مروری بر فنون مختلف تشخیص جعل کارت اعتباری

چکیده

استفاده از کارت های اعتباری به عنوان یک پیشرفت گسترده در فن آوری تجارت به وجود آمده و رشد کرده است. کارت اعتباری به یک روش بسیار مهم پرداخت تبدیل شده است ، بنابراین با افزایش معاملات با کارت اعتباری، کلاه برداری از کارت اعتباری نیز امروزه مکرر انجام می شود. [1] بنابراین، یک سیستم تشخیص کلاه برداری برای حفظ قابلیت اطمینان در سیستم پرداخت ضروری است. معیار اطمینان در معاملات برای صاحبان کارت اعتباری مهم است به طوری که آن ها بتوانند برای خدمات و محصولات که در اینترنت ارائه شده است با خیال راحت پرداخت الکترونیکی انجام دهند. در یک پست بانک بسیاری از معاملات به طور همزمان انجام می شود، بنابراین یک سیستم تشخیص کلاه برداری باید بین معامله مشروع، کلاه برداری مشکوک و معامله نامشروع تمایز قائل شود. [4] بسیاری از تکنیک های مدرن و جدید که در شبکه عصبی، هوش مصنوعی، شبکه بیزی ، داده کاوی، سیستم ایمنی مصنوعی، الگوریتم سیستم نزدیکترین همسایه K ، درخت تصمیم، اساس منطق فازی ، بردار پشتیبانی ماشین ، ماشین یادگیری ، برنامه نویسی ژنتیک و غیره بر این اساس وجود دارد ، که در تشخیص کارت های اعتباری مختلف در معاملات جعلی توسعه یافته اند. این مقاله نشان دهنده یک نظرسنجی از تکنیک های مختلف که مکانیزم تشخیص کلاه برداری در کارت اعتباری استفاده می شود.

کلمات کلیدی: روش های تشخیص کلاه برداری کارت اعتباری؛ کلاه برداری در کارت اعتباری؛ تجارت الکترونیک

I. مقدمه

سیستم های پرداخت الکترونیکی تجارت با توجه به استفاده گسترده از خرید مبتنی بر اینترنت و بانکداری به طور فزاینده ای محبوبیت پیدا کرده است. [4] کلاه برداری از کارت اعتباری یکی از بزرگترین تهدیدها برای سازمان تجارت امروز است. با این حال، غلبه بر کلاه برداری ، درک مکانیسم های اجرای یک کلاه برداری به طور موثر مهم است. به عنوان مثال ما نیاز به درک تکنیک های سایبری کلاه برداری از کارت اعتباری داریم. [1] از آنجا که پیش از این کلاه برداری فقط با شناسایی صورت حساب کارت اعتباری انجام شده است، جلوگیری از معاملات جعلی بسیار سخت بوده

. بنابراین نیاز به اطمینان در معاملات بدون مواجهه برای صاحبان کارت اعتباری در هنگام استفاده از کارت های اعتباری خود در پرداخت های الکترونیکی برای کالاها و خدمات ارائه شده در اینترنت یک معیار است.

انواع کلاه برداری:

کلاه برداری از کارت اعتباری به دو نوع تقسیم بندی می شوند؛

(I) کلاه برداری آنلاین از کارت اعتباری (و یا کلاه برداری بدون کارت) و

(II) کلاه برداری آفلاین از کارت اعتباری (کلاه برداری با کارت)

کلاه برداری آنلاین از کارت اعتباری (همچنین به عنوان کلاه برداری سایبری از کارت اعتباری شناخته می شود) که بدون حصور کارت اعتباری انجام می شود اما در عوض، از اطلاعات کارت اعتباری برای خرید الکترونیکی کالاها و خدمات را بر روی اینترنت استفاده می شود. [4] کلاه برداری آنلاین از کارت اعتباری با یک کارت اعتباری که در بیشتر موارد دزدیده شده است یا جعلی است انجام می شود و در نتیجه در یک فروشگاه محلی و یا یک مکان فیزیکی برای خرید برخی از کالا و یا خدمات مورد استفاده قرار می گیرد.

در بسیاری از کلاهبرداری های سایبری کارت اعتباری وجود دارد. برخی از آن ها[1] :

(I) اطلاعات خریداران با کارت اعتباری : این کلاهبرداران با مهارت های رایانه ای حرفه ای کمی مانند برنامه نویسی کامپیوتر، شبکه و غیره با سرقت یا هک اطلاعات کارت اعتباری در وب سایت غیر قانونی فروش کارت اعتباری، به سرعت خرید کالا و محصولات آنلاین انجام می دهند.

(II) دزد فیزیکی کارت اعتباری: این کلاهبرداران از لحاظ جسمی کارت های اعتباری را سرقت میکنند و ممکن است با استفاده از اطلاعات موجود در آن پرداخت الکترونیکی در اینترنت انجام دهند.

(III) هکرها کلاه سیاه : کسانی که امنیت کامپیوتر را نقض و به دنبال نیت بدخواهانه و یا منافع شخصی هستند. آن ها اهداف خود را با استفاده از یک فرآیند دو جانبه شناخته شده به عنوان "مرحله قبل از هک کردن" انتخاب می کنند؛ که شامل هدف قرار دادن، تحقیقات و جمع آوری اطلاعات و در نهایت حمله است. این هکرها در برنامه نویسی کامپیوتر و شبکه های کامپیوتری بسیار ماهر و با چنین مهارت های آن ها می توانند یک شبکه از رایانه را هدف قرار

دهند. هدف اصلی آن ها نفوذ و یا هک کردن و سرقت اطلاعات شخصی و خصوصی مانند اطلاعات کارت اعتباری، اطلاعات حساب بانکی و غیره برای منافع شخصی است.

II. تکنیک های مورد استفاده توسط کلاه برداران از کارت اعتباری

به منظور شناسایی فعالیت های کلاه برداری سایبری از کارت اعتباری در اینترنت، یک مطالعه در مورد چگونگی اطلاعات کارت اعتباری به سرقت رفته ، انجام شد است. [1] در اینجا برخی از روش های مختلف که برای سرقت اطلاعات کارت اعتباری توسط کلاه برداران استفاده می شود بیان شده است.

(I) کلاه برداری از کارت اعتباری بواسطه نرم افزار ژنراتور: این نرم افزار برای تولید شماره کارت اعتباری معتبر و تاریخ انقضای مورد استفاده است. برخی از این نرم افزار ها قادر به ایجاد شماره کارت اعتباری معتبر مانند کارت اعتباری شرکت و یا صادر کنندگان است زیرا با استفاده از الگوریتم ریاضی لوهان کارت اعتباری شرکت و یا صادر کنندگان در ایجاد شماره کارت اعتباری برای مصرف کنندگان کارت اعتباری و یا کاربران خود استفاده می کند. در برخی از موارد، این نرم افزار توسط هکرها کلاه سیاه که اطلاعات کارت اعتباری بر روی یک فایل ذخیره شده است ، پایگاه داده نرم افزار می تواند اطلاعات کارت اعتباری معتبر را به روش دیگری برای کلاهبرداران سایبری کارت اعتباری که نرم افزار را خریداری کرده اند نمایش داده و برای هک استفاده می شود. این روش در برخی موارد توسط هکرها کلاه سیاه برای فروش هک اطلاعات کارت اعتباری به دیگر کلاهبرداران اینترنتی کارت اعتباری با مهارت های کامپیوتری کم مورد استفاده قرار می گیرد.

(II) کلید خوانی و شنود: هکرها کلاه سیاه که مهارت های حرفه ای برنامه نویسی و یا کامپیوتر دارند با نصب و شنود خودکار برنامه های کامپیوتری و با کلیدخوانی تمام ورودی صفحه کلید کامپیوتر برای هدف بازیابی اطلاعات شخصی مانند اطلاعات کارت اعتباری، و غیره استفاده می کنند، این کلاهبرداران قادر به آلوده کردن کاربران " با ارسال ایمیل های هرزنامه به کاربران کامپیوتر و درخواست از آن ها برای دانلود بازی های رایگان و یا نرم افزار هستند و زمانی که دانلود انجام شد شنود از کیلاگر به طور خودکار دریافت می شود". آن ها صفحه کلید ورودی بر روی یک

شبکه می سازند. بنابراین، هر کاربر ندانسته می تواند اطلاعات خصوصی خود را از طریق این نرم افزار ها به اشتراک بگذارد. گاهی اوقات این نرم افزار نیز با کلاهبرداران دیگر که دانش کامپیوتر و یا مهارت ندارد .

(III) شبیه سازی سایت ، نرم افزارهای جاسوسی و سایت تاجر : این نرم افزار نیز توسط هکرها کلاه سیاه، نصب شده و کاربران " برای پیگیری تمام فعالیت های وب سایت رایانه. با ردیابی و شناخت فعالیت های وب سایت از کاربران بر روی اینترنت ایجاد می شود، آن ها سایت های الکترونیکی و یا بانکی که به طور منظم توسط کاربر بازدید می شوند و ارسال کاربران برای استفاده از آن با شدت بازیابی اطلاعات خصوصی و یا شخصی است. همچنین در مورد سایت های تجاری جعلی، وب سایت های جعلی را ایجاد می کند که محصولات ارزان به کاربران ارائه شده و در نتیجه پرسش از کاربر برای پرداخت توسط کارت های اعتباری صورت می گیرد. با هر پرداخت در این سایت جعلی ، اطلاعات کارت اعتباری کاربر به سرقت می رود.

(IV) اطلاعات کارت اعتباری از لحاظ فیزیکی به سرقت رفته : کلاهبرداران می توانند کارت اعتباری را سرقت و از اطلاعات آن برای خرید کالا و محصولات آنلاین استفاده کنند.

(V) وب سایت های خرید CC / CVV2 : کلاهبرداران سایبری کارت اعتباری که مهارت های رایانه ای حرفه ای ندارند برای استفاده از پرداخت الکترونیکی جعلی برای برخی از کالاها و خدمات بر روی اینترنت اطلاعات کارت اعتباری هک شده در این وب سایت را خریداری می کنند.

III. روش های تشخیص کلاه برداری از کارت اعتباری

انجام بررسی از روش های مختلف برای تشخیص کلاه برداری ما را به این نتیجه رساند که برای تشخیص کلاه برداری از کارت اعتباری بسیاری روش های بسیاری به وجود آمده است.

روش ترکیبی با استفاده از تئوری دمپستر شافر و نظریه های بیزی.

هیبریداسیون Blast-Ssaha

مدل پنهان مارکوف.

الگوریتم ژنتیک

شبکه عصبی

شبکه های بیزی

الگوریتم نزدیکترین همسایه K

تشخیص جریان بر اساس معکوس نزدیکترین همسایه K (SODRNN)

سیستم مبتنی بر منطق فازی

درخت تصمیم گیری

سیستم فازی

بردار پشتیبانی ماشین

استراتژی یادگیری متا

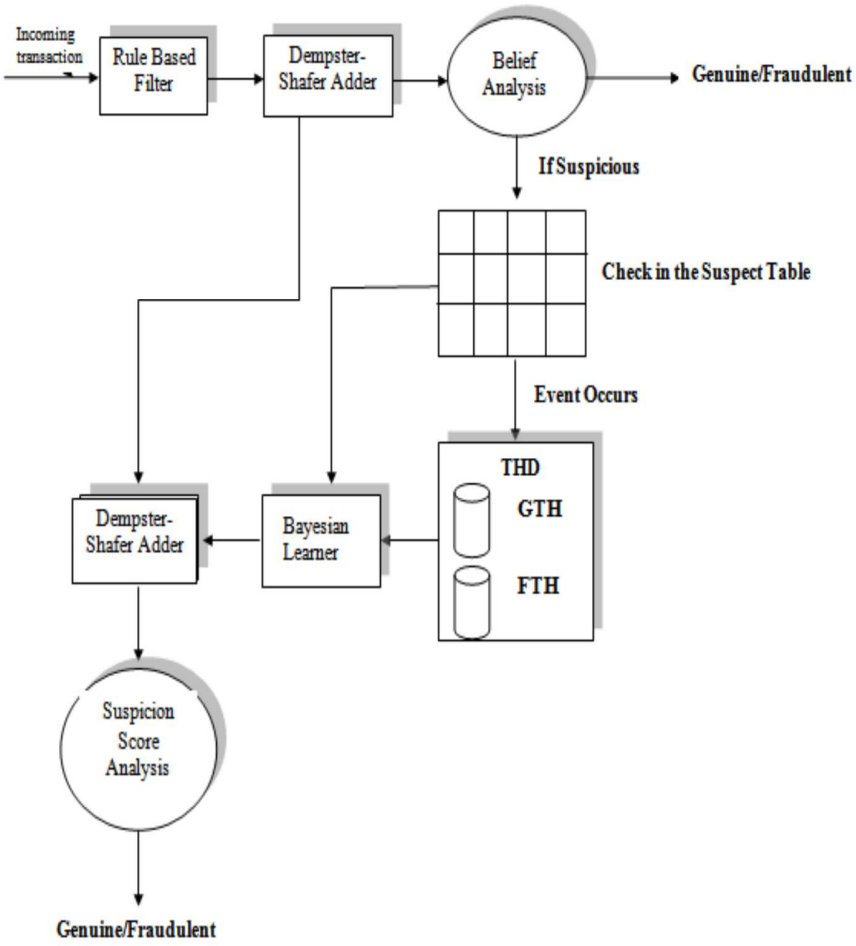
(I) روش ترکیبی با استفاده از تئوری دمپستر شافر و یادگیری بیزی

این سیستم ادغام سه روش تشخیص کلاه برداری از کارت اعتباری است ، به عنوان مثال، فیلتر مبتنی بر قانون، نظریه دمپستر شافر و یادگیری بیزی است. دمپستر برای ترکیب و شواهد متعدد وابسته از جزء بر اساس قانون برای محاسبه باور اولیه در مورد هر معامله های دریافتی استفاده شده است. [10] نمره که از طریق یادگیری بیزی با استفاده از پایگاه داده از هر دو دارنده کارت واقعی و همچنین کلاه برداری به روز شد است. THD جزء معامله از سیستم تشخیص کلاه برداری در بالا است. سابقه از هر دو معامله جعلی و واقعی برای ساخت سیستم های که به ما اجازه استخراج اطلاعات از ویژگی های دو گروه داده های در دسترس است استفاده می شود. برای انجام این کار، یک سابقه خوب معاملات (GTH) برای مشتریان فردی از رفتار گذشته خود و سابقه معاملات عمومی کلاه برداری (FTH) از انواع مختلف داده ها کلاه برداری گذشته ساخت شده است.

تاریخ هر معامله مجموعه ای از ویژگی هایی است که شامل اطلاعات مانند شماره کارت، مبلغ معامله و زمان آخرین خرید ساخته شده است . در حالی که مشاهده رفتار هزینه های فعلی بر روی یک کارت اعتباری، رفتار هزینه گذشته از نظر فراوانی معاملات در آن کارت نیز انباشته شده و مورد تجزیه و تحلیل قرار گرفته است. اطلاعات مبلغ معامله در

THDبرای تشخیص نقاط دورافتاده مورد نیاز است. [10] معماری FDS انعطاف پذیر است به طوری که قوانین جدید با استفاده از هر روش موثر دیگر را می توان در مرحله بعد به رشد بیشتر حکومت مبتنی گنجانده شده است. یادگیری بیزی به صورت پویا به رفتار در حال تغییر مشتریان واقعی و همچنین کلاهبرداران در طول زمان انطباق با FDS کمک می کند. نظریه دمپستر شافر عملکرد خوب، به ویژه در شرایط مثبت می دهد ، و یادگیری بیزی برای بهبود بیشتر دقت سیستم کمک می کند.

این امر دقت بالا را کاهش می دهد آلارم کاذب و بهبود سرعت کشف و شناسایی و همچنین در تجارت الکترونیکی قابل اجرا است. اما بسیار گران است و سرعت پردازش آن نیز کم است.

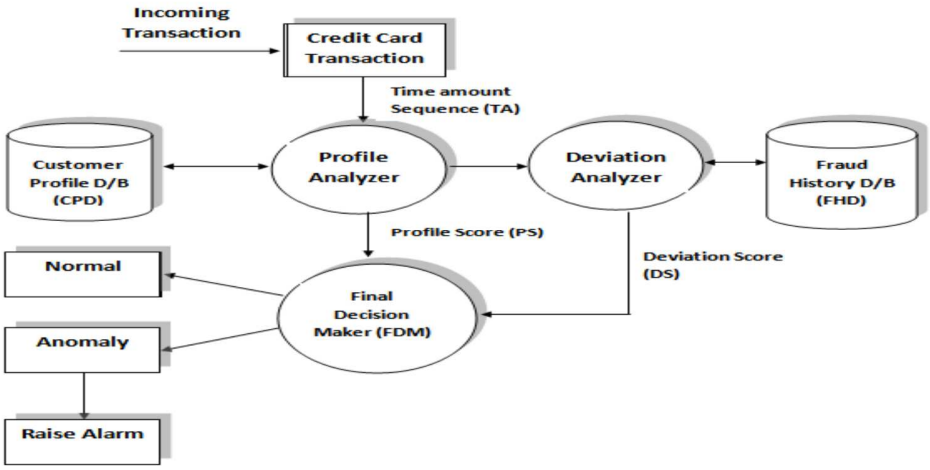


شکل 1 :بلوک دیاگرام سیستم تشخیص کلاه برداری با استفاده از دمپستر شافر تئوری و بیزی شبکه.

(II) هیبریداسیون Blast-Ssaha:

در این روش تشخیص کلاه برداری، هیبریداسیون BLAST و الگوریتم SSAHA استفاده شده است. [6] به همین دلیل بعنوان الگوریتم BLAH-FDS شناخته شده است. BLAST و الگوریتم SSAHA الگوریتم همردیفی توالی بسیار کارآمد است بنابراین این دو الگوریتم از هم ترازی توالی یک روش کارآمد به منظور بررسی رفتار هزینه از مشتریان استفاده می شود. [7] BLAH-FDS یک الگوریتم همردیفی توالی دو مرحله ای است که در آن تجزیه و تحلیل مشخصات (PA) مقایسه و تعیین تشابه توالی ورودی معاملات در یک کارت اعتباری داده شده با دارنده کارت واقعی صورت می گیرد. اگر معاملات غیر معمول باشد یافته های تجزیه و تحلیل مشخصات وجود دارد، پس آن ها را با یک تجزیه و تحلیل انحراف (DA) برای هر تراز با رفتار جعلی گذشته به تصویب می رسانند. داوری نهایی در مورد ماهیت معامله بر اساس مشاهدات ساخته شده و توسط این دو تجزیه و تحلیل انجام گرفته است.

وقتی که یک تراکنش انجام شده است، دنباله های ورودی به دو توالی شناخته شده و به عنوان توالی مقدار- زمان (TA) با هم ادغام شدند. تهراناونیو با توالی که به کارت اعتباری در ضوابط مشخصات پایگاه (CPD) مربوط تراز وسط قرار دارد. این فرایند تراز با استفاده از الگوریتم BLAST SSAHA که باعث افزایش سرعت فرایند هست انجام می شود. اگر TA شامل معامله واقعی باشد، سپس به خوبی با توالی در CPD انجام می شود. اگر هر گونه معامله جعلی در TP وجود داشته باشد، پس عدم تطابق در فرایند رخ می دهد. این عدم تطابق تولید دنباله D منحرف می کند که با پایگاه تاریخچه کلاه برداری (FHD) همتراز قرار دارند. [8] شباهت زیادی بین انحراف دنباله D و FHD در معاملات جعلی وجود دارد. PA ارزیابی نمره مشخصات (PS) با توجه به شباهت بین TA و DA CPD است. نمره انحراف (DS) با توجه به شباهت بین D و FHD ارزیابی می شود. FDM در نهایت نمره کل (PS - DS) را افزایش می دهد که کمتر از آستانه هشدار (AT) قرار دارد. عملکرد BLAHFDS خوب است و دقت آن بالا می باشد. همچنین سرعت پردازش به اندازه کافی سریع است. در آن فهرست کلاه برداری در ارتباط از راه دور و کلاه برداری بانکی تشخیص داده می شود. اما شبیه سازی آن از کارت های اعتباری قابل تشخیص نیست.



شکل 2: الگوریتم -سیستم کشف کلاه برداری BLAST SSAHA

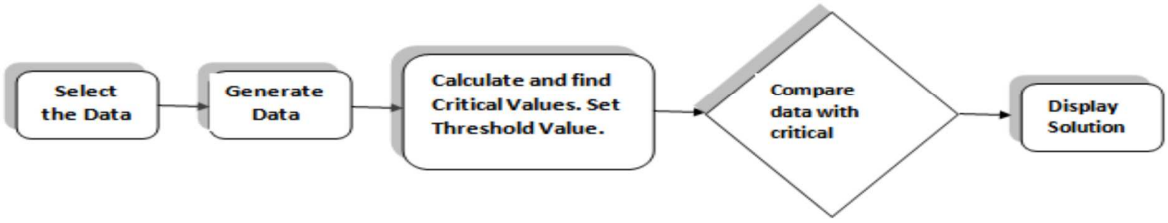
(III) مدل پنهان مارکف (مدل پنهان مارکف):

مدل پنهان مارکوف یک مجموعه متناهی از حالات است. هر دولت با یک توزیع احتمال در ارتباط است. انتقال در میان این کشورها توسط مجموعه ای از احتمالات به نام احتمال انتقال اداره می شود. [2] در یک دولت خاص ممکن است نتیجه و یا مشاهده تولید نماد مرتبط با مشاهده توزیع احتمال باشد. طبقه بندی مدل پنهان مارکف دارنده کارت " مشخصات هزینه ها بر اساس رفتار از نظر مقدار کم، متوسط و بالا است. مجموعه ای از احتمالات برای مقدار معامله است که به هر دارنده کارت داده می شود. مقدار هر معامله و سپس با صاحب کارت ورودی است ، اگر توجیه یک مقدار آستانه از پیش تعریف شده باشد پس از معامله مشروع دیگری به عنوان معامله جعلی اعلام نمی شود . [3] در مدل پنهان مارکف کاربر اصلی هرگز وارد نمی شود. ورود به سیستم برای معاملات بانک است که ساخته شده است. مدل پنهان مارکف کار خسته کننده یک کارمند در بانک را را کاهش می دهد. مدل پنهان مارکف ایجاد هشدار می کند. مدل پنهان مارکف بر روی رفتار انسان در زمان انجام خرید آنلاین کار می کند.

(IV) تشخیص کلاه برداری از کارت اعتباری با استفاده از الگوریتم ژنتیک:

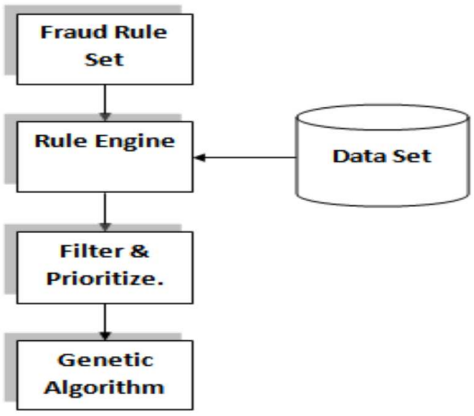
الگوریتم ژنتیک از الگوریتم های تکاملی است که با هدف به دست آوردن راه حل های بهتر به لحاظ فنی در از بین بردن کلاه برداری، اهمیت بالا به توسعه سیستم های پرداخت الکترونیکی امن و کارآمد برای تشخیص اینکه آیا یک معامله جعلی است یا نه ارائه شده است. [8] در طول اعتباری معامله با کارت، کلاه برداری در زمان واقعی و تعداد

هشدار نادرست با استفاده از الگوریتم ژنتیک به حداقل می رسد. کلاه برداری شناسایی شده بر روی رفتار مشتری استوار است. [15]



شکل 3: یک روش ساده از الگوریتم ژنتیک

روش الگوریتم ژنتیک به تعداد از پیش تعیین شده تکرار می شود ، و بهترین راه حل پیدا شده است. این روش یک روش پارامتری است و باید یک عملکرد بهتر ارائه دهد. [15] لیستی از پارامترها و تنظیمات مورد نیاز برای تولید معاملات جعلی را ایجاد می کند. چنین پارامترهایی برای محاسبه مقادیر بحرانی مورد نیاز هستند، برای محاسبه تعداد فراوانی استفاده از کارت اعتباری، محل کارت اعتباری ، اضافه برداشت کارت اعتباری، تعادل کنونی بانک ، میانگین هزینه های روزانه و غیره استفاده می شود



شکل 4 :طراحی سیستم

هدف آن به دست آوردن راه حل های بهتر و مطلوب است . این الگوریتم به کارت اعتباری سیستم بانک برای تشخیص کلاه برداری اعمال می شود، احتمال معاملات کلاه برداری پس از تراکنش های کارت اعتباری توسط بانک ها می تواند به سرعت پیش بینی شود. و یک سری از استراتژی های ضد کلاه برداری می تواند برای جلوگیری از زیان بزرگ بانک ها و کاهش خطرات به تصویب برسد.

(V) تشخیص داده پرت بر اساس نزدیک ترین همسایه معکوس K (SODRNN)

SODRNN، برای تشخیص داده پرت بر اساس نزدیکترین همسایه معکوس K عمل می کند. این الگوریتم شامل دو روش: مدیریت جریان و مدیریت پرس و جو است. همچنین تمام پنجره باید به حافظه اختصاص داده شود. [11] مدیریت جریان اشیاء جریان داده ورودی دریافت و به روز رسانی کارآمد پنجره می باشد. هنگامی که یک جریان جدید می آید، تنها به روز رسانی knnlist و rknnlist از اشیاء را در پنجره جاری تحت تاثیر قرار می دهد، به منظور حفظ پنجره فعلی به جای تمام اشیاء جریان داده ها در پنجره جاری ، هنگامی که شی ورودی جدید وارد شده باشد، به آن نیاز دارد. تنها یک پاس از اسکن پنجره فعلی برای پیدا کردن همه اشیاء که نزدیکترین همسایه K را تحت تاثیر قرار می دهد. به روز رسانی knnlists اشیاء را در پنجره فعلی rknnlists در همان زمان به روز رسانی تحت تاثیر قرار می دهد. [11] حذف نیازهای جسم منقضی شده تنها به روز رسانی rknnlists از اشیاء را در پنجره جاری با توجه به knnlist تحت تاثیر قرار می دهد ، و سپس به روز رسانی knnlists از اشیاء را در پنجره جاری با توجه به rknnlist تحت تاثیر قرار داده است. هنگامی که یک کاربر نیاز به یک پرس و جو دارد، مدیر پرس و جو از پنجره فعلی اسکن می گیرد و بازگشت اشیاء N که RNNk (P) کوچک به عنوان نقاط دورافتاده از پرس و جو است.

این الگوریتم، تعداد اسکن را تنها به یک کاهش می دهد. چک اعتبار کارت اعتباری و تشخیص خطاها در یک دنباله از اعداد صورت می گیرد بنابراین تشخیص اعداد معتبر و نامعتبر به راحتی در آن انجام می گیرد.

(VI) شبکه عصبی مصنوعی:

شبکه های عصبی مصنوعی (ANN) برای تشخیص کلاه برداری اعمال می شود، به طور عمده در زمینه طبقه بندی نظارت شده هستند. شبکه های عصبی مصنوعی (ANN) را می توان در به رسمیت شناختن ویژگی های به موقع و

پیش بینی استفاده کرد. [12] استفاده از شبکه های عصبی به خاطر این واقعیت است که شبیه سازی مغز به ویژه شناسایی الگو و حافظه انجمنی انگیزه آن است. شبکه عصبی الگوهای مشابهی را به رسمیت می شناسد، پیش بینی ارزش و یا حوادث بر اساس حافظه انجمنی الگوهای آن از آینده است. این مدل قادر به یادگیری از گذشته است و در نتیجه، به مرور زمان در نتایج آن بهبود رخ می دهد. همچنین آن ها می توانند قوانین را استخراج و فعالیت های آینده را بر اساس وضعیت فعلی پیش بینی کنند. با به کارگیری شبکه های عصبی ، بانک ها می توانند استفاده از یک کارت جعلی را، سریع تر و کارآمدتر تشخیص دهند.

در شرایط عملی تر ، ابزار مدل سازی داده های آماری شبکه های عصبی غیر خطی می باشد. [12] آن ها با مدل روابط پیچیده بین ورودی و خروجی و برای پیدا کردن الگوهای موجود در داده استفاده می شود.

دو مرحله در شبکه عصبی وجود دارد:

الف) مرحله آموزش و

ب) مرحله شناخت.

یادگیری در یک شبکه عصبی که به نام آموزش است. دو نوع اصلی از روش های آموزشی شبکه های عصبی می باشد:

الف) همراه با نظارت و

ب) بدون نظارت.

در آموزش تحت نظارت، نمونه هر دو پرونده های جعلی و غیر جعلی برای ایجاد مدل ها استفاده می شود. از سوی دیگر، آموزش بدون نظارت به سادگی برای آن دسته از معاملات، که اکثر متفاوت از آن هایی که طبیعی است به نظر می رسد. همچنین تکنیک های بدون نظارت دانش قبلی معاملات جعلی و غیر جعلی به پایگاه داده نیاز ندارد. NN ها می توانند بهترین نتیجه را برای تنها مجموعه داده های بزرگ در معاملات را تولید کنند. و آن ها نیاز به یک مجموعه آموزش طولانی داده دارند.

دو نوع شبکه عصبی در سیستم تشخیص کلاه برداری از کارت اعتباری استفاده می شود:

(I) شبکه عصبی پس انتشار(BPNN)

یادگیری این الگوریتم برای آموزش شبکه عصبی محبوب ترین روش می باشد. این یک روش بهینه سازی سیستم پویا چند مرحله است که تابع هدف را به حداقل می رساند. یک روش یادگیری تحت نظارت است و یک کلیت از دلتا می باشد. آن بیشتر برای شبکه غذا مفید است که شبکه هیچ بازخوردی ندارد. این لایه ها از سه لایه ورودی، پنهان و خروجی تشکیل شده است. دریافتی معاملات از لایه ورودی عبور از لایه های پنهان عبور و سپس به لایه خروجی می رسد. این روش نیز به عنوان انتشار به جلو شناخته شده است. داده های ورودی بارها و بارها شبکه عصبی را تغذیه می کنند. هر خروجی از شبکه عصبی با خروجی مورد نظر مقایسه و خطا محاسبه شده است. این خطا پس از آن به شبکه عصبی انتقال و برای تنظیم وزن به طوری که خطا با هر تکرار کاهش یابد و شبکه عصبی به تولید خروجی مورد نظر نزدیک تر شود مورد استفاده قرار می گیرد. این فرایند به عنوان آموزش شناخته شده است. برای آموزش NN می توان آن را برای یک سیستم کارت اعتباری به طوری که آخرین داده های یک یا دو سال از همه مصرف کنندگان مورد نیاز است استفاده می شود. [11] در طول آموزش، شبکه برای معاشرت خروجی با الگوهای ورودی آموزش دیده است. پس از آموزش در زمانی که شبکه استفاده می شود، آن برای شناسایی الگوی ورودی و و ارتباط با الگوی خروجی تلاش می کند. قدرت شبکه های عصبی مورد آزمایش قرار گرفته است که یک الگوی است که در آن هیچ خروجی مرتبط با آن، به عنوان یک ورودی داده نشده است. هنگامی که کارت های اعتباری توسط یک کاربر غیر مجاز استفاده شود از بررسی سیستم تشخیص الگوی مورد استفاده توسط شبکه عصبی کلاه برداری با الگوی منطبق با دارنده اصلی کارت که در شبکه عصبی آموزش داده شده است، سیستم آن را به رسمیت نمی شناسد. [12]

با این حال، این الگوریتم نیاز به زمان طولانی آموزش، آزمایش های گسترده، آموزش مجدد پارامترها، مانند تعداد نورون پنهان، نرخ یادگیری و تکانه، برای تعیین بهترین عملکرد دارد.

(II) شبکه عصبی نقشه خود سازماندهی (SOMNN)

این روش یادگیری شبکه های عصبی بدون نظارت است. در کارت اعتباری SOM تشخیص کلاه برداری شده است و برای تشکیل پروفایل مشتری و تجزیه و تحلیل الگوهای کلاه برداری استفاده می شود. [5] در این روش داده های

معامله برای اولین بار شناسایی و پیش پردازش شده است. این داده ها در SOM به عنوان ورودی و وزن های نورون ها تنظیم می شود. در پایان این دوره آموزشی، داده ها را به مجموعه واقعی و جعلی از طریق فرایند خود سازمان دسته بندی می کنند. این شبکه شامل دو لایه است:

الف) یک لایه ورودی و

ب) یک لایه نقشه برداری

در شکل یک شبکه دو بعدی. هدف از این لایه این است که:

(I) طبقه بندی و خوشه داده های ورودی

(II) شناسایی و استخراج الگوهای پنهان در داده های ورودی

(III) اقدام به عنوان یک مکانیزم فیلترینگ برای لایه های بیشتر.

در این روش تمام معاملات در سیستم پرداخت را به مجموعه ای واقعی و جعلی با پیروی از دو فرضیه طبقه بندی می کنند:

1. اگر یک معامله ورودی جدید شبیه به تمام معاملات قبلی مجموعه نباشد، آن را جعلی در نظر می گیرد.
2. اگر یک معامله ورودی جدید شبیه به تمام معاملات قبلی از مجموعه واقعی باشد، آن را واقعی در نظر می گیرد.

(VII)درخت های تصمیم گیری و ماشین آلات بردار پشتیبان:

مدل های طبقه بندی شده ی درخت تصمیم و ماشین بردار پشتیبان (SVM) در مشکل کارت اعتباری و تشخیص کلاه برداری به کار رفته و توسعه یافته است . در این روش، هر حساب به طور جداگانه با استفاده از توصیف مناسب ردیابی، و معاملات اقدام به شناسایی و نشان داد به صورت عادی و یا مشروع کرده است. شناسایی در نمره تولید شده توسط مدل طبقه بندی توسعه یافته است. هنگامی که یک معامله جدید ادامه دارد، طبقه بندی می تواند پیش بینی کند که آیا معامله طبیعی یا کلاه برداری است.

در این روش، در مرحله اول، تمام اطلاعات جمع آوری پیش پردازش شده است و قبل از ما شروع فاز مدل سازی انجام شده است. از آنجا که، توزیع داده ها با توجه به طبقات بسیار نامتوازن است، نمونه برداری تا طبقه تحت نمونه با

استفاده از سوابق طبیعی انجام گرفته است به طوری که مدل باید فرصتی برای یادگیری ویژگی های سالم بودم و یا جعلی بودن پروفایل داشته باشد. [13] برای این کار، متغیرهایی که در تاسیس معاملات جعلی و مشروع موفق هستند را انجام دهید. سپس، این متغیرها به شکل نمونه طبقه بندی شده پرونده مشروع هستند. بعدها، این نمونه ها طبقه بندی شده از پرونده مشروع با آن هایی که ترکیب جعلی دارند به شکل سه نمونه با جعل های مختلف به نسبت سابقه است. اولین مجموعه با نسبت یک رکورد جعلی به یک رکورد طبیعی است؛ دوم ، با نسبت یک رکورد جعلی به چهار رکورد طبیعی است؛ و آخرین نسبت یک رکورد جعلی با آن هایی که طبیعی است.(13)

متغیرها باعث تفاوت در سیستم های تشخیص کلاه برداری می شوند. انگیزه اصلی ما در تعریف متغیرها که به شکل داده استفاده شده است افتراق مشخصات کاربر کارت جعلی از مشخصات کاربر مشروع کارت است. نتایج نشان می دهد که طبقه بندی SVM و دیگر روش درخت تصمیم گیری بهتر از SVM در حل مشکل تحت بررسی است. با این حال، اندازه آن از مجموعه داده های آموزشی بزرگتر است، دقت عملکرد، مدل SVM بر اساس معادل مدل درخت تصمیم گیری می باشد، اما تعداد جعل مشخص شده توسط مدل SVM هنوز هم کمتر از تعداد جعل مشخص شده توسط روش درخت تصمیم گیری است.

(VIII) سیستم بر اساس منطق فازی:

(I) هدف از شبکه های عصبی فازی برای پردازش حجم زیادی از اطلاعات است که مشخص نیست به طور گسترده در زندگی ما اعمال می شود. سیده و همکاران در سال 2002 شبکه های عصبی فازی که در ماشین های موازی برای سرعت بخشیدن به تولید قانون برای تشخیص کلاه برداری در کارت اعتباری مشتری خاص بود ارائه داده اند. کار او داده کاوی و کشف دانش در پایگاه داده (KD) است. در این روش، او با استفاده از روش GNN (شبکه عصبی گرانول) با استفاده از شبکه عصبی فازی بر اساس (FNNKD) کشف دانش کرده است، برای آموزش سریع شبکه و اینکه با چه سرعتی می توان تعدادی از مشتریان را برای تشخیص کلاه برداری به صورت موازی پردازش کرد. [8] جدول معامله وجود دارد که شامل زمینه های مختلف مانند مقدار معامله ، تاریخ بیانیه، تاریخ ارسال، زمان بین معاملات، کد معامله، روز، شرح معامله، و غیره است، اما برای اجرای این روش تشخیص کلاه برداری در کارت اعتباری، تنها زمینه های

قابل توجهی از پایگاه داده ها را به یک فایل متنی ساده با استفاده از نمایش داده شد مناسب SQL استخراج شده است. در این روش تشخیص معامله برای هر مشتری مقدار داده های ورودی کلیدی است. این پیش پردازش داده ها در کاهش اندازه داده ها و پردازش، که باعث می شود سرعت آموزش خفیف تری شود و الگوهای آموزش کمک کرده است. در این روند از شبکه عصبی فازی، داده ها را به سه دسته طبقه بندی می کنند :

1. اول برای آموزش،

2. دوم برای پیش بینی، و

3. سوم برای تشخیص کلاه برداری.

روال سیستم تشخیص برای هر مشتری به شرح زیر است:

پردازش داده ها از یک پایگاه داده سرور.SQL

استخراج داده ها پیش پردازش به یک فایل متنی.

نرمال بودن داده ها و توزیع آن به 3 دسته (آموزش، پیش بینی، تشخیص)

برای عادی سازی داده توسط یک عامل GNN ورودی در محدوده 0 تا 1 را پذیرفته است، اما مقدار معامله برای یک مشتری خاص تنها حداکثر مقدار معامله در کل کار ، هر عدد بزرگتر یا برابر با صفر بوده است . در این روش تشخیص، دو پارامتر مهم هستند که در طول آموزش استفاده می شود:

آموزش و خطا

چرخه آموزش.

با افزایش چرخه آموزش، خطا ی آموزش کاهش خواهد یافت. دقت و صحت نتایج بستگی به این پارامترها دارد. در مرحله پیش بینی، حداکثر خطای پیش بینی مطلق محاسبه شده است. [8] همچنین در مرحله تشخیص کلاه برداری ، خطا تشخیص مطلق محاسبه شده و اگر خطا تشخیص مطلق بزرگتر از صفر باشد آن چک می شود تا ببینید که آیا این خطا ی مطلق بیشتر از حداکثر خطای پیش بینی شده مطلق است یا نه. اگر یافت شود درست است سپس آن معامله را جعلی نشان می دهد در غیر این صورت معامله گزارش شده امن است. هر دو چرخه آموزش و طبقه بندی

داده برای نتایج بسیار مهم است. داده ها برای آموزش شبکه عصبی و پیش بینی بهتر آن وجود دارند. آموزش خطا کمتر پیش بینی می شود و تشخیص را دقیق تر می سازد. خطا زیاد تشخیص کلاه برداری است، امکان معامله با کلاه بردار وجود دارد.

(II) سیستم فازی داروینی

این روش با استفاده برنامه نویسی ژنتیک برای توسعه قوانین منطق فازی که قادر به طبقه بندی معاملات کارت اعتباری به آن هایی که "مشکوک" و غیر مشکوک هستند می باشد . این شرح و تفصیل استفاده از یک سیستم فازی تکاملی است که قادر به طبقه بندی معاملات مشکوک و غیر مشکوک با کارت اعتباری است. سیستم توسعه یافته شامل دو عنصر اصلی :

(I) برنامه نویسی ژنتیک (GP) الگوریتم جستجو و

(II) یک سیستم خبره فازی.

هنگامی که داده ها به سیستم FDS ارائه شده، اولین سیستم داده به سه گروه کم، متوسط و بالا به عنوان خوشه بندی فازی شناخته شده است. ژنوتیپ و فنوتیپ از سیستم GP برخی از قوانینی است که مطابقت با توالی های دریافتی با دنباله گذشته دارد. برنامه نویسی ژنتیک به منظور توسعه یک سری از قوانین فازی استفاده شده است طول متغیر است که تفاوت بین کلاس داده قرار داده شده در یک پایگاه داده را مشخص می کند. امن و مشکوک: هدف اصلی این سیستم تشخیص کلاه برداری شامل کار چالش برانگیز دسته بندی داده ها است. برای طبقه بندی معاملات، زمانی که پرداخت سر رسیده مشتری است و یا پرداخت سر رسیده کمتر از سه ماه است، معامله به عنوان غیر مشکوک در نظر گرفته می شود، در غیر این صورت به عنوان مشکوک در نظر گرفته می شود.

فازی داروینی داده های مشکوک و غیر مشکوک را به راحتی تشخیص می دهد و همچنین کلاه برداری کارت اعتباری به سرقت رفته را تشخیص می دهد. این سیستم دارای دقت بسیار بالا و تولید یک هشدار اشتباه پایین در مقایسه با روش های دیگر است، اما بسیار گران قیمت است. سرعت سیستم نیز کم است.

(IX) تشخیص کلاه برداری با استفاده از آموزش متا:

یادگیری متا یک استراتژی است که با استفاده از یادگیری ترکیب و ادغام تعدادی از طبقه بندی ها و یا به طور جداگانه مدل را فراهم می کند. بنابراین، یک طبقه بندی متا نسبتا با پیش بینی های طبقه بندی پایه آموزش داده شده است. [14] این سیستم دو فن آوری های کلیدی دارد:

(I) تشخیص عوامل کلاه برداری که یاد بگیرند که چگونه برای کشف کلاه برداری می کنند و ارائه خدمات تشخیص نفوذ درون یک واحد سیستم اطلاعات جمعی ، و

(II) یادگیری سیستم متا ترکیبی از دانش جمعی به دست آمده توسط عوامل محلی است. این یک سیستم امن و یکپارچه است.

عوامل طبقه بندی محلی یک بار مشتق شده و یا طبقه بندی پایه در برخی از سایت ها تولید شده است، دو یا بیشتر عوامل از جمله یک عامل طبقه بندی جدید را می توان به عنوان مثال یک طبقه بندی متا عنوان کرد که توسط یک عامل یادگیری متا تشکیل شده است. [14] این سیستم یادگیری متا اجازه خواهد داد که موسسات مالی برای به اشتراک گذاشتن مدل های خود در معاملات جعلی با تبادل عوامل طبقه بندی در یک سیستم عامل امن و بدون افشای اطلاعات مشکلی نداشته باشند. در این روش محدودیت های رقابتی و قانونی خود وجود دارد، و آن ها می توانند این اطلاعات را به اشتراک بگذارید.

IV. نتیجه گیری و کارهای آینده

روش های مختلفی برای تشخیص کلاه برداری از کارت اعتباری وجود دارد. در این مقاله، ما یک مطالعه مقایسه ای برخی از روش های تشخیص کلاه برداری در کارت اعتباری را ارائه داده ایم . اگر یکی از آن ها یا ترکیبی از الگوریتم ها برای سیستم کارت اعتباری بانک استفاده شود تشخیص کلاه امکان پذیر می شود، احتمالا معاملات جعلی می تواند پس از تراکنش های کارت اعتباری توسط بانک ها شناخته شود. مجموعه ای از استراتژی های ضد کلاه برداری می توان برای جلوگیری از زیان بانک ها و کاهش خطرات هرچه زودتر به تصویب برسد. این مقاله نسبت سهم راه های موثر در تشخیص کلاه برداری از کارت اعتباری را ارائه می دهد. جدول مقایسه برای مقایسه مکانیسم های تشخیص مختلف بر اساس پارامترهایی مانند، دقت، سرعت و هزینه آماده است.

روش	مدل پنهان مارکف	FDS	DST & BN	BSH	GA	SODRNN	ANN	Meta-learning	FNN	SVM	SOM
دقت	پایین	خیلی بالا	بالا	بالا	متوسط	متوسط	متوسط	بالا	خوب	متوسط	بالا
سرعت تشخیص	سریع	خیلی پایین	پایین	خوب	خوب	خوب	سریع	پایین	خیلی سریع	پایین	سریع
هزینه	خیلی گران	خیلی گران	گران	در حد متوسط	ارزان	گران	گران	گران	گران	گران	گران

جدول 1: مقایسه روش های مختلف تشخیص کلاه برداری.

اختصارات:

مدل پنهان مارکف - مدل مخفی مارکوف

FDS - سیستم فازی داروینی

DST - نظریه دمپستر شافر

BN - شبکه بیزی

BSH – هیبریداسیون Blast-Ssaha

GA - الگوریتم ژنتیک

SODRNN - جریان تشخیص پرت بر اساس معکوس نزدیکترین همسایه K

ANN - شبکه های عصبی مصنوعی

FNN - شبکه عصبی فازی

SVM - ماشین پشتیبان بردار

SOM - نقشه شبکه خود سازمانده عصبی