نوزدهمین کنفرانس ملی سالانه انجمن کامپیوتر ایران
دانشکده مهندسی کامپیوتر، دانشگاه شهید بهشتی، تهران، ۱۵-۱۳ اسفندماه ۱۳۹۲

تشخیص نامه الکترونیکی جعلی در بانکداری الکترونیک با رویکرد داده کاوی

مرضیه حسنی [۱] ، زرین تاج برنایی [۲] ، علی اکبر نیک نفس [۳]

۱ دانشجوی کارشناسی ارشد دانشگاه علوم و تحقیقات ، بوشهر
hasanistar@yahoo.com
۲ استادیار ، پژوهشکده برق و فناوری اطلاعات، سازمان پژوهشهای علمی صنعتی ایران ، تهران
bornaee@irost.org
۳ استادیار ، گروه مهندسی کامپیوتر ، دانشگاه شهید باهنر کرمان ، کرمان
پژوهشکده برق و فناوری اطلاعات، سازمان پژوهشهای علمی و صنعتی ایران، تهران
Niknafs@uk.ac.ir

چکیده

نامه الکترونیک جعلی یکی از مسائل اصلی در دنیای اینترنت است که منجر به خسارت مالی زیادی برای سازمانها و کاربران شده است .در این مقاله ، تحقیق وسیعی درباره روشهایی که در حال حاضر برای شناسایی نامه های الکترونیک جعلی بکار می رود ، صورت گرفته است ؛ سپس یک مدل شناسایی نامه الکترونیک جعلی مطابق با روشهای داده کاوی ارائه می گردد . در این مدل، با توجه به ویژگیهای موثر استخراج شده و مجموعه داده موجود، روش داده کاوی دسته بندی برای تفکیک نامه های الکترونیک جعلی و غیر جعلی معرفی می شود . نتایج تحقیق نشان داد که روشهای دسته بندی داده کاوی، روشی موثر در امر تشخیصنامه های الکترونیکجعلی است. نرخ بالای صحت و نرخ تشخیص غلط پایین (FP) و مقایسه معیارهای مرسوم داده کاوی سایر دسته بندها نظیر F-measure–Recall–TP و منحنی های ROC و تحلیل انها، از دیگر یافته های این تحقیق است.

کلمات کلیدی : نامه های الکترونیک جعلی، دسته بندی، داده کاوی، بانکداری الکترونیکی

۱- مقدمه

۱-۱- نامه الکترونیک جعلی و نحوه عملکرد آن

نامه الکترونیک جعلی یکنوع خاص از پیام هرزنامه[1]است. چنین نامه های الکترونیک یک مکانیزم مجرمانه است که از یک شرکت قانونی یا بانک نشات میگیرد . سپس از طریق یک لینک تعبیه شده درون نامه الکترونیک ،جاعل سعی میکند که کاربر را به سمت وب سایت جعلی هدایت بکند که این وب سایتها بدین منظور طراحی شده اند که به صورت جاعلانه ای به اطلاعات مالی نظیر نام کاربری، کلمه عبور و شماره کارت اعتباری دسترسی پیدا بکنند[3-1]. نامه های الکترونیک جعلی یک حمله بالقوه به تجارت الکترونیک است چرا که آنها عادت دارند افراد یا سازمان های مالی تحت اینترنت را مورد حمله قرار دهند.طبق گزارش جرایم اینترنتی [۵]، حملات جعلی، با نرخ

[1]Spam