

**CHENNAI – PONDICHERRY**

**MULTI-OWNER KEYWORD SEARCH OVER SHARED DATA WITHOUT SECURE CHANNELS IN THE CLOUD**

**Abstract:**

Searchable encryption allows cloud users to outsource the massive encrypted data to the remote cloud and to search over the data without revealing the sensitive information. Many schemes have been proposed to support the keyword search in a public cloud. However, they have some potential limitations. First, most of the existing schemes only consider the scenario with the single data owner. Second, they need secure channels to guarantee the secure transmission of secret keys from the data owner to data users. Third, in some schemes, the data owner should be online to help data users when data users intend to perform the search, which is inconvenient. In this paper, we propose a novel searchable scheme which supports the multi-owner keyword search without secure channels. More than that, our scheme is a non-interactive solution, in which all the users only need to communicate with the cloud server. Furthermore, the analysis proves that our scheme can guarantee the security even without secure channels. Unlike most existing public key encryption based searchable schemes, we evaluate the performance of our scheme, which shows that our scheme is practical.