

## **Effective mining on large databases for intrusion detection**

### **ABSTRACT**

Data mining is a common automated way of generating normal patterns for intrusion detection systems. In this work a large dataset is customized to be suitable for both sequence mining and association rule learning. These two different mining methods are then tested and compared to find out which one produces more accurate valid patterns for the intrusion detection system. Results show that higher detection rate is achieved when using apriori algorithm on the proposed dataset. The main contribution of this work is the evaluation of the association rule learning that can be used for further studies in the field of database intrusion detection systems.

**Keyword:** Data mining; Apriori; Sequence mining; Database intrusion detection