عنوان مقاله:
استفاده از تکنیک یادگیری ماشین برای تحلیل و شناسایی بدافزار ها

محل انتشار:
چهارمین کنفرانس ملی مهندسی برق کامپیوتر و فناوری اطلاعات (سال: 1396)

تعداد صفحات اصل مقاله: 20

نویسندگان:
فرهنگ پدیداران مقدم - *استادیار گروه کامپیوتر، موسسه آموزش عالی اشراق بجنورد*

سعید فتاحی - *دانشجوی کارشناسی ارشد مهندسی نرم افزار کامپیوتر، موسسه آموزش عالی اشراق بجنورد*

خلاصه مقاله:
امروزه اینترنت به بخش ضروری کار مردم و زندگی تبدیل شده است. این امر شرایط ارتباطی مطلوب را برای بدافزارها فراهم می کند و در سال های اخیر اندروید نیز در سطح جهانی برای گوشی های هوشمند پیش بینی شده است. پیشرفت سریع اندروید و اینترنت افزایش تهدیدات بدافزارهایی که فعالیت های خطرناک را انجام می دهد، گسترش یافته است. بنابراین بدافزارها بی نهایت و سریع گسترش یافته و تبدیل به یکی از تهدیدات اصلی امنیت شبکه فعلی است. بدافزارها تکنیک های مختلفی را برای اجتناب از روش های ردیابی موجود برای تشخیص دقیق آن ها به چاش می کشد. شرکت های تحقیق و کمپانی ضدویروس ناکارآمدی روش تشخیص مبتنی بر امضاها را شناسایی کرده و به روش شناختی مبتنی بر دستگاه مبتنی بر یادگیری برای غلبه بر محدودیت های روش تشخیص متبنی بر امضا تغییر داده اند. اولین و مهم ترین گام در رویکرد شناسایی مبتنی بر ماشین استخراج ویژگی است. ویژگی ها شامل مجوز، کد بایت جاوا، ترافیک شبکه، تماس های سیستم و سایر موارد هستند. براساس ویژگی استخراج شده، تکنیک های شناسایی اندروید یادگیری مبتنی بر ماشین می تواند به تحلیل استاتیک، پویا و ترکیبی طبقه بندی شود. براساس فرآیند بدافزار، از ویژگی اصلی استخراج و انتخاب ویژگی برای تشخیص بدافزار، این مقاله الگوریتم یادگیری ماشین را مانند خوشه بندی، طبقه بندی و تحلیل ارتباط معرفی می کند. یادگیری مبتنی بر ویژگی نقشی حیاتی در ایجاد و حفظ امنیت ایفا می کند. تعیین نرم افزار براساس ویژگی های استخراج شده از ان چه یک فرآیند، خوب و چه بد، و به خصوص طبقه بندی به یک خانواده malware درست، امنیت سیستم عامل را بهبود می بخشد، و از اطلاعات کاربر حیاتی محاظت می کند. در این مقاله، ما یک سیستم طبقه بندی مبتنی بر ویژگی ترکیبی را برای نمونه های نرم افزارهای Android ارایه می کنیم. ویژگی های استاتیک مانند مجوزهای درخواست شده توسط کاربردهای تلفن همراه، بار الکتریکی پنهان، و ویژگی های پویا مانند API های API، خدمات نصب شده، اتصالات شبکه برای طبقه بندی استخراج می شوند. ما از یادگیری ماشینی و ارزیابی سطح در دقت طبقه بندی کننده های مختلف با استفاده از ویژگی های نرم افزارهای Android استفاده می کنیم و چگونه از الگوریتم یادگیری دستگاه برای بدافزار و انواع آن استفاده کنیم. از این رو، این مقاله به بررسی روش های مختلف تشخیص مبتنی بر یادگیری ماشین و ایجاد مسیرهای احتمال آینده می پردازد.

کلمات کلیدی:
یادگیری ماشین، طبقه بندی، تجزیه و تحلیل بدافزار، ویژگی، خوشه بندی و تجزیه و تحلیل انجمن