

**CHENNAI – PONDICHERRY**

**SECURE K-NN QUERY ON ENCRYPTED CLOUD DATA**

**WITH MULTIPLE KEYS**

**Abstract:**

The k-nearest neighbors (k-NN) query is a fundamental primitive in spatial and multimedia databases. It has extensive applications in location-based services, classification & clustering and so on. With the promise of confidentiality and privacy, massive data are increasingly outsourced to cloud in the encrypted form for enjoying the advantages of cloud computing (e.g., reduce storage and query processing costs). Recently, many schemes have been proposed to support k-NN query on encrypted cloud data. However, prior works have all assumed that the query users (QUs) are fully-trusted and know the key of the data owner (DO), which is used to encrypt and decrypt outsourced data. The assumptions are unrealistic in many situations, since many users are neither trusted nor knowing the key. In this paper, we propose a novel scheme for secure k-NN query on encrypted cloud data with multiple keys, in which the DO and each QU all hold their own different keys, and do not share them with each other; meanwhile, the DO encrypts and decrypts outsourced data using the key of his own. Our scheme is constructed by a distributed two trapdoors public-key cryptosystem (DT-PKC) and a set of protocols of secure two-party computation, which not only preserves the data confidentiality and query privacy but also supports the offline data owner. Our extensive theoretical and experimental evaluations demonstrate the effectiveness of our scheme in terms of security and performance.