فصلنامه رویکردهای پژوهشی نوین در
مدیریت و حسابداری
سال هشتم، شماره ۹۳، تابستان ۱۴۰۳، ص ۳۸۱-۳۷۱

Journal of New Research Approaches
in Management and Accounting
ISSN: 2588-4573
http://www.majournal.ir

تشخیص نفوذ توزیع شده در محیط‌های ابری براساس تکنیک داده‌کاوی

سارا فرزای [۱]
همایون مؤتمنی [۲]
مریم دانتیسم [*۳]

تاریخ دریافت: ۱۴۰۳/۰۳/۰۱ تاریخ چاپ: ۱۴۰۳/۰۵/۰۶

چکیده

محیط ابری نشان دهنده تکامل اینترنت در آینده می‌باشد. اینترنت شیوه زندگی مردم را تغییر داده است و تعاملات میان انسانها از دنیای واقعی به فضای مجازی گسترش یافته است. تهدیدات امنیتی می‌تواند در هر قسمتی از جمله سخت‌افزار یا نرم‌افزار پدید آید که باید منابع تهدید را از دسترسی محافظت نمود. یکی از راههای مقابله با حملات و نفوذها در اینترنت اشیاء استفاده از سیستم تشخیص نفوذ است هدف از پژوهش حاضر ارائه مدلی جهت تشخیص نفوذ توزیع شده در محیط‌های ابری براساس تکنیک داده کاوی می باشد و روش پژوهش پیمایشی است و پایگاه داده استفاده شده در این پژوهش KDD-NSL می‌باشد. این پایگاه داده دارای ۴۱ ویژگی و یک کلاس است .این ویژگی ها به ۴ دسته تقسیم می شوند: ویژگی های پایه، ویژگی های محتوایی، ویژگی های ترافیک زمانی، ویژگی های ترافیک میزبان و نتایج بدست آمده از این تحقیق نشان میدهد که علاوه بر سرعت بالا در تشخیص، الگوریتم درخت تصمیم از دقت بالایی نیز برخوردار میباشد .با این حال نتایج ما ممکن است دارای مشکلاتی نیز باشند، زیرا وقتی عمل انتخاب ویژگی را انجام میدهیم ممکن است ویژگیهایی که انتخاب میکنیم به درستی انتخاب نشوند. پس برای اینکه نتایج بهتر و دقیقتری انجام دهیم نیاز به تجربه در محیط های متفاوتی را داریم .نتایج حاصل از این الگوریتم ها به دو دسته دادههای نرمال و غیرنرمال تقسیم میشوند.

واژگان کلیدی

تشخیص نفوذ، توزیع شده، محیط های ابری، تکنیک داده کاوی

۱. گروه کامپیوتر، موسسه آموزش عالی طبری، بابل، ایران.
۲. گروه مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد ساری، ساری، ایران.
۳. گروه کامپیوتر، موسسه آموزش عالی روزبهان، ساری، ایران. (نویسنده مسئول: com.gmail@360dantism)

بیان مساله

رایانش ابری نوعی سیستم موازی و توزیعی از رایانه های متصل بهم و مجازی است که به صورت پویا و بر اساس توافقات سطح سرویس و به عنوان یک یا چند منبع محاسباتی مجتمع ارائه می شود رایانش ابری به معنای انتقال پویای منابع و قابلیتهای فناوری اطلاعات به عنوان سرویس روی اینترنت است صنعت رایانش ابری اکوسیستم بزرگی از مدل ها فروشندگان و بازارهای مختلف است خدمات رایانشی پنج ویژگی کلیدی و چهار مدل استقرار و سه مدل خدمات دارد پنج مشخصه اصلی شامل تجمیع منابع دسترسی وسیع از طریق شبکه انعطاف پذیری ،سریع سرویس خودکار مبتنی بر تقاضا و سرویس اندازه گیری شده می باشد. سه مدل خدمات عبارتند از : زیرساخت به عنوان سرویس پلتفرم، سرویس نرم افزار به عنوان انواع مدل عرضه، شامل ابرخصوصی ابرانجمنی، ابر عمومی و ابر هیبرید است . در نمایش دیاگرام شبکه های کامپیوتری بطور معمول از شکل یک ابر به عنوان روشی تلخیصی برای پنهان کردن زیر ساخت های پیچیده ای که درون شبکه وجود دارد استفاده می گردد در رایانش ابری نیز کلمه "ابر" از همین استعاره گرفته شده است و برای اینترنت و زیرساختها در رایانش ابری نیز بکار میرود آنچه که این مفهوم را مقیاس پذیر و کارآمد می سازد، معماری سرویس گرا است به این ترتیب که منابع به جای اینکه بر روی سیستمهای کاربران نصب شوند بر روی سرورهای ارائه دهندگان نگهداری می شوند این تکنولوژی نوین برای آسان تر شدن استفاده از منابع اطلاعاتی سخت افزاری برنامه های کاربردی شبکه ها و زیر ساخت ها اختراع شده است.

رایانش ابری با هدف ارائه دسترسی راحت و بر اساس تقاضا به شبکه به یک مجموعه مشترک از منابع محاسباتی قابل تنظیم فرستاده شده که می تواند به سرعت تهیه و با حداقل تلاش مدیریت یا تعاملات ارائه دهنده خدمات عرضه شود (فراندز و همکاران[1]، ۲۰۱۸). ویژگی‌های ابری عملکرد الاستیک مبتنی بر پرداخت و تقاضا، مدل محاسبات سازمانی را تغییر می‌دهد، زیرساخت‌های داخلی را از مراکز داده خارج از محل تغییر می‌دهد که از طریق اینترنت قابل دسترسی هستند و توسط ارائه‌دهندگان میزبانی ابری مدیریت می‌شوند.

با این حال، بسیاری از مسائل امنیتی با انتقال به این پارادایم محاسباتی از جمله تشخیص نفوذ به وجود می‌آیند. صرف‌نظر از تحولات مهم فناوری‌های امنیت اطلاعات در سال‌های اخیر، نفوذها و حملات به شکست سیستم‌های تشخیص نفوذ موجود در محیط‌های ابری ادامه می‌دهند(اقبال و همکاران، ۲۰۱۶) مهاجمان تکنیک‌های پیچیده جدیدی را توسعه دادند که می تواند کل پلتفرم ابری یا حتی بسیاری از آن‌ها را در عرض چند دقیقه از بین ببرد. رکوردهای جدید هر ساله توسط مهاجم شکسته می شود. اخیراً یک حمله مخرب DDoS بیش از ۷۰ سرویس حیاتی اینترنت از جمله Github ، Twitter، Amazon، Paypal و غیره را از بین برده است. (دیم و همکاران، ۲۰۱۸).

ابزارهای نفوذ و حمله پیچیده تر شده‌اند و Cloud IDS های موجود را با حجم زیادی از داده‌های ترافیک شبکه، رفتارهای پویا و پیچیده و انواع جدید حملات به چالش می‌کشند. واضح است که یک IDS برای سیستم ابری باید حجم زیادی از داده های ترافیک شبکه را تجزیه و تحلیل کند، رفتارهای حمله جدید را به طور موثر تشخیص دهد و به دقت بالا ببرد. با این حال، پیش پردازش، تجزیه و تحلیل و تشخیص نفوذ در محیط های ابری با استفاده از تکنیک های سنتی از نظر محاسبات، زمان و بودجه بسیار پرهزینه شده است.

1. Fernandes et all

بنابراین، تشخیص نفوذ موثر در محیط‌های ابری نیازمند پذیرش تکنیک‌های جدید توزیع‌شده و هوشمند مانند تکنیک‌های یادگیری ماشینی است.

در این پژوهش ما یک سیستم تشخیص نفوذ مبتنی بر یادگیری ماشین توزیع شده برای محیط‌های ابری ارائه می‌کنیم. سیستم پیشنهادی برای درج در اجزای شبکه لبه ارائه‌دهنده ابر طراحی شده است. این اجازه می دهد تا ترافیک شبکه ورودی به مسیریاب های شبکه لبه ابری را رهگیری کند. یک الگوریتم پنجره کشویی مبتنی بر زمان برای پیش پردازش ترافیک شبکه گرفته شده در هر روتر ابری و ارسال آن به یک ماژول تشخیص ناهنجاری با استفاده از طبقه‌بندی کننده بیزی استفاده می شود. روتر ابری مجموعه‌ای از گره‌های سرور کالا بر اساس Hadoop و MapReduce برای هر ماژول تشخیص ناهنجاری در دسترس هستند تا در هنگام افزایش تراکم شبکه از آن استفاده کنند. برای هر پنجره داده های ترافیک شبکه ناهنجار روی هر روتر با یک سرور ذخیره سازی مرکزی همگام می شوند. سپس، طبقه‌بندی‌کننده‌های یادگیری گروهی بر اساس جنگل تصادفی برای انجام آخرین مرحله طبقه‌بندی چند کلاسه به منظور شناسایی نوع هر حمله استفاده می‌شود.

سیستم پیشنهادی در پلتفرم ابری پیاده‌سازی شده است که از Hadoop و MapReduce برای توزیع و مقیاس‌بندی محاسبات بر روی خوشه‌های موجود استفاده می‌کند.

MapReduce یک تکنیک پردازش و یک مدل برنامه نویسی برای محاسبات توزیع شده بر اساس زبان برنامه نویسی جاوا است. الگوریتم های MapReduce از دو بخش یا کلاس اصلی Map و Reduce تشکیل شده است. کلاس Map مجموعه‌ای از داده‌ها را می‌گیرد و آن‌ها را به مجموعه دیگری از داده‌ها تبدیل می‌کند، جایی که عناصر جداگانه به چند تا (جفت کلید/مقدار) تقسیم می‌شوند. کلاس Reduce خروجی یک نقشه را به عنوان ورودی می گیرد و آن تاپل های داده را در مجموعه کوچکتری از تاپل ها ترکیب می کند. یک پلتفرم رایانش ابری است که قادر است به راحتی تجزیه و تحلیل داده ها را در زمان واقعی ارائه دهد. این چارچوب به طور گسترده ای برای اکتشاف، پردازش و تجزیه و تحلیل داده های ساخت یافته و غیرساختار یافته استفاده می شود (هولمز[2]، ۲۰۱۸). با توجه به مواردی که عنوان سئوال اصلی به این صورت است تشخیص نفوذ توزیع شده برای محیط های ابری براساس تکنیک داده کاوی چگونه است؟

پیشینه تحقیق

پوجا و همکاران[3] (۲۰۲۲) پژوهشی در مورد سیستم‌های تشخیص نفوذ در الگوی محاسبات ابری انجام دادند و الگوی رایانش ابری به سرعت در حال رشد است و به کاربران امکان می دهد خدمات را از طریق اینترنت به صورت پرداخت به ازای استفاده دریافت کنند و برای توسعه، استقرار و دسترسی به برنامه های کاربردی تلفن همراه راحت است. در حال حاضر، امنیت یک نگرانی ضروری برای داشتن ماهیت باز و توزیع شده ابر است. حجم زیادی از داده ها مسئول هکرهای فریبنده هستند. بنابراین، توسعه IDS کارآمد یک کار ضروری است. این مقاله چهار سیستم تشخیص نفوذ را برای تشخیص حملات مورد تجزیه و تحلیل قرار داد. دو مجموعه داده معیار استاندارد، یعنی NSL-KDD و-UNSW ۱۵NB، برای شبیه سازی استفاده شد. علاوه بر این، این مطالعه چالش‌های فزاینده برای امنیت داده‌های حساس کاربر را

2. Holmes
3. Poja et all

برجسته می‌کند و توصیه‌های مفیدی برای رسیدگی به مسائل شناسایی شده ارائه می‌دهد. در نهایت، نتایج پیش‌بینی‌شده نشان می‌دهد که روش هیبریداسیون با طبقه‌بندی‌کننده ماشین بردار پشتیبان از تکنیک‌های موجود در مورد مجموعه داده‌های مورد بررسی بهتر عمل می‌کند.

احمدیا و همکاران(۲۰۱۸) پژوهشی در مورد سیستم تشخیص نفوذ توزیع شده برای محیط های ابری بر اساس تکنیک های داده کاوی انجام دادندو سیستم پیشنهادی به گونه ای طراحی شده است که در کنار اجزای شبکه لبه ارائه دهنده ابر در Cloud قرار گیرد. این امکان رهگیری ترافیک شبکه ورودی به روترهای شبکه لبه لایه فیزیکی را فراهم می کند. یک الگوریتم پنجره کشویی مبتنی بر زمان برای پیش پردازش ترافیک شبکه گرفته شده در هر روتر Cloud و ارسال آن به یک ماژول تشخیص ناهنجاری با استفاده از طبقه‌بندی کننده Naive Bayes استفاده می‌شود. مجموعه‌ای از گره‌های سرور کالا مبتنی بر Hadoop و MapReduce برای هر ماژول تشخیص ناهنجاری در دسترس هستند تا در هنگام افزایش تراکم شبکه از آن استفاده کنند. برای هر پنجره زمانی، داده های ترافیک شبکه ناهنجار در هر سمت روتر با یک سرور ذخیره سازی مرکزی همگام می شوند. در مرحله بعد، طبقه‌بندی‌کننده‌های یادگیری گروهی مبتنی بر جنگل تصادفی برای انجام آخرین مرحله طبقه‌بندی چند کلاسه به منظور شناسایی نوع هر حمله استفاده می‌شود.

ادهاماد و همکاران[۴] (۲۰۱۸) تحقیقی با موضوع سیستم تشخیص نفوذ توزیع شده برای محیط های ابری بر اساس تکنیک های داده کاوی انجام داده اند. نتایج بدین صورت بود ، تقریبا دو دهه بعد از ظهور انها؛ محاسبات ابری همچنان در میان سازمان ها و کاربران فردی در حال افزایش است. بسیاری از مسائل امنیتی همراه انتقال برای این الگوی محاسباتی شامل با مقدار زیادی از تشخیص نفوذ به وجود می اید. ابزارهای حمله و نفوذ با شکستن سیستم های تشخیص نفوذ سنتی ابری موجود از کمبود دقت تشخیص؛ نرخ مثبت کاذب اطلاعات ترافیک شبکه و رفتارهای پویا پیچیده تر شده است بالا و زمان اجرای بالا رنج می برد. در این مقاله ما یک یادگیری توزیع ماشینی بر مبنی سیستم تشخیص نفوذ برای محیط های ابری را ارائه می دهیم. سیستم پیشنهاد شده برای مندرجات در سمت ابری به وسیله اندازه همراه اجزای شبکه لبه از از لایه فیزیکی اجازه می routers ابرهای ارائه شده است. اینها به ترافیک رهگیری شبکه های ورودی به لبه شبکه ابری استفاده router مبتنی بر زمان برای پیش پردازش شبکه گرفتار ترافیک در هر دهد. یک الگوریتم پنجره کشویی استفاده می شود. یک مجموعه از گره های Naive Bayes می شود و سپس در نمونه تشخیص ناهنجاری دسته بندی برای هر نمونه تشخیص ناهنجاری از زمانی که تراکم شبکه MapReduce و Hadoop سرور کالا بر مبنی یک برای یک router افزایش می یابد؛ در دسترس است. برای هر پنجره زمانی؛ داده ترافیک ناهنجاری شبکه در هر طرف تصادفی Forest سرور ذخیره سازی مرکزی هماهنگ شده است. بعد؛ یک طبقه بندی یادگیری گروهی بر مبنی یک برای اجرای یک مرحله دسته بندی چند کلاسه نهایی به منظور تشخیص انواعی از هر حمله استفاده می شود

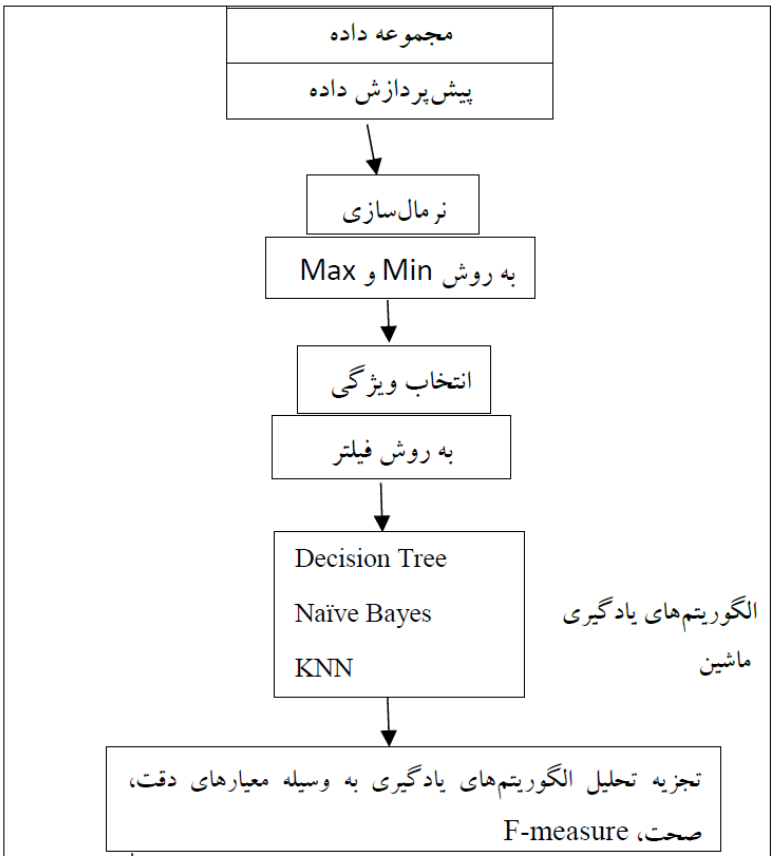
روش تحقیق

روش تحقیق اکتشافی است شناسایی نفوذ توزیع در این بخش سعی شده تشخیص نفوذ را با استفاده از الگوریتم های با ناظر یادگیری ماشین شامل، الگوریتم درخت تصمیم، و الگوریتم بیزین وK نزدیکترین همسایه و انتخاب ویژگی به روش فیلتر صورت گرفته است .روش پیشنهادی یک روش ترکیبی از الگوریتم های یادگیری ماشین برای تشخیص نفوذ است که از تمامی خواص الگوریتم ها استفاده میشود. فرآیند تشخیص از سمت محیط ابری شروع میشود و سپس با

4. Adhamad et all

یک بررسی اولیه برای آسیب پذیری در این قسمت انجام میشود و اگر یک رفتار عادی و مشکوک مشاهده شود داده برای بررسی بیشتر به سمت سیستم تشخیص نفوذ فرستاده میشود. در این قسمت نیز با نرمال سازی و انتخاب ویژگی های مهم داده برای الگوریتم های استفاده شده مقدار خطا به حداقل رسانده شده است.

چارچوب پیشنهادی یک مکانیزم یادگیری ماشین برای تشخیص نفوذ در محیط ابری میباشد. در شکل ۱ چارچوب کلی روش پیشنهادی بیان شده است.



شکل ۱ چارچوب روش کلی پیشنهادی

جامعه و نمونه

پایگاه داده استفاده شده در این پژوهش KDD-NSL میباشد. این پایگاه داده دارای ۴۱ ویژگی و یک کلاس است .این ویژگی ها به ۴ دسته تقسیم می شوند: ویژگی های پایه، ویژگی های محتوایی، ویژگی های ترافیک زمانی، ویژگی های ترافیک میزبان.

ویژگیهای پایه: این ویژگیها، ویژگیهای اتصالات TCP فردی هستند.

ویژگیهای محتوایی: این ویژگیها صفاتی هستند که در رابطه با دانش دامنه پیشنهاد شده اند.

ویژگیهای ترافیک زمانی: این ویژگیها صفاتی هستند که با استفاده از یک پنجره زمان دو ثانیه ای محاسبه میشوند.

ویژگی های ترافیک میزبان: این ویژگی ها صفاتی هستند که برای ارزیابی حمالت بیشتر از دو ثانیه طراحی شده‌اند.

انتخاب ویژگی

با استفاده از انتخاب ویژگی زیر مجموعه ای M تایی از میان مجموعه N تایی انتخاب میکنیم، که برای اینکار از روش فیلتر استفاده میکنیم .در این روش داده هایی که دارای رتبه بندی کمتری هستند در واقع دادههایی که قدرت دسته بندی

کمتری دارند را حذف میکنیم و پردازش را بر اساس بقیه پایگاه داده انجام میدهیم. در این تحقیق، از روش فیلتر برای انتخاب ویژگی و از نرم افزار KNIMEبرای انجام آن استفاده کرده ایم

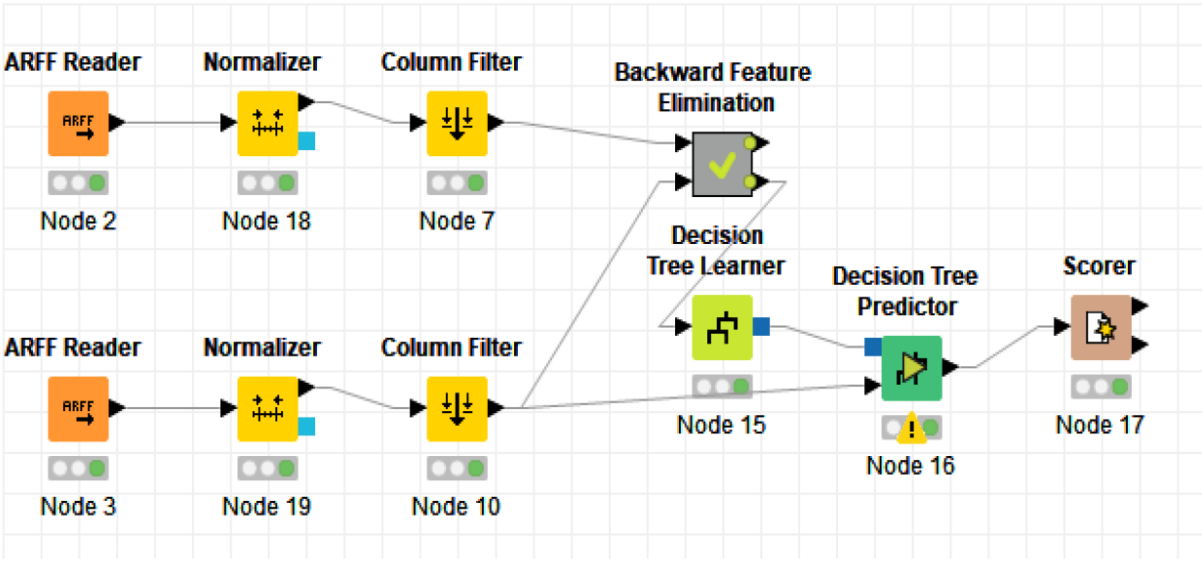
در این روش میتوان ویژگی هایی که دارای دقت بالایی هستند را انتخاب کرد و درصد خطا را پایین آورد .در این پروژه این روش را با استفاده از الگوریتم های یادگیری درخت تصمیم انجام داده و طبق مشاهدات الگوریتم درخت تصمیم از دقت بالایی برای بدست آوردن دقت ویژگی ها و همچنین دارای سرعت بالایی نیز میباشد درنتیجه این انتخاب ویژگی با الگوریتم درخت تصمیم انجام شده است. در این انتخاب، ویژگی هایی با دقت های بالا را با استفاده از گره فیلتر موجود در KNIME انتخاب کرده ایم. لازم به ذکراست که اگرالگوریتم داده شده برخی گروه ها از ویژگی های با همان دقت را نشان می دهد ، گروهی با تعداد کمتری از ویژگی ها انتخاب می شوند و ویژگی ایندکس از صفر شروع می شود و براساس نزولی طبقه بندی شده اند.

تنظیم پارامترهای الگوریتم های یادگیری ماشین

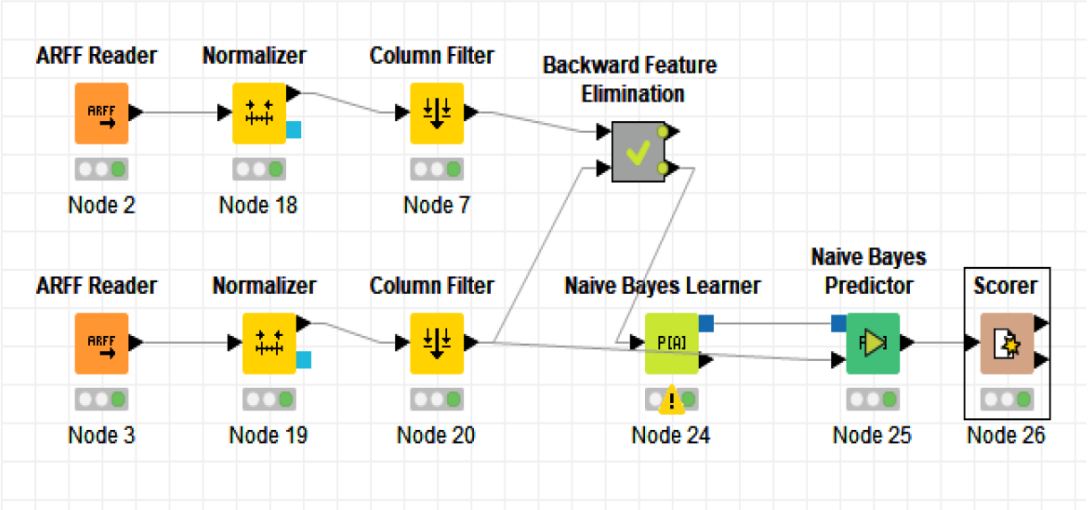
در این بخش از چند الگوریتم یادگیری ماشین با توجه به ویژگی های انتخاب شده برای هر الگوریتم دقت تشخیص حمله سنجیده میشود. الگوریتم های یادگیری ماشین معمولا با تنظیم پارامترهای متفاوت قابل تنظیم هستند، از اینرو باید بهترین پارامترها برای این الگوریتم ها انتخاب شوند تا منجرب به دقت بالا شوند. برای درخت تصمیم برای اینکه ویژگی هایی را انتخاب کنیم که اطاعات بیشتری در اختیار ما بگذارند از شاخص جینی استفاده کرده ایم. برای هر ویژگی که شاخص جینی کمتری داشته باشد آن ویژگی اطالعات بیشتری به ما میدهد. شاخص جینی برای دادههایی که دارای قسمتهای بزرگ هستند استفاده میشود. در این الگوریتم حداکثر عمق درخت را برابر با ۱۰۰ قرار دادیم زیرا در این عمق الگوریتم در بهترین حالت خود قرار میگیرد .یک پارامتر قابل تنظیم برای الگوریتم k نزدیکترین همسایه نیز برای بدست آوردن اطالعات دقیق باید k را به صورت بهینه قرار دهیم، که طبق مشاهدات بدست آمده بهترین مقدار آن در این پایاننامه برابر با ۳ قرار داده شده است .در روش بیزین نیز دقت تشخیص را برابر با ۰،۰۰۱ قرار داده تا حتی کوچکترین احتمالات را نیز در نظر بگیرد تا بهترین پاسخ را برگرداند

٤-٥ابزار استفاده شده برای پیاده سازی

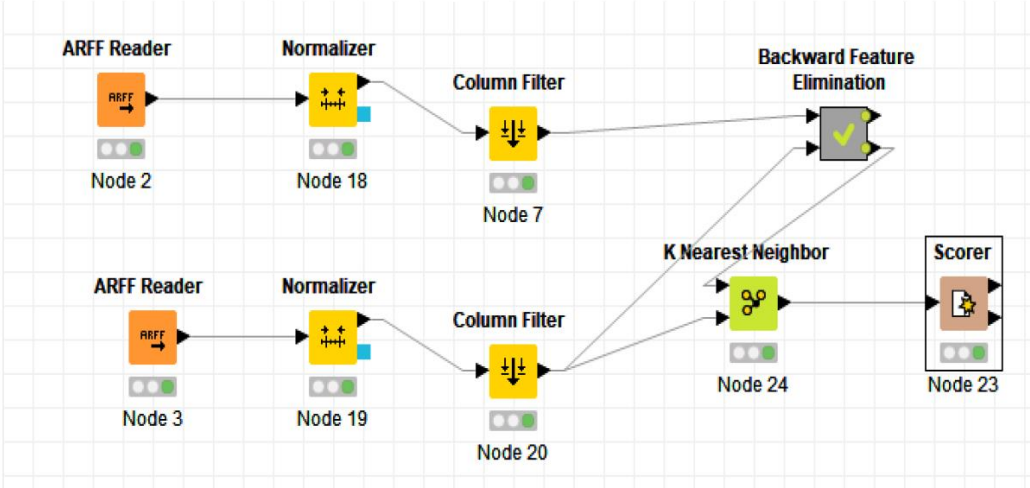
برای پیاده سازی این مقاله از نرم افزار نایم۱ استفاده شده است. نایم یک نرم افزار متن باز و یکپارچه برای تجزیه و تحلیل دادهها و گزارش کردن میباشد، که به زبان جاوا نوشته شده است. از ویژگی های این نرم افزار این است که به کاربر اجازه میدهد به صورت بصری جریان داده را بسازد، این نرم افزار فرآیند تحلیل را همان طوری که درک و پیاده سازی شده، ذخیره می کند. یکی از ویژگی های مهم این نرم افزار وجود گره های بسیار برای انجام پروژهای یادگیری ماشین و داده کاوی میباشد. معماری هسته نایم امکان پردازش دادهها با حجم بزرگ را فراهم میکند که فقط به فضای موجود در هارد دیسک محدود میشوند.



شکل ۲- نمونه استفاده شده از نرم افزارKNIME برای الگوریتم درخت تصمیم



شکل ۳- نمونه استفاده شده از نرم افزارKNIME برای الگوریتم بیزین

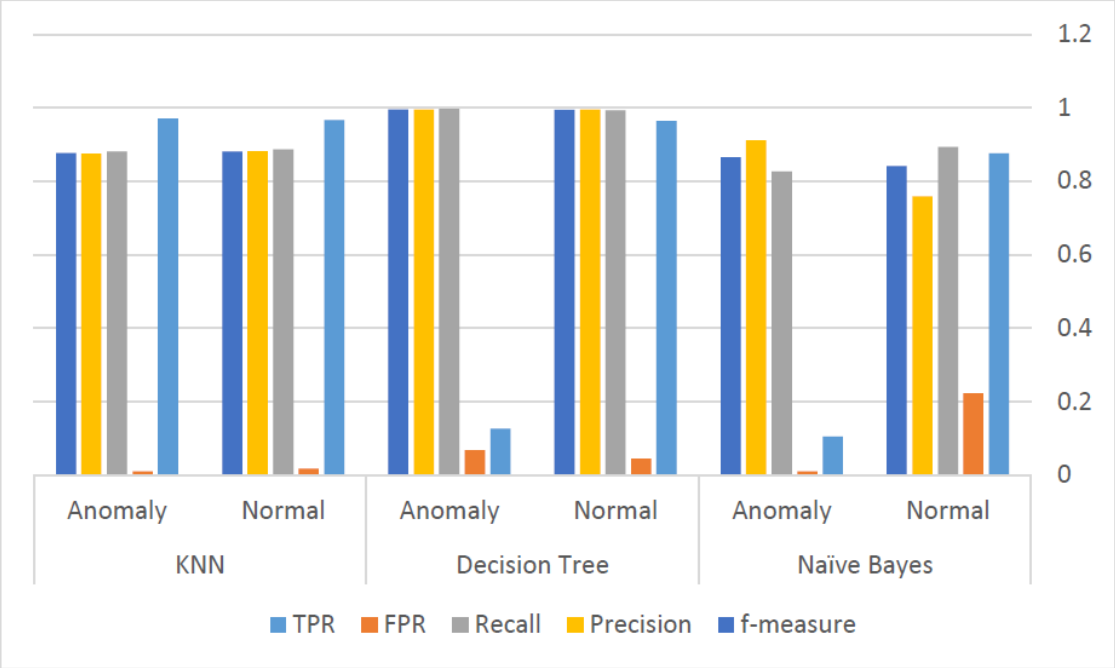


شکل ٤- نمونه استفاده شده از نرم افزارKNIME برای الگوریتم همسایه

جدول ۳- ارزیابی الگوریتم های طبقه بندی با توجه به دیتا برای کلاس های نرمال و غیر نرمال

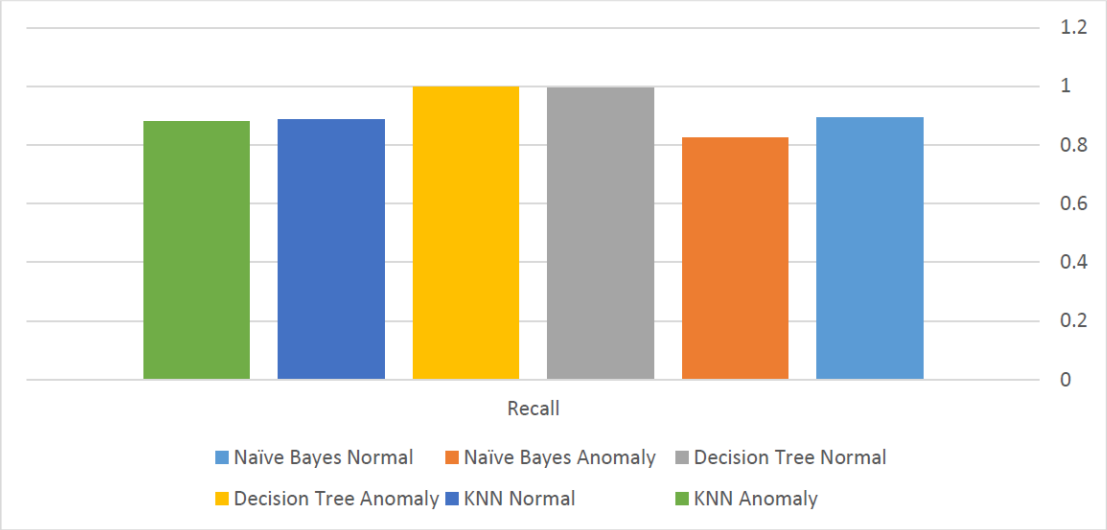
Creation Algoritm	class	TPR	FPR	Recall	precision	F-measure
Naïve bayes	normal	0.867	0.223	0.893	0.759	0.841
	anomlay	0.105	0.105	0.826	0.911	0.866
Decision	normal	0.964	0.964	0.993	0.996	0.994
	anomlay	0.126	0.126	0.997	0.995	0.996
KNN	normal	0.967	0.967	0.887	0.882	0.881
	anomlay	0.971	0.971	0.881	0.875	0.887

شکل یک مقایسه کلی بین نواحی مثبت و منفی، دقت، صحت و measure-F را با توجه به کلاس نرمال و غیرنرمال نشان میدهد.نتایج نشان میدهد که الگوریتم درخت تصمیم با داشتن دقت ۰,۹۹۶ درصد در کلاس نرمال و ۰,۹۹۵ درصد در کلاس غیر نرمال دقیقترین الگوریتم است.

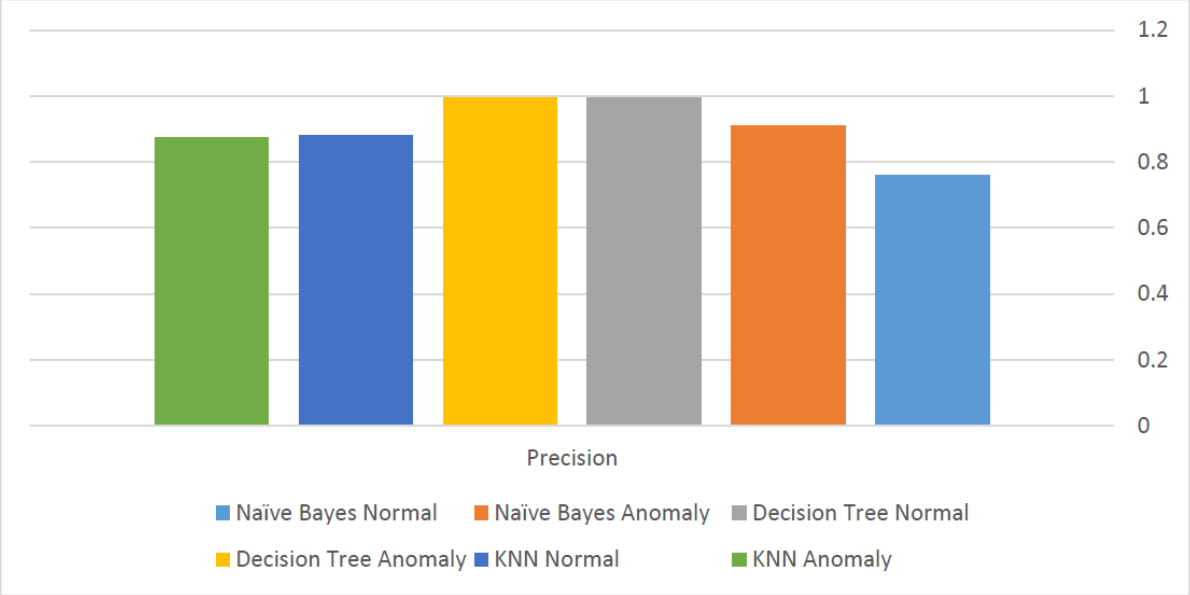


شکل ۵- مقایسه کلی بین دسته بندها با توجه به دیتاست KDD-NSL

با توجه به کلاس نرمال و غیر نرمال در ادامه هر کدام از معیارها را به صورت جداگانه برای درک بیشتر نمایش دادهایم، همانطور که مشاهده میکنید الگوریتم درخت تصمیم نسبت به الگوریتم بیزین و نزدیکترین همسایه دقیقتر میباشد. پس برای تشخیص نفوذ از این الگوریتم استفاده میکنیم.



شکل ٦– مقایسه معیار RECALL برای کلاس نرمال و غیر نرمال برای دیتا



شکل ۷–مقایسه معیارPRECISION برای کلاس های نرمال و غیر نرمال

مقایسه با روشهای دیگر درستی یک الگوریتم بر اساس Precision و Accuracy بررسی میشود. که در واقع دقت تکرارپذیر و دقت درست الگوریتمها هستند. دقت تکرارپذیر در واقع دادههایی هستند که تقریبا درست میباشند و در واقع مقداری است که به هدف بسیار نزدیک میباشند و دقت درست در واقع درستی هدف است یعنی خود هدف است.

نتیجه گیری

محیط ابری نشان دهنده تکامل اینترنت در آینده میباشد. اینترنت شیوه زندگی مردم را تغییر داده است و تعاملات میان انسانها از دنیای واقعی به فضای مجازی گسترش یافته است. در این میان، محیط ابری ابعاد جدیدی در این فرآیند ایجاد کرده است و ارتباطات میان اشیاء با دیدگاه در هر زمان، هر مکان و با هر وسیله را امکانپذیر میسازد .با توجه به اینکه محیط ابری جزئی از اینترنت آینده خواهد بود از این پس خود دادهها و اطلاعات باید نقطه ی تمرکز راهکارهای ارتباطی و شبکه بندی باشد .از اینرو، اخیرا مبحث امنیت اینترنت اشیاء مورد توجه بسیاری از پژوهشگران قرار گرفته

است. هر چند کحیط ابری دروازه بزرگ و مهمی را برای ورود به دنیایی با قابلیتهای بیششتر برای بشرباز کرده، در عین حال تهدیداتی بزرگتر از همیشه را نیز متوجه زندگی ما کرده است. در این میان، اولین قدم برای فرار از این تهدیدات این است که هر فرد و نهادی مسئول حفاظت از اطلاعات خود باشد. تهدیدات امنیتی میتواند در هر قسمتی از جمله سخت افزار یا نرم افزار پدید آید که باید منابع تهدید را از دسترسی محافظت نمود. یکی از راههای مقابله با حملات و نفوذها در اینترنت اشیاء استفاده از سیستم تشخیص نفوذ است .در این پروژه از یک سیستم تشخیص نفوذ مبتنی بر الگوریت مهای یادگیری ماشین براساس پایگاه داده Kdd-NSL استفاده کرده ایم. سپس این دادهها براساس الگوریتمهای درخت تصمیم و بیزین و نزدیکترین همسایه دسته بندی شدند. نتایج بدست آمده از این تحقیق نشان میدهد که علاوه بر سرعت بالا در تشخیص، الگوریتم درخت تصمیم از دقت بالایی نیز برخوردار میباشد .با این حال نتایج ما ممکن است دارای مشکلاتی نیز باشند، زیرا وقتی عمل انتخاب ویژگی را انجام میدهیم ممکن است ویژگیهایی که انتخاب میکنیم به درستی انتخاب نشوند. پس برای اینکه نتایج بهتر و دقیقتری انجام دهیم نیاز به تجربه در محیط های متفاوتی را داریم .نتایج حاصل از این الگوریتم ها به دو دسته دادههای نرمال و غیرنرمال تقسیم میشوند. در نتیجه باعث میشود داده هایی که به عنوان غیرنرمال تشخیص داده شده اند شناسایی و نتوانند بکار خود ادامه دهند.

منابع و ماخذ

البدوی، امیر.، محمدی، رضا و عالم خان، آفاق. (۱۳۸۵).ارزیابی اثرات مدیریت ارتباط با مشتری و موانع شخصی سازی در موسسات مالی مجله بانک و اقتصاد، ۶۹: .۴۳-۴۵

بشیری موسوی سید علیرضا افسر امیر و محجوبی ،فرد آرش (۱۳۹۴). تحلیل ارزش مشتری در بانک با استفاده از تکنیک داده کاوی و تحلیل سلسله مراتبی فازی. پژوهشهای مدیریت در ایران، ۱۹(۱): ۴۳-۲۳.

بهشتی، عطیه و اعلایی محبوبه (۱۳۹۷). ضرورت و مزایای استفاده از گیمیفیکیشن در صنعت بیمه بیست و پنجمین همایش ملی بیمه و توسعه، تهران، ۱۳ آذرماه.

ترکستانی، محمد صالح ،قربانی مریم و فروتن مریم (۱۳۹۳) کاربردهای داده کاوی در مدیریت ارتباط با مشتریان صنعت بیمه ایران بیست و یکمین همایش ملی و هفتمین همایش بین المللی بیمه و توسعه، ۱۳ آذرماه.

سلامت منش، مهرداد و نیکجو، امیر. (۱۳۹۲). مدیریت ارتباط با مشتریان بیمه. پیام بیمه ایران، ۱۷(۳۹۸) ۸-۱

مختاری، احسان و میرروشن دل سیدابواقاسم. (۱۳۹۵) پیش بینی رفتار مشتریان بیمه با استفاده از تکنیکهای داده کاوی کنفرانس ملی نوآوری در مدیریت سیستمها و فناوری اطلاعات با رویکرد هوشمندی کسب و کار :تهران دانشگاه الزهرا، ۲۸

ویسی، هادی و غروی ،عرفانه (۱۳۹۳) رویکرد مبتنی بر داده کاوی در مدیریت ارتباط با مشتری و بازاریابی مطالعات رفتار مصرف کننده، ۲(۲): ۴۴-۲۵.

Wind, Y. (1978). Issues and advances in segmentation research. Journal of Marketing Research.

Chen, S. C. & Huang M. Y. (2011). Constructing credit auditing and control & management model with data mining technique. Expert Systems with Applications

Aljarah, I. And Ludwig, S. A. (1). MapReduce Intrusion Detection System based on a Particle Swarm Optimization Clustering Algorithm. . IEEE Congress on Evolutionary Computation Conference (IEEE CEC').

Arora, P., Wadhawan, R. C. And Ahuja, S. P. (1). Cloud Computing Security Issues in Infrastructure as a Service. International Journal of Advanced Research in Computer Science and Software Engineering. Boss, G., Malladi, P., Quan, D., Leregni, L. And Hall, H. (Y). Cloud Computing, " IBM Corporation, White Paper.

Che, J., Duan, Y., Zhang, T. And Fan, J. (1). Study on the security models and strategies of cloud computing. International Conference on Power Electronics and Engineering Application. pp—095

Gupta, P. And Kaliyar, P. (۲۰۲). History Aware Anomaly Based IDS for Cloud IaaS. INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY. pp.

Gupta, S., Kumar, P. And Abraham, A. (1). A Profile Based Network Intrusion Detection and Prevention System for Securing Cloud Environment. International Journal of Distributed Sensor Networks.

Hassan, Q. F., Riad, A. M. And Hassan, A. E. (1). Software reuse in the emerging cloud computing era.

He, J., Tang, Ch., Yang, Y. And Qiao, Y. "D-IDS: IaaS user-oriented Intrusion Detection System. Y. Fourth International Symposium on Information Science and Engineering (ISISE). pp. T-10.

Holtz, M. D., David, B. M., Timoteo, R. And Junior, S. (1). Building Scalable Distributed Intrusion Detection Systems Based on the MapReduce Framework.

Jeong, H. J., Hyun, W., Lim, J. And You, I. Anomaly Teletraffic Intrusion Detection Systems on Hadoop-Based Platforms: A Survey of Some Problems and Solutions. Yoth IEEE International Conference on Network-Based Information Systems (NbiS). pp. VTT-VV..

Kholidy, H. A. And Baiardi, F. (1). CIDS: A framework for Intrusion Detection in Cloud Systems. .IT Ninth International Conference on Information Technology- New Generations (ITNG). pp. TV9_TAO .

Manavi, S., Mohammadalian, S., Udzir, N. I. And Abdullah, A. (1). Secure Model for Virtualization Layer in Cloud Infrastructure. International Journal of Cyber-Security and Digital Forensics (IJCSDF) .

Mell, P. And Grance, T. (1). The NIST Definition of Cloud Computing. National Institute of Standards and Technology (NIST), Standard Definition ...

Okuhara, M., Shiozaki, T. And Suzuki, T. (•). Security Architecture for cloud computing. pp.

Sathya, A. And Vasanthraj, K. (1). Network Activity Classification Schema in IDS and Log Audit for Cloud Computing. International Conf. on Information Communication and Embedded Systems (ICICES). pp.

Taghavi Zargar, S., Takabi, H. And Joshi, J. B.D. DCDIDP: A Distributed, Collaborative, and Data- driven Intrusion Detection and Prevention Framework for Cloud Computing Environments. CollaborateCom Y., Orlando, Florida, USA.

Tanenbaum, A. S. and Wetherall, D. J. Computer Networks, th ed.:Prentice Hall.

Yang, Sh., Chen, W. And Wang, Y. (1). ICAS: AN INTER-VM IDS LOG CLOUD ANALYSIS SYSTEM. Y. IEEE International Conference. pp. YA-YA

Roy, P. K., Bhuiyan, A., Janke, A., Desmond, P. M., Wong, T. Y., Storey, E., Abhayaratna, W. P. & Ramamohanarao, K. (2014). Automated segmentation of white matter lesions using global neighbourhood given contrast feature-based random forest and markov random field. International Conference on Healthcare Informatics, 1: 1-6.

Ngai, E. W. T., Xiu, L., & Chau, D. C. K. (2009). Application of data mining techniques in customer relationship management: A literature review and classification. Expert Systems with Applications, 36(2), 2592-2602.

Zichermann, G., & Cunningham, C. (2011). Gamification by design: Implementing game mechanics in Web and mobile apps. Sebastopol, scientific Research: O'Reilly Media.