Abstract

Association rule mining discovers correlations between different itemsets in a transaction database. It provides important knowledge in business for decision makers. While most of previous studies concern the mining task in a centralized scenario, the mining procedure does
not necessarily involve a single party only. For example, the database owner may outsource the mining task to a third party service provider. The database is sent to the service provider and the service provider computes and returns the association rules for the database owner. As another situation, different companies cooperate together to find out the global trend in the industry. The companies have to share the statistical information on their databases with others to find out the global rules. All these examples show that mining procedures may involve parties other than database owner. In such cases, we need to satisfy (1) data security to prevent dishonest parties from stealing information in the database and (2) result integrity to prevent dishonest parties from corrupting the mining result. In this paper, we summarize our research work in ensuring security of association rule mining in some common scenarios. To be specific, we will discuss (i) security issues in incremental distributed association rule mining; (ii) security issues in outsourcing of association rule mining.

References

- Cloud service provider,

Index Terms

Computer Science

Emerging Trends in Technology
Keywords
Association Rule Mining  Service Provider  Database  Outsourcing  Distributed