دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه

ISSN: 3060-6055

مدل تشخیص فیشینگ URL ها بر اساس یادگیری ماشین

پریسا دانشجو[1]*، سعید احمدی[2]

دانشیار،دانشکده فنی مهندسی،دانشگاه آزاد اسلامی- واحد تهران غرب،تهران،ایران [1]، Daneshjoo.p@wtiau.acir
دانشگاه آزاد اسلامی- واحد تهران غرب[2]، [2]Saeed.ahmadi.edu@gmail.com

چکیده

حمله‌های فیشینگ همیشه تهدیدات قابل توجهی برای امنیت اینترنت بوده‌اند. یکی از معمولی‌ترین شکل‌های فیشینگ، از طریق URLها است، جایی که مهاجمان، URLهای تقلبی را به شکل URLهای معتبر در می‌آورند تا کاربران گول بخورند و برروی آنها کلیک کنند. فنون یادگیری ماشینی، امیدهایی برای شناسایی URLهای فیشینگ به‌وجود آورده‌اند، اما اثربخشی آنها براساس رویکرد استفاده شده می‌تواند تغییر کند.

اهداف: هدف این پژوهش، پیشنهاد دو روش یادگیری ماشینی، «شبکه‌های عصبی کانوالی» (CNN) و «خود توجهی چندسره»(MHSA)، برای شناسایی URLهای فیشینگ است. علاوه بر آن، ارزیابی و مقایسه اثربخشی این رویکرد در مقایسه با روش ها و مدل های دیگر است.

روش تحقیق: یک مجموعه داده از URLها گردآوری و به آنها برچسب فیشینگ یا معتبر داده شد. عملکرد چندین مدل استفاده کننده از روش های یادگیری ماشینی مختلف، شامل CNN و MHSA، برای دسته بندی این URLها با استفاده از معیارهای مختلف، مانند دقت، صحت، فراخوانی و نمره F1، ارزیابی شد.

نتایج: نتایج نشان می‌دهند که ترکیب مدل‌های CNN و MHSA عملکرد بهتری نسبت به دیگر مدل‌های انفرادی دارد و به دقت 98.3٪ می‌رسد که در مقایسه با روش‌های نوین موجود، بهبود قابل توجهی در شناسایی URLهای فیشینگ فراهم می‌کند.

نتیجه‌گیری: ترکیب CNN و MHSA رویکردی موثر برای آشکارسازی URLهای فیشینگ است. این روش نسبت به روش‌های نوین موجود عملکرد بهتری دارد و روشی دقیق و مطمئن‌تر برای آشکارسازی URLهای فیشینگ فراهم می‌کند. نتایج این مطالعه، پتانسیل استفاده از روش‌های ترکیبی در بهبود دقت و اطمینان روش‌های آشکارسازی URL فیشینگ مبتنی بر یادگیری ماشینی را نشان می‌دهند.

کلمات کلیدی – فیشینگ؛ آدرس URL؛ یادگیری عمیق؛ لایه کانوالی؛ خود توجهی چندسر

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه

ISSN: 3060-6055

مقدمه

فیشینگ یکی از رایج ترین روش های دسترسی به داده های شخصی است [1]. برای به حداقل رساندن آسیب یک حمله فیشینگ، لازم است که آن را در کوتاه ترین زمان ممکن شناسایی کنیم. تقریباً تمامی انواع حمله فیشینگ از URLهای فیشینگ استفاده می‌کنند[1].

URLهای فیشینگ به وبسایت‌ها یا صفحات وبی لینک شده‌اند. این وبسایت ها یاصفحات وب به‌نحوی طراحی شده‌اند که شبیه وبسایت‌های معتبر و قانونی به نظر برسند، اما در واقعیت کار سایت‌های مخربی هستند که توسط مجرمان سایبری ایجاد شده‌اند. آن‌ها با استفاده از این وبسایت‌ها اطلاعات شخصی همچون اطلاعات ورود به حساب (لاگین)، شماره‌های کارت اعتباری و سایر داده‌های حساس را سرقت می کنند [1].

نمی‌توان بیشتر از این حد روی اهمیت تشخیص URLهای فیشینگ تاکید کرد، زیرا آن‌ها تهدید مهمی نسبت به افراد و سازمان‌ها هستند. در اینجا دلایلی راجع به ضرورت تشخیص URLهای فیشینگ را بیان می‌کنیم[1]:

1- حفاظت در برابر سرقت هویت: URLهای فیشینگ معمولاً برای فریب افراد و افشای اطلاعات لاگین، جزئیات حساب بانکی و سایر اطلاعات شخصی طراحی شده‌اند. افراد و سازمان‌ها می‌توانند با تشخیص این URLها از خود در برابر سرقت هویت، حفاظت کنند [1].
2- جلوگیری از زیان‌های مالی: حملات فیشینگ زیان‌های مالی شدیدی را به افراد و سازمان‌ها تحمیل می‌کنند. سازمان‌ها می‌توانند با تشخیص و مسدودکردن URLهای فیشینگ، از سرقت پول و داده‌های حساس توسط مجرمان سایبری جلوگیری کنند [1].
3- حفاظت در برابر بدافزار: URLهای فیشینگ معمولاً حاوی لینک‌هایی به نرم افزارهای مخرب هستند و این نرم افزارها در شرایط خاصی به رایانه یا شبکه آسیب می‌زنند. سازمان‌ها با تشخیص و مسدودسازی این URLهای فیشینگ، از آلوده شدن به بدافزار و رخنه داده‌ها جلوگیری کنند [1].
4- حفظ اعتماد: ممکن است سازمان‌هایی که قربانی حملات فیشینگ هستند اعتماد مشتریان، کارفرمایان و شرکای خود را از دست بدهند. سازمان‌ها با تشخیص و پیشگیری از حملات فیشینگ، اعتبارشان را حفظ و از گسترش اخبار منفی جلوگیری می کنند [1].

به‌طور خلاصه، تشخیص URLهای فیشینگ، نقش اساسی را در حفاظت در برابر سرقت هویت، زیان مالی، خنثی‌سازی آلودگی بدافزار و حفظ اعتماد دارد. افراد و سازمان‌ها باید هوشیاری لازم را برای شناسایی و گزارش دهی URLهای فیشینگ داشته باشند تا در جهان دیجیتال امن باقی بمانند.

ادبیات پژوهش

فیشینگ چیست؟

فیشینگ یکی از رایج‌ترین روش‌های دسترسی به داده‌های شخصی است[1]. برای به حداقل رساندن آسیب یک حمله فیشینگ، لازم است که آن را در کوتاه‌ترین زمان ممکن، شناسایی کنیم. تقریباً تمامی انواع حمله فیشینگ از URLهای فیشینگ استفاده می‌کنند[1].

URLهای فیشینگ به وبسایت‌ها یا صفحات وبی لینک شده‌اند. این وبسایت‌ها یا صفحات وب به‌نحوی طراحی شده‌اند که شبیه وبسایت‌های معتبر و قانونی به نظر برسند، اما در واقعیت کار سایت‌های مخربی هستند که توسط مجرمان سایبری ایجاد شده‌اند. آن‌ها با استفاده از این وبسایت‌ها اطلاعات شخصی همچون اطلاعات ورود به حساب (لاگین)، شماره‌های کارت اعتباری و سایر داده‌های حساس را سرقت می‌کنند [1].

نمی توان بیشتر از این حد روی اهمیت تشخیص URLهای فیشینگ تاکید کرد، زیرا آن‌ها تهدید مهمی نسبت به افراد و سازمان ها هستند. در اینجا دلایلی راجع به ضرورت تشخیص URLهای فیشینگ را بیان می کنیم [1]:

5- حفاظت در برابر سرقت هویت: URLهای فیشینگ معمولاً برای فریب افراد و افشای اطلاعات لاگین، جزئیات حساب بانکی و سایر اطلاعات شخصی طراحی شده اند. افراد و سازمان ها می توانند با تشخیص این URLها از خود در برابر سرقت هویت حفاظت کنند [1].
6- جلوگیری از زیان های مالی: حملات فیشینگ زیان های مالی شدیدی را به افراد و سازمان ها تحمیل می کنند. سازمان ها می توانند با تشخیص و مسدودکردن URLهای فیشینگ، از سرقت پول و داده های حساس توسط مجرمان سایبری جلوگیری کنند [1].
7- حفاظت در برابر بدافزار: URLهای فیشینگ معمولاً حاوی لینک هایی به نرم افزارهای مخرب هستند، و این نرم افزارها در شرایط خاصی به رایانه یا شبکه آسیب می زنند.سازمان ها با تشخیص و مسدودسازی این URLهای فیشینگ، از آلوده شدن به بدافزار و رخنه داده ها جلوگیری کنند [1].

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه
ISSN: 3060-6055

8- حفظ اعتماد: ممکن است سازمان هایی که قربانی حملات فیشینگ هستند اعتماد مشتریان، کارفرمایان و شرکای خود را از دست بدهند. سازمان ها با تشخیص و پیشگیری از حملات فیشینگ، اعتبارشان را حفظ می کنند و از گسترش اخبار منفی جلوگیری می کنند [1].

به‌طور خلاصه، تشخیص URLهای فیشینگ، نقش اساسی را در حفاظت در برابر سرقت هویت، زیان مالی، خنثی سازی آلودگی بدافزار و حفظ اعتماد دارد. افراد و سازمان ها باید هوشیاری لازم برای شناسایی و گزارش دهی URLهای فیشینگ را داشته باشند تا در جهان دیجیتال امن باقی بمانند.

URLهای فیشینگ و یادگیری ماشین چه هستند؟

یک URL فیشینگ، یک لینک مخرب است که مهاجم روی اینترنت توزیع می کند. هدف وی این است که کاربران را فریب داده و به داده های حساس آن ها همچون رمزهای عبور، شماره‌های کارت اعتباری و سایر اطلاعات شخصی دسترسی پیدا کند.

یادگیری ماشین یک تکنیک هوش مصنوعی است که طی آن الگوریتم های رایانه ای بر اساس حجم های وسیعی از داده ها آموزش دهی می شوند. در مقوله تشخیص URLهای فیشینگ، می‌توان از یادگیری ماشین برای تشخیص الگوهای مشکوک در آدرس های لینک استفاده کرد. این الگوها می‌توانند نشانه ای از حملات فیشینگ بالقوه باشند.

تشخیص URLهای فیشینگ با یادگیری ماشین از تحلیل حجم های وسیعی از داده ها استفاده می کند. این داده ها حاوی ویژگی های مختلفی همچون URL، شرایط ظاهری صفحه وب، زمینه و غیره هستند. می توان مدل های یادگیری ماشینی که برای تشخیص URLهای فیشینگ به‌کار رفته را روی نمونه های واقعی سایت های فیشینگ و سایت های معتبر (غیرفیشینگ) آموزش داد. بدین ترتیب آن ها امکان شناسایی لینک های مشکوک بر اساس مدل آموزش دهی شده را به‌دست می آورند.

بر این اساس، استفاده از یادگیری ماشین برای تشخیص URLهای فیشینگ، روش موثری برای حفاظت از کاربران در برابر حملات سایبری مرتبط با فیشینگ است.

ارزیابی روش های مختلف تشخیص فیشینگ

مشکل تشخیص URLهای فیشینگ این است که آن ها به‌نحوی طراحی شده که دقیقاً شبیه URLهای قانونی به نظر برسند، بنابراین وضعیت کاربران برای تفکیک آن ها از URLهای معتبر دشوار می شود. این URLها اکثراً شبیه وبسایت های شناخته شده همچون وبسایت های بانکی یا تجارت الکترونیک طراحی می شوند، و با فریب کاربران باعث افشای اطلاعات حساس می شوند [4].

یکی از چالش های تشخیص URLهای فیشینگ این است که آن ها به شدت هدفمند و شخصی سازی شده هستند، در نتیجه تشخیص شان با روش های مرسوم مبتنی بر قوانین دشوار است. علاوه بر این، روش های فیشینگ پیچیده تر شده اند و برای تشخیص به تکنیک های پیشرفته تری نیاز دارند [3].

برای مقابله با حملات فیشینگ، چندین روش برای تشخیص URLهای فیشینگ توسعه یافته‌اند. این روش ها عبارتند از:

1- لیست های سیاه: لیست های سیاه حاوی URLهای فیشینگ معلومی هستند که توسط متخصصان امنیت شناسایی شده اند. مرورگرها، ارائه دهندگان ایمیل و نرم افزارهای امنیتی می توانند از این لیست ها برای جلوگیری از دسترسی کاربران به وبسایت های فیشینگ شناخته شده استفاده کنند [1]. بسیاری از برندهای محبوب همچون گوگل، مایکروسافت، اپل و خیلی موارد دیگر، از لیست سیاه به عنوان ابزاری برای محافظت در برابر URLهای فیشینگ استفاده می کنند. این شرکت ها از روش های مختلفی برای نگهداری و به‌روزرسانی لیست های سیاه خود استفاده می کنند که خزنده های خودکار و گزارش‌های کاربر دو نمونه از آن ها هستند. به عنوان مثال، سرویس مرورگری امن گوگل، به‌طور مرتب لیست وبسایت های غیرامن خود، از جمله وبسایت های فعال در حملات فیشینگ را به‌روزرسانی می‌کند و قبل از بازدید کاربران از آن ها هشدار صادر می‌کند. فیلتر کنترل هوشمند مایکروسافت در مرورگرهای اج و اینترنت اکسپلورر ادغام شده و با لیست سیاه از کاربران در برابر وبسایت های به‌طور بالقوه مخرب حفاظت می کند [12].

2- فیلترهای سیستم نام دامنه (DNS): می توان از این فیلترها برای مسدودسازی دسترسی به URLهای فیشینگ شناخته شده استفاده کرد. هنگامی که کاربری سعی می‌کند به یک وبسایت فیشینگ شناخته شده دسترسی پیدا کند، فیلتر DNS کاربر را به یک صفحه امن انتقال داده یا دسترسی به

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه
ISSN: 3060-6055

سایت را به‌طور کامل قطع می‌کند[6]. چندین برند محبوب وجود داشته که از فیلترینگ DNS به عنوان روشی برای حفاظت در برابر URLهای فیشینگ استفاده می کنند. برخی از این برندها شامل سیسکو، باراکودا نتورکز، سوفوس، مک آفی و سیمانتک هستند. این شرکت ها خدمات فیلترینگ DNS را ارائه داده و به سازمان ها کمک کرده دسترسی به سایت های فیشینگ شناخته شده و نیز آدرس های IP و دامنه های مخرب را ممنوع کنند. سازمان ها با اتکا به این روش، به صورت بیش فعالانه ای از شبکه ها و کاربران خود در برابر حملات فیشینگ حفاظت می کنند.

3- آموزش های آگاه سازی کاربر: آموزش دهی به کاربران راجع به خطرات حملات فیشینگ و نحوه آشکارسازی (تشخیص) URLهای فیشینگ، می تواند روش موثری برای جلوگیری از این حملات باشد. می توان به کاربران آموزش داد که نشانه های URLهای فیشینگ، از جمله اشتباه در املای نام دامنه یا وجود کاراکترهای غیرعادی در URL را جستجو کنند [6]. شرکت های محبوب زیادی همچون مایکروسافت، گوگل و آمازون آموزش های آگاه سازی کاربر را به عنوان بخشی از پروتکل های امنیتی شان به کاربران ارائه می کنند. برای نمونه، مایکروسافت آموزش های زیادی از جمله وبینارها و دوره های آنلاین را فراهم کرده است و به کارکنانش کمک می کند طرح های فیشینگ را شناسایی و از آن ها اجتناب کنند. گوگل نیز منابع مشابهی فراهم می کند که حملات فیشینگ شبیه سازی شده یکی از آن ها است. این حملات میزان آگاهی کارکنان را تست می کنند. همچنین بسته های آموزشی فراهم شده که به ارتقای مهارت کارکنان می انجامند [15].

4- الگوریتم های یادگیری ماشین: می توان از الگوریتم های یادگیری ماشین برای تشخیص URLهای فیشینگ استفاده کرد. این کار با تحلیل خصوصیات URL از جمله نام دامنه، طول URL و وجود کلیدواژه های خاص انجام می شود. این الگوریتم‌ها توانایی تشخیص شباهت های بین URLهای فیشینگ و وبسایت های شناخته شده فیشینگ را هم دارند [2]. یادگیری ماشین در مقایسه با لیست سیاه یا فیلتر DNS رویکرد موثرتری برای آشکارسازی URLهای فیشینگ محسوب می شود. دلیلش این است که می تواند با تهدیدهای جدید و در حال تکامل تطبیق پیدا کند. لیست سیاه و فیلترینگ DNS به نگهداری از لیست های URLهای فیشینگ شناخته شده یا دامنه ها وابسته هستند و هنگامی که مهاجمان URLها یا دامنه های جدیدی ایجاد می کنند بلافاصله منسوخ می شوند [13].

از سوی دیگر، مدل های یادگیری ماشین می توانند الگوها و ویژگی های URLها و صفحات وب را تحلیل کنند و حملات فیشینگ جدید و ناشناخته را حتی در صورت رویت نشدن در گذشته تشخیص دهند. همچنین این مدل ها می توانند از داده های گذشته اطلاعات مفیدی را استخراج کنند و دقت را در طول زمان افزایش دهند، لذا در تشخیص URLهای فیشینگ کارآمدتر می شوند.

علاوه بر این، یادگیری ماشین می تواند ویژگی های مختلف فرای URL یا دامنه را تحلیل کند که از جملهآنها ظاهر صفحه وب و زمینه ای است که لینک در آن قرار داشته‌است. بدین ترتیب کار مهاجمان برای ممانعت از تشخیص، صرفاً با استفاده از دامنه ها یا URLهای مختلف دشوارتر می شود [14]. به طور کُلی، یادگیری ماشین رویکرد بیش فعالانه تر و تطبیقی برای آشکارسازی URLهای فیشینگ است، بنابراین ابزار مناسب تری برای حفاظت در برابر تهدیدهای سایبری رو به گسترش تلقی می شود.

به عنوان جمع بندی بحث، باید گفت: آشکارسازی URLهای فیشینگ بخش اساسی جلوگیری از حملات فیشینگ است. روش های مختلفی برای تشخیص URLهای فیشینگ توسعه داده شده اند، از جمله لیست های سیاه، فیلترهای DNS، الگوریتم های یادگیری ماشین و آموزش آگاهی کاربر. این روش ها به افراد و سازمان ها کمک کرده در برابر حملات فیشینگ امن باقی بمانند و از اطلاعات حساس شان حفاظت کنند.

می توان از این روش ها و مدل های یادگیری ماشین به عنوان راه حل مسئله استفاده کرد:

1- یادگیری نظارت شده: این روش با آموزش دهی یک مدل یادگیری ماشین؛ روی مجموعه داده برچسب گذاری شده از URLهای فیشینگ و URLهای قانونی اجرا می‌شود. می توان از این مدل برای طبقه بندی URLهای جدید به دو دسته فیشینگ و قانونی، بر اساس الگوهای یادگیری شده در طول آموزش استفاده کرد [17].

2- یادگیری نظارت نشده: در این روش، مدل یادگیری ماشین بر روی مجموعه داده غیربرچسب گذاری شده از URLها آموزش داده می شود و تشخیص الگوها و ناهنجاری ها در داده ها که نشانه بالقوه URLهای فیشینگ بوده یاد گرفته می شود [17].

3- یادگیری نیمه نظارتی: این روش مولفه های یادگیری نظارت شده و غیرنظارت شده را ترکیب می کند. مدل یادگیری ماشین روی مجموعه کوچکی از داده های برچسب گذاری شده URLهای فیشینگ و قانونی آموزش داده می شود. همچنین یادگیری روی مجموعه داده غیربرچسب گذاری شده برای تشخیص الگوهای جدید و ناهنجاری ها در داده ها به‌کار می رود [17].

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه
ISSN: 3060-6055

4- یادگیری عمیق: روش های یادگیری عمیق از جمله شبکه های عصبی کانوالی (CNN) یا شبکه های عصبی بازگشتی (RNN) برای تشخیص URLهای فیشینگ کاربرد دارند. آن ها ویژگی ها را مستقیماً از داده های خام همچون اسکرین شات های وبسایت یا لاگ های ترافیک شبکه یاد می گیرند [17].

5- یادگیری ترکیبی: در این روش چندین مدل یادگیری ماشین با هم ترکیب شده تا عملکرد کُلی ارتقا یابد. روش های ترکیبی می توانند به طور مشخص برای آشکارسازی URLهای فیشینگ مفید باشند. در حقیقت آن ها انواع مختلف مدل ها با نقاط قوت و ضعف مختلف را با یکدیگر ترکیب می کنند [17][3].

هر روش نقاط ضعف و قوت خاص خودش را دارد، لذا باید چندین روش را آزمایش کرد تا موثرترین روش تشخیص URLهای فیشینگ با یادگیری ماشین شناسایی شود.

روش های یادگیری عمیق

یادگیری عمیق یکی از زیرمجموعه های یادگیری ماشین است و از شبکه های عصبی مصنوعی برای تحلیل و طبقه بندی داده ها استفاده می کند. اما روش های مرسوم یادگیری ماشین به انتخاب و مهندسی غیرماشینی(دستی) ویژگی ها برای طبقه بندی وابسته هستند. این مدل ها ویژگی ها را از روی داده های خام یاد می گیرند و می توانند الگوهای پیچیده تری را کشف کنند. این روش ها معمولاً URL عادی را به یک ماتریس تبدیل می کنند [18] سپس شاخص هایی را برای مدل منتخب فراهم می کنند تا قانونی بودن یا فیشینگ بودن URL را مشخص کنند.

از لحاظ آشکارسازی URLهای فیشینگ، رویکردهای یادگیری عمیق نرخ های دقت بالاتری را نسبت به روش های مرسوم یادگیری ماشین فراهم می کنند. علتش این است که مدل های یادگیری عمیق می توانند الگوها و ویژگی های حساس را شناسایی کنند که ممکن است در حالت عادی برای انسان ها یا روش های مرسوم یادگیری ماشین مخفی باقی می مانند.

البته بهتر است اشاره کنیم که رویکردهای یادگیری عمیق به داده ها و منابع محاسباتی بیشتری در مقایسه با روش های مرسوم یادگیری ماشین نیاز دارند و این حالت برای برخی سازمان ها دردسرساز است. البته انتخاب بین رویکردهای یادگیری عمیق و روش های مرسوم یادگیری ماشین، به نیازها و منابع خاص هر سازمان بستگی دارد.

شبکه عصبی کانوالی

شبکه عصبی کانوالی (CNN) یک نوع الگوریتم یادگیری عمیق است که برای وظایف تشخیص تصویر و الگو بسیار کارآمد است. این روش یک تصویر ورودی را دریافت می کند، یک سری فیلترها را اعمال کرده تا ویژگی ها را در سطوح انتزاعی مختلف استخراج کند سپس از ویژگی ها برای طبقه بندی تصویر به دسته های مختلف استفاده می کند [16].

CNNها به‌طور متداول در کاربردهای بینایی رایانه به‌کار می روند و آشکارسازی URLهای فیشینگ یک مورد از آن ها است. دلیلش این است که URLهای فیشینگ غالباً حاوی تصاویر یا لوگوهایی هستند که برای تقلید وبسایت های قانونی و فریب کاربران برای کلیک روی آن ها طراحی شده اند. با آموزش دهی یک CNN روی یک مجموعه داده بزرگ از URLهای فیشینگ و قانونی، شبکه الگوها و ویژگی هایی را که نشانه های خرابکاری هستند، شناسایی می کنند.

یکی از دلایلی که CNNها بهترین روش تشخیص URLهای فیشینگ هستند، توانایی شان برای یادگیری خودکار از ویژگی های مطلوب داده های خام ورودی است. در حقیقت به‌جای اعمال دستی ویژگی ها بر اساس دانش دامنه، شبکه می تواند استخراج مناسب ترین ویژگی ها را با توجه به وظیفه موجود انجام دهد. علاوه بر این، CNNها به‌شدت مقیاس پذیر هستند و این یعنی آن ها می توانند مجموعه داده های بزرگ را مدیریت کنند و روی خوشه‌های رایانشی قوی آموزش داده شده تا دقت شان افزایش یابد.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه

ISSN: 3060-6055

خودتوجهی چندسره

خودتوجهی چندسره، تکنیکی است که در یادگیری عمیق، بخصوص در حوزه پردازش زبان طبیعی (NLP) به‌کار می رود. این حالت نمونه تعمیم یافته ای از خودتوجهی است که به شبکه عصبی این امکان را داده تا اهمیت بخش های مختلف توالی ورودی را در حین پردازش بسنجد. خودتوجهی چندسره این مفهوم را گسترش داده و عملیات خودتوجهی را به‌صورت موازی انجام می دهد. لذا مدل می تواند نمایش های متعدد از توالی ورودی را یاد بگیرد و الگوهای پیچیده تر را تشخیص دهد.

در زمینه آشکارسازی های URLهای فیشینگ، خودتوجهی چندسره برای استخراج ویژگی ها از متن URL و تشخیص الگوهای مهم مرتبط با فیشینگ کاربرد دارد. مدل با توجه به سرهای توجه چندگانه جنبه های مختلف URL را یاد می گیرد که وجود کلیدواژه های مشکوک یا نام های دامنه غیرعادی دو مورد هستند. آن ها به صورت یک نمایش نهایی ترکیب شده و برای طبقه بندی کاربرد دارند.

هرچند CNNها یک روش محبوب برای آشکارسازی URLهای فیشینگ هستند، اما خودتوجهی چندسره می تواند در شرایط خاص مزیت هایی را فراهم کند. برای مثال در پردازش توالی های طولانی متن موثرتر است، اما فیلترهای کانوالی مرسوم در تشخیص این الگوها دچار مشکل می شوند. علاوه بر این، خودتوجهی چندسره، تفسیرپذیرتر از CNNها است و به محققان اجازه می دهد بخش های مختلف ورودی را که در تصمیم نهایی طبقه بندی تاثیر بیشتری دارند بهتر درک کنند. این در حالی است که اثربخشی خودتوجهی چندسره در نهایت به مجموعه داده ها و مسائل مشخص بستگی دارد.

یافته‌ها

ما می توانیم با مدل های یادگیری ماشین وبسایت های فیشینگ را تشخیص دهیم. دقت این مدل ها به مجموعه داده های به‌کاررفته برای آموزش و تست، ویژگی های استخراجی از وبسایت ها و الگوریتم ها و طبقه بندی‌های به‌کاررفته بستگی دارد. مجموعه داده های مختلفی برای آموزش کارایی دارند که Alexa و خزنده عمومی (common crawl) برای سایت های قانونی برای فیشینگ قابل استفاده هستند. phish tank و open-fish هم برای URLهای مشکوک گزارشی توسط کاربران کاربرد دارند. از چندین ویژگی برای مقایسه روش‌های یادگیری ماشین استفاده شده که صحت، نرخ مثبت کاذب، بازیابی، دقت و امتیاز F-1 از آن جمله هستند. رایج ترین و موثرترین روش های تشخیص URL فیشینگ شامل بیز ساده، جنگل تصادفی، CNN، MLP، MHSA، LSTM، CNN+RNN هستند. صحت در تمام روش‌های بالا و بین 96 تا 99.84 ٪ است، اما عوامل دیگری همچون زمان آموزش، منابع محاسباتی و مقاومت در برابر نویز هم برای تعیین روش مناسب تر و بهتر به‌کار می روند.

شناسایی تکنیک های انتخاب و مهندسی ویژگی

همانطور که گفتیم، چندین ویژگی هستند که برای مقایسه روش های یادگیری ماشین در امر تشخیص URLهای فیشینگ کاربرد دارند. برخی ویژگی های پرکاربرد به این شرحند:

1- صحت: درستی کُلی مدل طبقه بندی را می سنجد. محاسبه آن با تقسیم تعداد نمونه های به‌درستی طبقه بندی شده بر تعداد کل نمونه ها انجام می شود.
2- نرخ مثبت کاذب (FPR): نسبت پیش بینی های مثبت کاذب به تعداد کل نمونه های منفی را می سنجد. FPR بالا بدین معنی است که مدل URLهای غیرفیشینگ را به عنوان فیشینگ شناسایی کرده است.
3- بازیابی: نسبت پیش بینی های مثبت صحیح به تعداد کل نمونه های مثبت را می‌سنجد. بازیابی بالا یعنی مدل به‌درستی درصد بالایی از URLهای فیشینگ را تشخیص می دهد.
4- دقت: نسبت پیش بینی های مثبت صحیح به تعداد کل نمونه های پیش بینی شده مثبت را می سنجد. دقت بالا یعنی مدل با دقت URLهای فیشینگ را شناسایی می‌کند.
5- امتیاز F-1: به عنوان میانگین موزون دقت و بازیابی تعریف شده است. یک امتیاز واحد و متعادل بین دقت و بازیابی را ارائه می دهد.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه
ISSN: 3060-6055

صحت، FPR، بازیابی، دقت، و امتیاز F1، مناسب ترین ویژگی ها برای مقایسه روش های یادگیری ماشین در تشخیص URLهای فیشینگ هستند. دلیلش این است که آن ها ارزیابی کاملی از عملکرد مدل فراهم می کنند. هرچند صحت درستی کُلی را می سنجد، اما دقت، FPR، بازیابی و امتیاز F-1 اطلاعاتی از توانایی مدل برای تشخیص URLهای فیشینگ فراهم کرده و از مثبت های کاذب ممانعت می کنند. این شاخص ها نقش اساسی را در تشخیص فیشینگ دارند و ناتوانی در تشخیص URLهای فیشینگ منجر به تهدیدهای امنیتی می شود. نرخ مثبت کاذب بالا نیز باعث ناامیدی کاربر و بی‌اعتمادی به سیستم می شود.

برای درک بهتر نحوه تحلیل شاخص ها، نتایج را این‌گونه بیان می کنیم:

- مثبت صحیح (TP) تعداد URLهای فیشینگی است که به درستی طبقه بندی شده‌است.
- منفی صحیح (TN) تعداد URLهای قانونی است که به عنوان قانونی طبقه‌بندی شده‌است.
- مثبت کاذب (FP) تعداد URLهای قانونی است که به عنوان فیشینگ طبقه‌بندی شده‌است.
- منفی کاذب (FN) تعداد URLهای قانونی است که به عنوان قانونی طبقه‌بندی شده‌است.

پس از انتخاب ویژگی ها برای ارزیابی و مقایسه مدل ها، می توان آن ها را این‌گونه تعریف کرد:

- $Acc = TP + TN / TP + TN + FN$
- $FRP = FP / FP + TN$
- $Rec = TP / TP + FN$
- $Pre = TP / TP + FP$
- $F1 = 2* Pre*Rec / Pre + Rec$

مقایسه عملکرد

برخی از پرکاربردترین و موثرترین روش‌های به‌کاررفته برای تشخیص URLهای فیشینگ به این شرح هستند:

1- بیز ساده: یک الگوریتم احتمالاتی مبتنی بر قضیه بیز است. فرض می شود تمام ویژگی ها مستقل از هم هستند. این الگوریتم با محاسبه احتمال فیشینگ بودن URL بر اساس وقوع ویژگی های خاص در آن عمل می کند. الگوریتم روی مجموعه داده های برچسب گذاری شده آموزش داده شده و در حین تست، از احتمالات فراگیری شده برای طبقه بندی URLهای جدید به دو دسته قانونی یا فیشینگ استفاده می کند. بیز ساده یک روش آسان و سریع است و کارایی خوبی در تشخیص URLهای فیشینگ نشان داده است [1].

2- جنگل تصادفی: یک الگوریتم یادگیری ترکیبی است که درخت های تصمیم متعدد را ایجاد و پیش بینی ها را ترکیب کرده تا به تصمیم نهایی برسد. هر درخت جنگل روی یک زیرمجموعه تصادفی از مجموعه اطلاعات آموزش داده شده است. در حین تست، الگوریتم پیش بینی های تمام درخت ها را ترکیب کرده تا تصمیم نهایی را اتخاذ کند. جنگل تصادفی به‌خاطر دقت و مقاومت در برابر داده های نویزی مشهور است [1].

3- CNN (شبکه عصبی کانوالی): یک الگوریتم یادگیری عمیق بوده که با الهام گیری از ساختار مغز انسان ساخته شده است. آن ها با اعمال فیلترهای کانوالی برای استخراج ویژگی ها از داده های ورودی عمل می کنند. این ویژگی ها از لایه های نورون عبور کرده و نمایش های پیچیده از داده ها را یاد می گیرند. آن ها توانایی عملکرد مطلوب در تشخیص URLهای فیشینگ با یادگیری ویژگی هایی همچون نام دامنه، طول URL، و n-گرم های کاراکتر را نشان داده اند [21].

4- MLP (پرسپترون چندلایه): یک نوع شبکه عصبی مصنوعی است که از چند لایه نورون تشکیل شده است. هر نورون شبکه ورودی ها را از لایه قبلی دریافت و تابع فعالسازی غیرخطی را اعمال می کند تا خروجی ایجاد کند. MLPها با پس انتشار، یک الگوریتم یادگیری نظارت شده آموزش داده می شوند. این الگوریتم وزن های نورون ها را به‌نحوی تنظیم کرده که خطای بین خروجی های واقعی و پیش بینی شده حداقل شود. MLPها عملکرد مناسبی در تشخیص URLهای فیشینگ دارند و این کار را با یادگیری عمر دامنه، مجوزهای SSL و طول دامنه انجام می دهند [27].

5- MHSA (خودتوجهی چندسره): یک مدل تحولی و یکی از الگوریتم های یادگیری عمیق است که در پردازش زبان طبیعی کاربرد دارد. این الگوریتم با اعمال چند سر خودتوجهی به داده های ورودی عمل می کند تا اطلاعات را استخراج کند سپس خروجی های این سرها ادغام شده و از چند لایه نورون عبور کرده و برای یادگیری نمایش های داده به‌کار می روند. MHSA عملکرد مطلوبی در تشخیص URLهای فیشینگ داشته و ویژگی هایی همچون نام دامنه، طول URL، n-گرم های کاراکتر را یاد می گیرد [27].

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه
ISSN: 3060-6055

6- LSTM (حافظه طولانی کوتاه مدت): یک شبکه عصبی بازگشتی (RNN) است که برای غلبه بر مشکل گرادیان محوشونده RNNهای معمولی طراحی شده‌است. این شبکه ها قادر به یادگیری وابستگی های بلندمدت در داده های متوالی، با یادآوری و فراموشی گزینشی اطلاعات در طول زمان هستند. آن ها این توانایی را با سلول های حافظه به‌دست می‌آورند که به عنوان «واحدهای گیت دار»، ورود و خروج جریان اطلاعات از سلول را کنترل می کنند [20].

7- CNN+ RNN: یک مدل یادگیری عمیق ترکیبی است که نقاط قوت CNN و RNN را در هم ادغام کرده است. برای تشخیص URLهای فیشینگ، بخش CNN ویژگی های محلی URLها را یاد می گیرد اما بخش RNN وابستگی های متوالی بین آن ها را نشان می دهد [22].

با توجه به این جدول، مشاهده می کنیم که میزان صحت در تمام روش ها نسبتاً زیاد است و بین 96 ٪ الی 99.84 ٪ است. اما صحت به تنهایی برای اثبات برتری کافی نیست زیرا عوامل دیگری همچون زمان آموزش دهی، منابع محاسباتی، مقاومت در برابر نویز هم باید در نظر گرفته شوند.

جدول 4-1: مقایسه عملکرد

ردیف	الگوریتم تشخیصی ML	صحت	FPR	بازیابی	دقت	F1
1	بیز ساده [19]	97.18				
2	جنگل تصادفی [21]	97				
3	CNN [20]	96.61	3.5	97.09	96.61	96.85
4	LSTM [20]	97.20	1.8	98.63	96.45	97.53
5	MLP [20]	96.65		96.65	96.65	96.65
6	RNN +CNN [22]	97.9	3.10	98.39	96.76	97.57
7	LSTM + CNN [23]	93.28	1.80	97.13	99.12	98.11

ارزیابی کارایی راه حل های موجود

با توجه به جدول ارائه شده، کارایی روش های مختلف یادگیری ماشین در تشخیص URLهای فیشینگ بر حسب شاخص های صحت، FPR، بازیابی، دقت و امتیاز F-1 ارزیابی می شود.

1- بیز ساده [19]: صحت آن 97.18 ٪ است که نسبتاً بالا است. البته هیچ اطلاعاتی راجع به FPR، بازیابی، دقت، F1 وجود ندارند.

2- جنگل تصادفی [21]: صحت 97 ٪ بوده اما اطلاعاتی راجع به FPR، بازیابی، دقت و F1 وجود ندارند.

3- CNN [21]: صحت 96.61 ٪ بوده، و FPR نسبتاً زیاد و 3.5 ٪ است. بازیابی آن زیاد و 97.09 ٪ است و این یعنی اکثر URLهای فیشینگ را به‌درستی تشخیص داده است، اما دقتش مقداری از 96.61 ٪ کمتر است یعنی برخی URLهای قانونی را به عنوان URLهای فیشینگ طبقه بندی کرده است. امتیاز F1 96.85 ٪ است.

4- LSTM [20]: بالاترین صحت به میزان 97.2٪ را دارد و FPR کم در حد 1.8 ٪ دارد. بازیابی آن زیاد و 98.63 ٪ است یعنی اکثر URLهای فیشینگ را به درستی شناسایی کرده است. البته دقتش مقداری کمتر از 96.45 ٪ است و این یعنی برخی URLهای قانونی را به عنوان URL فیشینگ طبقه بندی می کند. امتیاز F1 این روش 97.53 ٪ است.

5- MLP [20]: صحت آن 96.65 ٪ است، اما اطلاعاتی راجع به FPR، بازیابی، دقت و F1 وجود ندارند.

6- CNN + RNN [22]: صحت آن 97.7 ٪ است و FPR نسبتاً بالا در حد 3.10 ٪ دارد. بازیابی آن 98.39 ٪ است که مقدار زیادی است و نشان داده که اکثریت URLهای فیشینگ را به درستی تشخیص می دهد. اما دقتش کمی کمتر از 96.76 ٪ است ، یعنی برخی URLهای قانونی را به عنوان فیشینگ طبقه بندی کرده است. امتیاز F1 آن 97.57 ٪ است.

7- CNN + LSTM [23]: این روش کمترین صحت به میزان 93.28 ٪ را دارد و FPR آن کم و 1.8 ٪ است. بازیابی آن بالا و 97.13 ٪ است. این نشان داده که اکثر URLهای فیشینگ را به درستی تشخیص داده است. دقت آن بیشترین مقدار و 99.12 ٪ است و این یعنی تعداد خیلی کمی از URLهای قانونی را به عنوان URL فیشینگ طبقه بندی کرده است. امتیاز F1 این روش 98.11 ٪ است.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه

ISSN: 3060-6055

به عنوان جمع بندی، می توان گفت LSTM موثرترین روش از لحاظ صحت و FPR است. CNN + LSTM از بالاترین دقت برخوردار است و می توان گفت URLهای قانونی خیلی کمی را به عنوان URL فیشینگ طبقه بندی کرده است. CNN + RNN و بیز ساده صحت نسبتاً بالایی داشته اما FPR شان هم نسبتاً زیاد است. جنگل تصادفی و MLP صحت بالایی دارند اما اطلاعاتی راجع به FPR، بازیابی، دقت و F1 ارائه نمی دهند.

ترکیب دو روش بهتر از به‌کارگیری یک روش است زیرا ضعف ها و نقاط قوت هر یک را پوشش می دهد، و حالت ترکیبی منجر به بهبود عملکرد می شود. برای مثال CNN + RNN در داخل جدول صحت بیشتری از بیز ساده داشته، اما بیز ساده سریع تر است و به منابع محاسباتی کمتری نیاز دارد. با ترکیب این دو روش، سیستم تشخیص URL های مخرب دقیق تر و کارآمدتری را خواهیم داشت.

CNN (شبکه عصبی کانوالی) و MHSA (خودتوجهی چندسره) هر دو در زمره معماری های قدرتمند یادگیری عمیق هستند. آن ها در وظایف مختلف پردازش زبان طبیعی از جمله تشخیص URLهای فیشینگ عملکرد موفقی داشته اند. ترکیب CNN و MHSA می تواند با به‌کارگیری نقاط قوت هر دو روش، عملکرد تشخیصی را ارتقا دهد.

CNN یک نوع شبکه عصبی است که فیلترهای کانوالی را به داده های ورودی اعمال می‌کند و بیشتر برای تشخیص تصویر به‌کار می رود. در حوزه NLP، CNN می تواند ویژگی های مهم متن را با اعمال «پنجره لغزان» به توالی ورودی یاد بگیرد و در گام بعدی الگوهای محلی کلمات را استخراج می کند. این ویژگی های محلی ترکیب شده و به نمایش سطح بالاتری از متن ورودی تبدیل می شوند. کارایی CNN در تشخیص URLهای فیشینگ با استخراج ویژگی های n- گرم از URLها و استفاده از آن ها برای آموزش طبقه بند نشان داده شده است.

از سوی دیگر، MHSA یک مدل تبدیل محور است که با خودتوجهی مجموع وزنی توکن های ورودی را محاسبه می کند. لذا مدل می تواند وابستگی های سراسری و روابط گسترده (محدوده طولانی) بین کلمات و توالی را تشخیص دهد. کارایی MHSA در NLP برای مدلسازی معنی ظاهری متن ثابت شده است. این کار با توجه به کلمات مناسب در توالی ورودی انجام می شود. می توان از MHSA در بحث تشخیص URLهای فیشینگ برای یادگیری «نمایشی از URL» استفاده کرد. این نمایش معنی ظاهری و زمینه را شناسایی می کند.

ترکیب CNN و MHSA باعث دستیابی به مزایای هر دو مدل می شود. همچنین با اتکا به توانایی های مکمل آن ها عملکرد تشخیصی را ارتقا می دهد. CNN از قدرت تشخیص الگوهای محلی و ویژگی های n- گرم URL برخوردار است، اما MHSA معنی ظاهری و زمینه را مدلسازی می کند. روش ترکیبی دو پیش بینی را ادغام کرده و صحت و مقاومت بیشتری در برابر URLهای فیشینگ مختلف ایجاد می کند.

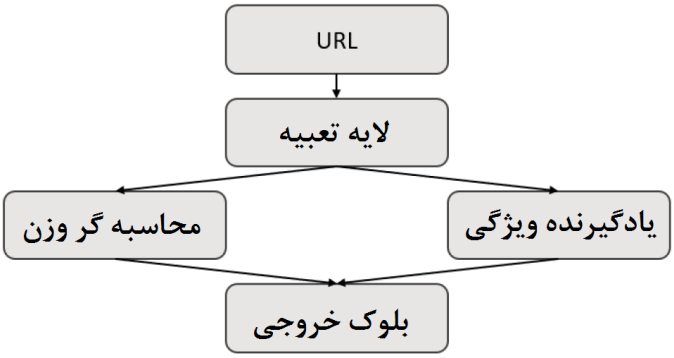
نمای کُلی از مدل

به‌دلیل اینکه خودتوجهی چندسره (MHSA) از عملکرد عالی در پردازش زبان طبیعی (NLP) برخوردار است و از قدرت محاسبه وزن های ویژگی ها و تشخیص وابستگی ها بین کاراکترهای مختلف متن برخوردار است، می تواند در تحلیل URLها نیز مفید باشد و حتی بهتر از LSTM عمل کند. همچنین به خاطر کارایی CNNها در یادگیری خودکار ویژگی‌ها بدون مداخله انسان، ترکیب نمودن این تکنیک برای بهره‌مندی از نقاط قوت آن و بهبود قدرت تشخیص وبسایت های فیشینگ امکان پذیر است.

هنگامی که مدلی را برای ترکیب دو تکنیک یادگیری ماشین ایجاد می کنیم، می توان بخش هایی از آن را تفکیک کرد. به عنوان گام نخست، «لایه تعبیه» ای را تعریف می‌کنیم که URL ورودی را با کدگذاری وان هات به نمایش ماتریسی تبدیل می کند. علاوه بر این، به‌خاطر استفاده از دو تکنیک، می توان دو نسخه از ماتریس را برای یادگیری ویژگی و محاسبه وزن ویژگی به‌کار گرفت. یکی از نسخه ها در حین محاسبه وزن به لایه های MHSA اعمال شده تا وزن ها را محاسبه کند. اما به‌طور همزمان در فرایند استخراج ویژگی، نسخه بعدی از ماتریس URL برای یادگیری ویژگی ها به لایه های کانوالی اعمال می شود. بنابراین خروجی لایه قبلی به منزله ورودی لایه بعدی تلقی می‌شود. بعد از اتمام دو فرایند همزمان، دو بخش خروجی به بلوک خروجی خورانده می‌شوند تا نتیجه نهایی طبقه بندی محاسبه شود.

بلوک خروجی ابتدا ویژگی های اصلی و دو نسخه را به عنوان وزن های ویژگی ورودی دریافت می کند. خروجی به یک لایه تماماً مرتبط با تابع فعال‌سازی سیگموئید اعمال می‌شود و خروجی بین 0 تا 1 ایجاد می کند. اگر خروجی بیشتر از 0.5 باشد، URL ورودی قانونی فرض می شود و در غیر این صورت «فیشینگ» تلقی می شود.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه
ISSN: 3060-6055



شکل 4-1: نمای کلی از مدل

عملکرد مدل

با در نظرگرفتن مزایای ترکیب CNN و خودتوجهی چندسره، معماری مدل شامل 3 مولفه اصلی خواهد بود: یک لایه تعبیه، یک یادگیرنده ویژگی و یک محاسبه‌گر وزن.

لایه تعبیه، رشته URL را به ماتریسی تبدیل می کند. تعداد سطرهای آن ماتریس برابر طول URL و دارای 84 ستون است که 84 کاراکتر بالقوه در URL را نشان می دهند. برای نمایش هر کاراکتر از کدگذاری وان هات استفاده می شود و ماتریس از طریق شبکه عصبی به 64 ستون خلاصه می شود. URLهایی با طول های مختلف به‌وسیله رشته ای با طول ثابت، با تریمینگ یا پدینگ پردازش می شوند.

یادگیرنده ویژگی، ویژگی ها را از ماتریس خروجی لایه تعبیه خارج می کند. این کار با استفاده از یک لایه کانوالی، دو لایه باقیمانده و یک لایه تماماً متصل انجام می‌شود. لایه کانوالی حاوی 5 کرنل مرسوم و لایه پولینگ حداکثری است. لایه های باقیمانده مسئله تجزیه اشباع صحت را حل می کنند. این کار با جمع کردن ورودی و خروجی لایه کانوالی انجام می شود. لایه تماماً متصل، قدرت بیان شبکه عصبی و کارایی استخراج ویژگی را افزایش می دهد.

محاسبه گر وزن حاوی یک لایه MHSA، دو لایه باقیمانده و یک لایه تماماً متصل است. این واحد مسئول محاسبه وزن های ویژگی ها است. خروجی لایه تعبیه با کدگذاری موقعیتی اعمال شده و حاوی اطلاعات موقعیت نسبی کاراکترها در توالی رشته URL است. ماتریس کدگذاری موقعیتی به‌وسیله توابع سینوس و کسینوس به‌دست می آید. سپس ماتریس خروجی به لایه MHSA که حاوی 8 سر است اعمال می شود. در نهایت ماتریس ویژگی حاصل شده و برای طبقه بندی یا پیش بینی به‌کار می رود.

نتیجه بلوک خروجی یک مقدار بین 0 الی 1 است. هر چقدر مقدار خروجی بیشتر باشد (بزرگتر از 0.5)، احتمال فیشینگ بودن URL کمتر است.

شاخص های عملکردی مدل به‌طور کلی این‌گونه هستند:

- صحت: 0.9834
- نرخ مثبت کاذب : 0.0176
- دقت: 0.9844
- بازیابی: 0.9814

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه
ISSN: 3060-6055

- امتیاز F1: 0.9830

تحلیل معنی این شاخص های عملکردی:

1- صحت: صحت مدل 0.9834 است و بدین معنی است که 98.34 ٪ از URLهای فیشینگ مجموعه داده را به درستی تشخیص داده است.
2- FPR: 0.0176 است ، بدین معنی که 1.76 ٪ URLهای غیرفیشینگ به اشتباه، URL فیشینگ تلقی شده اند.
3- دقت: 0.9844 است به این معنی که 98.44 ٪ URLهای شناسایی شده به عنوان فیشینگ توسط مدل، واقعاً URL فیشینگ هستند.
4- بازیابی: 0.9816 است، یعنی مدل به‌درستی 98.16 ٪ تمام URLهای فیشینگ واقعی مجموعه داده را شناسایی کرده است.
5- امتیاز F1: 0.9830 است، بدین معنی که مدل توازن خوبی بین دقت و بازیابی حاصل کرده است.

این نتایج به‌طور کلی بدین معنی هستند که ترکیب CNN و MHSA عملکرد بسیار خوبی در تشخیص URLهای فیشینگ داشته است. علاوه بر این، صحت، دقت، بازیابی و F1 بالا و FPR پایین هستند.

تحلیل نتایج

جدول زیر با توجه به نتایج تحقیق ارائه شده است و عملکرد تکنیک های مختلف یادگیری ماشین برای تشخیص وبسایت های فیشینگ را مقایسه می کند.

جدول 4-2: مقایسه عملکرد با روش ترکیبی پیشنهادی

ردیف	الگوریتم تشخیص ML	صحت	FPR	بازیابی	دقت	F1
1	بیز ساده [19]	97.18				
2	جنگل تصادفی [21]	97				
3	CNN [20]	96.61	3.5	97.09	96.61	96.85
4	LSTM [20]	97.20	1.8	98.63	96.45	97.53
5	MLP [20]	96.65		96.65	96.65	96.65
6	CNN + RNN [22]	97.9	3.10	98.39	96.76	97.57
7	CNN + LSTM [23]	93.28	1.8	97.13	99.12	98.11
	CNN + MHSA	98.34	1.76	98.44	98.16	98.30

تحلیل و مقایسه کامل تکنیک های مختلف یادگیری ماشین که برای تشخیص URL فیشینگ مبتنی به‌کاررفته بر اساس جدول ارائه شده اند:

1- بیز ساده [19]: صحت آن 97.18 ٪ است. یک الگوریتم ساده و محبوب است که با داده هایی با ابعاد زیاد با فرض مستقل بودن تمام ویژگی ها از هم به‌خوبی عمل می کند، اما شرایط اکثراً این‌گونه نیست.
2- جنگل تصادفی [21]: صحت آن 97 ٪ است. این الگوریتم یک روش یادگیری ترکیبی است که درخت های تصمیم مختلف را ایجاد و پیش بینی هایشان را ترکیب می کند تا صحت را افزایش و بیش برازش را کاهش دهد.
3- CNN [20]: صحت این الگوریتم 96.61 ٪ است. FPR 3.5 ٪، بازیابی 97 ٪، دقت 96.61٪ و F1 96.85 ٪ هستند. CNNها به وفور برای طبقه بندی تصویر کاربرد دارند، اما برای طبقه بندی متن نیز قابل استفاده هستند. FPR 3.5 ٪ است و نشان می دهد 3.5 ٪ URLهای قانونی به اشتباه URL فیشینگ تلقی شده اند.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه
ISSN: 3060-6055

4- LSTM [20]: صحت آن 97.20 ٪ ، FPR آن 1.8 ٪، بازیابی 98.63 ٪ ، دقت 96.45 ٪ و F1 97.53 هستند.LSTMها یک نوع شبکه عصبی بازگشتی هستند که وابستگی های بلندمدت در داده های متوالی را شناسایی می کنند. FPR کم و بازیابی زیاد بیانگر کارایی مدل در تشخیص URLهای فیشینگ با مثبت های کاذب حداقلی هستند.

5- MLP [20]: صحت آن 96.65 ٪ است و هیچ شاخص دیگری در جدول مطرح نشده است. MLPها یک نوع شبکه عصبی فیدفوروارد بوده که می توانند روابط غیرخطی بین داده های ورودی و خروجی را یاد بگیرند.

6- CNN + RNN [22]: صحت آن 97.9 ٪ است، FPR 3.1 ، بازیابی 98.39 ، دقت 96.76 ٪، F1 95.57 هستند. ترکیب شدن CNN با RNN باعث تشخیص ویژگی های مکانی و توالی داده های ورودی می شود، لذا عملکرد در مقایسه با استفاده یک جنبه ای از هر مدل بهبود می یابد.

7- CNN + LSTM [23]: صحت آن 93.28، FPR 1.80 ٪، بازیابی 97.13 ٪ ، دقت 99.12 ٪ ، F1 98.11 هستند. ترکیب CNN با LSTM باعث تشخیص ویژگی های محلی و سراسری در داده های ورودی می شود و عملکرد را ارتقا می دهد. البته صحت و F1 کم نشان داده مدل همچون بقیه در این کار موثر نیست.

8- CNN+ MHSA: این الگوریتم دارای بالاترین صحت به میزان 98.34 ٪ است، FPR آن کمترین به مقدار 1.76 ٪ است. بازیابی 98.44٪، دقت 98.16 ٪ و F1 98.30 هستند. CNN + MHSA ترکیب این دو روش است و وابستگی های بلندمدت در داده های ورودی را تشخیص می دهد. همچنین به‌طور همزمان به بخش های مختلف توالی توجه می کند. هرچند FPR با تکنیک پس پردازش، یادگیری فعال، ارزیابی مستمر و حلقه های بازخورد قابل بهبود است. این رویکرد عملکرد مدل را بهبود داده و توازن بهتری بین مثبت های کاذب و منفی های کاذب ایجاد می کند. این مدل در این کار بهترین گزینه است و صحت بالا، مثبت های کاذب کم و دقت و بازیابی زیاد از قابلیت هایش هستند.

به عنوان جمع بندی، باید گفت CNN + MHSA بهترین عملکرد را دارد، و LSTM، CNN+ RNN و جنگل تصادفی در رده های بعدی قرار می گیرند.

1. بحث و بررسی

1-5: سوال 1- کدام نوع از الگوریتم های یادگیری ماشین برای تشخیص URLهای فیشینگ به‌کار رفته است و چطور می توان آن ها را آموزش داد و بهینه سازی کرد؟

برای مقابله با حملات فیشینگ، روش های مختلفی برای تشخیص URLهای فیشینگ توسعه داده شده اند. این روش ها شامل لیست سیاه، فیلترهای DNS، آموزش های آگاه کردن کاربر و الگوریتم های یادگیری ماشین هستند. هر روش نقاط ضعف و قوت خودش را دارد. ترکیب روش ها می تواند حفاظت موثری نسبت به این حملات فراهم کند.

لیست های سیاه و فیلترهای DNS به لیست های تهیه شده از URLها یا دامنه های مخرب بستگی دارند و با ایجاد دامنه ها و URLهای جدید توسط مهاجمان، به‌سرعت منسوخ می‌شوند. البته آن ها در مسدودسازی سایت های فیشینگ و جلوگیری از دسترسی کاربران موثر عمل می کنند. آموزش های آگاه سازی کاربران می توانند به تشخیص کلاهبرداری های فیشینگ کمک کنند، اما در برابر حملات پیچیده و شخصی روی قربانیان ناکارآمد هستند.

ما می توانیم از الگوریتم های یادگیری ماشین برای تشخیص URLهای فیشینگ استفاده کنیم. خصوصیات URLها از جمله نام دامنه، طول URL، وجود کلیدواژه های خاص تحلیل می شوند. این الگوریتم ها شباهت های بین URLهای فیشینگ و وبسایت های فیشینگ شناخته شده را تشخیص می دهند. یادگیری ماشین در زمینه تشخیص URLهای فیشینگ موثرتر از لیست سیاه یا فیلتر DNS است. دلیلش این است که با تهدیدهای جدید و تکاملی هماهنگ می شوند. مدل های یادگیری ماشین می توانند الگوها و ویژگی های URL ها و صفحات وب را تحلیل و حملات فیشینگ جدید و نامشخص را پیش بینی کنند، هرچند قبلاً رخ نداده باشند. همچنین این مدل ها از داده های گذشته نکاتی را یاد می گیرند و دقت شان را در طول زمان ارتقا می دهند، بنابراین در زمینه تشخیص این URLها موثرتر عمل می کنند.

یادگیری ترکیبی باعث ترکیب چندین مدل یادگیری ماشین می شود و عملکرد کلی را بهبود می بخشد.

سوال 1-1: کدام نوع از مجموعه‌های داده برای آموزش الگوریتم های یادگیری ماشین به‌کار می روند؟

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه

ISSN: 3060-6055

چند نوع الگوریتم یادگیری ماشین موجود هستند که برای تشخیص URLهای فیشینگ به‌کار می روند. آن ها بر اساس مجموعه داده های منتخب عمل کرده و شامل یادگیری نظارت شده، یادگیری غیرنظارت شده، یادگیری نیمه نظارت شده، یادگیری عمیق و یادگیری ترکیبی هستند. هر روش نقاط ضعف و قوت خودش را دارد. انتخاب الگوریتم ممکن است به نیازهای خاص یک سازمان و ماهیت حملات فیشینگ در حال تشخیص وابسته باشد.

یادگیری نظارت شده با آموزش دهی یک مدل یادگیری عمیق روی مجموعه داده برچسب گذاری شده همراه است. URLهای فیشینگ و قانونی در این مجموعه داده مستقر هستند. می توان از مدل برای طبقه بندی URLهای جدید به عنوان فیشینگ یا قانونی استفاده کرد. این کار با توجه به الگوهای یادگیری شده در طول آموزش انجام می شود. یادگیری نظارت شده می تواند در تشخیص حملات فیشینگ معلوم موثر باشد، اما در زمینه حملات فیشینگ ناشناخته یا جدید چنین تضمینی وجود ندارد.

در یادگیری غیرنظارت شده، یک مدل یادگیری ماشین روی مجموعه داده غیربرچسب گذاری شده از URLها آموزش داده می شود. بدین ترتیب الگوها و ناهنجاری های داده ای که نشانه وجود URLهای فیشینگ هستند مشخص می شوند. یادگیری غیرنظارت شده برای تشخیص حملات فیشینگ جدید و ناشناخته مفید است، اما ممکن است مثبت های کاذب را ایجاد کند.

یادگیری نیمه نظارت شده، مولفه های یادگیری نظارت شده و غیرنظارت شده را در هم ترکیب می کند. این مدل روی مجموعه داده کوچک برچسب گذاری شده از URLهای معتبر و فیشینگ آموزش داده می شود، اما یادگیری بر حسب مجموعه داده برچسب گذاری نشده انجام می شود تا الگوها و ناهنجاری های جدید در داده ها شناسایی شوند. یادگیری نیمه نظارتی می تواند در شناسایی حملات جدید و ناشناخته موثر باشد و مثبت های کاذب را به حداقل برساند.

روش های یادگیری عمیق همچون CNN یا RNN، برای تشخیص URLهای فیشینگ کاربرد دارند. آن ها ویژگی ها را مستقیماً از روی داده های خام ، همچون اسکرین شات های وبسایت یا لاگ های ترافیک شبکه یاد می گیرند. یادگیری عمیق می تواند در شناسایی حملات جدید و ناشناخته موثر باشد اما به حجم زیادی از داده های برچسب گذاری شده و منابع محاسباتی نیاز دارد.

هرچند روش های مختلفی برای آموزش داده ها بر حسب مجموعه داده وجود دارند، مورد به‌کاررفته در اینجا به دو بخش یکسان تقسیم شده است: URL 2000 قانونی و URL 2000 فیشینگ. این تفکیک متعادل تضمین می کند که مدل به سمت یکی از دو دسته منحرف نشده است، و هر دو نوع URL را با دقت شناسایی می کند.

سوال 1-2: چه شاخص های دقتی (صحت) برای مقایسه الگوریتم ها به‌کار می روند؟

این شاخص های دقت الگوریتم ها را در حوزه تشخیص فیشینگ با هم مقایسه می کنند:

1- صحت: نشان می دهد مدل تا چه اندازه URL را به‌درستی به عنوان فیشینگ یا قانونی طبقه بندی می کند؟ به صورت نسبت URLهای به‌درستی طبقه بندی شده به تعداد URLهای موجود در مجموعه تست تعریف می شود.
2- دقت: شاخصی است که نشان داده مدل به چه شکلی URLهای فیشینگ را به‌درستی شناسایی می کند. به عنوان نسبت تعداد مثبت های صحیح (URLهای فیشینگ که به درستی فیشینگ تلقی می شوند) به مجموع تعداد URLهای شناسایی شده به همین عنوان توسط مدل تعریف می شود.
3- بازیابی: شاخصی که نشان داده مدل تا چه اندازه تمام URLهای فیشینگ را درست شناسایی می کند. به صورت نسبت تعداد مثبت های صحیح به تعداد کل URLهای فیشینگ واقعی در مجموعه تست تعریف می شود.
4- امتیاز F1: شاخصی از عملکرد کلی مدل است و دقت و بازیابی را شامل می شود. به عنوان میانگین موزون دقت و بازیابی تعریف می شود.

سوال 1-3: کدام الگوریتم های یادگیری ماشین بهترین نتایج را در تشخیص وبسایت های فیشینگ دارند؟

به‌دلیل اینکه ارزیابی کارایی الگوریتم های مختلف به چند شاخص از جمله صحت، FPR ، بازیابی، دقت و امتیاز F1 بستگی دارد، نتایج ارائه شده به این صورت هستند:

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه
ISSN: 3060-6055

صحت روش بیز ساده زیاد و به اندازه 97.18 ٪ است. صحت جنگل تصادفی 97٪ است، صحت CNN 96.61 ٪ است اما FPR بالا در حد 3.5 ٪ دارد و این نشانه طبقه بندی برخی URLهای قانونی به عنوان فیشینگ است. LSTM بالاترین صحت را دارد (97.20٪) و FPR اندکی دارد (1.8 ٪). یعنی اکثر URLهای فیشینگ را به‌درستی طبقه بندی کرده و تعداد کمی URL قانونی را به عنوان فیشینگ طبقه بندی می کند.

روش MLP دارای صحت 96.65 ٪ است. روش CNN + RNN صحت 97.9 ٪ دارد اما FRP نسبتاً زیادی دارد (3.10 ٪). روش CNN+ LSTM دارای کمترین صحت (93.28 ٪) است، اما بالاترین دقت به میزان 99.12 ٪ را هم دارد. این یعنی تعداد بسیار کمی از URLهای قانونی را به عنوان فیشینگ طبقه بندی می کند.

به‌طور خلاصه، روش LSTM موثرترین روش از لحاظ صحت و FPR است، ولی CNN+ LSTM بیشترین دقت را دارد. به‌خاطر نقاط ضعف و قوت، ترکیب این دو روش بهتر از استفاده تکی است و باعث بهبود عملکرد کلی می شود.

برای مثال، روش CNN+ RNN صحت بیشتری نسبت به بیز ساده دارد، اما بیز ساده سریع تر است و به منابع محاسباتی کمتری نیاز دارد. ترکیب دو روش سیستم تشخیصی دقیق تر و موثرتری را به وجود می آورد.

5-2: سوال 2- روش ترکیبی پیشنهادی تا چه اندازه در شناسایی URLهای فیشینگ موثر است؟

روش پیشنهادی ترکیبی (MHSA و CNN) عملکرد بهتری در تشخیص URLهای فیشینگ داشته است. ترکیب شدن باعث ارتقای عملکرد نسبت به CNN و LSTM می شود. نتایج جدول 2 نشان داده که صحت و F1 روش پیشنهادی به ترتیب 98.34 و 98.30 ٪ هستند. البته FPR روش پیشنهادی 1.76 ٪ است و این یعنی تعداد بیشتری از صفحات قانونی را فیشینگ تلقی می کند.

علاوه بر این، زمان آموزش دهی روش پیشنهادی نسبتاً کم است و میانگین 32 دقیقه در هر اجرا (دوره زمانی) را دارد.

به طور خلاصه، باید گفت روش ترکیبی دو تایی (خودتوجهی چندسره و CNN) عملکرد بهتری در تشخیص URLهای فیشینگ دارد. این روش صحت و امتیاز F1 بالایی دارد. زمان آموزش آن نسبتاً کم و FPR آن اندکی بیشتر است، لذا کارایی روش ترکیبی پیشنهادی در شناسایی URLهای پیشنهادی نسبتاً بالا است.

5-3: سوال 3- روش ترکیبی پیشنهادی تا چه اندازه در شناسایی URLهای فیشینگ در مقایسه با سایر روش ها کارآمد است؟

با توجه به نتایج، روش پیشنهادی در مقایسه با بقیه روش ها عملکرد بسیار خوبی دارد. ساختارهای مختلف از جمله CNN، LSTM، CNN-CNN، CNN-LSTM با روش ترکیبی پیشنهادی (CNN و خودتوجهی چندسره) مقایسه شده اند.

این روش در تشخیص URLهای فیشینگ نسبت به بقیه روش ها بسیار موثر است. مدل پیشنهادی با 5 روش پرکاربرد مقایسه شده و کمترین FPR به میزان 0.26 ٪ بیشترین صحت به میزان 99.84٪ و F1 به میزان 99.84 را حاصل می کند. همچنین تمام روش های قبلی را از لحاظ بازیابی با نرخ 99.95 ٪ شکست می دهد. هرچند FPR روش پیشنهادی بیشتر از CNN-LSTM (0.82٪) است، اما کماکان از بقیه روش ها کمتر است.نتیجه این است که ترکیب دو روش برای تشخیص URLهای فیشینگ در مقایسه با سایر روش ها به‌شدت موثر است.

اطلاعات زیر نشان می دهند که ترکیب دو شبکه به بهبود عملکرد مدل کمک می کند. زمان آموزش دهی روش پیشنهادی نیز از CNN-LSTM و سایر روش ها کمتر است، لذا می توان گفت که روش پیشنهادی (ترکیبی) کارایی بالاتری دارد.

نتیجه گیری و پیشنهادها

حملات فیشینگ یکی از تهدیدهای اساسی نسبت به امنیت آنلاین هستند. روش های مختلفی برای تشخیص و پیشگیری از آن ها پیشنهاد شده اند. الگوریتم های یادگیری ماشین به عنوان یک رویکرد امیدوارکننده برای شناسایی URLهای فیشینگ معرفی شده اند، زیرا توانایی یادگیری از داده ها و تطبیق پذیری با تهدیدهای جدید و توسعه یافته را دارند. ما در این مطالعه انواع الگوریتم های به‌کاررفته برای تشخیص URLهای فیشینگ، مجموعه داده های به‌کاررفته برای آموزش، شاخص های صحت ارزیابی عملکرد را بررسی کرده ایم.

دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه

ISSN: 3060-6055

نتایج، بیانگر این هستند که الگوریتم های مختلف یادگیری ماشین، دارای نقاط ضعف و قوت مختلفی در تشخیص URLهای فیشینگ هستند. یادگیری نظارت شده روشی موثر برای تشخیص حملات شناخته شده است، اما یادگیری غیرنظارت شده می تواند برای شناسایی حملات جدید و مجهول به‌کار رود. یادگیری نیمه نظارتی، توازنی بین این دو روش تلقی می شود. یادگیری عمیق قدرت یادگیری مستقیم ویژگی ها از روی داده های خام را دارد و برای تشخیص حملات جدید و ناشناخته به‌کار می‌رود اما به انبوهی از داده های برچسب گذاری شده و منابع محاسباتی نیاز دارد.

از لحاظ شاخص های صحت، می توان گفت بیز ساده و جنگل تصادفی، دارای صحت های بالاتر به میزان 97.18 ٪ و 97 ٪ هستند. صحت روش CNN اندکی کمتر و 96.61 ٪ است، اما FPR بیشتری به اندازه 3.5 ٪ دارد. این یعنی تعداد بیشتری از URLهای قانونی به عنوان URL فیشینگ دسته بندی شده اند. LSTM دارای بالاترین صحت به میزان 97.20 ٪ است و نرخ مثبت کاذب پایین به اندازه 1.8 ٪ دارد، لذا اکثر URLهای فیشینگ را به‌درستی تشخیص داده و فقط چند مورد به اشتباه قانونی تلقی می شوند.

با توجه به این تحقیق، کارآمدترین روش تشخیص، یک روش ترکیبی شامل CNN و خودتوجهی چندسره است. دلیلش این است که این روش بهترین عملکرد را داشته و صحت آن 98.34 ٪ است. FPR آن کمترین مقدار (1.76٪). بازیابی 98.44، دقت 98.16 و F1 98.3 هستند. این مدل CNN را با MHSA ترکیب کرده و به تشخیص وابستگی های طولانی مدت و تحلیل همزمان چند بخش کمک می کند. به‌طور کلی بهتر از سایر مدل ها از جمله LSTM، CNN + RNN و جنگل تصادفی عمل می کند.

به‌طور کلی، این مطالعه پتانسیل(ظرفیت) الگوریتم های یادگیری ماشین برای تشخیص URLهای فیشینگ را بررسی کرده است. همچنین ترکیب کردن روش ها از جمله لیست های سیاه، فیلتر DNS، آموزش آگاهی به کاربران و الگوریتم های یادگیری ماشین را پیشنهاد می‌کند که می توانند حفاظت لازم در برابر حمله را فراهم کنند. از سوی دیگر، انتخاب الگوریتم به نیازهای خاص سازمان و ماهیت حمله فیشینگ بستگی دارد. برای بررسی کارایی سایر روش ها و ظرفیت شان در شرایط واقعی به تحقیقات بیشتری نیاز داریم.

ISSN: 3060-6055

منابع

[1] James, L. (2006). Banking on phishing. In James, L. (Ed.), Phishing Exposed (pp. 1-35). Syngress. ISBN 9781597490306

[2] Sundara Pandiyan, S., Selvaraj, P., Burugari, V. K., Benadit P, J., & Kanmani, P. (2022). Phishing attack detection using Machine Learning. Measurement: Sensors, 24, 100476. ISSN 2665-9174

[3] Ahammad, S. K. H., Kale, S. D., Upadhye, G. D., Pande, S. D., Babu, E. V., Dhumane, A. V., & Bahadur, M. D. K. J. (2022). Phishing URL detection using machine learning methods. Advances in Engineering Software, 173, 103288. ISSN 0965-9978

[4] Berners-Lee, T., Masinter, L., & McCahill, M. (Eds.). (1994). Uniform Resource Locators (URL). Request for Comments: 1738. Network Working Group. CERN. Standards Track. Updated by: 1808, 2368, 2396, 3986, 6196, 6270, 8089. Obsoleted by: 4248, 4266. Errata Exist

[5] L. Wenyin, G. Liu, B. Qiu and X. Quan, "Antiphishing through Phishing Target Discovery," in IEEE Internet Computing, vol. 16, no. 2, pp. 52-61, March- April 2012, doi: 10.1109/MIC.2011.103

[6] Safi, A., & Singh, S. (2023). A systematic literature review on phishing website detection techniques. Journal of King Saud University - Computer and Information Sciences, 35(2), 590-611. ISSN 1319-1578

[7] Vrbančič, G., Fister, I., & Podgorelec, V. (2020). Datasets for phishing websites detection. Data in Brief, 33, 106438. ISSN 2352-3409

[8] Zheng, F., Yan, Q., Leung, V. C. M., Yu, F. R., & Ming, Z. (2022). HDP-CNN: Highway deep pyramid convolution neural network combining wordlevel and character-level representations for phishing website detection. Computers & Security, 114, 102584. ISSN 0167-4048

[9] Wei, W., Ke, Q., Nowak, J., Korytkowski, M., Scherer, R., & Woźniak, M. (2020). Accurate and fast URL phishing detector: A convolutional neural network approach. Computer Networks, 178, 107275. ISSN 1389-1286

[10] Sahingoz, O. K., Baykal, S. I., & Bulut, D. (2018). Phishing detection from urls by using neural networks. Computer Science & Information Technology (CS & IT), 41-54.

[11] Remmide, M. A., Boumahdi, F., Boustia, N., Feknous, C. L., & Della, R. (2022). Detection of Phishing URLs Using Temporal Convolutional Network. Procedia Computer Science, 212, 74-82. ISSN 1877-0509.

[12] Marwa M. Emam, Nagwan Abdel Samee, Mona M. Jamjoom, Essam H. Houssein, Optimized deep learning architecture for brain tumor classification using improved Hunger Games Search Algorithm, Computers in Biology and Medicine, Volume 160, 2023, 106966, ISSN 0010-4825

[13] Sundara Pandiyan S, Prabha Selvaraj, Vijay Kumar Burugari, Julian Benadit P, Kanmani P, Phishing attack detection using Machine Learning, Measurement: Sensors, Volume 24, 2022, 100476, ISSN 2665-9174,

[14] Kai Florian Tschakert, Sudsanguan Ngamsuriyaroj, Effectiveness of and user preferences for security awareness training methodologies, Heliyon, Volume 5, Issue 6, 2019, e02010, ISSN 2405-8440

[15] Mohsen Soori, Behrooz Arezoo, Roza Dastres, Machine learning and artificial intelligence in CNC machine tools, A review, Sustainable Manufacturing and Service Economics, 2023, 100009, ISSN 2667-3444,

ISSN: 3060-6055

[16] Tianyuan Liu, Hangbin Zheng, Pai Zheng, Jinsong Bao, Junliang Wang, Xiaojia Liu, Changqi Yang, An expert knowledge-empowered CNN approach for welding radiographic image recognition, Advanced Engineering Informatics, Volume 56, 2023, 101963, ISSN 1474-0346,

[17] Jun Ma, Guolin Yu, Weizhi Xiong, Xiaolong Zhu, Safe semisupervised learning for pattern classification, Engineering Applications of Artificial Intelligence, Volume 121, 2023, 106021, ISSN 0952-1976

[18] Benavides-Astudillo, E., Fuertes, W., Sanchez-Gordon, S., Rodriguez- Galan, G., Martínez-Cepeda, V., Nuñez-Agurto, D. (2023). Comparative Study of Deep Learning Algorithms in the Detection of Phishing Attacks Based on HTML and Text Obtained from Web Pages. In: Botto-Tobar, M., Zambrano Vizuete, M., Montes León, S., Torres-Carrión, P., Durakovic, B. (eds) Applied Technologies. ICAT 2022. Communications in Computer and Information Science, vol 1755. Springer, Cham. https://doi.org/10.1007/978-3-031-24985-3_28

[19] J. Kumar, A. Santhanavijayan, B. Janet, B. Rajendran and B. S. Bindhumadhava, "Phishing Website Classification and Detection Using Machine Learning," 2020 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2020, pp. 1-6, doi: 10.1109/ICCCI48352.2020.9104161.

[20] Do, Q.N.; Selamat, A.; Krejcar, O.; Yokoi, T.; Fujita, H. Phishing Webpage Classification via Deep Learning-Based Algorithms: An Empirical Study. Appl. Sci. 2021, 11, 9210. https://doi.org/10.3390/ app11199210

[21] M. N. Alam, D. Sarma, F. F. Lima, I. Saha, R. -E. -. Ulfath and S. Hossain, "Phishing Attacks Detection using Machine Learning Approach," 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2020, pp. 1173-1179, doi: 10.1109/ICSSIT48917.2020.9214225.

[22] Y. Huang, Q. Yang, J. Qin and W. Wen, "Phishing URL Detection via CNN and Attention-Based Hierarchical RNN," 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, 2019, pp. 112-119, doi: 10.1109/TrustCom/BigDataSE.2019.00024.

[23] M. A. Adebowale, K. T. Lwin and M. A. Hossain, "Deep Learning with Convolutional Neural Network and Long Short-Term Memory for Phishing Detection," 2019 13th International Conference on Software, Knowledge, Information Management and Applications (SKIMA), Island of Ulkulhas, Maldives, 2019, pp. 1-8, doi: 10.1109/SKIMA47702.2019.8982427.

[24] Bahnsen, A. C., Bohorquez, C. E., Villegas, S., Vargas, J., & González, F. A. (2017). Classifying phishing URLs using recurrent neural networks. In 2017 APWG symposium on electronic crime research (eCrime) (pp. 1–8). Scottsdale, AZ, USA.

[25] Bahnsen, A. C., Bohorquez, C. E., Villegas, S., Vargas, J., & González, F. A. (2017). Classifying phishing URLs using recurrent neural networks. In 2017 APWG symposium on electronic crime research (eCrime) (pp. 1–8). Scottsdale, AZ, USA.

[26] Zhang J., Li X. Phishing detection method based on borderline-smote deep belief network security, privacy, and anonymity in computation, communication, and storage. SpaCCS 2017, Lecture notes in computer science, vol. 10658, Springer, Cham (2017), pp. 45-53

[27] Yang P., Zhao G., Zeng P. Phishing website detection based on multidimensional features driven by deep learning IEEE Access, 7 (2019), pp. 15196-15209