
بسم الله الرحمن الرحيم

گروه مهندسی کامپیوتر

پایان‌نامه برای دریافت درجه کارشناسی ارشد«MSc»

گرایش: شبکه‌های کامپیوتری

عنوان:

ارائه یک روش هوشمند تشخیص حملات فیشینگ با استفاده از الگوریتم بهینه‌سازی فاخته و شبکه عصبی مصنوعی

گروه مهندسی کامپیوتر

پایان‌نامه برای دریافت درجه کارشناسی ارشد «M.Sc.»

گرایش : شبکه‌های کامپیوتری

عنوان:

ارائه یک روش هوشمند تشخیص حملات فیشینگ با استفاده از الگوریتم بهینه‌سازی فاخته و شبکه عصبی مصنوعی

هیئت محترم داوران:

نام و نام خانوادگی استاد راهنما	تاریخ	امضا
نام و نام خانوادگی استاد داور	تاریخ	امضا
نام و نام خانوادگی استاد داور	تاریخ	امضا

تعهدنامه اصالت رساله دکتری یا پایان‌نامه کارشناسی ارشد دانشگاه آزاد اسلامی

این‌جانب ..... دانش‌آموخته مقطع کارشناسی ارشد ناپیوسته در رشته شبکه‌های کامپیوتری که در تاریخ از پایان‌نامه / رساله خود تحت عنوان**" ارائه یک روش هوشمند تشخیص حملات فیشینگ با استفاده از الگوریتم بهینه‌سازی فاخته و شبکه عصبی مصنوعی "** با کسب نمره ۱۹,۲۵ و درجه عالی دفاع نموده‌ام بدین‌وسیله متعهد می‌شوم :

۱ – این پایان‌نامه / رساله حاصل تحقیق و پژوهش انجام‌شده توسط این‌جانب بوده و در مواردی که از دستاوردهای علمی و پژوهشی دیگران (اعم از پایان‌نامه، کتاب، مقاله و .....) استفاده نموده‌ام، مطابق ضوابط و رویه موجود، نام منبع مورداستفاده و سایر مشخصات آن را در فهرست مربوطه ذکر و درج کرده‌ام.

۲ – این پایان‌نامه/ رساله قبلاً برای دریافت هیچ مدرک تحصیلی (هم‌سطح، پائین تر یا بالاتر) در سایر دانشگاه‌ها و مؤسسات آموزش عالی ارائه نشده است.

۳ چنانچه بعد از فراغت از تحصیل، قصد استفاده و هرگونه بهره‌برداری اعم چاپ کتاب، ثبت اختراع، و..... از این پایان‌نامه را داشته باشم، از حوزه معاونت پژوهشی واحد مجوزهای مربوطه را اخذ نمایم.

٤ – چنانچه در هر مقطع زمانی خلاف موارد فوق ثابت شود، عواقب ناشی از آن را می‌پذیرم و واحد دانشگاهی مجاز است با این‌جانب مطابق ضوابط و مقررات رفتار نموده و در صورت ابطال مدرک تحصیلی‌ام هیچ‌گونه ادعایی نخواهم داشت.

نام و نام خانوادگی

تاریخ و امضاء

به نکته زیر توجه شود

نمره از ۱۸,۱ تا ۲۰ با درجه عالی

نمره از ۱٦,۱ تا ۱۸ با درجه بسیار خوب

نمره از ۱٤,۱ تا ۱٦ با درجه خوب

معاونت پژوهش و فن آوری

به نام خدا

منشور اخلاق پژوهش

بایاری از خداوند سبحان و اعتقاد به اینکه عالم محضر خدا است و همواره ناظر بر اعمال انسان و به منظور پاسداشت مقام بلند دانش و پژوهش و نظر به اهمیت جایگاه دانشگاه در اعتلای فرهنگ و تمدن بشری ما دانشجویان و اعضاء هیئت علمی واحدهای دانشگاه آزاد اسلامی متعهد می گردیم اصول زیر را در انجام فعالیت های پژوهشی مد نظر قرار داده و از آن تخطی نکنیم:

۱-اصل حقیقت جویی: تلاش در راستای پی جویی حقیقت و وفاداری به آن و دوری از هرگونه پنهان سازی حقیقت

۲-اصل رعایت حقوق: التزام به رعایت کامل حقوق پژوهشگران و پژوهیدگان (انسان، حیوان و نبات) و سایر صاحبان حق

۳-اصل مالکیت مادی و معنوی: تعهد به رعایت کامل حقوق مادی و معنوی دانشگاه و کلیه همکاران پژوهش

۴-اصل منافع ملی: تعهد به رعایت مصالح ملی و در نظر داشتن پیشبرد و توسعه کشور در کلیه مراحل پژوهش

۵-اصل رعایت انصاف و امانت: تعهد به اجتناب از هرگونه جانب داری غیر علمی و حفاظت از اموال، تجهیزات و منابع در اختیار

۶-اصل رازداری: تعهد به صیانت از اسرار و اطلاعات محرمانه افراد، سازمان ها و کشور و کلیه افراد و ستادهای مرتبط با تحقیق

۷-اصل احترام: تعهد به رعایت حریم ها و حرمت ها در انجام تحقیقات و رعایت جانب نقد و خودداری از هرگونه حرمت شکنی

۸-اصل ترویج: تعهد به رواج دانش و اشاعه نتایج تحقیقات و انتقال آن به همکاران علمی و دانشجویان به غیر از مواردی که منع قانونی دارد

۹-اصل برائت: التزام به برائت جویی از هرگونه رفتار غیر حرفه ای و اعلام موضع نسبت به کسانی که حوزه علم و پژوهش را به شائبه های غیر علمی می آلایند.

فهرست مطالب

عنوان | صفحه

فهرست شکل‌ها

عنوان | صفحه

فهرست جداول

عنوان | صفحه

فهرست نمودارها

عنوان صفحه

چکیده

همزمان با رشد و توسعه تکنولوژی و فراگیر شدن استفاده از فضای اینترنت جهت تبادل و اشتراک‌گذاری اطلاعات و داده‌های کاربران مختلف، مهاجمین نیز از روش‌های گوناگون و با انگیزه‌های مختلف اقدام به سوءاستفاده، تخریب یا سرقت این اطلاعات می‌نمایند. فیشینگ، یکی از بزرگ‌ترین تهدیداتی است که عمده کاربران و مشاغل اینترنتی با آن مواجه هستند. تاکنون روش‌های متعددی برای کشف صفحات فیشینگ پیشنهاد گردیده است ولی ارائه روشی که به درستی قادر به تشخیص دقیق الگوهای شناخته شده قبلی براساس ویژگی‌های خاص وب‌سایت‌های فیشینگ و شناسایی حملات جدید باشد، هنوز هم یک مسأله چالش برانگیز است. در پایان‌نامه پیش رو مدلی ارائه شده است که از شبکه عصبی و الگوریتم فاخته به منظور تفکیک وب‌سایت‌های فیشینگ از نمونه‌های قانونی استفاده می‌نماید. با پیاده‌سازی این مدل بر روی مجموعه داده شامل ۱۱۰۵۵ صفحه فیشینگ و قانونی، نرخ تشخیص ۹۹,۰۶ درصد در تفکیک وب‌سایت‌های فیشینگ به‌دست آمده است که نسبت به روش‌های مشابه مورد مقایسه، نتایج بهتری ارائه می‌نماید.

کلمات کلیدی: تشخیص فیشینگ، شبکه عصبی، الگوریتم فاخته، بهینه سازی ازدحام ذرات

فصل اول

کلیات تحقیق

۱-۱-مقدمه

اینترنت نه‌تنها برای کاربران عادی، بلکه برای شرکت و سازمان‌های بزرگ جهت انجام فعالیت‌های تجاری برخط، بسیار مهم است. بسیاری از شرکت‌ها خرید، فروش و خدمات برخط را پیشنهاد می‌دهند. بنابراین کاربران اینترنت ممکن است توسط حملات مختلفی موردحمله قرار گیرند. این حملات می‌تواند باعث خسارات مالی شده و یا اطلاعات شخصی افراد را فاش کند. فیشینگ نوعی حمله اینترنتی است که هدف آن سرقت اطلاعات شخصی کاربران، مانند نام کاربری و رمز است. وب‌سایت‌های فیشینگ، با جعل ظاهر وب‌سایت اصلی این کار را انجام می‌دهند. ظاهر این وب‌سایت‌ها بسیار شبیه به وب‌سایت‌های اصلی طراحی می‌شود. فیشینگ به‌تلاش برای بدست آوردن اطلاعاتی مانند نام کاربری، گذرواژه، اطلاعات حساب بانکی و ... از طریق جعل یک وب‌سایت، آدرس ایمیل و ...گفته می‌شود. شبکه‌های اجتماعی و وب‌سایت‌های پرداخت آنلاین ازجمله اهداف حملات فیشینگ هستند [۱]. علاوه بر آن، ایمیل‌هایی که با این هدف ارسال می‌شوند و حاوی پیوندی به یک وب‌سایت هستند در اکثر موارد حاوی بدافزار هستند. همان‌طور که از تعریف فیشینگ مشخص است، موفقیت این نوع حملات، اغلب به فریفته‌شدن کاربر بستگی دارد. حملات فیشینگ مبتنی بر فریب، با بهره‌گیری از تکنیک‌های روانشناسی و تحریک احساس طمع، ترس و یا اعتماد کاربر، او را فریب می‌دهند. برای مثال، مهاجم ممکن است با نمایش پیشنهادهای ویژه و یا جوایز نقدی، کاربر را ترغیب به تکمیل یک فرم، مشاهده یک صفحه و یا دریافت یک فایل کرده و از این طریق اطلاعات او را سرقت کند. به‌دلیل سادگی و کارایی این روش، در سال‌های اخیر، حملات متعددی به این شیوه صورت گرفته و این آمار رو به

افزایش است. کاربران شبکه‌های اجتماعی و وب‌سایت‌های پرداخت آنلاین از جمله اهداف حملات فیشینگ هستند [۲].

راه‌حل‌های مختلفی جهت مقابله با فیشینگ توسعه داده شده‌اند. اما با این حال هنوز هم فقدان دقت و راه‌حل‌های بلادرنگ مشکل اساسی است، چون ترکیبی از ویژگی‌های کمی مانند تعداد اتصال یا عدم‌اطمینان می‌باشد. در سال‌های اخیر، بسیاری از الگوریتم‌های یادگیری ماشین برای حل مشکلات طبقه‌بندی توسعه یافته‌اند و به‌طور گسترده‌ای برای تشخیص وب‌سایت‌های فیشینگ بکار گرفته شده‌اند. بیشتر الگوریتم‌های یادگیری ماشین پارامترهای تعیین‌شده‌ای دارند، اما وفق دادن پارامترها با یک خروجی مطلوب دشوار است. حملات فیشینگ یکی از مهم‌ترین تهدیدات امنیتی است که به سرقت اطلاعات حساس کاربران می‌پردازد. در این پایان‌نامه روشی جهت شناسایی صفحات فیشینگ با استفاده از ویژگی‌ها آدرس سایت ارائه شده است.

۲-۱- بیان مسئله

با گسترش سریع اینترنت، تهدیدات امنیتی نیز به سرعت در حال افزایش هستند. یکی از مهم‌ترین این تهدیدات حملات فیشینگ است. فیشینگ یک وبسایت جعلی است که ظاهری همانند وب سایت قانونی دارد. آدرس‌های سایت فیشینگ به روش‌های مختلفی برای کاربران ارسال می‌شود که معروف‌ترین روش‌ها استفاده از ایمیل است. فیشینگ به نحوی کاربران را متقاعد می‌کند که ایمیل از سایت قانونی است و از آن‌ها می‌خواهد که بر روی لینک موجود در ایمیل کلیک کنند. کاربران با مراجعه به این وب‌سایت‌ها اطلاعات حساس خود از جمله نام کاربری، رمز عبور، اطلاعات کارت‌های بانکی و اعتباری خود را وارد می‌کنند. فیشینگ همچنین با استفاده از تکنیک‌های مهندسی اجتماعی به گمراه کردن کاربران اینترنتی می‌پردازد تا اطلاعات محرمانه آن‌ها را بدست بیاورد. در این تکنیک فیشرها با طراحی یک سایت که شبیه به سایت مورد نظر است، کار خود را آغاز می‌کنند. پس از انجام این مرحله آن‌ها باید روشی را پیدا کنند که کاربران را مجبور کند تا در سایت آن‌ها وارد شده و اطلاعات محرمانه خود را وارد کنند. این اطلاعات بوسیله فیشرها مورد سوء استفاده قرار می‌گیرند. تاکنون الگوهای مختلفی برای مقابله با حملات فیشینگ ارائه شده‌اند؛ اما با وجود

تمام این تلاش‌ها، خطر این حملات هنوز از میان نرفته است. یکی از مهم‌ترین دلایل این موضوع، قابلیت سازگاری مهاجمان با روش‌های مقابله و تغییر روند خود با هزینه اندک برای فریب آن‌هاست.

روش‌های ارائه شده برای مقابله با این‌گونه حملات نقاط ضعف خود را داشته و هیچ‌کدام به‌تنهایی ممکن است توانایی مقابله مؤثر با حملات فیشینگ را نداشته باشند. لزوم بررسی این تحقیق، ارائه راه‌کاری ترکیبی و اکتشافی جهت مقابله با حملات فیشینگ به‌صورت مؤثر و کارا بوده، به شکلی که با هزینه معقول و نرخ تولید نتایج اشتباه قابل قبول، امکان کشف حملات و طبقه‌بندی آن‌ها را داشته باشد.

۳-۱- ضرورت و اهمیت موضوع

اهمیت موضوع به این دلیل می‌باشد که روش‌های پیشرفته فیشینگ که توسط حمله‌کنندگانی خبره ابداع می‌شوند به شکل روزافزون در حال گسترش بوده و افراد تازه کار به‌واسطه ابزارهایی که در اینترنت یافت می‌شوند به‌راحتی امکان ایجاد وب‌سایت‌های فیشینگ را دارند. از این‌رو استفاده از تکنیک‌های مقابله با فیشینگ از قبیل لیست سفید، لیست سیاه، روش‌های مبتنی بر کشف و تشابه ظاهری کارایی خود را در مقابله با سایت‌های فیشینگ از دست داده‌اند. لیست‌های مجاز و غیرمجاز فقط هنگامی مؤثر می‌باشد که آدرس وب‌سایت‌های فیشینگ پیش‌تر در لیست‌ها ثبت شده باشد و درغیر صورت این روش‌ها ناکارآمد می‌باشد. بروزرسانی مداوم این لیست‌ها در این دو روش الزامی می‌باشد. باتوجه به وابستگی جهان امروز به خدمات مجازی و همچنین گستردگی حجم مبادلات اینترنتی و تجارت الکترونیک و در عین حال استفاده کاربران اینترنتی از شبکه‌های اجتماعی به شکل فراگیر، امکان سوء استفاده فیشرها از ضعف روش‌های موجود بیش از پیش فراهم آورده است. از این‌رو ارائه روشی ترکیبی و اکتشافی که توانایی پوشش نقاط ضعف روش‌های دیگر را داشته باشد، می‌تواند نقش مؤثری را در جلوگیری از افشای اطلاعات محرمانه کاربران و در نتیجه افزایش امنیت شبکه‌های اینترنتی ایفا کند [۳].

٤-١- نوآوری پایان‌نامه

در این پایان‌نامه با بکارگیری پارامترهای موثر در شناسایی صفحات فیشینگ، روشی برای شناسایی سایت‌های فیشینگ با دقت بالا، ارائه شده است. در این روش پیشنهادی از الگوریتم بهینه‌سازی ازدحام ذرات و ماشین بردار پشتیبان برای کاهش ویژگی‌ها استفاده شد. الگوریتم ماشین بردار پشتیبان به عنوان تابع هزینه و الگوریتم بهینه‌سازی ازدحام ذرات استراتژی جستجو است و در نهایت برای طبقه‌بندی صفحات به دو دسته‌ی فیشینگ و سالم از الگوریتم فاخته و شبکه عصبی استفاده خواهیم کرد، چون دقت دسته‌بندی بالایی دارد. در مرحله طبقه‌بندی الگوریتم فاخته، برای بهبود کارایی الگوریتم شبکه عصبی با این الگوریتم ترکیب می‌شود.

٥-١- اهداف پایان‌نامه

هدف کلی تحقیق حاضر ارائه چارچوبی جهت شناسایی صفحات و وب‌سایت‌های فیشینگ و در نتیجه جلوگیری از به سرقت رفتن اطلاعات محرمانه کاربران در فضای مجازی می‌باشد. بدیهی است چنین چارچوبی می‌تواند به مدیران امنیت و به‌طور کلی سیستم‌های امنیت، در محافظت و تضمین امنیت سیستم‌های تحت وب کمک شایانی نماید. همچنین با توجه به تکنیک‌های جدید سرقت اطلاعات با استفاده از صفحات فیشینگ، ارائه روشی برای مقابله با این تکنیک‌های مدرن که قابلیت بروزسازی خودکار و یادگیری روش‌های جدید مورد استفاده در حملات فیشینگ را داشته باشند، کمک شایانی به حفظ امنیت کاربران خواهد نمود.

علاوه بر هدف ذکر شده، این پایان‌نامه اهداف ویژه‌ای را نیز دنبال می‌کند. به‌ویژه این‌که تحقیق حاضر در صدد مشخص نمودن اهمیت شناسایی موثر سایت‌های فیشینگ می‌باشد. همچنین با بررسی و مقایسه روش‌های کشف و مقابله با فیشینگ سعی در آشکارسازی نقاط ضعف و قوت آن‌ها و در نتیجه تحلیل روش‌های مناسب جهت پوشش نقاط ضعف و بهبود نقاط قوت می‌باشد.

٦-١- ساختار پایان‌نامه

در ادامه پایان‌نامه به‌صورت زیر سازماندهی شده است.

در فصل دو انواع مختلف حملات فیشینگ بررسی شده است. در این فصل تمامی تکنیک‌های تشخیص فیشینگ و نحوه‌ی استفاده از آن‌ها به طور کامل شرح داده شده است. در فصل سوم مروری بر پیشینه‌های پژوهشی و کارهای انجام شده مرتبط با این پایان‌نامه پرداخته شده است و آخرین تحقیقات انجام شده در زمینه تشخیص فیشینگ مورد بررسی قرار گرفته است. در فصل چهارم معماری سیستم پیشنهادی مورد بحث قرارگرفته می‌شود. در فصل پنجم، شبیه‌سازی و ارزیابی روش پیشنهادی مطرح خواهد شد، درنهایت نتیجه‌گیری کلی از پایان‌نامه گرفته‌شده و پیشنهادهایی برای توسعه و بهبود روش‌های پیشنهادی، ارائه می‌شود.

فصل دوم

مبانی تحقیق

فیشینگ یک حمله پیچیده است که برای فریب کاربران در اینترنت استفاده می‌شود. به‌کسانی که این حملات را انجام می‌دهند در اصطلاح فیشر گفته می‌شود. هدف فیشرها بدست آوردن اطلاعات خاص از یک گروه از کاربران خاص در اینترنت است. اطلاعات کاربران می‌تواند شامل نام کاربری و کلمه عبور در شبکه‌های اجتماعی و یا شماره کارت اعتباری و کلمه عبور در وب‌سایت‌های بانکی و مؤسسات مالی باشد. فیشینگ در واقع یک تکنیک فریبنده است که از تکنولوژی پیشرفته اینترنت برای فریب کاربران استفاده می‌کند. فیشرها نه تنها از آسیب‌پذیری‌هایی که در پروتکل‌ها و وب موجود است استفاده می‌کنند بلکه از امکانات موجود در آن‌ها برای اهداف فریبکارانه خود استفاده می‌کنند.

۱-۲- حملات فیشینگ

فیشینگ یک تکنیک مهندسی اجتماعی[1] است که به‌وسیله یک هکر[2] یا حمله‌کننده[3] برای سرقت اطلاعات کاربران استفاده می‌شود. در این حالت حمله‌کننده وانمود می‌کند یک شخص یا یک سازمان مورد اعتماد است. امروزه اغلب کاربران با دنیای آنلاین عجین شده‌اند، در حالی‌که شاید از خطرات معمول این دنیا بی‌اطلاع باشند. یک هکر یا یک حمله‌کننده می‌تواند هر کسی را به‌راحتی در دام کلاهبرداری فیشینگ خود گرفتار کند. البته تمام این مسئله به کاربر بستگی دارد که برای شناسایی و ممانعت به‌عمل آوردن فیشینگ، هوشمندانه عمل

[1] Social Engineering
[2] hacker
[3] attacker