عنوان مقاله:
ارایه روشی برای شناخت خودکار بدافزار با استفاده از الگوریتم کاوش الگوهای متوالی وشبکه عصبی

محل انتشار:
سومین کنفرانس ملی مهندسی برق و کامپیوتر سیستمهای توزیع شده و شبکه های هوشمند (سال: 1395)

تعداد صفحات اصل مقاله: 6

نویسندگان:
محمدعلی قدوسی محصل - *گروه کامپیوتر دانشگاه آزاد اسلامی واحد کاشان کاشان ایران*

مهدی اسماعیلی - *گروه کامپیوتر دانشگاه آزاد اسلامی واحد کاشان کاشان ایران*

خلاصه مقاله:
در این تحقیق، بر اساس توالیهای استخراج شده از مجموعه نمونه فایل،یک الگوریتم استخراج توالی موثر برای کشف الگوهای ترتیبی مخرب پیشنهادمیشود. این ساختار یک چارچوب ترکیبی متشکل از الگوکاوی و شبکه عصبی به نام ANNMD است. این ساختار شامل سه بخش است. بخش اول استخراج دستورات پرتکرار است. بخش دوم کاوش توالی الگوها را به عهده دارد و الگوهای توالی محتمل به خرابی را شناسایی میکند. در بخش سوم شبکه عصبی با استفاده ورودیهای بخش دوم آموزش دیده و بهعنوان مدل شناسایی بدافزار استفاده میشود. چارچوب داده کاوی توسعه یافته متشکل از روش الگو کاوی ترتیبی پیشنهادی است و طبقه بند ANN به خوبی می تواند الگوهای مخرب را از مجموعه نمونه فایل جمع آوری شده برای شناسایی نمونههای بدافزار جدید مورد استفاده قرار دهد. یک مطالعه تجربی جامع در مجموعه دادههای واقعی به منظور بررسی چارچوب تشخیصی ما انجام شد. نتایج تجربی نشان می دهد که چارچوب ما بهتر از دیگر روشهای تشخیص مبتنی بر دادههای کاوی در شناسایی فایلهای اجرایی مخرب جدید عمل می کند و در زمینه صحت6 درصد، دقت 8,5 درصد و بازخوانی مجدد 8 درصدبهتر عمل می کند.

کلمات کلیدی:
بدافزار، الگو کاوی، شبکه عصبی، کشف الگوهای ترتیبی