Abstract may share their outsourced information with countless.

Abstract -As Cloud Computing is highly dominating technology in recent days, entiresensitive information is being stored onto the cloud. For maintaining data confidentiality, sensitive data are generally encrypted, which makes effective data utilizationa very complex task. The Existing searchable encryption schemes provides a wayfor secure search over encrypted data using keywords and retrieving thenecessary files. Whereas these techniques support only exact keyword search. That is, there is no acceptance of slight typos and format inconsistencieswhich are typical user searching behavior. Because of this drawback, theexisting techniques becomes incompatible in cloud computing, affecting thesystem usability.

This makes the user searching experiences very frustratingand results in low system efficiency. This paper includes the formalization andsolution of the problem of effective fuzzy keyword search over encrypted clouddata as well as preserving keyword privacy. Fuzzy keyword search helps toenhance the system usability by generating the matching files when users’searching inputs exactly match the predefined keywords or the closest possiblematching files based on keyword similarity semantics, when exact match fails. KEYWORDS: Encryption, Fuzzy Keyword, Cloud Computing I. INTRODUCTION As Cloud Computingis highly dominating technology in recent days, entire sensitive information isbeing stored onto the cloud, such as emails, healthrecords, government documents, personal data etc. By putting away theirinformation into the cloud, the data owners can be relieved from the burden ofdata storage and maintenance so as to enjoy the on-demand high quality datastorage service.

However, the cloud server may no longer be fully trusted. The sensitivedata usually should be encrypted prior to outsourcing for data privacy andpreventing unsolicited accesses. However, data encryption makes effective datautilization a very challenging task given that there could be a large amount ofoutsourced data files.

Besides, in Cloud Computing, information owners mayshare their outsourced information with countless. The individual users mightwant to only retrieve certain specific data files they are interested in duringa given session. One of the most popular ways is to selectively retrieve filesthrough keyword-based search instead of retrieving all the encrypted files backwhich is completely impractical in cloud computing scenarios. Suchkeyword-based search technique allows users to selectively retrieve files ofinterest and has been widely applied in plaintext search scenarios, such asGoogle search. Unfortunately, data encryption restricts user’s ability toperform keyword search and thus makes the traditional plaintext search methodsunsuitable for Cloud Computing. Besides this, data encryption also demands theprotection of keyword privacy since keywords usually contain importantinformation related to the data files.

Although encryption of keywords can protectkeyword privacy, it further renders the traditional plaintext search techniquesuseless in this scenario. To securely search over encrypted data, searchableencryption techniques have been developed in recent years. Searchableencryption schemes usually build up an index for each keyword of interest andassociate the index with the files that contain the keyword. By integrating thetrapdoors of keywords within the index information, effective keyword searchcan be realized while

both file content and keyword privacy are well-preserved. Although allowing for performing searches securely and effectively, theexisting searchable encryption techniques do not suit for cloud computingscenario since they support only exact keyword search. That is, there is no toleranceof minor typos and format inconsistencies. It is quite common that users' searching input mightnot exactly match those pre-set keywords due to the possible typos, representation inconsistencies, and/or her lack of exact knowledge about thedata.

The naive way to support fuzzy keyword search is through simple spellcheck mechanisms. However, this approach does not completely solve the problemand sometimes can be ineffective due to the following reasons: on the one hand, it requires additional interaction of user to determine the correct word fromthe candidates generated by the spell check algorithm, which unnecessarilycosts user's extra computation effort; on the other hand, when there are caseswhere user by mistake types some othervalid keywords (for example, search for " hat" by carelessly typing " cat"), thespell check algorithm would not even work at all, as it can never differentiatebetween two actual valid words. In this way, the downsides of existing plansimplies the imperative requirement for new methods that help lookingadaptability, enduring both minor grammatical mistakes and arrangementirregularities. In this paper, we are concentrating on enablingeffective yet privacy-preserving fuzzy keyword search in Cloud Computing. This paper includes theformalization and solution of the problem of effective fuzzy keyword searchover encrypted cloud data as well as preserving keyword privacy. Fuzzykeyword search helps to enhance the

system usability by generating the matchingfiles when users’ searching inputs exactly match the predefined keywords or theclosest possible matching files based on keyword similarity semantics, whenexact match fails. The edit distance is used to quantify keywordssimilarity and developing a novel technique, i. e.

, a wildcard-based technique, for the construction of fuzzy keyword sets. This technique eliminates the needfor computing all the fuzzy keywords and the resultant size of the fuzzykeyword sets is significantly reduced. Based on the constructed fuzzy keywordsets, the efficient fuzzy keyword search scheme is proposed.