Detection and prevention of malicious activities on RDBMS relational database management systems

Abstract :

Insider attacks formed the biggest threaten against database management systems. There are many mechanisms have been developed to detect and prevent the insider attacks called Detection of Malicious Activities in Database Systems DEMIDS. The DEMIDS consider as one of the last defenses mechanism of the database security system. There are many mechanisms that have been developed to detect and prevent the misuse activities like delete, and update data on the database systems. These mechanisms utilize auditing and profiling methods to detect and prevent the malicious activities. However these mechanisms still have problems to detect the misuse activities such as limit to detect the malicious data on authorized commands. This study will address these problems by propose a mechanism that utilizes dependency relationship among items to detect and prevent the malicious data by calculate a number of relations among data items. If the number of relations among items is not allowed any modification or deletion then the mechanism will detect activity as malicious activity. The evaluation parameters such as detect, false positive and false negative rate use to evaluate the accuracy of proposed mechanism.