Abstract

There is a huge database which contains some private and public information. When we are mining the useful information from the enterprise data, there can be issues regarding disclosure of the private data. Many times, the sensitive data can be directly or indirectly derived from the answered queries, to overcome these issues we extend the differential privacy model. In this privacy model, source database table is divided into some parties which hold different attributes for the same set of individuals. We have addressed the problem of private data exposure, which can be prevented by forming vertically partitioned databases. This partitioning is by an exponential mechanism algorithm which guarantees that the other party can't derive extra information from the answered query. The proposed algorithm also provides the security for the data which is release from the scatter pattern. To improve query response time of the system some schemes are used like Vertical Partitioning Scheme (VPS), Statistics Collector, and Partitioning Generator.

References

- N. Mohammed, D. Alhadidi, B. C. M. Fung, "Secure Two-Party Differentially
Vertically Partitioning of Database for Secured Data Release

Private Data Release for Vertically Partitioned Data, "Proc. IEEE TRANSACTION ON DEPENDABLE AND SECURE COMPUTING Volume. 11, No. 1, Jan/Feb 2014, pp. 59-70


Index Terms

Computer Science
Secutiry
Keywords
Secure Data Integration; VPS; Statistics Collector; Partitioning Generator.