IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 06-07

Implementation Of K-Nn Classification Over Secure Encrypted Relational Data

[1]Aniket Bobade, [2]Rashmi Mishra, [3]Shewta Moon, [4]Anukshka Indurkar,
[5]Rashmi Ghuse , [6]Mr. Yuvraj Suresh Suryawanshi
Abha Gaikwad-Patil College Of Engg (Final Year Student)

Abstract: *Now a day's data mining has been used in many fields such as banking, medicine, scientific research and among government agencies. Classification is one of the commonly used tasks in data mining applications. For the last two decade, due to the rise of various privacy issues, many theoretical and practical solutions to the classification problem have been proposed under different security tasks. However, todays demand of cloud computing, users now have the big scope to outsource their data, in encrypted form, as well as the data mining tasks to the cloud. Since the data on the cloud is in encrypted form, existing privacy preserving classification methods or techniques are not applicable. In this project, proposed a secure k-NN classifier model over the encrypted data in the cloud. The proposed k-NN protocol protects the confidentiality of the data, user's input query, and data access patterns. The aim of our proposed work is the first to develop a secure k-NN classifier over encrypted data under the standard semi-honest model.*

I. Introduction

Today's digital infrastructure supports innovative ways of storing, processing, and disseminating data. In fact, we can store our data in remote servers, access reliable and efficient services provided by third parties, and use computing power available at multiple locations across the network. Furthermore, the growing adoption of portable devices (e.g., PDAs, mobile phones) together with the diffusion of wireless connections in home and work environments have led to a more distributed computing scenario. These advantages come at a price of higher privacy risks and vulnerabilities as a huge amount of (private) information is being circulated and stored, often not under the direct control of its owner. Be that as it may, when information are encoded, independent of the fundamental encryption plan, performing any information mining assignments turns out to be extremely difficult without ever unscrambling the information. There are other security concerns, shown by the accompanying sample. Data mining over encrypted data (denoted by DMED) [3] on a cloud also needs to protect a client's record when the record is a part of a data mining process. However cloud can also abstract useful and sensitive information about the outsource data items by observing the data access patterns even if the data are encrypted. Therefore, the privacy/security requirements of the DMED problem on a cloud are of three types: (1) privacy of the encrypted data, (2) privacy of a user's query record, and (3) hiding data access patterns

SOFTWARE REQUIREMENTS

Software Specifications

Operating System :	Windows
Front End :	Java, JSP, netbeans
Back End :	mysql

HARDWARE REQUIREMENTS

1. Hard Disk – 500 GB.
2. RAM – 4 GB.
3. Processor – Dual Core or Above.
4. Mouse.
5. Keyboard.
6. Monitor.
7. Printer.

II. Conclusion

To protect user privacy, many privacy-preserving classification techniques have been proposed over the last two decade. The existing techniques are not applicable to out sourced database environment s where the data resides in encrypted form on a third- party server. This paper proposed a new privacy-preserving k-NN classification protocol over encrypted data in the cloud. Our proposed protocol protects the confidentiality of the

data, user's input query, and secures the data access patterns. We also calculated the performance of our protocol under different parameter settings. Since improving the efficiency of SMIN n is an import ant first step f or improving the performance of our PPkNN protocol.