In relevancy to the keywords [18]. in

In5, authors have proposed practical symmetric searchable encryption method. Inthis scheme the file is encrypted word by word. To search for a keyword, usersends the encrypted keyword and the key to the cloud. This key shall be used tooperate on the encrypted user data and then decrypted keyword shall be used tosearch in decrypted data.

The drawback of this scheme is that the wordfrequency will be revealed. In 6, the first public key encryption withkeyword search (PEKS) was proposed that lead to asymmetric searchableencryption method. The scheme suffers frominference attack (illegitimate knowledge of data in cloud) on trapdoor searchableencryption method. In 7 8, different techniquesthat work on encrypted data were discussed, along with comparative study ofdifferent searchable and homomorphic encryption schemes.

These existing solutions are not sufficient to protect data in cloud from unauthorizedusers because of low degree of transparency. Since the cloud user and the cloudprovider are in the different trusted domain, the outsourced data may beexposed to the vulnerabilities 10 11 12 13 14 15. To preserve thedata privacy we need to design a searchable algorithm that works on encrypteddata 16. The search techniques may use single keyword or multiple keywords17. In larger database the search may result in many documents to be matchedwith keywords. This causes difficulty for a cloud user to go through alldocuments. Search based on ranking is another solution, wherein the documentsare ranked based on their relevancy to the keywords 18.

Insearchable encryption related studies, computation time and computationoverhead are the two most frequently used parameters for analyzing theperformance of their schemes. Computation time (also called “ runningtime”) is the length of time required to perform a computational processfor example searching a keyword, generating trapdoor etc. Computation overheadis related to CPU utilization in terms of resource allocation measured in time.

Thus, an effective high performance multi-keyword rankedsearch over the encrypted cloud data is required. In9 19, authors have proposed & analyzed performance of two efficient searchableencryption schemes: CRSA/B+ tree and ECC/B+ tree. Inthis paper, the performance of ECC/B+ tree is analyzed under multi-userenvironment and compared the same with single user.