
بسم الله الرحمن الرحيم

پردیس علوم

دانشکده ریاضی، آمار و علوم کامپیوتر

شناسایی وب‌سایت‌های جعلی (فیشینگ) بر مبنای روش ELM

نگارنده:

شهرزاد عصمت

استاد راهنما:

دکتر هدیه ساجدی

پایان‌نامه برای دریافت درجه کارشناسی

در رشته علوم کامپیوتر

چکیده

ماشین با یادگیری سریع (ELM) و انواع آن یک مدل شبکه‌ی عصبی رو به جلو برای طبقه‌بندی و دسته‌بندی و رگرسیون و تقریب و ... است که در سال‌های اخیر بسیار مورد توجه قرار گرفته است. این روش، یک روش کارآمد و سریع برای یادگیری ویژگی است. مدل ELM می‌تواند یک قالب یکپارچه را با انواع انتقال ویژگی‌های وسیعی که می‌توان در لایه مخفی استفاده کرد، فراهم می‌کند که می‌تواند به طور مستقیم در دسته‌بندی چند دسته‌ای و رگرسیون به کار رود. مدل ELM بر روی شبکه‌های تعمیم یافته فیدفوروارد با تک لایه مخفی (SLFN) کار می‌کند. در مدل ELM لایه مخفی[1] نیاز به تنظیم ندارد و توابع این لایه که یک انتقال ویژگی به فضای جدید است از قبل مشخص است. این روش می‌تواند در دنیای امروز که اینترنت اهمیت ویژه‌ای پیدا کرده است به ما کمک کند. این اهمیت نه تنها برای کاربرهای شخصی است بلکه برای سازمان‌ها و ارگان‌هایی که تجارت الکترونیک انجام می‌دهند نیز اهمیت دارد. در دنیای اینترنت این کاربران و منافع آن‌ها هر روزه مورد حمله‌های اینترنتی و رفتارهایی که موجب زیان‌های اقتصادی و دزدی هویت و اطلاعات شخصی هستند، قرار می‌گیرند که به آن فیشینگ گفته می‌شود. ما با این روش به دنبال شناسایی وب‌سایت‌های جعلی‌ای هستیم که عامل این حمله‌ها هستند. با استفاده از ویژگی وب‌سایت و الگوریتم یادگیری ELM این وب‌سایت‌ها را با درصد خطای اندکی شناسایی می‌کنیم.

[1] hidden layer

فهرست مطالب

فصل ۱

یادگیری ماشین

یادگیری ماشین یکی از کاربردهای هوش مصنوعی (AI) است که سیستم‌ها را قادر می‌سازد به طور خودکار و از طریق تجربه و بدون برنامه‌ریزی، یاد بگیرند و خود را بهبود دهند. تمرکز این تکنولوژی بر توسعه برنامه‌های کامپیوتری می‌باشد که به داده‌ها دسترسی دارند و می‌توانند از این داده‌ها استفاده کرده تا خودشان یاد بگیرند. فرایند یادگیری با مشاهدات و داده‌هایی مثل نمونه‌ها و تجربه‌های مستقیم و یا دستورالعمل‌ها آغاز می‌شود تا الگویی در داده‌ها پیدا شود و در آینده تصمیمات بهتری بر پایه مثال‌هایی که ما فراهم کرده‌ایم، اتخاذ شود. هدف اولیه این است که اجازه دهیم کامپیوترها بدون دخالت یا کمک انسان، به طور خودکار یاد بگیرند و اقدامات را مطابق با آن انجام دهند.

۱.۱ برخی از روش‌های یادگیری ماشین Machine Learning

الگوریتم‌های یادگیری ماشین اغلب به عنوان نظارت شده یا نظارت نشده، دسته‌بندی می‌شوند.

- الگوریتم‌های یادگیری ماشین تحت نظارت می‌توانند آنچه را که در گذشته آموخته شده است به منظور پیش‌بینی رویدادهای آینده با استفاده از مثال‌های برچسب‌گذاری شده برای داده‌های جدید اعمال کنند. با شروع فرایند تجزیه و تحلیل یک مجموعه داده شناخته شده، الگوریتم یادگیری، یک تابع

انتزاعی برای پیش‌بینی مقادیر خروجی تولید می‌کند. سیستم می‌تواند اهداف هر ورودی جدید را پس از آموزش کافی فراهم کند. الگوریتم یادگیری همچنین می‌تواند خروجی خود را با خروجی صحیحِ در نظر گرفته شده مقایسه کرده و به منظور تغییر مدل، خطای خود را پیدا کند.

- در مقابل، الگوریتم‌های یادگیری ماشین بدون نظارت زمانی استفاده می‌شود که اطلاعات مورد استفاده برای آموزش، طبقه‌بندی و برچسب‌گذاری نشده‌اند. در یادگیری بدون نظارت، ماشین یاد می‌گیرد که چگونه سیستم‌ها می‌توانند یک تابع را برای توصیف یک ساختار پنهان از داده‌های بدون برچسب داشته باشند. سیستم، خروجی درست را تشخیص نمی‌دهد، اما این داده‌ها را بررسی می‌کند و می‌تواند نتیجه‌گیری از مجموعه داده‌ها را برای توصیف ساختارهای پنهان از داده‌های بدون برچسب به کار بگیرد.

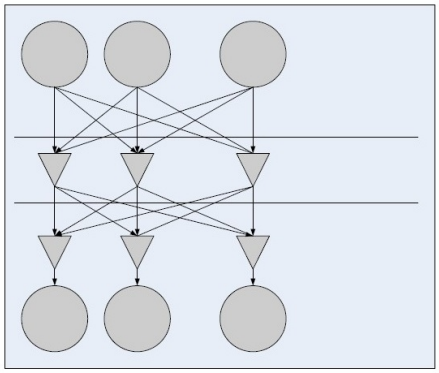
- الگوریتم‌های یادگیری ماشین نیمه‌نظارتی در جایی بین یادگیری تحت نظارت و بدون نظارت قرار می‌گیرند، زیرا از آموزش با برچسب و بدون برچسب استفاده می‌کنند – معمولا مقدار کمی از داده‌ها برچسب‌گذاری شده و مقدار زیادی از داده‌ها، بدون برچسب هستند. سیستم‌هایی که از این روش استفاده می‌کنند، می‌توانند به طور قابل توجهی دقت یادگیری را بهبود دهند. معمولا، یادگیری نیمه نظارتی زمانی انتخاب می‌شود که داده‌های برچسب‌دار به دست آمده مستلزم منابع تخصصی و مرتبط به منظور آموزش آن / یادگیری از آن است. در غیر این صورت، به دست آوردن داده‌های بدون برچسب به طور کلی نیازی به منابع اضافی ندارد.

- الگوریتم‌های یادگیری تقویتی، یک روش یادگیری است که با تولید عمل‌ها و کشف اشتباهات و پاداش‌ها با محیط خود ارتباط برقرار می‌کند. بازخورد آزمایشی و خطا و پاداش تاخیر بیشتر مربوط به یادگیری تقویت است. این روش به ماشین‌ها و عوامل نرم‌افزاری اجازه می‌دهد تا به طور خودکار رفتار مطلوب را در یک زمینه خاص به منظور به حداکثر رساندن عملکرد آن تعیین کند. بازخورد پاداش ساده برای عامل به منظور این است که یاد بگیرد که بهترین عمل کدام است؛ این به عنوان تقویت کننده سیگنال شناخته شده است.

یادگیری ماشین امکان تجزیه و تحلیل مقادیر عظیم داده را فراهم می‌کند. در حالی که عموماً سریع‌تر و دقیق‌تر نتایج را برای شناسایی فرصت‌های سودآور یا خطرناک ارائه می‌دهد، ممکن است به وقت و منابع بیشتری برای آموزش درست آن نیاز باشد. ترکیب یادگیری ماشین با هوش مصنوعی AI و فناوری‌های شناختی می‌تواند آن را حتی در پردازش حجم بیشتری از اطلاعات موثرتر واقع کند.

۲.۱ شبکه عصبی چیست؟

روشی برای محاسبه است که بر پایه اتصال به هم پیوسته چندین واحد پردازشی ساخته می‌شود. شبکه از تعداد دلخواهی سلول یا گره یا واحد یا نرون تشکیل می‌شود که مجموعه ورودی را به خروجی ربط می‌دهند. نوع خاص آن شبکه عصبی مصنوعی روشی عملی برای یادگیری توابع گوناگون نظیر توابع با مقادیر حقیقی، توابع با مقادیر گسسته و توابع با مقادیر برداری می‌باشد. یادگیری شبکه عصبی در برابر خطاهای داده‌های آموزشی مصون بوده و این‌گونه شبکه‌ها با موفقیت به مسائلی نظیر شناسائی گفتار، شناسائی و تعبیر تصاویر، و یادگیری روبات اعمال شده‌است.



شکل ۱.۱: شبکه عصبی رو به جلو

قابلیت‌های شبکه عصبی:

- محاسبه یک تابع معلوم
- تقریب یک تابع ناشناخته

- شناسائی الگو
- پردازش سیگنال
- یادگیری انجام موارد فوق

از موارد کاربرد روزمره شبکه‌های عصبی می‌توان به شبکه‌های آدالاین اشاره نمود که در خطوط مخابراتی جهت کاهش نویز به کار می‌رود و نیز در سیستم‌های تشخیص متن و صدا و ...نیز کاربرد فراوان دارد.[۳]

مسائل مناسب برای یادگیری شبکه‌های عصبی

- خطا در داده‌های آموزشی وجود داشته باشد. مثل مسائلی که داده‌های آموزشی دارای نویز حاصل از دادهای سنسورها نظیر دوربین و میکروفن‌ها هستند.
- مواردی که نمونه‌ها توسط مقادیر زیادی زوج ویژگی_مقدار نشان داده شده باشند. نظیر داده‌های حاصل از یک دوربین ویدئوئی.
- تابع هدف دارای مقادیر پیوسته باشد.
- زمان کافی برای یادگیری وجود داشته باشد. این روش در مقایسه با روش‌های دیگر نظیر درخت تصمیم نیاز به زمان بیشتری برای یادگیری دارد.
- نیازی به تعبیر تابع هدف نباشد. زیرا به سختی می‌توان وزن‌های یادگرفته شده توسط شبکه را تعبیر نمود.

آنچه در همه مدل‌های یادگیر مشترک است و اساس الگوی یادگیری بر آن بنا نهاده شده، پس خور عملی است که عامل هوشمند یا ماشین روی محیط انجام داده است که باعث کسب تجربه می‌شود. حال این تجربه می‌تواند به صورت تشویق و تنبیه در مدل‌های صحیح و خطا به کار گرفته شود یا موجب ارزش‌گذاری استدلال صورت گرفته شود. به همین ترتیب در سیستم‌های احساسی پس خور محیط موجب بروز رفتار جدید می‌گردد. نگرش به یادگیری نیز از زوایای مختلف میسر است. از یک دیدگاه یادگیری را می‌توان به

یادگیری عادتی و آگاهانه تقسیم کرد[۴] یا از زاویه‌ای دیگر یادگیری به دو گروه با ناظر و بدون ناظر تقسیم می‌شود که در اولی یک مهندس دانش جهت آموزش دادن سیستم، مدتی را صرف می‌کند و با ارسال پیام‌هایی به سیستم، آن را از انجام صحیح یا غلط بودن و یا چگونگی انجام کار مطلع می‌سازد. در مدل دیگر، هرچند ممکن است معلم در کنار سیستم حاضر باشد اما ارتباط آنها محاوره‌ای نبوده و سیستم بایستی خود الگوی مناسب را بیابید.[۵] البته در بررسی سیستم‌های مختلف بایستی توجه کرد که هرچه پویایی برنامه افزایش یابد، مدت زمانی که طول می‌کشد تا سیستم به مرز خبرگی برسد افزایش خواهد یافت. در نتیجه در سیستم‌های یادگیر (بسته به مدل پیاده شده و میزان مجرد بودن سیستم از محیط) مدت زمانی جهت آموزش دادن سیستم صرف می‌شود که در این بازه زمانی پاسخ‌ها از ریسک بالایی برخوردار هستند و قابل اطمینان نمی‌باشند که این مساله را می‌توان با عنوان ضعف یک سیستم یادگیر (و در مجموع یک سیستم هوشمند و خود اصلاح) در نظر گرفت.

انواع یادگیری:

یادگیری تقویتی این نوع آموزش با برخورد و اثر متقابل عامل هوشمند و محیطی که در آن قرار دارد ایجاد می‌شود. آموزش به صورت Online انجام می‌گیرد. یعنی پیشرفت هر لحظه قابل مشاهده و بررسی است. آموزش تقویتی بر روی سیستم‌های فیزیکی دنیای واقعی پیاده‌سازی می‌شود. [۶] آموزش تقویتی به عامل‌ها اجازه می‌دهد که در برابر حالت‌های مختلف به وجود آمده برای سیستم و در شرایط ایجاد شده بر طبق سیستم تنبیه و پاداش تصمیم‌گیری نمایند و عمل درست را از بین اعمال قابل اجرا انتخاب و به عنوان پاسخ در قبال حالت دریافتی از محیط به آن بازگردانند. هنگام بروز حالتی معین در سیستم، عامل با دریافت آن از محیط، عمل مناسب را انتخاب کرده و انجام می‌دهد و اگر چنانچه این عمل درست بود پاداش دریافت کرده و اگر اشتباه بود تنبیه می‌گردد. از این رو در مواجه شدن با حالت‌های یکسان و مشابه و یا حالت تکراری در محیط، عامل می‌داند که کدام پاسخ به محیط از همه شایسته‌تر است. آموزش تقویتی باعث می‌شود عامل رفتار صحیح را بر اساس پاسخ‌هایی که از محیط دریافت می‌کند بیاموزد[۶] یعنی تعداد پاداش‌های زیاد نشانه تمایل عامل به رفتار درست

و صحیح در مقابل شرایط محیطی می‌باشد. این رفتار می‌تواند تنها یک بار یادگیری شده و یا هر بار به صورت تکاملی پیش برود. اگر چنانچه یک مساله توسط رفتار عامل حل شد، بیشترین میزان پاداش به آن تعلق می‌گیرد و لذا یادگیری عامل در خصوص آن تکمیل می‌شود. از ویژگی‌های این نوع یادگیری این است که نیاز به آموزش دهنده محاوره‌ای دارد. ایجاد وزن یعنی آن که به رفتار مناسب و صحیح از طرف عامل نمره‌ای اختصاص داده و در ازای رفتار نادرست از آن بکاهیم و در واقع به نوعی او را تنبیه کنیم[۷] و در نتیجه عامل را به سمت رفتار مناسب سوق دهیم.

یادگیری مبتنی بر منطق و استنتاج و مورد مجموعه دیگری از مدل‌های یادگیری در ماشین، آنهایی هستند که مبتنی بر استدلال و منطق می‌باشند. به این معنی که سیستم پس از دریافت شرایط محیط، بر اساس منطق قرار داده شده در آن استدلال کرده و یک قاعده استخراج می‌کند (البته این قاعده ممکن است به صورت صریح نبوده و ضمنی باشد) سپس با استفاده از یک پایگاه دانش، حالت‌های مختلف یا قواعد را در آن ذخیره می‌کند تا جهت مراجعات بعدی از آن بهره گیرد. بحث اصلی در اینجا روی استدلال یا منطقی که در این نوع یادگیری صورت می‌پذیرد نیست. چرا که این بحث مربوط به استنتاج و منطق و پایگاه دانش می‌شود. اینجا بحث اصلی نوع مدلی است که بر پایه استنتاج بنا نهاده شده است. این نوع را دسته‌بندی‌های گوناگونی کرده‌اند. مثلاً به چهار گونه Inductive-Logical I، nductive-Statistical، Abductive و Analogical تقسیم کرده‌اند. [۸] اما ما در اینجا آنها را به طور کلی به دو دسته تقسیم می‌کنیم؛ مواردی که حالت‌های مختلف سیستم را در پایگاه دانش ذخیره می‌کنند و در بازیابی فرآیند استنتاج انجام می‌شود. مانند Case-base. مواردی که حالت‌های مختلف سیستم پس از ارزیابی اولیه و در مقایسه با قواعد موجود در پایگاه دانش، موجب تولید و کشف قاعده جدید می‌شوند که قاعده جدید در پایگاه دانش ذخیره می‌شود. بطور کلی یادگیری‌های Rule-base مانند Inductive learning یا Decision Trees.

در مدل اول، سیستم بایستی حالت موجود محیط را با حالت‌های مختلف موجود در پایگاه دانش مقایسه کرده و حالت مناسب را برگزیند و سپس به استدلال بپردازد که این مساله باعث می‌شود زمان

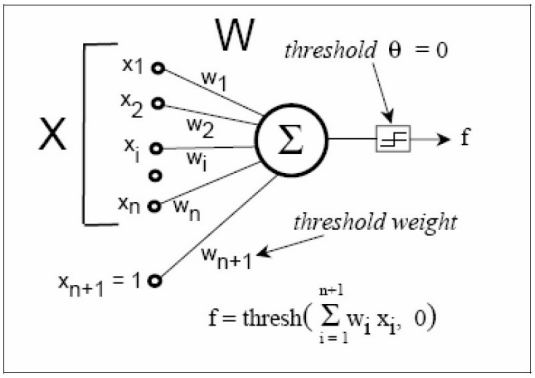
زیادی هنگام بازیابی و اعمال رفتار مناسب از جانب سیستم سپری شود. همچنین با هر بار فراگیری حالت جدید، سیستم مجبور به سازماندهی مجدد پایگاه دانش می‌باشد که این مساله نیز زمان زیادی می‌گیرد.[۹] در مدل دوم نیز به واسطه این که در پایگاه دانش قاعده صریح ذخیره شده است (و نه حالت) یافتن قاعده یا قاعده‌های متناسب با حالت موجود محیط دشواری‌های خاصی دارد ضمن این که استخراج قاعده از حالت‌های مختلف رخ داده نیز خود نیاز به منطق استنتاجی قوی دارد که به نوبه خود تعریف آن دشوار است.

مشکل اساسی این نوع مدل‌ها این است که زمان زیادی صرف ذخیره و بازیابی پایگاه دانش می‌شود و در واقع جهت سیستم‌های بلادرنگ مناسب نیستند. در عوض جواب‌های نسبتاً مطمئنی ارائه می‌دهند و می‌توان با کمک آنها سیستم‌های هوشمندی تولید کرد که استدلال کنند و منطق کشف نمایند. مشکل دیگر این که معمولاً پایگاه دانش فضای زیادی اشغال می‌کند و در مواردی که محیط وسیع و پیوسته با حالت‌های متعدد و نامحدود داشته باشیم، با مشکل حافظه مواجه هستیم. به علاوه آن که هرچه سیستم به خبرگی نزدیک‌تر شود(پایگاه دانش بزرگ‌تر شود) زمان تصمیم‌گیری افزایش می‌یابد که البته این مساله در Real-baseها بهتر از Case-baseها می‌باشد.

یادگیری احساسی معمولاً در سیستم‌های کنترلی جهت حفظ پایداری سیستم باید بیش از یک معیار لحاظ شود تا بتوان پاسخ قابل قبولی از سیستم انتظار داشت. یکی از روش‌های موفق که در سال‌های اخیر در سیستم‌های کنترلی طرح است، کنترل کننده عاطفی با تکیه بر تغییر پارامترهای سیستم، بر مبنای یک سیگنال عاطفی پیوسته است معنای این گفته این است که در سیستم کنترلی مورد نظر، عواملی را به عنوان عواطف پایه در نظر می‌گیریم که هر کدام از آنها در صورت بروز برخی محرک‌ها از جانب محیط تحریک شده و فعال می‌شوند که البته یافتن عواطف پایه بسته به طراحی ساختار کنترلی دارد. پس از تعریف، عامل تلاش می‌کند که با اعمال اثر عاطفه تعریف شده، وضعیت سیستم را بهینه سازد.

یادگیری توسط شبکه‌های عصبی مصنوعی با الگو گرفتن از عملکرد مدل Walter Pitts و Waren Mc Culloch ایده اصلی آن در ۱۹۴۰ توسط نرون‌های عصبی مغز انسان مطرح شد. فرضیات

مهم در شبکه‌های عصبی مصنوعی از این قرار است: داده پردازی اطلاعات در اجزای ساده به نام نرون صورت میگیرد. اطلاعات بین نرون‌ها از طریق ارتباطات آنها ردوبدل می‌شود. هر یک از این رابطه‌ها دارای وزن W مختص به خود هستند که در مقدار اطلاعات ردوبدل شده با سایر نرون ها ضرب می‌شوند و به مرور زمان این وزن‌ها تنظیم می‌گردند. در واقع از این منظر است که شبکه از محیط تاثیر پذیرفته و آموزش می‌بینند. هر یک از نرون‌ها برای محاسبهٔ خروجی خود، دارای یک تابع فعال‌سازی است که معمولاً تابعی غیر خطی است و روی ورودی‌ها اعمال می‌شود. هر نرون در صورتی خروجی خواهد داشت که حاصل تابع فعال‌سازش آن از یک آستانه بیشتر شود. شکل یک نرون به همراه پارامترهای مذکور را در شکل زیر مشاهده می‌کنیم. شبکه‌های عصبی یاد می‌گیرند



شکل ۲.۱: یک شبکه عصبی

که مسأله‌ای را حل کنند و در واقع برنامه‌ریزی قبلی نمی‌شوند. در واقع تنظیم وزن‌های ورودی هر نرون عصبی باعث یادگیری کل شبکه می‌شود که این تنظیم بر اساس مدل پیاده‌سازی شده می‌تواند با ناظر یا بدون ناظر صورت پذیرد. شبکه‌های عصبی مصنوعی می‌توانند دارای لایه‌های متعددی باشند و یا یک لایه باشند. مدل‌سازی با سیستم‌های غیرخطی ، مقاوم بودن و تحمل آسیب‌ها، قابل یادگیر بودن (یعنی توانایی تنظیم وزنهای شبکه) قابلیت تعمیم، سرعت بالا به دلیل پردازش‌های موازی، قابلیت سازگاری با تغییرات سیستم و ...از ویژگی‌های شبکه‌های عصبی مصنوعی هستند. از کاربردهای شبکه‌های عصبی می‌توان به ذخیره و بازبینی داده‌ها، دسته‌بندی اشکالی که مشابه هم هستند و بهینه‌سازی تعیین جواب با وجود قیود مختلف، تقریب توابع و ...اشاره کرد.

۳.۱ الهام از طبیعت

مطالعه شبکه‌های عصبی مصنوعی تا حد زیادی ملهم از سیستم‌های یادگیر طبیعی است که در آنها یک مجموعه پیچیده از نرون‌های به هم متصل در کار یادگیری دخیل هستند. گمان می‌رود که مغز انسان از تعداد $۱۰^{۱۱}$ نرون تشکیل شده باشد که هر نرون با تقریبا $۱۰^{۴}$ نرون دیگر در ارتباط است. سرعت سوئیچنگ نرون‌ها در حدود $۱۰^{-۳}$ ثانیه است که در مقایسه با کامپیوترها ($۱۰^{-۱۰}$ ثانیه) بسیار ناچیز می‌نماید. با این وجود آدمی قادر است در ۰/۱ ثانیه تصویر یک انسان را بازشناسائی نماید. این قدرت فوق العاده باید از پردازش موازی توزیع شده در تعدادی زیادی از نرون‌ها حاصل شده باشد. نوعی از شبکه عصبی برمبنای یک واحد محاسباتی به نام پرسپترون ساخته می‌شود. یک پرسپترون برداری از ورودی‌های با مقادیر حقیقی را گرفته و یک ترکیب خطی از این ورودی‌ها را محاسبه می‌کند. اگر حاصل از یک مقدار آستانه بیشتر بود خروجی پرسپترون برابر با ۱ و در غیر اینصورت معادل ۱ – خواهد بود.

فصل ۲

ماشین یادگیری سریع ELM

۱.۲ ELM

ELM در اصل برای شبکه‌های عصبی با فیدبک از پیش لایه پنهان تک (SLFNs) توسعه یافته است و سپس برای SLNFs کلی تعمیم‌یافته است که در آن لایه پنهان مستلزم نورون یکسان نمی‌باشد. ELM نخست به صورت تصادفی وزن‌های ورودی و بایاس‌های لایه پنهان را اختصاص می‌دهد و سپس به صورت تحلیلی وزن‌های خروجی SLFNs را تعیین می‌کند. آن می‌تواند عملکرد کلی بهتری را نسبت به الگوریتم‌های یادگیری مرسوم دیگر در سرعت یادگیری بسیار سریع به دست آوردبه علاوه ELM کمتر نسبت به پارامترهای توسط کاربر مشخص شده حساس می‌باشد و می‌تواند سریع‌تر و راحت‌تر گسترش یابد.

بـه ازای N نـمـونـه متمـایز دلـخواه (x_j, t_j)، که در آن $x_J = [x_{j1}, x_{j2}, \ldots, x_{jn}]^T \in \mathbb{R}^n$ و $t_j = [t_{j1}, t_{j2}, \ldots, t_{jm}]^T \in \mathbb{R}^m$ می‌باشد، SLFNs استاندارد با L گره پنهان و تابع فعال‌سازی $g(x)$ به صورت ریاضی بدین صورت مدل می‌شود

$$\sum_{j=1}^{L} \boldsymbol{\beta}_j g_i(\mathbf{x}_i) = \sum_{i=1}^{L} \boldsymbol{\beta}_i g(\mathbf{w}_i \cdot \mathbf{x}_j + b_i) = \mathbf{o}_j, \qquad (j = 1, 2, \ldots, N) \qquad (۱.۲)$$

که در آن $\mathbf{w}_i = [w_{i1}, w_{i2}, \ldots, w_{in}]^T$ بردار وزنی است که گره پنهان iام را به گره‌های ورودی متصل می‌کند، $\boldsymbol{\beta}_i = [\beta_{i1}, \beta_{i2}, \ldots, \beta_{im}]^T$ بردار وزنی است که گره پنهان iام را به گره‌های خروجی متصل می‌کند،

b_i آستانه مربوط به گره پنهان iام می‌باشد و $o_i = [o_{j1}, o_{j2}, \ldots, o_{jm}]^T$ بردار خروجی jام SLFNs می‌باشد.

SLFNs استاندارد با L گره پنهان و تابع فعال‌سازی $g(x)$ می‌تواند این N نمونه را با صفر تقریب زند.

این موضوع به معنای $\sum_{j=1}^{L} \|o_j - t_j\| = 0$ است و $\boldsymbol{\beta}_i$، $\mathbf{w}_i$ و b_iای وجود دارد بطوری که

$$\sum_{j=1}^{L} \boldsymbol{\beta}_i g(\mathbf{w}_i \cdot \mathbf{x}_j + b_i) = t_j, \qquad (j = 1, 2, \ldots, N) \tag{۲.۲}$$

معادله فوق می‌تواند بطور فشرده به صورت زیر بیان شود

$$H\boldsymbol{\beta} = T, \tag{۳.۲}$$

که در آن

$$\begin{aligned} & H(\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_L, b_1, b_2, \ldots, b_L, x_1, x_2, \ldots, x_L) \\ & = [h_{ij}] \\ & = \begin{bmatrix} g(\mathbf{w}_1 \cdot \mathbf{x}_1 + b_1) & g(\mathbf{w}_2 \cdot \mathbf{x}_1 + b_2) & L & g(\mathbf{w}_L \cdot \mathbf{x}_1 + b_L) \\ g(\mathbf{w}_1 \cdot \mathbf{x}_2 + b_1) & g(\mathbf{w}_2 \cdot \mathbf{x}_2 + b_2) & L & g(\mathbf{w}_L \cdot \mathbf{x}_2 + b_L) \\ M & M & M & M \\ g(\mathbf{w}_1 \cdot \mathbf{x}_N + b_1) & g(\mathbf{w}_2 \cdot \mathbf{x}_N + b_2) & L & g(\mathbf{w}_L \cdot \mathbf{x}_N + b_L) \end{bmatrix}_{N \times L} \end{aligned} \tag{۴.۲}$$

و

$$\boldsymbol{\beta} = \begin{bmatrix} \beta_{11} & \beta_{12} & L & \beta_{1m} \\ \beta_{21} & \beta_{22} & L & \beta_{2m} \\ M & M & M & M \\ \beta_{L1} & \beta_{L2} & L & \beta_{Lm} \end{bmatrix}_{L \times m} \quad , \quad \mathbf{T} = \begin{bmatrix} t_{11} & t_{12} & L & t_{1m} \\ t_{21} & t_{22} & L & t_{2m} \\ M & M & M & M \\ t_{N1} & t_{N2} & L & t_{Nm} \end{bmatrix}_{N \times m} \tag{۵.۲}$$

H ماتریس خروجی لایه پنهان شبکه عصبی نامیده می‌شود و ستون iاُم H خروجی گره پنهان iاُم با توجه به ورودی‌های $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_N$ می‌باشد. کوچکترین راه حل با حداقل مربعات نرم مربوط به سیستم خطی فوق به صورت زیر است

$$\hat{\boldsymbol{\beta}} = \mathbf{H}^{\dagger}\mathbf{T} \tag{۶.۲}$$

که در آن $\mathbf{H}^{\dagger}$ Moore-Penrose می‌باشد که معکوس H را تعمیم می‌دهد. سپس تابع خروجی ELM می‌تواند به صورت زیر مدل شود:

$$f(x) = \mathbf{h}(x)\beta = \mathbf{h}(x)\mathbf{H}^{\dagger}\mathbf{T}. \qquad (۷.۲)$$

انواع توابع فعال‌ساز:

۱. Sigmoid function

$$G(a, b, x) = \frac{۱}{۱ + \exp(-(a \cdot x + b))}.$$

۲. Hard-limit function

$$G(a, b, x) = \begin{cases} ۱ & a \cdot x - b \geq ۰ \\ ۰ & \text{otherwise} \end{cases}$$

۳. Gaussian function

$$G(a, b, x) = \exp(-b\|x - a\|^{۲}).$$

۴. Multiquadric function

$$G(a, b, x) = (\|x - a\|^{۲} + b^{۲})^{۱/۲}.$$

فصل ۳

کارهای مرتبط

اگرچه راه‌حل‌های زیادی درباره‌ی مسأله فیشینگ داده شده است اما این راه‌حل‌ها هیچ کدام نمی‌توانند درست تصمیم‌گیری کنند چون مثبت کاذب (false positive) بالایی دارند. ما در این بخش چند تلاش انجام شده در این زمینه را بررسی می‌کنیم. یکی از کارهای انجام شده [۵] در این زمینه بر مبنای الگوریتم‌های طبقه‌بندی تجمعی است. نویسنده ۲۷ ویژگی متفاوت از وب‌سایت‌های متفاوت را جمع‌آوری کرده است که در جدول ۱ نشان داده شده است. برای به دست آوردن آن دسته از ویژگی‌هایی که ۳ مقدار نادقیق حقیقی و اصل و مشکوک را دارند، نویسندگان آزمایش‌هایی را با استفاده از تکنیک‌های داده کاوی MCAR، CBA، C4.5، PRISM، PART و JRip انجام داده‌اند. نتایج به دست آمده نشان داد که رابطه‌ی مهمی بین ویژگی‌های "domain identity" و "URL" برقرار است. سپس نویسندگان از ۲۷ ویژگی برای پیش‌بینی نوع وب‌سایت‌ها براساس یک روش نادقیق داده کاوی استفاده کردند. با این که این روش یک راه حل امیدوار کننده به نظر می‌رسد اما در آن روشن نیست که چگونه این ویژگی‌ها مخصوصا ویژگی‌های مربوط به عوامل انسانی از وب‌سایت استخراج می‌شوند علاوه بر این مدل آنها با یک رویکرد چند سطحی (multilayered) کار می‌کند. هر لایه باید قوانین خودش را داشته باشد با این حال این روشن نیست که آیا این قوانین براساس تجربیات انسانی هستند با این که با یک روش استدلالی به دست آمده‌اند. همچنین نویسنده یک وب‌سایت را یا بسیار جعلی یا جعلی یا مشکوک یا حقیقی یا بسیار حقیقی دسته‌بندی می‌کند

Features	Phishing factor indicator
URL and domain identity	Using IP address
	Request URL
	URL of anchor
	DNS record
	Abnormal URL
Security and encryption	SSL certificate
	Certification Authority
	Abnormal cookie
	Distinguished names certificate (DN)
Sourse code and Java Script	Redirect pages
	Straddling attack
	Pharming attack
	Using on mouseOver
	Serve form handler
Page style and content	Spelling errors
	Copying website
	“submit” button
	Using pop-ups windows
	Disabling right click
Web address bar	Long URL address
	Replacing similar characters for URL
	Adding prefix or suffix
	Using the @ symbol to confuse
	Using hexadecimal character codes
Social human factor	much emphasis on security and response
	Generic salutation
	Buying time to access accounts

جدول ۱.۳: ویژگی‌های وب‌سایت‌ها

اما مرز این طبقه‌بندی را روشن نمی‌کند. اصولا روش‌های نادقیق (fuzzy) داده کاوی نمی‌توانند روش‌های مناسبی برای تصمیم‌گیری‌هایی با دقت فوق‌العاده باشند.

روش دیگری که در شناسایی وب‌سایت‌های جعلی به کار رفته CANTINA با ویژگی‌های اضافه است. نویسندگان ۱۰۰ وب‌سایت جعلی و ۱۰۰ وب‌سایت قانونی را در آزمایش‌هایشان استفاده کرده‌اند. بر اساس CANTINA، ۸ ویژگی برای شناسایی وب‌سایت‌های جعلی لازم است. (domain age , known image

.(,suspicious URL , suspicious link , IP address , dots in URL, forms and TF-IDF
چند تغییر روی ویژگی‌ها در حین آزمایش ایجاد شده است که عبارت‌اند از: ویژگی forms به عنوان filterای در نظر گرفته شده است برای تصمیم‌گیری در مورد قانونی بودن وب‌سایت چون وب‌سایت‌های تقلبی‌ای که موجب از دست رفتن اطلاعات کاربران می‌شود، باید شامل forms با بلوک‌های ورودی باشد. ویژگی‌های known image و domain age در نظر گرفته نشده‌اند چون نویسندگان آن را ناچیز دانسته‌اند.

نویسندگان ۳ نوع آزمایش روی مجموعه‌ی داده‌ها انجام داده‌اند که اولین آن یک CANTINA با مجموعه ویژگی‌های کاهش یافته (dots in URL , IP address ,suspicious URL , suspicious link) است. دومین آزمایش شامل این آزمایش است که آیا ویژگی‌های جدید domain top-page similarity آنقدری قابل توجه هستند که نقش کلیدی در شناسایی نوع وب‌سایت داشته باشد یا نه. آزمایش سوم نتایج را پس از اضافه کردن یک ویژگی جدید به CANTINA کاهش یافته در آزمایش اول بررسی می‌کند. با مقایسه‌ی کارکرد مدل جدید پس از اضابه شدن ویژگی جدید متوجه شده‌اند که این ویژگی جدید نقش کلیدی در تعیین نوع وب‌سایت دارد. درست‌ترین الگوریتم، شبکه‌ی عصبی با ضریب خطای ۷,۵ درصد بود که بعد از SVM، Random forest با ضریب خطای ۸,۵ درصد قرار دارد این در حالی است که NAÏVE Bayes دارای بدترین ضریب خطای ۲۲,۵ درصد است.

یک روش جدیدتر به نام dynamic security skins در ۲۰۱۰ روی این موضوع انجام شد. چون هر دو طراح سیستم و فیشرها (سارقان) به ظاهر و اینترفیس هم برای محافظت هم برای گول زدن اهمیت می‌دهند، این روش به این صورت است که یک تصویر سری را به اشتراک می‌گذارند که به سرورها این امکان را می‌دهد که هویت خود را با یک تایید ساده از سمت کاربر تایید کنند. این تکنیک نیاز دارد که کاربران نایید کنند خود را توسط مقایسه‌ی تصویر مورد انتظار را با تصویر تولید شده توسط سرور انجام دهند. نویسندگان شمای خود را با نسخه‌ی توسعه یافته Mozilla Firefox browser پیاده‌سازی کردند. نتجه‌ی عمده و مخرب این شما این است که کاربران باید سختی تشخیص جعلی و اصلی بودن وبسایت از روی این شما را خود به دوش بکشند. هم چنین این رویکرد نیاز به یک تغییر بنیادین در زیرساخت کاربر و سرور دارد. علاوه بر این، این تکنیک اگر کاربران از کامپیوترهای عمومی استفاده کنند نمی‌تواند هیچ‌گونه

حفاظتی را تامین کند.

فصل ۴

نتایج

در این پروژه با استفاده از مجموعه داده‌های جمع‌آوری شده به آدرس:

https://archive.ics.uci.edu/ml/machine-learning-databases/00327/Training

الگوریتم یادگیری ELM با بررسی ویژگی‌های مربوط به وب‌سایت‌ها در مورد جعلی و غیر جعلی بودن آن‌ها تصمیم‌گیری می‌کند. در بررسی ما ۱۷ ویژگی مورد بررسی قرار گرفته‌اند که برخی دودویی هستند و دارای مقادیر جعلی و قانونی هستند و برخی دیگر دارای دیگر ۳ مقداری هستند و دارای مقادیر جعلی و قانونی و مشکوک هستند. این ویژگی‌ها عبارت‌اند از:

```
having_IP_Address  { -1,1 }
URL_Length   { 1,0,-1 }
Shortining_Service { 1,-1 }
having_At_Symbol   { 1,-1 }
double_slash_redirecting { -1,1 }
Prefix_Suffix  { -1,1 }
having_Sub_Domain  { -1,0,1 }
```

SSLfinal_State { -1,1,0 }

Domain_registeration_length { -1,1 }

Favicon { 1,-1 }

port { 1,-1 }

HTTPS_token { -1,1 }

Request_URL { 1,-1 }

URL_of_Anchor { -1,0,1 }

Links_in_tags { 1,-1,0 }

SFH { -1,1,0 }

Submitting_to_email { -1,1 }

Abnormal_URL { -1,1 }

Redirect { 0,1 }

on_mouseover { 1,-1 }

RightClick { 1,-1 }

popUpWidnow { 1,-1 }

Iframe { 1,-1 }

age_of_domain { -1,1 }

DNSRecord { -1,1 }

web_traffic { -1,0,1 }

Page_Rank { -1,1 }

Google_Index { 1,-1 }

Links_pointing_to_page { 1,0,-1 }

Statistical_report { -1,1 }

```
Result  { -1,1 }
```

به اختصار درباره‌ی چند ویژگی از ویژگی‌های فوق در زیر توضیح داده شده است:

۱. استفاده از IP address: داشتن IP address در قسمت hostname در URL به این معناست که کاربر با احتمال خوبی می‌تواند مطمئن باشد که کسی در حال تلاش برای سرقت اطلاعات شخصی اوست. این ویژگی دودویی است. مثالی از استفاده از IP address در زیر آمده است:

http://91.121.10.211/*chems/webscr/verify

۲. long URL: سارقان اطلاعات به دنبال این هستند که بخش مشکوک URL را مخفی کنند که این کار به این صورت انجام می‌شود که یا از کاربر دوباره درخواست اطلاعاتی می‌شود که قبلاً آنها را تایید کرده است یا این که صفحه‌ای با domain مشکوک باز شود. از نظر علمی هیچ طول قابل اعتماد مشخصی از domain وجود ندارد که از طریق آن بتوان URL وب‌سایت‌های جعلی از قانونی را تشخیص داد. با این حال اگر طول URL کمتر از ۵۴ کاراکتر باشد قانونی، اگر بین ۵۴ تا ۷۵ باشد مشکوک و در غیر این صورت جعلی است. این ویژگی ۳ مقداری است.

۳. داشتن نماد @ در URL: همانطور که قبلا ذکر شد سارقان به دنبال مخفی کردن بخش مشکوک URL هستند. یکی دیگر از چیزهایی که موجب مشکوک شدن می‌شود وجود @ در URL است. این نماد مرورگر را به این سمت هدایت می‌کند که هر چیزی قبل این نماد را نادیده بگیرد و بعد آن را در نظر بگیرد. این ویژگی دودویی است.

۴. اضافه کردن پسوند و پیشوند به URL: سارقان به دنبال این هستند که کاری کنند که URL را طوری تغییر شکل دهند که شبیه قانونی باشد. یک تکنیک برای این کار این است که به URL پسوند یا پیشوند اضافه کنند تا شکل قانونی بگیرد. این ویژگی دودویی است.

۵. داشتن sub-domain در URL: یک تکنیک دیگر برای گول زدن کاربران اضافه کردن sub-domain است این کار باعث می‌شود کاربران باور کنند که با یک وب‌سایت معتبر روبرو هستند.

این ویژگی ۳ مقداری است به این صورت که اگر URL یک sub-domain داشته باشد مشکوک است و اگر بیشتر از یک sub-domain داشته باشد، جعلی و اگر sub-domain نداشته باشد قانونی در نظر گرفته می‌شود.

۶. سوء استفاده از HTTPs: وجود HTTP به هنگامی که اطلاعات حساسی در حال انتقال است این مساله را آشکار می‌سازد که این وب‌سایت با یک وب‌سایت درست مرتبط است. با این حال سارقان ممکن است از HTTPهای غیر معتبر برای گول زدن کاربران استفاده کنند. یک روش پیشنهاد شده برای چک کردن HTTP این است که ببینیم که آیا توسط GoeTrust و GoDAddy و Network Solution و Thawte و VeriSign تایید شده است یا نه! این ویژگی ۳ مقداری است.

۷. Request URL: یک صفحه‌ی وب شامل متن و چند چیز دیگر مثل عکس‌ها و فیلم‌ها است. اغلب، این چیزها از یک صفحه‌ی وب با domain یکسان باید بارگذاری شوند. اگر این چیزها توسط یک domain متفاوت با domain تایپ شده در URL address bar باشد، آنگاه با احتمال بالایی مشکوک به جعلی بودن است. نسبتی که چیزهای بارگذاری شده از یک domain متفاوت مقدار داده شده به این ویژگی را مشخص می‌کند. اگر این نسبت کمتر از ۲۰ درصد باشد، قانونی است اگر ۲۰ تا ۵۰ درصد باشد مشکوک و در غیر این صورت جعلی است. این ویژگی ۳ مقداری است.

چندین آزمایش انجام شده است که در هر یک مقادیر پارامترها تغییر داده شده‌اند تا به بهترین ضریب درستی و کمترین درصد خطا برسیم. بخشی از مجموعه‌ی داده‌ها را به عنوان مجموعه داده‌ی آموزشی و بخشی از آن را به عنوان مجموعه داده‌ی آزمایش در نظر گرفتیم.

این روش نسبت به سایر روش‌ها این برتری را دارد که درستی آن با تغییر پارامترها بهبود یافته است. در این روش با توجه به ویژگی‌های هر وب‌سایت و مجموعه داده‌های یادگیری، داده‌های آزمایشی بررسی می شوند . در جدول‌های زیر نتایج آزمایش‌های انجام شده و پارامترها نشان داده شده است .

چندین آزمایش انجام شد که در هر یک، یک پارامتر را تغییر دادیم. در مدل ما تفاوت درستی پیش‌بینی مجموعه داده‌های تست و آموزش کم است و این به این معناست که میزان خطا کم شده است.

در این مدل نوع تابع فعال‌ساز و تعداد نورون‌های لایه‌ی مخفی را هر بار تغییر داده‌ام تا به درصد درستی بهتری روی داده‌های تست آزمایش برسیم. انواع تابع‌های فعال‌ساز مورد استفاده عبارتند از:

Sigmoidal function Sine function Hardlim function Triangular basis function

Radial basis function (for additive type of SLFNs instead of RBF type of SLFNs)

نتایج آزمایش‌های انجام شده:

پارامتر ش آزمایش	تابع فعال‌ساز	تعداد نورون‌های پنهان	درستی مجموعه داده‌های آموزشی	درستی مجموعه داده‌های آزمایش	زمان اجرا
۱	Sigmoid	۲	۰/۶۴۳۱	۰/۶۵۲۷	۰/۱۸۷۵
۲	Sigmoid	۲۰	۰/۸۹۱۴	۰/۸۶۰۶	۰/۰۹۳۸
۳	Sigmoid	۲۰۰	۰/۹۳۲۰	۰/۹۲۶۸	۱/۲۸۱۳
۴	Sigmoid	۲۰۰۰	۰/۹۵۷۰	۰/۹۷۶۰	۵۴/۹۶۸۸
۵	Sin	۲۰۰۰	۰/۹۶۶۴	۰/۹۲۲۲	۵۶/۸۴۳۸
۶	Hardlim	۲۰۰۰	۰/۹۷۴۷	۰/۹۴۶۶	۵۵/۸۹۰۶
۷	Tribas	۲۰۰۰	۰/۹۶۷۴	۰/۹۲۸۰	۵۵/۲۰۳۱
۸	Radbas	۲۰۰۰	۰/۹۷۰۱	۰/۹۲۶۸	۵۴/۸۵۹۴
۹	Sigmoid	۳۰۰۰	۰/۹۸۲۴	۰/۹۵۳۵	۱۳۰/۶۲۵۰
۱۰	Sigmoid	۲۵۰۰	۰/۹۷۷۶	۰/۹۵۷۰	۸۵/۲۳۴۴

جدول ۱.۴: نتایج آزمایش‌ها

نتیجه‌گیری:

بر اساس آزمایش‌های فوق بهترین نتیجه مربوط به تابع فعالساز Sigmoid با ۲۰۰۰ نورون در لایه‌ی پنهان است، که درستی مجموعه داده‌های آموزشی در آن ۰/۹۵۷۰ و درستی مجموعه داده‌های آزمایشی ۰/۹۷۶۰ است.

مراجع

[1] S. M. I. H. Z. X. D. a. R. Z. Guang-Bin Huang, "IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETIC," vol. 42, 2012.

[2] A. S. P. B. O. S. C. J. a. A. L. Y. Miche, "OP-ELM: Optimally pruned extreme learning machine," IEEE Trans. Neural Netw., vol. 21, p. 158–162, 2010.

[3] Q. Z. a. L. C. W. Deng, "Regularized extreme learning machine," Proc. IEEE Symp. CIDM, p. 389–395, 2009.

[۴] مقاله بررسی تطبیقی نظریه های یادگیری در روانشناسی و مدل های یادگیری ماشین . لیلا چراغ مولایی و علیرضا انصاری

[۵] کتاب maining Data علیخانزاده

[۶] اصول NeuroScience.McGraehill

[۷] مبانی NeuroScience

[۸] مبانی شبکه های عصبی . دکتر محمد باقر منهاج

[۹] هوش مصنوعی. دکتر فهیمی

University of Tehran

College of Science

School of Mathematics, Statistics, and Computer Science

Predicting phishing websites based on ELM method

By:

Shahrzad Esmat

Under Supervision of:

Dr. Hedieh Sajedi

A thesis submitted to Graduate Studies Office

In partial fulfillment of the requirements for the degree

of B.Sc in Computer Science

2018