عنوان مقاله:
کاربرد داده کاوی و متن کاوی درتشخیص ایمیل های فیشینگ

محل انتشار:
دومین همایش ملی پژوهش های مهندسی رایانه (سال: 1395)

تعداد صفحات اصل مقاله: 10

نویسندگان:
لعیا زنگی آبادی - *دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات، موسسه آموزش عالی بهمن یار، کرمان، ا یران*

علی ناصراسدی - *مربی گروه کامپیوتر، مجتمع آموزش عالی زرند، دانشگاه شهید باهنر کرمان، کرمان، ایران*

خلاصه مقاله:
از آنجا که رایج ترین روش برای شروع حملات فیشینگ ارسال ایمیل است تکنیک های متفاوتی برای تشخیص این نوع ایمیل هاوجود داردکه با توجه به پژوهش های گذشته می توان گفت تشخیص این نوع ایمیل ها به تنهایی و بدون کمک، کار آسانی نیستبلکه با استفاده از روش های داده کاوی و متن کاوی، موفقیت در تشخیص این نوع حملات بیشتر می شود. این مقاله یک مطالعهتحقیقاتی است که برای تشخیص حملات فیشینگ به بررسی روش های داده کاوی از طریق فراداده ایمیل و بررسی روش هایمتن کاوی، از طریق محتوای ایمیل می پردازد. همچنین با توجه به اینکه طبقه بندی ایمیل های فیشینگ یکی از مشکلات اساسیدر حوزه پژوهش های امنیتی آنلاین است توجه به تفاوت الگوریتم های تشخیص این حمله برای یافتن بهترین و بهینه ترین روشکلاس بندی و قرار دادن در پوشه هرزنامه ضروری است. نتایج نشان می دهد که در تشخیص ایمیل های فیشینگ با استفاده ازURL استفاده از یک الگوریتم یادگیری ماشین مانند شبکه عصبی ART روش کارایی است اما عملی نیست، همچنین در تشخیص و طبقه بندی با استفاده از متنکاوی محتوای ایمیل نیز الگوریتم ژنتیک کارایی بهتری دارد اما به علت اینکه درخت تصمیم باقوانین اگر آنگاه کار میکند و مراحل غیر واضح ندارد به کارگیری درخت تصمیم ترجیح داده می شود.

کلمات کلیدی:
فیشینگ ، داده کاوی، متن کاوی، طبقه بندی، یادگیری ماشین