Security of Outsourcing of Association Rule Mining - Review

Shumin Guo

Problem Description

Outsourcing transactional data for association rule mining has the requirement of protecting sensitive data and sensitive association rules. This paper proposes an algorithm to deal with this problem.

Contribution of this paper

This paper has proposed a secure encryption scheme based on one-to-n substitution encryption and transforms sensitive transactions non-deterministically, while at the same time, correct decrytion is guaranteed. Comprehensive formal analysis is given about the enhanced one-to-n encryption algorithm including the decrytion guarantee. In the proposed algorithm, fake items are added to increase the difficulty of breaking the ciphers. Also, this paper defines algorithms to recover association from the encrpyted rules and the computational complexity is analyzed.

The author also suggested parameters to control the complexity by controlling the length of fake items and the mapping. And experimental results show that the proposed algorithm is efficient.

Weaknesses of this paper

The security analysis can be a little more comprehensive. No discussion about attacking sensitive association rules is given in the paper.