عنوان مقاله:
مقایسه و بررسی الگوریتم های داده کاوی قانون محور و ماشین بردار پشتیبان برای تشخیص نفوذ

محل انتشار:
همایش مهندسی کامپیوتر و توسعه پایدار با محوریت شبکه های کامپیوتری، مدلسازی و امنیت سیستم ها (سال: 1392)

تعداد صفحات اصل مقاله: 8

نویسندگان:
حسن فضلی مقصودی - *دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات دانشگاه علوم و فنون مازندران*

حسین مومنی - *استادیار دانشگاه علوم کشاورزی و منابع طبیعی گرگان*

خلاصه مقاله:
با رشد فناوری اطلاعات،امنیت شبکه به عنوان یکی از مباحث مهم و چالش بسیار بزرگ مطرح است. سیستم های تشخیص نفوذ، مولفه اصلی یک شبکه امن است. سیستم های تشخیص نفوذ ستنی نمی توانند خود را با حملات جدید تطبیق دهند از این رو سیستم های تشخیص نفوذ مبتنی بر دادهکاوی امروزه پیشنهاد میشود .مشخص نمودن الگوهای در حجم زیاد داده،کمک بسیار بزرگی به ما میکند. متدهای داده کاوی با مشخص نمودن یک برچسب دودویی (بسته نرمال، بسته ناهنجار) و همچنین مشخص نمودن ویژگی ها و خصیصه با الگوریتم های دسته بندی می توانند داده غیر نرمال تشخیص دهند. از همین رو دقت و درستی سیستم های تشخیص نفوذ افزایش یافته و باتبع امنیت شبکه بالا میرود.در این روش ما الگوریتم های مختلف قانون محور و ماشین بردار پشتیبان را روی مجموعه داده خود تست کرده و بهترین الگوریتم RULE Induction singleattribute است که دقت آن 82.45% است.

کلمات کلیدی:
سیستم تشخیص نفوذ، دادهکاوی، بسته، قانون محور، ماشین بردار پشتیبان