KNN CLASSIFICATION FOR ENCRYPTED QUERCY DATA IN CLOUD

Dr. D. Keran Hanirex, Dr. A. Muthu Kumaravel,
1 Associate Professor & Head, Department of Computer science,
2 Dean – Arts & Science, BIHER
1, 2 Faculty of Arts & Science, BIHER
1, 2 Chennai-73
1 keranahanirex.cse@bharathuniv.ac.in, 2 dean.arts@bharathuniv.ac.in

Abstract:

Data mining consists of various applications in financial and medical. Data Mining perform various tasks. Classification is one of the main task in data mining. In this paper classification is integrated in Cloud computing. Whenever the user created data in offload that can be encrypted and sent to the cloud. This paper uses classification technique for security in cloud. This paper implements KNN classification and prove its efficiency.

Keywords : Security, Classification , KNN classifier, encryption, Security

Introduction:

Data mining is the process of exploring hidden pattern from the database. Data mining also known as Knowledge Discovery[15,16,17,18,19,20] in Databases. To avoid data overhead the data can be offloaded to the cloud by the companies. Cloud computing provide access to secure data[1]. Assume that if one company stores the data in offline to the cloud. Suppose if the company search particular data the query should be generated at the user side and securely sent to the cloud through the encryption scheme.

Currently we are having various encryption techniques to hide the user access pattern data. This system uses KNN classification for identifying classification pattern.

Literature Survey:

Various encryption scheme are introduced. Shamir proposed secret encryption scheme which uses random prime number generation for the key. This method is also not safe against intruders[2]. In earlier system if the client’s private key is exposed, anyone can access the secure data[3]. Various privacy preserving techniques have been introduced to secure data in cloud environment[4]. Paper [5] proposes harmonic encryption scheme for security of data. Secure multiparty model has been proposed to solve the various security issues in Cloud environment. Various classification techniques have been proposed in data mining[6,7]. This paper uses KNN classification[21,22,23,24,25,26,27] scheme for secure data. This method uses euclidean distance for classification of data based on the queries by maintaining privacy of data[8].
System Architecture:

Modules:

User Interface Design: To associate with server client must give their client id and secret key to interface the server. Server will maintain data transfer and downloading of information. This system uses LIC data for analysis.

User Process Module: This module download client information.

Secure multiplication (SM): This module provide encryption process.

Secure Minimum(SM): This process generates key.

Decrypt classified data: This module gives decrypted classified data.

Results & Discussions:

This paper uses LIC data. The client given the query to the server. The query is encrypted and the data are classified based on KNN classification [9,10,11, 12,13,14] algorithm. The results are encrypted and returned back to the client.

Sample Screenshots:
Conclusion:

In this paper we have implemented the secure classification data using KNN classification algorithm. This paper presents security of encrypted data for a query using secure multiplication technique. This paper uses classification technique which identify the data related to the query.
References:

15. D. Kerana Hanirex, Dr. K. P. Kaliyamurthie, “Mining Frequent Itemsets in Association Rule Mining Using Improved SETM Algorithm”, Springer: Artificial Intelligence and Evolutionary


