عنوان مقاله:
بررسی و تشخیص نفوذ با استفاده از الگوریتم های داده کاوی

محل انتشار:
چهارمین کنفرانس ملی پژوهش های کاربردی در علوم برق و کامپیوتر و مهندسی پزشکی (سال: 1399)

تعداد صفحات اصل مقاله: 15

نویسندگان:
صادق بهادری
ناصر مدیری

خلاصه مقاله:
سیستم های تشخیص نفوذ، مولفه اصلی یک شبکه امن است. سیستم های تشخیص نفوذ سنتی نمی توانند خود را با حملات جدید تطبیق دهند از این رو امروزه سیستم های تشخیص نفوذ مبتنی بر داده کاوی مطرح گردیده اند. مشخص نمودن الگوهای در حجم زیاد داده، کمک بسیار بزرگی به ما میکند. روشهای داده کاوی با مشخص نمودن یک برچسب دودویی (بسته نرمال، بسته غیرنرمال) و همچنین مشخص نمودن ویژگیها و خصیصه با الگوریتم های دسته بندی میتوانند داده غیر نرمال تشخیص دهند . از همین رو دقت و درستی سیستمهای تشخیص نفوذ افزایش یافته و در نتیجه امنیت شبکه بالا میرود. در این مقاله ما مدلی پیشنهادی ارائه می نماییم که الگوریتم های مختلف دسته بندی را روی مجموعه داده خود تست نموده و نتایج شبیه سازی نشان میدهد در درخت تصمیم الگوریتم J48 ، شبکه عصبی الگوریتم Neural net ، شبکه بیزین الگوریتم HNB ، مدل کاهل الگوریتم K-STAR، در ماشین بردار پشتیبان الگوریتم LibSVM و در مدل قانون محور الگوریتمRule Induction Single Attribute دارای بهترین جواب از نظر پارامترهای مختلف ارزیابی برای سیستم تشخیص نفوذ است. بین تمامی الگوریتمها با این مجموعه داده، الگوریتم J48 دارای بالاترین مقدار درستی به میزان 85.49%، دارای بالاترین میزان دقت به مقدار 86.57% و دارای بالاترین مقدار یادآوری به مقدار 86.57% میباشد.

کلمات کلیدی:
داده کاوی، کشف تقلب، یادگیری بانظارت، تشخیص نفوذ و حملات