In this paper, we propose data mining approach for database intrusion detection. In each database, there are a few attributes or columns or columns that are more important or sensitive to be tracked or sensed for malicious modifications as compared to the other attributes. Our approach concentrates on mining pre-write as well as post-write data dependencies among the important or sensitive data items in relational database. These dependencies are generated in the form of association rules. Any transaction that does not follow these dependency rules are identified as malicious. We also suggest removal of redundant rules in our proposed algorithm to minimize the number of comparisons during detection phase.

References


of International Conference on Pattern Recognition and Machine Intelligence (PReMi'05), 660-665.


Index Terms

Computer Science Security
Keywords

Data Mining, Intrusion Detection System, Data Dependency, Sensitive Attributes.