 1, 2015.
[12] T. Seidl, "Optimal Multi-Step k -Nearest Neighbor Search," no. June, 1998.

