عنوان مقاله:
ارائه یک روش ترکیبی داده کاوی و یادگیری ماشین به منظور تشخیص نفوذ در شبکه های کامپیوتری

محل انتشار:
کنفرانس ملی علوم مهندسی، ایده های نو (۸) (سال: 1393)

تعداد صفحات اصل مقاله: 6

نویسنده:
مصطفی برومند زاده - *دانشگاه پیام نور، عضو هیئت علمی گروه فنی مهندسی کامپیوتر و فناوری اطلاعات، خوزستان، ایران*

خلاصه مقاله:
افزایش کارایی سیستم های تشخیص نفوذ که امروزه به عنوان یکی از عناصر اصلی زیر ساخت های امنیت در بسیاری از سازمان ها می باشند چالشی انکار ناپذیر است. این سیستم ها، مدل ها و الگوهای سخت افزاری و نرم افزاری هستند که به خودکار کردن فرآیندها می پردازند. سیستم تشخیص نفوذ در قالب یک آلارم دهنده به کاربران عمل میکند، که گاهاً این آلارم ها صحیح و در برخی موارد نادرست می باشند. دراین مقاله به منظور مقاله با این حالات، از سیستم های تشخیص نفوذ مبتنی بر داده کاوی استفاده شده و نهایتاً با ارائه یک روش ترکیبی از روش های دسته بندی و تکنیک های کاهش ویژگی، کارایی سیستم های تشخیص نفوذ را 96.20 % بهبود بخشیدیم.

کلمات کلیدی:
نفوذ، تشخیص نفوذ، سیستم های تشخیص نفوذ، دسته بندی حملات