عنوان مقاله:
تشخیص نفوذ به شبکه به کمک داده کاوی و استفاده از یادگیری ماشین به روش ماشین بردار پشتیبان

محل انتشار:
فصلنامه کارافن, دوره 17, شماره 4 (سال: 1399)

تعداد صفحات اصل مقاله: 21

نویسندگان:
امیر عباس نامجوی راد - *عضو هیئت علمی ، دپارتمان مهندسی برق و کامپیوتر، آموزشکده شهید دادبین ، دانشگاه فنی حرفه ای استان کرمان، ایران.*

مهدی دادگرپور - *دانشجوی کارشناسی ارشد، دپارتمان مهندسی فناوری اطلاعات، دانشکده آموزش های الکترونیکی، دانشگاه شیراز، شیراز، ایران.*

خلاصه مقاله:
با توجه به گسترش روزافزون شبکههای کامپیوتری، تشخیص نفوذ به شبکه، یکی از اجزای اصلی برقراری امنیت در شبکههای کامپیوتری شناخته میشود که ابزار اصلی آن، کنترل ترافیک شبکه و تحلیل رفتارهای کاربران است. یکی از راههای اجرای چنین سیستمهایی، استفاده از دستهبندیها میباشد که با استفاده از مشخص کردن الگوها در حجم زیاد داده، کمک بزرگی به ما میکند. با استفاده از روشهای دادهکاوی و مشخص کردن یک برچسب دودویی (بسته نرمال، بسته غیرنرمال) و همچنین مشخص کردن ویژگیهای دادهها که میتوان دادههای غیرنرمال را تشخیص داد؛ از این رو دقت درستی سیستم تشخیص نفوذ، افزایش مییابد و در نتیجه، امنیت شبکه بالا میرود. مدل پیشنهادی در این مقاله، به بررسی الگوریتم ماشین بردار پشتیبان در انتخاب خصیصهها و تاثیر استفاده از الگوریتمهای یادگیری ماشین در میزان دقت و میزان تشخیص نفوذ در سیستم میپردازد که نتایج حاصل نشان میدهد که استفاده از این الگوریتم، به افزایش میزان دقت و تشخیص درست هشدارها نسبت به روشهای قبلی میانجامد.

کلمات کلیدی:
سیستم تشخیص نفوذ, الگوریتم, یادگیری ماشین, بردار پشتیبان, داده کاوی