عنوان مقاله:
استفاده از روش n-gram ترکیبی مبتنی بر آپکد فایل ها برای شناسایی بدافزارها

محل انتشار:
اولین کنفرانس ملی مهندسی کامپیوتر و فناوری اطلاعات (سال: 1395)

تعداد صفحات اصل مقاله: 7

نویسنده:
صلاح دین بلوچی

خلاصه مقاله:
مدل های شناسایی بدافزار به دو دسته پویا و ایستا تقسیم می شوند. در روش پویا، رفتارهای برنامه به هنگام اجرا مورد تجزیه و تحلیل و در روش ایستا ساختار اسمبلی فایلها بدون در نظر گرفتن رفتار برنامه مورد تجزیه و تحلیل قرار می گیرد، پژوهش حاضر از راهکارهای ایستا می باشد که فایل های اجرایی آزمایشی را به آپکدهای تشکیل دهنده تجزیه نموده و به استخراج خواص مبتنی بر مدل n-gram ترکیبی به ازای مقدار n=4 اقدام می کند. این خواص استخراجی به فرمت ورودی سازگار به نرم افزار داده کاوی Weka داده شد، با استفاده از الگوریتم داده کاوی Random Forest آزمایشات صورت گرفت.

کلمات کلیدی:
شناسایی بدافزار، داده کاوی، Random Forest ، n-gram