عنوان مقاله:
سیستم های تشخیص نفوذ داده کاو محور با الگوریتم یادگیری ماشین

محل انتشار:
اولین همایش تخصصی برق و کامپیوتر (سال: 1393)

تعداد صفحات اصل مقاله: 15

نویسندگان:
یونس قائدی - *دانشجوی کارشناسی ارشد نرم افزار، دانشگاه علوم و تحقیقات فارس، دانشکده فنی مهندسی، شیراز*

فرانک طاهری بروجنی - *دانشجوی کارشناسی ارشد نرم افزار، دانشگاه علوم و تحقیقات فارس، دانشکده فنی مهندسی، شیراز*

آیناز هاشمی نژاد - *دانشجوی کارشناسی ارشد نرم افزار، دانشگاه علوم و تحقیقات فارس، دانشکده فنی مهندسی، شیراز*

خلاصه مقاله:
در این پروژه قصد معرفی سیستم های تشخیص نفوذ بر مبنای داده کاوی و معرفی راه کارهای داده کاوی در جهت ارتقا سیستم های تشخیص نفوذ را داریم. به دلیل افزایش اطلاعات جمع آوری شده در شبکه که در فاز حسابرسی انجام میشود می توان از این داده ها در جهت تشخیص و حتی پیشگیری نفوذ استفاده کرد. با توجه به حجم بالای داده های در گیر در مسئله تشخیص نفوذ باید از روش هایی جهت کاهش این حجم داده برای بدست آوردن الگوهای ترافیکمشکوک و سالم استفاده کند. داده کاوی یکی از روش های شناخته شده و کارآمد جهت استخراج اطلاعات ارزشمند از حجم انبوهی از داده ها است. اهمیت سیستم های تشخیص نفوذ در آنجا به اوج خود می رسد که قبل از اینکه حمله بهاتمام برسد وقوع آن را گزارش کند و مانع از آسیب های احتمالی شود. بنابراین تشخیص نفوذ عبارت است از فرایندشناسایی و پاسخ به فعالیتهای مخرب که به صورت هدفمند، منابع شبکه را مورد تهاجم قرار می دهد. سیستم های تشخیص نفوذ از نظر نوع تشخیص به 2 گروه قابل دسته بندی هستند: تشخیص بر اساس امضا و تشخیص بر اساسناهنجاری. درتشخیص بر اساس امضا، امضا معادل با یک تهدید از قبل شناخته شده است. این تشخیص عبارت است از روند مقایسه رویداد های مشاهده شده با امضاهای شناخته شده به گونه ای که بتوان حمله ممکن را شناخت. تشخیص بر اساس امضافقط در شناسایی تهدیدات از قبل شناخته شده بسیار موثر است. تشخیص بر اساس ناهنجاری عبارت است از مقایسهرویدادهای مشاهده شده با فعالیت های نرمال تا میزان اختلاف و تفاوت آنها مشخص شود. ویژگی اصلی تشخیص بر اساس ناهنجاری این است که می تواند برای حملات ناشناخته و جدید کاملا موثر باشد. هنگامی که داده های جدیدبررسی و تحلیل می شوند، مدل ها باید متناسب با این داده ها بروز شوند که این بروز رسانی مدل ها خود به عنوان بزرگترین چالش در این مقاله بررسی می گردد.

کلمات کلیدی: