عنوان مقاله:
مروری برروی‌کردهای انتخاب ویژگی و طبقه بندی در سیستم های تشخیص نفوذ

محل انتشار:
ششمین کنفرانس بین المللی پژوهش های کاربردی در کامپیوتر، برق و فناوری اطلاعات (سال: 1400)

تعداد صفحات اصل مقاله: 19

نویسندگان:
تکتم پازش - *گروه مهندسی کامپیوتر،واحد مشهد،دانشگاه آزاد اسلامی،مشهد،ایران.*

عابد حسینی - *گروه مهندسی برق،واحد مشهد،دانشگاه آزاد اسلامی،مشهد،ایران.*

محمدعلی شیخ الطایفه - *گروه مهندسی عمران،واحد مشهد،دانشگاه فردوسی،مشهد،ایران.*

حسن شاکری - *گروه مهندسی کامپیوتر،واحد مشهد،دانشگاه آزاد اسلامی،مشهد،ایران.*

خلاصه مقاله:
سیستم تشخیص نفوذ دستگاه یا برنامه نرم افزاری است که شبکه یا سیستم ها را از نظر فعالیت های مخرب یا نقض خط مشی ها کنترل می کند. یکی از چالش های مهم در این زمینه، تشخیص درست حالت نرمال و حمله در سیستم می باشد . داده ها به طور کلی به دو دسته حمله و نرمال تقسیم می شوند. پژوهش های بسیاری در زمینه سیستم های تشخیص نفوذ مبتنی بر رو ش های یادگیری ماشین و یادگیری عمیق صورت گرفته است. روشهای صورت گرفته با وجود داشتن مزایایی که به همراه داشته اند به دلایلی از جمله پیچیدگی محاسباتی، زمان اجرای طولانی و دیگر موارد قادر به رسیدن به دقت مطلوب در سیستم های تشخیص نفوذ نبودهاند. همچنین به دلیل نوع وپیچیدگی حملات جدید افزایش دقت تشخیص همچنان به عنوان یک چالش باقی مانده است. دراین تحقیق به بررسی تکنیکهای یادگیری ماشین و یادگیری عمیق در زمینه افزایش دقت سیستمهای تشخیص نفوذ پرداخته ایم. نشان دادهایم که ترکیب این دو تکنیک در کنار روشهای پیش پردازش و انتخاب ویژگی میتوان دقت را در سیستمهای تشخیص نفوذ افزایش داد. همچنین بیشترین مجموعه داده مورد استفاده در سیستمهای تشخیص نفوذ NSL-KDD و ابزار پیاده سازی پایتون میباشد.

کلمات کلیدی:
سیستم تشخیص نفوذ،تکنیک های یادگیری ماشین، تکنیک های یادگیری عمیق، پایتون، پایگاه داده NSL-KDD

لینک ثابت مقاله در پایگاه سیویلیکا: