عنوان مقاله:
شناسایی بدافزار اندرویدی روز صفر با استفاده از شبکه های عصبی

محل انتشار:
فصلنامه پدافند الکترونیکی و سایبری, دوره 11, شماره 3 (سال: 1402)

تعداد صفحات اصل مقاله: 8

نویسنده:
بهزاد لک - *گروه فاوا - دانشگاه علوم انتظامی امین*

خلاصه مقاله:
با افزایش ضریب نفوذ اینترنت در زندگی و استفاده آحاد مردم از این فناوری در همه ابعاد، بکارگیری از دستگاه های گوشی تلفن همراه نیز به همین نسبت افزایش داشته است. این موضوع در کنار خلق مزایای فراوان، موجب گسترش و تسریع انتشار برخی برنامه های مخرب به نام بدافزار [۱]گردیده است. در این پژوهش سعی بر آن است که با استفاده از شبکه عصبی چندلایه و یادگیری ماشین تشخیص بدافزارهای روز صفر [۲]در تلفن های هوشمند صورت گیرد. برای این منظور از دیتاست [۳]استاندارد با بیش از ۱۵ هزار نمونه از انواع بدافزار و خوب افزار به صورت برچسب گذاری شده بهره گیری شده است. در مرحله پیش پردازش ابتدا با استفاده از نرمال سازی و یکسان سازی داده ها انجام می شود و با تجزیه وتحلیل مولفه های اصلی عمل انتخاب ویژگی صورت گرفته و از تعداد ۱۱۸۳ ویژگی تعداد ۲۱۵ ویژگی که واریانس بالاتری دارند انتخاب می شود و پس ازآن مدل پیشنهادی معرفی شده است که از طبقه بند شبکه عصبی چندلایه و الگوریتم بهینه سازی مبتنی بر آموزش و یادگیری است که با اعمال آن بر روی پایگاه داده های ذکرشده و مقایسه نتایج طبقه بندی آن با الگوریتم های ماشین بردار، الگوریتم ژنتیک ، نزدیک ترین همسایه و ... می توان دریافت که آموزش شبکه عصبی چندلایه یادگیری دقت و صحت را بالا می برد. نتایج استفاده از شبکه عصبی چندلایه مبتنی بر آموزش و یادگیری حاکی از دقت ۹۹% و صحت ۹۸% است.

کلمات کلیدی:
: بدافزار, اندروید, تجزیه و تحلیل, انتخاب ویژگی, یادگیری ماشین