# Traditional Searchable Encryption Security of Fuzzy Keyword in Cloud

[1]T. Gangadhar Rao, [2]Ch. Raja jacob
[1]Dept. of SE, Nova College of Engineering & Tech, Jangareddygudem, AP, India
[2]Dept. of CSE, Nova College of Engineering & Tech, Jangareddygudem, AP, India

**Abstract**
It has been Cloud Computing, more and more sensitive information being centralized into the cloud. it the protection of data privacy, sensitive data usually have to be encrypted before outsourcing, which makes effective data uti- lization a very challenging task. Which is traditional searchable encryption schemes allow a user to securely search over encrypted data through keywords and selectively retrieve files of interest, these techniques support only exact keyword search. That is, there is no tolerance of minor typos and format inconsistencies which, on the other hand, are typical user searching behavior and happen very frequently. This significant drawback makes existing techniques unsuitable in Cloud Computing as it greatly affects system usability, rendering user searching experiences very frustrating and system efficacy very low. In this paper, for the first time we formalize and solve the problem of effective fuzzy keyword search over encrypted cloud data while maintaining keyword privacy. Fuzzy keyword search greatly enhances system usability by returning the matching files when users' searching inputs exactly match the predefined keywords or the closest possible matching files based on keyword similarity semantics, when exact match fails. In our solution, we exploit edit distance to quantify keywords similarity and develop an advanced technique on constructing fuzzy keyword sets, which greatly reduces the storage and representation overheads. Through rigorous security analysis, we show that our proposed solution is Specific and privacy-preserving, while correctly realizing the goal of fuzzy keyword findout.

**Keywords**
???????????? Is Missing ????????????

## I. Introduction

It has been Cloud Computing more and more sensitive information are being centralized into the cloud, such as emails, personal health records, government documents, etc. By storing their data into the cloud, the data owners can be relieved from the burden of data storage and maintenance so as to enjoy the on-demand high quality data storage service. However, the fact that data owners and cloud server are not in the same trusted domain may put the oursourced data at risk, as the cloud server may no longer be fully trusted. It follows that sensitive data usually should be encrypted prior to out- sourcing for data privacy and combating unsolicited accesses. However, data encryption makes effective data utilization a very challenging task given that there could be a large amount of outsourced data files. Moreover, in Cloud Computing, data owners may share their outsourced data with a large number of users. The individual users might want to only retrieve certain specific data files they are interested in during a given session. One of the most popular ways is to selectively retrieve files through keyword.

## II. Related Work

Important Plaintext fuzzy keyword. Nowdays importance of fuzzy search has received attention in the context of plaintext searching in information retrieval community. It waas addressed this problem in the traditional information- access paradigm by allowing user to search without using try-and-see approach for finding relevant information based on approximate string those files are back which is set net works completely impractical in cloud computing scenarios. Such keyword-based search technique allows users to selectively retrieve files of interest and has been widely applied in plaintext Extreamly, data encryption restricts user's abil- ity to perform keyword search and thus makes the traditional plaintext search methods unsuitable for Cloud Computing. Besides this, data encryption also demands the protection of keyword privacy since keywords usually contain important information related to the data files. Although encryption of keywords can protect keyword privacy, it further renders the traditional plaintext search techniques useless in this scenario.

The specific encrypted data, searchable encryp- tion techniques have developed in recent years .Explorely encryption schemes usually build up an index for each keyword of interest and associate the index with the files that contain the keyword. By integrating the trapdoors of keywords within the index information, effective keyword search can be realized while both file content and keyword privacy are well-preserved. Although allowing for performing searches securely and effectively, the existing searchable encryption techniques do not suit for cloud computing scenario since they support only exact keyword search. That is, there is no tolerance of minor typos and format inconsistencies. It is quite common that users' searching input might not exactly match those pre-set keywords due to the possible typos, such as Illinois and Ilinois, representation inconsistencies, such as PO BOX and P.O. Box, and/or her lack of exact knowledge about the data. The naive way to support fuzzy keyword search is through simple spell check mechanisms. However, this approach does not completely solve the problem and sometimes can be ineffective due to the following reasons: on the one hand, it requires additional interaction of user to determine the correct word from the candidates generated by the spell check algorithm, which unnecessarily costs user's extra computation effort; on the other hand, in case that user accidentally types some other valid keywords by mistake (for example, search for "hat" by carelessly typing "cat"), the spell check algorithm would not even work at all, as it can never differentiate between two actual valid words. Thus, the drawbacks of existing schemes signifies the important need for new techniques that support searching flexibility, tolerating both minor typos and format inconsistencies.

In this paper, we focus on enabling effective yet privacy-matching. At the first glance, it seems possible for one to directly apply these string matching algorithms to the context of searchable encryption by computing the trapdoors on a character base within an alphabet. However, this trivial construction suffers from the dictionary and statistics attacks and fails to achieve the search privacy.

### A. Specific Searchable Encryption

Traditional searchable encryption has been widely studied in the context of cryptography. Among those works, most are focused on efficiency improvements and security definition formalizations. The first construction of searchable encryption was proposed by Song in which each word in the document is encrypted independently under a special two-layered encryption construction.

Encrypted set of file identifiers whose corresponding data files contain the keyword. As a complementary approach, Boneh et al. [5], presented a public-key based searchable encryption scheme, with an analogous scenario to that of [3]. Note that all these existing schemes support only exact keyword search.

## III. Problem Formulation

In this paper, we consider a cloud data system consisting of data owner, data user and cloud server. Given a collection of n encrypted data files $X=(F_1, F_2, \ldots, F_N)$ stored in the cloud server, a predefined set of distinct keywords $W=(w_1, w_2, ..., w_p\}$, the cloud server provides the search service for the authorized is appropriately done. An authorized user types in a request to selectively retrieve data files of his/her interest. The cloud server is responsible for mapping the searching request to a set of data files, where each file is indexed by a file ID and linked to a set of keywords.

## IV. The Straightforward Approach

Before introducing our construction of fuzzy keyword sets, we first propose a straightforward approach that achieves all the functions of fuzzy keyword findout.

Induction method. First, we prove it holds when n* = 1. There are nine cases should be considered: If w* is derived from the operation of deletion from both $w_i$ and w, then, $ed(w_i, w) \leq 1$ because the other characters are the same except the character at the same position. If the operation is deletion from $w_i$ and f (•) is equal to f (sk, •) or a random function. A has an access to an oracle $O_f$ (•) that takes as input secret value x and returns f (x). Upon receiving any request of the index computation, A answers it with request to the oracle $O_f$ (•). After making these trapdoor queries, the adversary outputs.

## V. Constructions of Effective Fuzzy Keyword Search in Cloud

The key idea behind our secure fuzzy keyword search is two-fold:

1. Building up fuzzy keyword sets that incorporate not only the exact keywords but also the ones differing slightly due to minor typos, format inconsistencies, etc.
2. Designing an efficient and secure searching approach for file retrieval based on the resulted fuzzy keyword sets.

## VI. Conclusion

In this paper, for the first time we formalize and g fuzzy search for achieving effective utilization of remotelsolve the problem of supporting efficient yet privacy-preserviny stored encrypted data in Cloud Computing. We design an advanced technique (i.e., wildcard-based technique) to construct the storage-efficient fuzzy keyword sets by exploiting a significant observation on the similarity metric of edit distance. Based on the constructed fuzzy keyword sets, we further propose an efficient fuzzy keyword search scheme. Through rigorous security analysis, we show that our proposed solution is securely traditionaly.

## References

[1] Google,"Britney spears spelling correction", Referenced [Online] Available: http://www.google.com/jobs/britney.html, June 2009.

[2] M. Bellare, A. Boldyreva, A. O'Neill,"Deterministic and efficiently searchable encryption", in Proceedings of Crypto 2007, Vol. 4622 of LNCS. Springer-Verlag, 2007.

[3] D. Song, D. Wagner, A. Perrig,"Practical techniques for searches on encrypted data", in Proc. of IEEE Symposium on Security and rivacy'00, 2000.

[4] E.-J. Goh,"Secure indexes", Cryptology ePrint Archive, Report 2003/216, 2003, [Online] Available: http://www.eprint.iacr.org/.

[5] D. Boneh, G. D. Crescenzo, R. Ostrovsky, G. Persiano, "Public key encryption with keyword search", in Proc. of EUROCRYP'04, 2004.

[6] B. Waters, D. Balfanz, G. Durfee, D. Smetters,"Building an encrypted and searchable audit log", in Proc. of 11th Annual Network and Distributed System, 2004.

[7] Y.-C. Chang, M. Mitzenmacher,"Privacy preserving keyword searches on remote encrypted data", in Proc. of ACNS'05, 2005.

[8] R. Curtmola, J. A. Garay, S. Kamara, R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions", in Proc. of ACM CCS'06, 2006.

Mr T.Gangadharrao well known Author and excellent teacher Received B.Tech(CSIT) and (M.Tech (SE)) from NOVA College of Engg and Tech, jangareddygudem,WG DT, AP. Jawaharlal Nehru Technological University is working as Asst Professor in Computer Science and Engineering fromAyaan College of Engineering and Technology, He has 2 years of teaching experience in various engineering colleges. To his credit couple of publications both national and international conferences /journals. His area of Interest includes OperatingSystems,Database Management System, Compiler Design, mobile computing, computer organization and other advances in computer Applications.

Mr Ch.Raja Jacob, well known Author and excellent teacher Received M.C.A and M.Tech (CSE) from Acharya Nagarjuna university is working as Associate Professor and HOD, Department of MCA, M.Tech Computer science engineering, Nova college of Engineering and Technology, He is an active member of ISTE. He has 7 years of teaching experience in various engineering colleges. To his credit couple of publications both national and international conferences /journals. His area of Interest includes Data Warehouse and Data Mining, information security, flavors of Unix Operating systems and other advances in computer Applications.