# Searching Multiple Keyword On Wildcard Using Privacy Preserving Algorithm And Searchable Encryption Techniques

**Sheeba Ann Thomas[1], Anju Rachel Oommen[2,] Smita C Thomas[3]**
[1, 2, 3] Dept of computer science and engineering
[1, 2, 3] Mountzion college of engineering , Kadamanitta, Pathanamthitta,India

***Abstract-*** *Data storage and privacy becomes a major issue nowadays in the cloud storage service because valuable and private information has to be encrypted before uploading the data to the cloud server which makes file searching process very difficult for the cloud users. To selectively fetch the data or files of their own requirements, various searching options are available only on the plain text data which is supported by the major cloud servers. Enormous searching methods are available on the encrypted data but they support only exact keyword search. Exact keyword search is not suitable for cloud storage systems, because it doesn't allow the users to typing errors or format misrepresentations, which greatly affects the search efficiency and makes user irritated. In this paper, we explored the existing encryption algorithms, and searching techniques and their applications and features in the existing cloud infrastructure. This will help the cloud service provider to decide which algorithm to choose for encryption and decryption which will facilitate more cloud users to utilize the cloud platform by simplifying the data storage and retrieval process in the cloud environment while preserving their privacy in the cloud.*

***Keywords***- Cloud storage service; Exact Keyword search; Privacy

## I. INTRODUCTION

In many cases, the storage services provided by the cloud companies cannot be fully trusted, so emails, personal health records, government documents and other sensitive information have to be encrypted before uploading to the cloud. Since the data uploaded by the data owners is encrypted, the searching of documents which contain specific keywords becomes rather difficult.

User downloads all the encrypted data and decrypts them with his/her secret key, and then he/she uses normal search methods to search documents containing specific keywords. This approach is obviously not effective and requires the users to have strong storage capacity. The plaintext searching methods which are present cannot be applied directly to encrypted cloud data, thus data encryption makes data search a big problem. To solve the problem above, there have been many researches on efficient and secure keyword search on encrypted data.

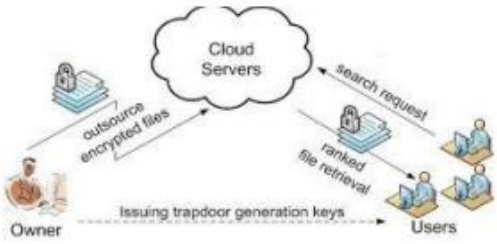


Fig 1.1 Cloud file storage and retrieval

## II. ANALYSIS OF VARIOUS ENCRYPTION ALGORITHMS IN CLOUD

### Data Encryption Standard (DES)

The Data Encryption Standard (DES) is a symmetrickey block cipher published by the National Institute of Standards and Technology (NIST). It uses single key (secret key) for both encryption and decryption. It operates on 64-bit blocks of data with 56 bits key. The round key size is 48 bits. The entire plaintext is divided into blocks of 64bit size; last block is padded if necessary. Multiple permutations and substitutions are used throughout in order to increase the difficulty of performing a cryptanalysis on the cipher. DES algorithm consists of two permutations (P-boxes) and sixteen Feistel rounds. Entire operation can divided into three phase. First phase is Initial permutation and last phase is the final permutations.

### Rivest-Shamir-Adleman (RSA)

RSA is a public key cipher developed by Ron Rivest, Adi Shamir and Len Adlemen in 1977. It is most popular asymmetric key cryptographic algorithm. This algorithm uses various data block size and various size keys. It has

asymmetric keys for both encryption and decryption. It uses two prime numbers to generate the public and private keys. These two different keys are used for encryption and decryption purpose. This algorithm can be broadly classified in to three stages; key generation by using two prime numbers, encryption and decryption. RSA today is used in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data. This algorithm is mainly used for secure communication and authentication upon an open communication channel. While comparing the performance of RSA algorithm with DES and DES, When we use small values of p & q(prime numbers) are selected for the designing of key, then the encryption process becomes too weak and one can be able to decrypt the data by using random probability theory and side channel attacks.

**Homomorphic EncryptionAlgorithm**

It is an encryption algorithm that provide remarkable computation facility over encrypted data(cipher text) and return encrypted result. This algorithm can solve many issues related to security and confidentiality issues. In this algorithm encryption and decryption taking place in client site and provider site operates upon encrypted data. This can solve threat while transferring data between client and service provider, it hide plaintext from service provider, provider operates upon ciphertext only. Homomorphic encryption allows complex mathematical operations to be performed on encrypted data without using the original data. For plaintexts X1 and X2 and corresponding ciphertext Y1 and Y2, a Homomorphic encryption scheme permits the computation of X1 Θ X2 from Y1 and Y2 without using P1 Θ P2.The cryptosystem is multiplicative or additive Homomorphic depending upon the operation Θ which can be multiplication or addition.

## III. SEARCHING TECHNIQUES

There are various searching techniques available, and to mention a few are as follows:

**Searchable Encryption:** It allows users to securely search complete encrypted data through keywords. This 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 pre-knowledge of the encrypted cloud data, have to post process every file got, in order, to find ones most matching their interest; another drawback, regularly getting all files containing the queried keyword further incurs unnecessary network traffic, when retrieve more than one files.

**Single Keyword Searchable Encryption:** A single keyword searchable encryption schemes usually builds an encrypted searchable index such that, it's content is hidden to the server, unless it is given appropriate trapdoors generated via secret key(s). Early work solves secure ranked keyword search which utilizes keyword frequency to rank results instead of returning undifferentiated results. 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. Traditional single keyword searchable encryption schemes are usually built in a way by creating an encrypted searchable index. Such indexes content will be hidden to the server. The information will be revealed only when the server gives the correct trapdoors that are generated via a secret key(s). The main drawback of single keyword-based search is that it is not comfortable enough to express complex information needs.

**Ranked Keyword Search:** Ranked search greatly enhances system usability by returning the matching files in a ranked order regarding to certain relevance criteria (eg. keyword frequency) thus, making one step closer toward practical deployment of privacy-preserving data hosting services in the context of cloud computing. To the best of knowledge it gives a legal status for the first time the problem of effective ranked keyword search over encrypted cloud data. Ranked keyword search strongly provides system usability by returning the matching files in ranked order concerning to certain relevance criteria, thus moving close towards the practical action of privacy preserving data presenting services in cloud.

**Boolean Keyword Search:** Boolean systems allowed customers to specify their information need using a combination of Boolean operators AND, OR and NOT. Boolean systems have several disadvantages, for example there are no any features of document ranking, and it is very difficult for a customer to make a good search request. Thus, the drawback of existing system specifies the important need for new techniques that support searching flexibility.

## IV. CONCLUSION

In this paper, we propose an efficient searchable symmetric encryption scheme to support wildcard search where one wildcard can represent any number of characters. By analysis of computation and storage complexity, we show that our scheme ismore efficient than previous schemes.We also propose that the new scheme is secure against adaptive attackers by chosen appropriate keywords. Moreover our scheme can support dynamic operation, i.e., addition and deletion. Our wildcard search technique is of independent

interest. We try to formalize and solve the problem of providing efficient fuzzy search for remotely stored data in cloud computing. We design two more advanced techniques (i.e., Grambased and Symbol-based tree traverse search techniques) to construct efficient fuzzy keyword sets. By providing security, we show that the proposed solution is secure and privacy-preserving. Experimental results demonstrates the efficiency of our proposed solution. We will continue to research on security mechanisms that support search ranking that sorts the searching results according to the relevance search and semantics that takes into consideration conjunction of keywords, sequence of keywords, and even the complex natural language semantics to produce highly relevant search results.

## V. ACKNOWLEDGEMENT

We would like to thank, first and foremost, Almighty God, without his support this work would not have been possible. We would also like to thank all the faculty members of Mount Zion college of engineering, for their immense support.

## REFERENCE

[1] D. Song, D.Wagner, and A. Perrig, "Practical Techniques for Searches on Encrypted Data".
[2] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, and P. Paillier, "Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions," Journal of Cryptology, Volume 21, Number 3, Pages 350-391, 2008.
[3] M. Bellare, A. Boldyreva, and A. O'Neill, "Deterministic and Efficiently Searchable Encryption," in Proc. of Crypto 2007, Volume 4622 of LNCS. Springer-Verlag, 2007.
[4] J. W. Byun, D. H. Lee, and J. Lim, "Efficient Conjunctive Keyword Search on Encrypted Data Storage System," Lecture Notes in Computer Science, Volume 4043, Public Key Infrastructure,