Abstract

Data mining has wide variety of real time application in many fields such as financial, telecommunication, biological, and among government agencies. Classification is the one of the main task in data mining. For the past few years, due to the increment in various privacy problem, many conceptual and feasible solution to the classification problem have been proposed under different certainty prototype. With the increment of cloud computing users have an opportunity to offload the data and processing to the cloud, in an encrypted form. The data in the cloud are in encrypted form, existing privacy preserving classification systems are not relevant. This paper reviews how to perform privacy preserving k-NN classification over encrypted data in the cloud. The recommended protocol preserves privacy of data, protect the user query, and hide the access mode.

References

1. P. Mell and T. Grance, “The nist definition of cloud computing (draft), NIST special
Review on k-Nearest Neighbor Classification over Semantically Secure Encrypted Relational Data

publication” vol. 800, p. 145, 2011.
2. Subodh Gangan, “A Review of Man-in-the-Middle Attacks”.

**Index Terms**

Computer Science Databases

**Keywords**

Security, k-NN classifier, outsourced databases, encryption