عنوان مقاله:
بالا بردن کارایی سیستم تشخیص نفوذ با روش ترکیبی داده کاوی و انتخاب ویژگی

محل انتشار:
دومین کنگره سراسری فناوریهای نوین ایران با هدف دستیابی به توسعه پایدار (سال: ۱۳۹۴)

تعداد صفحات اصل مقاله: ۷

نویسندگان:
سعید مزرعه - آموزشکده فنی و حرفه ای سما،دانشگاه آزاد اسلامی واحد سوسنگرد، سوسنگرد، ایران

سید محسن هاشمی - آموزشکده فنی و حرفه ای سما،دانشگاه آزاد اسلامی واحد سوسنگرد، سوسنگرد، ایران

عارف سیاحی - آموزشکده فنی و حرفه ای سما،دانشگاه آزاد اسلامی واحد سوسنگرد، سوسنگرد، ایران

خلاصه مقاله:
سیستم های تشخیص نفوذ وظیفه ی شناسایی و تشخیص هر گونه استفاده های غیرمجاز به سیستم، سوء استفاده و یا آسیب رسانی توسط هر دو دسته ی کاربران داخلی و خارجی را بر عهده دارند. سیستم های تشخیص نفوذ به صورت سیستم های نرم افزاری و سخت افزاری ایجاد شده و هر کدام مزایا و معایب خاص خود را دارند. سرعت و دقت از مزایای سیستم های سخت افزاری است و عدم شکست امنیتی آن ها توسط نفوذگران، قابلیت دیگر این گونه سیستم ها می باشد. تحقیق در زمینه تشخیص نفوذ برای مدت طولانی بیشتر روی تکنیک های تشخیص ناهنجاری و مبتنی بر سوء استفاده متمرکز شده است. در حالی که تشخیص بر اساس سوء استفاده، به طور کلی در محصولات تجاری به علت دقت بالا پیش بینی مورد علاقه بوده و در پژوهش های دانشگاهی تشخیص ناهنجاری به طور معمول به عنوان یک روش قوی تر با توجه به پتانسیل نظری آن برای مقابله با حملات جدید است. ما در این مقاله به ارائه یک روش ترکیبی داده کاوی به همراه تکنیک کاهش ویژگی و الگوریتم های درخت تصمیم پرداختیم. پس از تجزیه و تحلیل آماری که در این مجموعه داده ها انجام شد ارزیابی عملکرد سیستم های تشخیص نفوذ را به درصد قابل توجهی افزایش دادیم.

کلمات کلیدی:
الگوریتم های ترکیبی ، داده کاوی ، نفوذ ، تشخیص نفوذ ، کاهش ویژگی