

A Study on Privacy Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data

Mr. Aditya Sanjay Shukla

M. Tech Student, Department of Computer Engineering

Shri Sant Gadge Baba College of Engineering and Technology, Bhusawal, Maharashtra, India

Abstract: *The advent of cloud computing, data owners are motivated to outsource their complex data management systems from local sites to commercial public cloud for great flexibility and economic savings. But for protecting data privacy, sensitive data has to be encrypted before outsourcing, which obsoletes traditional data utilization based on plaintext keyword search. Thus, enabling an encrypted cloud data search service is of paramount importance. Considering the large number of data users and documents in cloud, it is crucial for the search service to allow multi-keyword query and provide result similarity ranking to meet the effective data retrieval need. Related works on searchable encryption focus on single keyword search or Boolean keyword search, and rarely differentiate the search results. In this paper, for the first time, we define and solve the challenging problem of privacy-preserving multi-keyword ranked search over encrypted cloud data (MRSE), and establish a set of strict privacy requirements for such a secure cloud data utilization system to become a reality. Among various multi-keyword semantics, choose the efficient principle of “coordinate matching”, i.e., as many matches as possible, to capture the similarity between search query and data documents, and further use “inner product similarity” to quantitatively formalize such principle for similarity measurement. With the great advent of the cloud computing the data owners are intent for outsource the complex data. As the encryption is done there is a necessary for the encrypted cloud data search service is importance. The stored data is relatively large so as, required multiple keywords in the search query and return document in the order of their relevance to these keywords searched. In this paper, the survey on searchable encryption focus on multiple keyword search*

Keywords: Privacy, Keyword Search, Multiple Keyword Search, Encryption