عنوان مقاله:

تشخیص بدافزار با استفاده از تکنیک های یادگیری ماشین

محل انتشار:

کنفرانس ملی فناوری های نوین در مهندسی برق و کامپیوتر (سال: 1396)

تعداد صفحات اصل مقاله: 11

نویسندگان:

زهرا شعبانی – دانشجوی کارشناسی ارشد، گروه مهندسی کامپیوتر، واحد ملایر، دانشگاه آزاد اسلامی، ملایر، ایران

حسن ظفری – استادیار گروه مهندسی کامپیوتر، واحد ملایر، دانشگاه آزاد اسلامی، ملایر، ایران

خلاصه مقاله:

در سال های اخیر با گسترش شبکه های کامپیوتری و افزایش دسترسی افراد به آن، این بستر اطلاعاتی به شکل فزاینده ای دستخوش انواع حملات گردیده است. عواملی از قبیل منافع مالی، اهداف سیاسی یا نظامی و نیز مقاصد شخصی سبب افزایش حوادث امنیتی در سیستم های اطلاعاتی میگردد. در نتیجه امنیت شبکه های کامپیوتری تبدیل به یکی از مهمترین دغدغه های اصلی کارشناسان شبکه و دیگر افراد مرتبط با شبکه ها شده است. طیف وسیعی از حملات و بدافزارها به دنبال رخنه و نفوذ در سیستم ها و سوءاستفاده از آنها هستند. در نتیجه ابزارهایی مانند دیوار آتش و آنتی ویروس ها به تنهایی قادر به تامین امنیت سیستم ها نیستند و سیستم های تشخیص نفوذ می توانند به شکل فعال استفاده های غیرمجاز و نیز سوءاستفاده از سیستم های اطلاعاتی توسط حمله گره ای داخلی و خارجی را شناسایی کنند. در این تحقیق بعد از تعریف نفوذ و سیستم تشخیص نفوذ، سعی شده است براساس الگوریتم ID3 و مجموعه داده KDD-CUP99 و با استفاده از زبان برنامه نویسی C، classifier# با دقت بالا برای تشخیص نفوذ ارایه شود.

کلمات کلیدی:

سیستم تشخیص نفوذ، یادگیری ماشین، درخت تصمیم .ID3، KDD-CUP99

لینک ثابت مقاله در پایگاه سیویلیکا: