

عنوان مقاله:

ارایه روشی جدید جهت توسعه الگوریتم K-Medoids به منظور تولید داده آموزشی کارا در سیستم های تشخیص نفوذ

محل انتشار:

بیست و دومین کنفرانس ملی سالانه انجمن کامپیوتر ایران (سال: 1395)

تعداد صفحات اصل مقاله: 6

نویسندگان:

لیلا خلوتی - دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات- شبکه، دانشگاه صنعتی شیراز، شیراز

رضا جاویدان - عضو هیات علمی دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی شیراز، شیراز

خلاصه مقاله:

با گسترش روز افزون استفاده از اینترنت و تهدیدهای امنیتی ناشی از آن، توسعه سیستم های موثر تشخیص نفوذ از اهمیت زیادی برخوردار شده است. به طور معمول در این نوع سیستم ها از روش های مختلف یادگیری ماشین و داده کاوی جهت تشخیص حمله ها استفاده می شود. از آنجا که کیفیت مجموعه داده ی آموزشی بکار گرفته شده در سیستم های تشخیص نفوذ نقش اساسی را در بهبود کارایی این نوع سیستم ها ایفا می کند، در این پژوهش الگوریتمی جهت ایجاد یک مجموعه داده ی آموزشی کارا بر پایه ی تغییر الگوریتم معروف K-Medoids مطرح شده است. معمولا خوشه بندی بهینه ی داده ها در الگوریتم K-Medoids به دو عامل تعداد خوشه ها و مقادیر اولیه ی مراکز خوشه ها بستگی دارد، که تعداد خوشه ها توسط کاربر و مقادیر اولیه بصورت تصادفی انتخاب می شوند. در روش پیشنهادی در این مقاله، این دو شاخص به گونه ای موثر و بدون نیاز به دخالت کاربر انتخاب شده اند و با استفاده از مراکز خوشه های ایجاد شده مجموعه داده ی آموزشی کارایی تولید شده است. در انتها جهت دسته بندی داده های تست، الگوریتم طبقه بندی Naïve Bayes بکارگرفته شده است. مجموعه داده ی اولیه مورد استفاده در این مقاله، KDD CUP'99 می باشد. بر اساس نتایج آزمایش های انجام گرفته، دقت، نرخ تشخیص و نرخ اعلان اشتباه ایجاد شده توسط روش مطرح شده در این مقاله به ترتیب برابرند با 93.6، 88.71 و 08.03. نتایج مطرح شده نشان می دهند که مجموعه داده ی آموزشی تولید شده توسط روش ارایه شده در این مقاله، کارایی بالاتری را به نسبت روش بسیار با کیفیت 10-fold cross validation در هر سه مورد ذکر شده فراهم می کند.

کلمات کلیدی:

سیستم تشخیص نفوذ، KDD CUP'99، خوشه بندی، K-Medoids، مجموعه داده، Naïve Bayes

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/635651>

