سومین کنفرانس بین المللی نوآوری و تحقیق در علوم مهندسی
گرجستان - تفلیس (۳۰ تیرماه ۱۳۹۸) آکادمی بین المللی علوم گرجستان
ICIRES 21 July 2019
www.icires.ir
info@icires.ir
CIU
NEW VISION UNIVERSITY NVU
Eco energy
GIAS

تشخیص حملات فیشینگ با انتخاب ویژگی مبتنی بر الگوریتم بهینه سازی پروانه

امیر زارع[۱] و کمال میرزائی[۲]
[۱]دانشجوی کارشناسی ارشد، دانشگاه آزاد اسلامی، واحد میبد، گروه کامپیوتر، ایران
amir30nov1993@gmail.com
[۲] عضو هیات علمی، دانشگاه آزاد اسلامی، واحد میبد، گروه کامپیوتر، ایران
k.mirzaie@maybodiau.ac.ir

چکیده – فیشنگ یک حمله مبتنی بر مهندسی اجتماعی یا بدافزار است که کاربران را به سمت صفحات جعلی در اینترنت هدایت نموده و اطلاعات مهم آنها را مورد سرقت قرار می‌دهد. شباهت صفحات جعلی به صفحات قانونی و اصلی باعث می‌شود که بیشتر کاربران فریب صفحات جعلی را خورده و اطلاعات مهم خود را در این صفحات درز نمایند. صفحات جعلی در اینترنت دارای مجموعه‌ای از ویژگی‌ها است که برای شناسایی حملات فیشینگ قابل استفاده است اما چالش مهم این روش‌های مبتنی بر داده‌کاوی در آن است که برخی ویژگی‌ها دارای اهمیت بیشتری بوده و برخی دیگر نیز اهمیت زیادی ندارند و دقت یادگیری را کاهش می‌دهند. انتخاب ویژگی یک مکانیزم موثر برای کاهش دادن خطای تشخیص حملات در یادگیری ماشین است از این جهت در این مقاله برای انتخاب ویژگی در تشخیص حملات فیشینگ از نسخه باینری شده الگوریتم بهینه‌سازی پروانه استفاده می‌شود. در روش پیشنهادی هر بردار ویژگی یک پروانه در نظر گرفته می‌شود و توسط این الگوریتم بردار ویژگی بهینه برای تشخیص فیشینگ استخراج می‌شود. نتایج پیاده‌سازی ما در محیط متلب و بر روی مجموعه داده فیشینگ نشان می‌دهد الگوریتم بهینه‌سازی پروانه می‌تواند با دقت بالا ویژگی‌های بهینه را تشخیص داده و دارای دقت و حساسیتی به ترتیب برابر ٪۹۸,۶۶ و ٪۹۷,۸۳ در تشخیص صفحات جعلی است و از طرفی نسبت به روش‌های مانند ماشین بردار پشتیبان، شبکه عصبی و درخت تصمیم‌گیری دقت بیشتری دارد.

کلید واژه- فیشینگ، سرقت اطلاعات، الگوریتم پروانه، انتخاب ویژگی

۱- مقدمه

وب‌سایتهای جعلی به عنوان یکی از تهدیدهای مهم در فناوری اطلاعات و تجارت الکترونیک به شمار می‌روند زیرا این صفحات بسیار شبیه صفحات قانونی بوده و اطلاعات کاربران را مورد سرقت قرار می‌دهند. حملات فیشینگ با استفاده از صفحات جعلی فضای وب را برای کاربران اینترنت ناامن نموده است و در این نوع حملات که می‌تواند مبتنی بر مهندسی اجتماعی یا مبتنی بر فریب توسط بدافزار می‌باشد یک کاربر به صورت خودکار یا توسط لینکهای جعلی به سمت صفحات وب جعلی هدایت شده و اطلاعات خود را در این صفحات وارد می‌نماید[۱]. فیشر با دریافت اطلاعات کاربران می‌تواند از آنها برای سرقت اطلاعات استفاده نماید. صفحات جعلی در اینترنت و حملات فیشینگ دارای مجموعه‌ای از ویژگی‌ها است که می‌تواند برای تشخیص صفحات جعلی استفاده شود. در بیشتر صفحات جعلی عمر دامنه اندک است زیرا این صفحات با سرعت ایجاد و سریع نیز شناسایی و حذف می‌شوند پس می‌توان از این ویژگی برای تشخیص صفحات جعلی و حملات فیشینگ استفاده نمود[۲]. اطلاعات مرتبط با دامنه فقط برای تشخیص حملات فیشینگ مهم نبوده بلکه اطلاعات مرتبط با لینک و آدرس نیز مهم می‌باشند و مشاهده می‌شود در بیشتر صفحات جعلی طول آدرس بیش از اندازه طولانی است[۳].