نشریه علمی پدافند غیرعامل

سال یازدهم، شماره ۱، بهار ۱۳۹۹، (پیاپی ۴۱): صص ۷۰-۶۳

علمی- ترویجی

تشخیص جرایم سایبری در ارتباطات برخط با رویکرد داده‌کاوی

محمد راستگو[۱]، مهرداد جلالی[۲*]

تاریخ دریافت: ۱۳۹۸/۰۷/۱۰
تاریخ پذیرش: ۱۳۹۸/۱۱/۲۸

چکیده

در سال‌های اخیر سایت‌های شبکه‌های اجتماعی برخط محبوبیت چشمگیری را به‌دست آورده‌اند. جرایم سایبری از رسانه‌های اجتماعی به عنوان پلتفرم جدید در پذیرش انواع مختلف جرایم رایانه‌ای مانند فیشینگ، اسپمینگ، اشاعه بدافزار و اذیت و آزار سایبری استفاده می‌کنند. در این تحقیق، با کمک استفاده از اطلاعات مفید در پیام‌ها، عملکرد تشخیص آزار و اذیت‌های سایبری را بهبود داده می‌شود. انتخاب بهترین مشخصه‌ها با قدرت جداکنندگی بالا بین توئیت‌های مزاحمت‌های سایبری و غیر مزاحمت‌های سایبری یک فعالیت پیچیده است که نیازمند تلاش قابل ملاحظه‌ای در ساخت مدل یادگیری ماشین می‌باشد. در این راستا عملکرد پنج روش طبقه‌بندی بیزساده، ماشین بردار پشتیبان، درخت تصمیم، k- نزدیک‌ترین همسایگی و شبکه عصبی را تحت پنج تنظیم مختلف به‌منظور انتخاب بهترین تنظیم برای مشخصه‌های پیشنهادی مقایسه شده است و با استفاده از الگوریتم‌های خفاش و ژنتیک و ازدحام ذرات پارامترهای C و سیگما را بهبود داده شده است و مقایسه‌ای بین پنج روش طبقه‌بندی با پارامترهای پیش فرض و پارامترهایی که با الگوریتم‌های بهینه‌ساز به‌دست آورده شده و مشخص شده است که الگوریتم خفاش از بین الگوریتم‌های دیگر بهینه‌ساز بهترین عملکرد را داشته است. با توجه به پژوهشی که انجام شده بیشترین دقت را با مدل SVM به ۸۶/۵۶ و بیشترین صحت را به ۸۷/۱۴ بوده است.

کلیدواژه‌ها: جرم، الگوریتم داده کاوی، ماشین بردار پشتیبان

۱- کارشناس ارشد مهندسی کامپیوتر، گرایش نرم‌افزار، دانشگاه امام رضا (ع)

۲- دانشیار، گروه مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد مشهد– (jalali@mshdiau.ac.ir)- نویسنده مسئول

۱. مقدمه

شبکه‌های اجتماعی، نسل جدیدی از سایت‌ها هستند که این روزها در کانون توجه کاربران شبکه جهانی اینترنت قرارگرفته‌اند. این‌گونه سایت‌ها بر مبنای تشکیل اجتماعات آنلاین فعالیت می‌کنند و هرکدام، دسته‌ای از کاربران اینترنتی را با ویژگی‌های خاصی گرد هم می‌آورند. این شبکه‌ها در کنار کارکرهای مثبتی که دارند، دارای ویژگی‌های منفی هستند که می‌توانند نقش ارزنده‌ای را در بروز رفتارهای بزهکارانه ایفا نمایند. این نقش را می‌توان از دو جهت بررسی کرد. اول از منظر نقشی که این شبکه‌ها می‌توانند در مهیا کردن بستری مناسب برای ارتکاب بزه در فضای سایبر فراهم نمایند، و دوم از منظر نقشی که این شبکه‌ها می‌توانند با تاثیرگذاری بر روی کاربران، عاملی مهم در وقوع بزه‌کاری در فضای حقیقی باشند. درنتیجه برای هر یک از نقش‌های پیش گفته می‌توان جرم شناختی ارائه کرد و مورد بررسی قرار داد [۱].

جهان امروز وارد عصری جدیدی شده است که مهم‌ترین نشانه آن، اهمیت یافتن اطلاعات و ارتباطات و تغییر در شیوه انتقال و ایجاد آن است. امروزه یکی از فراگیرترین و مهم‌ترین شیوه‌های ارتباطی، وب و فناوری‌های مبتنی بر آن است. فضای مجازی، عرصه‌ای بسیار وسیع برای تبادل اطلاعات و برقراری ارتباط است که به‌دلیل سرعت و تنوع در پردازش اطلاعات، بسیار مورد توجه مخاطبان قرار گرفته است. در حال حاضر، شبکه‌های اجتماعی مانند فیس‌بوک به پدیده‌ای تبدیل شده‌اند که هم دارای تهدید و هم دارای فرصت برای فضای فرهنگی محسوب می‌شود [۲].

تأثیر شبکه‌های اجتماعی بر وقوع جرم در فضای مجازی را می‌توان از طریق نقش بستری این شبکه‌ها تبیین کرد. در توضیح باید بیان داشت که گاه دراین شبکه‌ها، بستر و آماج مناسبی وجود دارد که بزهکاران بالقوه را به وقوع جرم تحریک و ترغیب می‌کند. در خصوص بستر ارتکاب جرم فراهم آمده در این شبکه‌ها می‌توان چنین عنوان داشت که در فضای حقیقی به جهت رویت‌پذیری ارتکاب جرم و دیده‌شدن مجرم، ارتکاب جرم با چالش روبه‌رو می‌شود؛ حال آن که در فضای سایبر چنین چالشی وجود ندارد و بزهکار به راحتی می‌تواند به ارتکاب جرم مبادرت ورزد. به دیگر سخن با توجه به اینکه که مجرمان در فضای سایبری از هویدا شدن هویت خویش در امان هستند، به سوی ارتکاب جرم سوق پیدا می‌کنند؛ حال آن‌که در فضای حقیقی به‌جهت نظارت طبیعی مردم یا به‌جهت نظارت فنی مثل دوربین‌های مداربسته، امکان شناخت هویت و دستگیری آنها بالا می‌رود.

به‌طور خاص، اذیت و آزار سایبری به‌عنوان یک مسأله اصلی در طی توسعه ارتباط برخط و رسانه‌های اجتماعی ظهور پیدا کرده‌اند. مزاحمت‌های سایبری می‌تواند به‌عنوان استفاده از فناوری اطلاعات و ارتباطات توسط فرد یا گروهی از کاربران به منظور آسیب به دیگران، تعریف شوند. آزار و اذیت‌های سایبری به‌طور وسیعی به‌عنوان مسأله سلامت ملی جدی تشخیص داده شده‌اند [۳].

در این پژوهش، با کمک استفاده از اطلاعات مفید در توئیت‌ها، عملکرد تشخیص آزار و اذیت‌های سایبری را بهبود داده می‌شود. به‌طور خاص، از بسیاری از مشخصه‌های مفید در توئیتر از قبیل فعالیت کاربر و محتوای توئیت به‌منظور آموزش مدل تشخیص خود و بهبود عملکرد آن استفاده می‌شود.

۲. پیشینه تحقیق

روش‌های خوشه‌بندی داده‌ها را براساس شباهتشان در یک کلاس قرار می‌دهند از اینرو می‌توان مظنونانی که دارای حالت و ویژگی‌های مشابه هستند شناسایی نمود یا نوع جنایت ارتکابی را از میان گروه‌های مختلف جرائم تشخیص داد. به‌منظور شناسایی و گروه‌بندی انواع جرائم مدلی براساس تکنیک‌های خوشه‌بندی توسط کارلیس و همکارانش ارائه گردید که یک مدل ترکیبی پواسون چند متغیره محدود با ساختار کواریانسی دو طرفه بود [۷].

مطالعه‌ای که با استفاده از رگرسیون روی اطلاعات مربوط به استفاده از اینترنت برای پیش‌بینی جرائم رایانه‌ای صورت گرفته، دو عامل میزان استفاده از کامپیوتر و عضویت در شبکه‌های اجتماعی را به‌عنوان متغیرهای اصلی پیش‌بینی کننده میزان جرائم کامپیوتری معرفی کرده است. علاوه‌بر این مشخص گردید که میزان جرائم کامپیوتری در مردان بیشتر از زنان و با افزایش تحصیلات دانشگاهی و کسب مهارت‌های کامپیوتری احتمال اینگونه جرائم در افراد افزایش می‌یابد [۴].

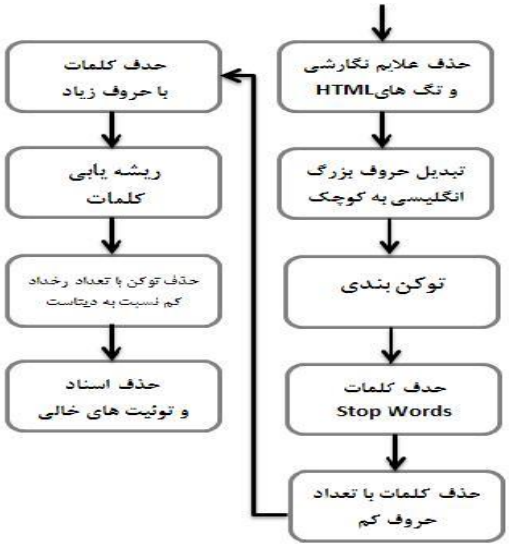
مون و همکاران [۹] از رگرسیون برای پیش‌بینی جرایم رایانه‌ای استفاده کردند. براساس نتایج به‌دست‌آمده میزان ساعات استفاده از رایانه و عضویت در گروه‌ها و شبکه‌های اینترنتی میزان جرائم را افزایش داده است.

خان و شیخ [۸] از یک سری روابط جبری در شبکه‌های اجتماعی استفاده کردند و با استفاده از جبری که به‌وجود آمده می‌توان در پیشگیری از جرایم در شبکه‌های اجتماعی استفاده کرد.

دیلمی و سینگ [۶] از ماشین بردار برای شناسایی جرایم سایبری استفاده شده است که از این ماشین برای طبقه‌بندی شبکه‌های اجتماعی فیسبوک استفاده شده است از سه الگوریتم طبقه‌بندی AdaBostM1، SVM و Navie Bayes به‌منظور پیداکردن یک درصد بالا از دقت طبقه‌بندی استفاده شده که از این سه الگوریتم SVM کارآمدتر و موثر از الگوریتم‌های دیگر است.

در مورد تشخیص خودکار گفتار نفرت از زبان توهین‌آمیز می‌باشد که در سال ۲۰۱۷ توسط دیویدسون و همکاران منتشر شده است. در این مقاله بعد از کاهش ابعاد داده شروع به اجرای الگوریتم‌های رگرسیون لجستیک، Bayes، درخت تصمیم‌گیری، جنگل‌های تصادفی و SVM خطی اجرا شد و مدل SVM بهترین نتیجه را در پی داشته است [۵].

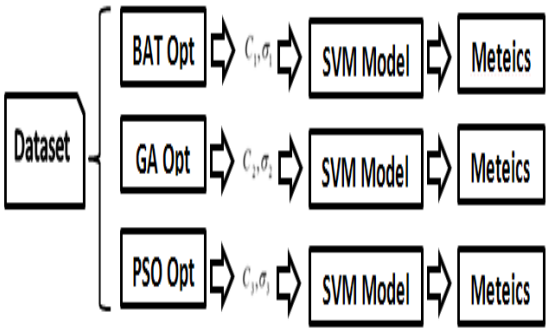
۳. روش پیشنهادی



شکل (۱): پیش پردازش‌ها و پردازش عددی

در این پژوهش، با استفاده از اطلاعات مفید در پیام‌ها، عملکرد تشخیص آزار و اذیت‌های سایبری را بهبود داده شده است. به‌طور خاص، از بسیاری از مشخصه‌های مفید در پیام از قبیل تعداد افرادی که پیام را تأیید کردند، تعداد کلمات تنفرآور، تعداد کلمات توهین‌آمیز، تعداد کلمات که توهین و تنفر نیست و محتوای پیام به‌منظور آموزش مدل تشخیص و بهبود عملکرد آن استفاده می‌شود. پایگاه داده مورد نظر شامل ۲۴۷۸۴ توئیت می‌باشد [۱۰] که در سال ۲۰۱۷ جمع‌آوری شده است. این پایگاه داده شامل ۷ فیلد مختلف به نام‌های Column_a، Count، hate_speech، offensive_language، Neither، class، tweet می‌باشد.

در این پژوهش پس از عملیات متن کاوی که در شکل (۱) و پیش پردازش‌ها و سپس پردازش عددی که شامل مخلوط‌کردن داده‌ها، نرمال‌سازی، PCA و سپس Kfold می‌باشد، سپس پنج روش طبقه‌بندی بیزساده، ماشین بردار پشتیبان، درخت تصمیم، k- نزدیک‌ترین همسایگی و شبکه عصبی را بر روی داده‌ها انجام داده و با بهینه‌کردن پارامترهای C و سیگما با الگوریتم‌های خفاش، ژنتیک و ازدحام ذرات شکل (۲) سعی شده است که در بهبود نتایج مورد نظر گام موثری برداشته شود.



شکل(۲): روند بهینه‌سازی

در این تحقیق به‌منظور تجزیه و تحلیل الگوریتم‌های مورد نظر از نرم‌افزار MATLAB ۲۰۱۷ استفاده شده است. در این پژوهش از دو ویژگی مهم برای بازنمایی دیتاست استفاده شده است. اولین ویژگی مهم، Bag Of Words یا کیسه کلمات هست. این ویژگی تعداد رخداد هر کلمه در یک سند را نشان می‌دهد. ویژگی دیگری که برای این پژوهش استفاده شده است، TFIDF است[۱۲]. این ویژگی از رخداد کلمات استفاده می‌کند و با رابطه‌ای خاص، یک فرم نرمال‌شده را به مقادیر می‌دهد. رابطه‌های (۳-۲-۱) محاسبه ویژگی TFIDF می باشد:

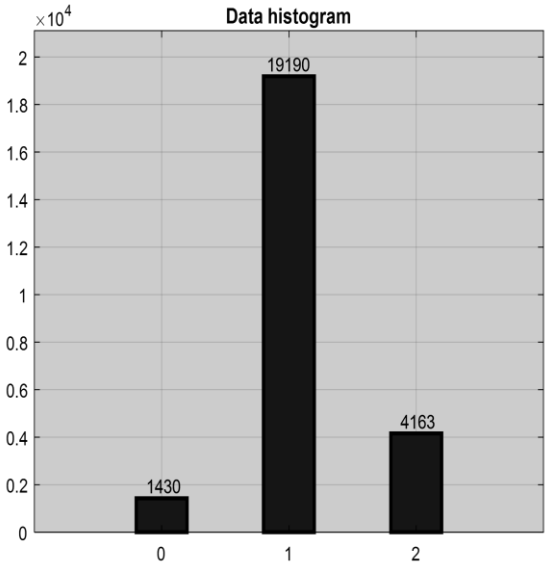
$$TFIDF=TF*IDF \quad (۱)$$

$$TF=\frac{\text{Number of occuracne word (i)in document (j)}}{\text{Total word in document (j)}} \quad (۲)$$

$$IDF=\log_2\left(\frac{\text{Total mumber of documents}}{\text{Number of documents with word(i)}}\right) \quad (۳)$$

۴. نتایج

دیتاست مورد استفاده، شامل حدود ۲۵ هزار نمونه است که به‌صورت توئیت کاربران شبکه اجتماعی ذخیره شده است. در شکل (۳) هیستوگرام توزیع داده‌ها مشاهده می‌شود.



شکل (۳): هیستوگرام داده‌ها

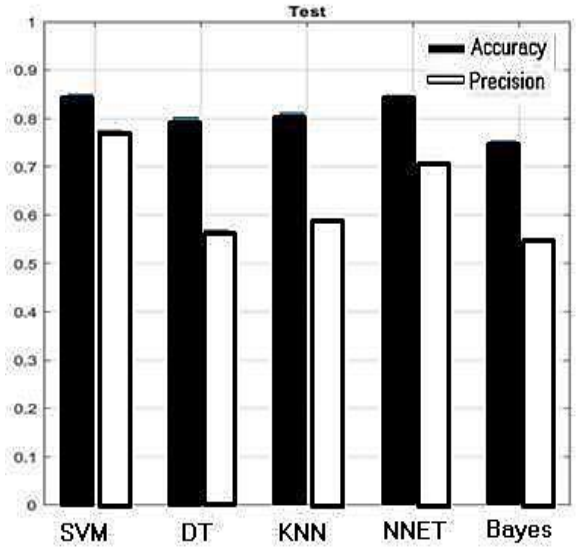
اولین معیار مهم در مسائل دسته‌بندی، دقت دسته‌بندی[1] است. اما دقت دسته‌بندی به تنهایی نمی‌تواند معیار مناسبی باشد، زیرا که داده‌ها غیرمتعادل هستند. پس از معیار دیگری به نام صحت دسته‌بندی[2] نیز استفاده شده است. رابطه‌های (۵-۴) دقت و صحت را محاسبه می‌کند: [۱۲].

$$\text{Accuracy}=\frac{TP}{TP+FP+TN+FN} \quad (۴)$$

$$\text{Precision}=\frac{TP}{TP+FP} \quad (۵)$$

شکل(۴) نتیجه پیاده‌سازی و عمل دسته‌بندی را روی دیتاست و به‌ازای مدل‌های مختلف نشان می‌دهد. این نتایج شامل دقت دسته‌بندی و صحت است. توجه شود که مقادیر معیارها بین ۰ تا ۱، مقیاس شده‌اند.

با توجه به نتایج مشاهده می‌شود بهترین عملکردها را شبکه عصبی و ماشین بردار پشتیان داشتند و بعد از انها نیز درخت تصمیم و نزدیک ترین همسایه مشابه هم بودند و در اخر نیز مدل بیز ساده قرار دارد.



شکل (۴): دقت و صحت مدل‌های دسته‌بندی به‌ازای مرحله تست با ویژگی Bag of Words

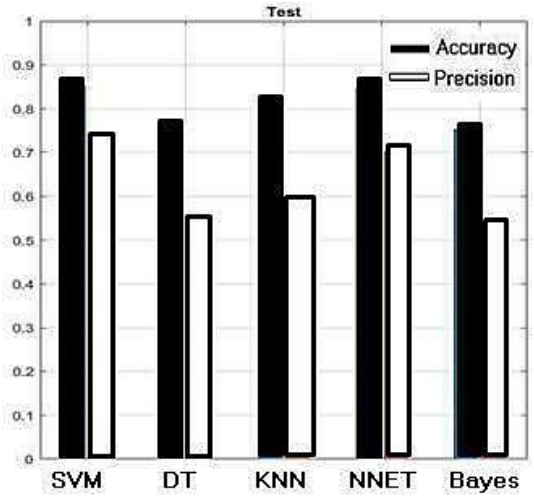
جدول (۱) مقادیر عددی شکل (۴) را نشان می‌دهند. بهترین دقت و صحت دسته‌بندی مربوط به SVM با دقت ۰/۸۵۱۴ و صحت ۰/۷۷۶۱ می‌باشد.

جدول (۱): نتایج دقت و صحت دسته‌بندی به‌ازای مدل‌های مختلف بر روی داده‌های تست با ویژگی‌های **Bag of Words**

	SVM	Decision tree	KNN	Neural Network	Naïve Bayes
دقت	۰/ ۸۵۱۴	۰/۸۰۳۰۳	۰/ ۸۱۲۲۴	۰/۸۴۸۵۷	۰/۷۵۴۷۴
صحت	۰/ ۷۷۶۱۴	۰/۵۷۰۵۲	۰/۵۸۵۴۷	۰/۷۰۷۶۴	۰/ ۵۳۱۲۵

حال نتایج دسته‌بندی را به‌ازای ویژگی TFIDF مورد بررسی قرار می‌گیرد. شکل (۵) نتایج حاصل از دسته‌بندی به‌ازای ویژگی‌های TFIDF را نشان می‌دهد. از لحاظ کلیت نتایج، همه چیز مشابه با حالت Bag of Words است.

[1] Accuracy
[2] Precision



شکل (۵): دقت و صحت مدل‌های دسته‌بندی به ازای مرحله تست با ویژگی‌های TFIDF

جدول (۲) مقادیر عددی شکل (۵) را ارائه می‌دهد. همان‌گونه که ذکر شد کلیت مقادیر مشابه با حالتی است که از ویژگی‌های Bag of Words استفاده شده است، اما اگر به معیارهای به‌دست‌آمده بیشتر دقت شود، مشاهده می‌شود، که به غیر از درخت تصمیم که عملکرد بدتری را نسبت به حالت قبلی ثبت شده است، (دقت از ۰/۸۰۳ به ۰/۷۶ رسیده است)، اما سایر مدل‌ها تفاوت آن‌چنانی نداشته‌اند. نکته مهم دیگر در مورد معیارهای به دست آمده از ماشین بردار پشتیبان است که هر چند دقت دسته‌بندی در حدود ۰/۸۵ مانده است، اما از لحاظ صحت دسته‌بندی افت قابل توجهی را متحمل شده است (از ۰/۷۷۶ به ۰/۷۲۲ رسیده است). پس به نظر می‌رسد که برای مدل ماشین بردار پشتیبان، استفاده از ویژگی‌های Bag of Words می‌تواند مفیدتر باشد. حال باید گفت که روش TFIDF یک روش آماری عددی است که تمایل دارد میزان اهمیت یک کلمه در یک سند را نشان دهد. این روش معمولاً یک فاکتور وزن است که در روش‌های بازیابی اطلاعات و بازیابی متن استفاده می‌شود. در این روش وزن کلمه با افزایش تعداد تکرار آن در متن افزایش می‌یابد، اما توسط تعداد کلمات موجود در متن کنترل می‌شود. دلیل آن این است که در صورت زیاد بودن طول متن، بعضی از کلمات به طور طبیعی بیشتر از دیگران تکرار خواهند شد، اگرچه چندان اهمیتی در معنی نداشته باشند. حال اگر متن استاندارد بود و کلمات در جمله تکراری نبود ،طبیعتا نتایج روش Bag Of Words بهتر می بود.

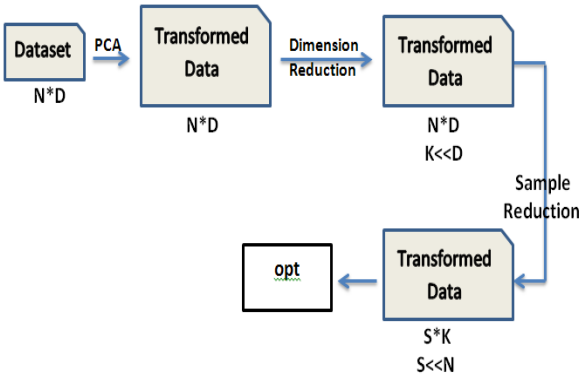
جدول (۲): نتایج دقت و صحت دسته‌بندی به‌ازای مدل‌های مختلف بر روی داده‌های تست با ویژگی‌های TFIDF

	SVM	Decision tree	KNN	Neural Network	Naïve Bayes
دقت	۰/۸۵۲۹۶	۰/۷۶۰۳	۰/۸۱۳۶۷	۰/۸۴۹۷۹	۰/۷۵۳۶۵
صحت	۰/۷۲۲۵۴	۰/۵۴۶۴۹	۰/۵۸۷۲۸	۰/۷۰۲۶۱	۰/۵۲۷۱۹

۴-۱. ترکیب ماشین بردار پشتیبان و روش‌های بهینه

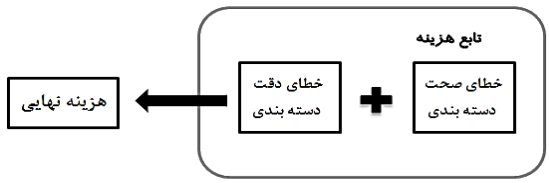
قسمت اصلی کار ترکیب ماشین بردار پشتیبان و الگوریتم بهینه‌سازی خفاش است، اما در کنار این الگوریتم بهینه‌سازی از روش‌های بهینه‌سازی دیگر نیز استفاده شده است، تا قابلیت الگوریتم خفاش را مورد بررسی قرار گیرد. الگوریتم‌های بهینه‌سازی دیگری که استفاده شده است، الگوریتم ژنتیک و الگوریتم ازدحام ذرات (PSO) است. هدف از این بهینه‌سازی این است که مهم‌ترین پارامترهای ماشین بردار پشتیبان بهینه‌سازی شود. به این صورت که دیتاست را به الگوریتم‌های بهینه‌سازی داده شود، تا این الگوریتم‌های بهترین پارامترهای C و σ را به دست آورند. سپس پارامترهای به دست آمده از هر الگوریتم به ماشین بردار پشتیبان داده می‌شود، تا آموزش ببینید و سپس دقت و صحت به‌دست‌آمده از عملکرد مدل دسته‌بندی را به‌ازای پارامترهای هر الگوریتم مورد محاسبه قرار می‌گیرد.

اما برای دیتاست حاضر، این روند یک چالش بزرگ محسوب می‌شود چرا که زمان آموزش ماشین بردار پشتیبان بالاست و متعاقبا زمان بهینه‌سازی نیز بسیار بالا خواهد رفت. برای حل این موضوع به جای استفاده از کل دیتاست از بخشی از دیتاست استفاده شده است . شکل(۶) این روند را نشان می‌دهد. برای این تحقیق تعداد مولفه‌های اصلی انتخابی (K) را برابر با ۲۰۰ و تعداد نمونه‌های انتخابی (S) را ۲۷۰۰ داده شده است. یعنی به‌ازای هر کلاس ۹۰۰ نمونه.



شکل (۶): روند کاهش ابعاد و نمونه‌های دیتاست با استفاده از تجزیه و تحلیل مولفه‌های اصلی PCA

تابع هزینه شکل (۷) را برابر با مجموع خطای دقت دسته‌بندی به علاوه خطای صحت دسته‌بندی در نظر گرفته شده است. این نوع از تابع هزینه باعث می‌شود که الگوریتم‌های بهینه‌سازی پارامترهایی را پیدا نکنند که مدل روی کلاس خاصی بایاس شود و دقت بالای دسته‌بندی بدهد اما صحت مناسبی نداشته باشد.



شکل(۷): تابع هزینه

الگوریتم خفاش به‌طور خلاصه در زیر آورده شده است [۱۳].

گام یک: ایجاد جمعیت اولیه خفاش‌ها $(\boldsymbol{x_i}, \boldsymbol{i = 1,..,n})$

گام دو: تعیین سرعت $\boldsymbol{v_i}$، فرکانس $\boldsymbol{f_i}$، نرخ پالس $\boldsymbol{r_i}$ و بلندی صدا $\boldsymbol{A_i}$ در مکان $\boldsymbol{x_i}$.

گام سه: مقداردهی اولیه زمان t=1

گام چهار: مقایسه موقعیت خفاش‌ها و تعیین بهترین خفاش

گام پنج: به‌روزرسانی موقعیت خفاش‌ها

گام شش: اگر $\boldsymbol{rand > r_i}$، آن‌گاه جواب در میان بهترین جواب‌ها با گام تصادفی کرده و با استفاده از یک جواب محلی در اطراف بهترین جواب انتخاب شده ایجاد می‌شود.

گام هفت: تولید یک جواب جدید با پرواز تصادفی

گام هشت: اگر $\boldsymbol{rand < A_i}$ و $\boldsymbol{f(x_i) < f(x^*)}$، آن‌گاه جواب‌های جدید پذیرفته می‌شوند و $\boldsymbol{r_i}$ افزایش و $\boldsymbol{A_i}$ کاهش می‌یابد.

گام نه: مرتب‌سازی خفاش‌ها و تعیین بهترین جواب $\boldsymbol{x^*}$

گام ده: اگر زمان t به حد خود رسید توقف الگوریتم و در غیر این‌صورت t=t+1 و به گام چهار برو.

حال پارامترهای الگوریتم خفاش که بر اساس تجربه و خطا به‌دست‌آمده را به‌صورت زیر می‌باشد.

پارامتر Loudness یا A (Loudness_A) : مقدار ۰/۹

پارامتر Pulse rate یا r (Pulse_Rate_r) : مقدار ۰/۱

ابعاد مسئله (nVar) : برابر با ۲ . به این معنی که نیاز به بهینه‌سازی دو پارامتر داریم

تعداد خفاش‌ها (Pop_Size) : ۱۰ عدد

تعداد تکرار الگوریتم (Bat_Iteration) : ۵۰ تکرار

حد پایین پارامترها (Lower_Bound) : ۰/۱ برای C و ۰/۱ برای σ

حد بالای پارامترها (Upper_Bound) : ۱۰۰ برای C و ۱۰ برای σ

برای الگوریتم ژنتیک و بهینه‌سازی ازدحام ذرات نیز، تعداد تکرار (نسل) را برابر با ۵۰ قرار داده شده است و سایر پارامترها، به صورت پیش‌فرض توسط متلب تعیین می‌شوند. مهم‌ترین پارامتر این الگوریتم‌ها سایز جمعیت است که برای بهینه‌سازی ازدحام ذرات برابر است با ۲*۱۰ که در اینجا ۲، تعداد پارامتری است که عمل بهینه‌سازی، بر روی آن انجام می‌شود و برای الگوریتم ژنتیک برابر با ۵۰ است.

۴-۲. نتایج بهینه‌سازی

در این بخش نتایج حاصل از ترکیب مدل دسته‌بند ماشین بردار پشتیبان و الگوریتم‌های بهینه‌سازی را ارائه شده است. بهینه سازی‌های انجام شده در دو بخش ارائه می‌شود. قسمت اول بر روی ویژگی‌های Bag Of Words و قسمت دوم بر روی ویژگی‌های TFIDF.

اسامی مدل‌هایی که در ادامه مشاهده خواهید کرد به شرح زیر هستند:

۱. Default_svm_pca_small: مدل ماشین بردار پشتیبان با پارامترهای پیش‌فرض که روی داده‌های کوچک شده (در بخش قبل در ابعاد $S \times k$ معرفی شده بودند) آموزش داده شده است.

۲. Bat_svm_pca_small: مدل ترکیبی ماشین بردار پشتیبان و الگوریتم خفاش که روی داده‌های کوچک شده آموزش اعمال شده‌اند.

۳. Ga_svm_pca_small: مدل ترکیبی ماشین بردار پشتیبان و الگوریتم ژنتیک روی داده‌های کوچک.

۴. Pso_svm_pca_mall: مدل ترکیبی ماشین بردار پشتیبان و الگوریتم بهینه‌سازی ازدحام ذرات روی داده‌های کوچک

۵. Defaul_svm_pca: مدل ماشین بردار پشتیبان با پارامترهای پیش‌فرض، روی داده‌های تبدیل شده تحت آنالیز مولفه‌های اصلی ($N \times D$)

۶. Bat_svm_pca: مدل ترکیبی ماشین بردار پشتیبان و الگوریتم خفاش روی داده‌های تحت تبدیل pca.

۷. Ga_svm_pca: مدل ترکیبی ماشین بردار پشتیبان و الگوریتم ژنتیک روی داده‌های تحت تبدیل pca.

۸. Pso_svm_pca: مدل ترکیبی ماشین بردار پشتیبان و الگوریتم بهینه‌سازی ازدحام ذرات روی داده‌های تحت تبدیل pca

با توجه به نتایج جدول (۳) حاصل شده روی داده‌های کوچک (pca_small)، مشاهده می‌شود، که از لحاظ دقت تست، الگوریتم خفاش توانسته است، پارامترهای بهینه‌ای را پیدا کند که دقت مناسب‌تری را ارائه دهد. اما از لحاظ صحت، الگوریتم pso، پارامترهای بهتری را یافته است. با این حال، الگوریتم‌های بهینه‌سازی توانسته است هم از لحاظ دقت و هم از لحاظ صحت عملکرد را بهبود داده‌اند. اما زمانی که این پارامترها روی کلیه داده‌ها اعمال می‌شود، دقت به نسبت به Svm با پارامترهای پیش‌فرض بدتر می‌شوند، اما صحت‌ها با اختلاف بسیار زیادی بهتر شده‌اند.

جدول (۳): جدول نتایج بهینه‌سازی با استفاده از ویژگی‌های Bag of Words

مدل	صحت تست	دقت تست
DEFAULT_SVM_PCA_SMALL	۰/۶۹۸۸	۰/۶۹۰۵
BAT_SVM_PCA_SMALL	۰/۷۳۷۱	۰/۷۰۴۱
GA_SVM_PCA_SMALL	۰/۷۴۸۵	۰/۷۰۰۴
PSO_SVM_PCA_SMALL	۰/۷۵۴۸	۰/۶۹۳۰
DEFAULT_SVM_PCA	۰/۶۹۹۳	۰/۸۶۵۶
BAT_SVM_PCA	۰/۷۰۶۲	۰/۸۶۲۵
GA_SVM_PCA	۰/۸۳۱۶	۰/۸۵۵۴
PSO_SVM_PCA	۰/۸۷۱۴	۰/۸۴۳۷

مشاهده می‌شود که چه روی داده‌های کوچک و چه روی داده‌های کامل، صحت‌ها افزایش یافته‌اند که در این میان افزایش صحت الگوریتم ژنتیک و pso قابل ملاحظه بوده است. اما از لحاظ دقت، الگوریتم خفاش نسبت به سایر الگوریتم‌های بهینه‌سازی رویکرد مناسب‌تری داشته است.

پارامترهای بهینه به دست آمده از مدل‌های ترکیبی به شرح زیر هستند:

BAT=[c=9.1920 , σ=9.2737]

GA =[c=4.2371 , σ=9.9649]

PSO=[c=04157 , σ=4.1994]

جدول (۴) نتایج مربوط به صحت و دقت دسته‌بندی را بعد از ترکیب مدل دسته‌بندی و الگوریتم‌های بهینه‌سازی را نشان می‌دهد. در این قسمت ویژگی‌های مورد استفاده TFIDF هستند.

جدول (۴): نتایج بهینه‌سازی با استفاده از ویژگی‌های TFIDF

مدل	صحت تست	دقت تست
DEFAULT_SVM_PCA_SMALL	۰/۷۰۶۲	۰/۶۹۷۹
BAT_SVM_PCA_SMALL	۰/۷۲۵۹	۰/۷۰۹۰
GA_SVM_PCA_SMALL	۰/۷۲۵۹	۰/۷۰۹۰
PSO_SVM_PCA_SMALL	۰/۷۲۵۹	۰/۷۰۹۰
DEFAULT_SVM_PCA	۰/۷۰۹۶	۰/۸۷۰۱
BAT_SVM_PCA	۰/۷۳۸۷	۰/۸۷۱۸
GA_SVM_PCA	۰/۷۳۳۸	۰/۸۷۱۷
PSO_SVM_PCA	۰/۷۲۹۵	۰/۸۷۱۵

الگوریتم‌های بهینه‌سازی توانسته‌اند، هم صحت و هم دقت را روی داده‌های کوچک شده بالا ببرند و هنگامی که همین پارامترهای بهینه به‌دست‌آمده را روی داده‌های اصلی که تحت تبدیل pca قرار گرفته‌اند،اعمال می شود ، مشاهده می‌شود که دقت svm با پارامترهای پیش‌فرض از ۰/۸۷۰۱ به دقت ۰/۸۷۱۸ در حالتی که از پارامترهای به‌دست‌آمده از الگوریتم خفاش استفاده شده، رسیده است. نکته مهم این است که پارامترهای بهینه‌سازی شاید در بالابردن دقت توانایی مناسبی نداشته‌اند و دقت را به‌طور محسوسی افزایش نداده‌اند، اما در بالا بردن صحت عملکرد بهتری داشته‌اند.

در نتایج به‌دست‌آمده مشاهده می‌شود که الگوریتم خفاش هم از لحاظ صحت و هم از لحاظ دقت، مقادیر تقریباً بهتری نسبت به دو الگوریتم بهینه‌سازی دیگر داده است به طوری که بهترین دقت به دست آمده ۰/۸۷۱۸ و بهترین صحت به دست آمده نیز ۰/۷۳۸۷ بوده است.

برخلاف قسمت قبلی که هیچ کدام از روش‌ها، پارامترهای مشابه به دیگری را ارائه نداده بودند. با این حال دقت‌ها و صحت‌هایی که ماشین بردار پشتیبان روی این پارامترها می‌دهد، تقریباً مشابه هستند که نشان می‌دهد انتخاب مقادیر بهینه کار دشواری است و مدل ماشین بردار پشتیبان، به‌گونه‌ای عمل می‌کند که زیاد حساس به پارامترهای خود نیست.

با توجه به نتایجی که روی دو نوع ویژگی Bag of Word و TFIDF به‌دست آمده است، می‌توان چنین نتیجه گرفت که الگوریتم‌های بهینه‌سازی، پارامترهای پایداری را زمانی که از ویژگی‌های TFIDF استفاده می‌کنند، می‌دهند. اما زمانی که از ویژگی‌های Bag of Words استفاده می‌شود تغییرات در پارامترهای بهینه و همچنین در عملکرد مدل‌ها، مخصوصاً در صحت دسته‌بندی به‌صورت ملموسی قابل ملاحظه است.

۵. نتیجه‌گیری

یکی از مسائلی که در این زمینه مطرح می‌شود بحث پردازش پیام ها در شبکه های اجتماعی است که ما را به سمت پردازش متن در یادگیری ماشین سوق می‌دهد. با استفاده از متن‌کاوی می‌توان، با توجه به پژوهشی که انجام شده بیشترین دقت را با مدل SVM به ۸۶/۵۶ و بیشترین صحت را به ۸۷/۱۴ بوده است که می توان با این دقت و صحت پیام‌های آزار و اذیت را شناسایی نمود و جهت پیشگیری از ان اقدام لازم را انجام داد. می توان گفت که این میزان دقت و صحت گام موثری در جهت کاهش جرایم سایبری می‌باشد. همچنین جهت ارزیابی کار و

اعتبارسنجی نیاز به پایگاه داده استاندارد لاتین است و می‌توان روش پیشنهادی را در سطح بومی پیاده‌سازی نمود.

مشاهده شده است که دو روش ماشین بردار پشتیبان و شبکه عصبی، از سایر روش‌ها، عملکرد بهتری داشتند و در این میان ماشین بردار پشتیبان هم از لحاظ دقت و هم از لحاظ صحت، عملکرد بهتری نسبت به شبکه عصبی داشت. سپس مدل ماشین بردار پشتیبان را با الگوریتم‌های بهینه‌سازی مثل الگوریتم خفاش، ژنتیک و بهینه‌سازی ازدحام ذرات ترکیب شده است. هر چند هدف اصلی تحقیق، ترکیب ماشین بردار پشتیبان و الگوریتم خفاش بود، اما با اضافه‌کردن الگوریتم ژنتیک و بهینه‌سازی ازدحام ذرات سعی بر مقایسه بهتر و اطمینان از عملکرد خفاش بوده است.

همچنین سه روش بهینه‌سازی خفاش، ژنتیک و PSO تقریباً مشابه با یکدیگر عمل می‌کنند و نسبت به یکدیگر برتری چشمگیری نداشته‌اند. با این حال الگوریتم خفاش، تا حد بسیار کمی، از سایر روش‌های بهینه‌سازی عملکرد بهتری داشته است، لازم به توضیح است، این بهبود، یک بهبود زیاد و چشمگیر نیست، زیرا مدل دسته‌بندی ماشین بردار پشتیبان، مدلی است که به‌خوبی روی داده‌ها سوار می‌شود و تغییر پارامترهای مدل تاثیر آن‌چنانی در افزایش و یا کاهش عملکرد ندارد.

۶. مراجع

1. A. Ebrahimi and S. Abolghasen, “Comprehensiveness to crime database in order to predict and identify crimes by using data mining techniques,” Electronic industries Journal, Term 6, 1394. (In Persian)

2. B. Javad’zade, “Analyzing the centrality of social networks in cyber scope dealing with soft threats approach,” Scientific–Promotional quarterly passive defense, sixth year, no. 1, pp. 69-78, 1394. (In Persian)

3. A. Abadi, “Electronic crimes detection by using data mining methods,” second national conference of computer engineering research, Ltamedan, Ekbatan research group,1395.(In Persian)

4. A. Buczak and M. Gifford, “Fuzzy association rule mining for community crime pattern discovery,” In ACM SIGKDD Workshop on Intelligence and Security Informatics, ACM, 2010.

5. T. Davidson, D. Warmsley, and M. Macy, “Automated hate speech detection and the problem of offensive language,” arxiv preprint arxiv:1703. 04009, 2017.

6. H. Deylami and Y. Singh, “Cybercrime detection techniques based on support vector machines,” Artificial Intelligence Research, vol. 2(1), no.1, 2012.

7. D. Karlis and L. Meligkotsidou, “Finite mixtures of multivariate Poisson distributions with application,” Journal of statistical Planning and Inference, vol. 137(6), pp. 1942-1960, 2007.

8. J. Khan and S. Shaikh, “Computing in social networks with relationship algebra,” Journal of Network and Computer Applications, vol. 31, no. 4, pp. 862-878, 2008.

9. B. Moon, J. McCluskey, and C. McCluskey, “A general theory of crime and computer crime: An empirical test,” Journal of Criminal Justice, vol. 38, no. 4, pp. 767-772, 2010.

10. Data.world, “Hate Speech and Offensive Language,” https://data.world/thomasrdavidson/hate-speech-and-offensive-language, 2017.

11. M. Malmasi, H. Shervin, and M. Zampieri, “Detecting Hate Speech in Social Media,” arxiv preprint arxiv:1712. 06427, 2017.

12. A. Gaydhani, V. Dama, and S. Kendra, “Detecting hate speech and offensive Language on Twitter using machine learnimg : An N-gram and TFIDF based approach,” avxiv:1809. 08651v1, 2018.

13. P. Tasi and P. Shyang, “Bat Algorithm Inspried Algorithm for Solving Numerical Optimization Problems,” Applied Mechanics and Materials, vol. 148-149, 2012.

Detection of Cybercrimes in Online Connections by the Data Mining Approach

M. Rastgoo, M. Jalali*

Abstract

At recent years, online social network sites have been popular dramatically. Cybercrimes use from social media as a new platform at acceptation of some types of computer crimes like phishing, spamming, malware spread and cyber harassment. In this research, we will improve the function of detecting cybercrime with the help of useful information in the messages. Choosing the best features with high separation. Strength between cyber harassment tweets and none cyber harassment is a complex activity which extremely needs substantially effort in making Machine Learning Model. In this way, we compare function of five classification methods Naive Bayes, Support Vector Machine, Decision Tree, k-Nearest Neighbor and Neural Network under five different tuning in order to selecting the best adjustment for suggested features. Also, we have improved C and Sigma parameters by using the bat, genetics and particle swarm algorithms. Additionally, we have compared five classification methods with default parameters and parameters obtained with optimization algorithms. Finally, we have shown that bat algorithm has had the best performance among other optimization algorithms. According to the research we did the most accuracy with the SVM model to 86.56 and the highest precision to 87.14.

Key Words: *Crime, Data Mining Algorithm, Support Vector Machine*

*Department of Computer Engineering, Islamic Azad University, Mashhad (jalali@mshdiau.ac.ir)- Writer-in-Charge