

عنوان مقاله:

بکارگیری تکنیک های داده کاوی جهت دسته بندی حملات و افزایش کارایی سیستم تشخیص نفوذ

محل انتشار:

همایش ملی مهندسی رایانه و مدیریت فناوری اطلاعات (سال: 1393)

تعداد صفحات اصل مقاله: 7

نویسندگان:

مهدی چعبی اهواری - دانشجوی کارشناسی ناپیوسته، رشته کامپیوتر، موسسه جهاد دانشگاهی خوزستان، ایران

محمد خدامرادی - عضو هیئت علمی دانشگاه آزاد اسلامی واحد ایذه، خوزستان، ایران

محمد خدایار - دانشگاه آزاد اسلامی واحد علوم و تحقیقات فارس، باشگاه پژوهشگران جوان و نخبگان، فارس، ایران

خلاصه مقاله:

سیستم های تشخیص نفوذ، سیستم هایی نرم افزاری یا سخت افزاری هستند که در واقع این سیستم ها جهت اعلان خطر استفاده می شوند. هر چه درصد این هشدارها بیشتر باشد، صحت، دقت و تشخیص صحیح آنها از اهمیت ویژه ای برخوردار است. روش های متعددی برای کمک به بالا بردن اعلان این هشدارها پیاده سازی شده اند. هر کدام از این روشها تا درصدی می تواند به ما در تشخیص حملات کمک کند. در این مقاله به مقایسه سه الگوریتم پرکاربرد و سریع Naïve Bayes، SVM، C4.5 در این زمینه می پردازیم. نتایج حاصل نشان از بهترین روش و دیگر پارامترها مرتبط می باشد.

کلمات کلیدی:

تشخیص نفوذ، داده کاوی، دسته بندی ترکیبی، Naïve Bayes، SVM، C4.5

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/282617>

