عنوان مقاله:
کاربرد الگوریتم های داده کاوی زمان واقعی درسیستم های تشخیص نفوذ

محل انتشار:
اولین همایش ملی رویکردهای نوین در مهندسی کامپیوتر و بازیابی اطلاعات (سال: 1392)

تعداد صفحات اصل مقاله: 5

نویسنده:
تهمینه مبادی فر - *کارشناسی ارشدفناوری اطلاعات*

خلاصه مقاله:
این مقاله نگاهی دارد به بررسی الگوریتم های داده کاوی سیستم های تشخیص نفوذ دریک محیط زمان واقعی هدف ازداده کاوی برپایه سیستم های تشخیص نفوذ کشف الگوهای رفتاری کاربران و برنامه ها است وشامل اطلاعات درمورد تشخیص نفوذداده کاوی اهمیت داده کاوی مبتنی برIDS و تکنیکهای داده کاوی که به سیستم تشخیص نفوذاعمال شده می باشد سیستم های تشخیص نفوذی که بر اساس داده کاوی طرحی شده اند درشبکه های کوچک و محلی دارای عملکردبسیارخوبی هستند ولی درشبکه های بزرگ بدلیل تولید هشدارهای اشتباه مثبت ومنفی درزمینه حملات شناخته شده استفاده میگردد این روش برمبنای اطلاعاتی که پس ازوقوع هرحمله ازرفتارهای آ« حمله و تحلیل آ«ها جمع اوری و ثبت میگردد استوار است بدین شکل سیستم میتواند با استفاده ازاین روش حملات اتی را شناسایی و جلوی نفوذوحمله را به شبکه بگیرد تحلیل برروی داده های یک حمله به منظوراستخراج امضا توسط کارشناسان خبره و سیستم های داده کاوی خاص انجام میگیرد دراین مقاله سعی داریم با استفاده ازتعاریف نفوذوداده کاوی به بررسی کاربردهای داده کاوی درتشخیص نفوذ بپردازیم

کلمات کلیدی:
Data Mining, Intrusion Detection Systems, Support Vector Machine