اولین رویداد دیتاتون بانک سپه
با همکاری کارخانه هوشمندسازی و نوآوری امیدینو
آذرماه ۱۴۰۳

مدل الگوریتم مارکوف پنهان و کاربرد آن در سیستم خبره بانکی با تشخیص و کشف تقلب در کارت های پرداخت

علی بشیری فرد[1]

۱-کارشناس عملیاتی (متصدی امور بانکی)، مهندسی تکنولوژی نرم افزار کامپیوتر،

آموزش عالی جهاد دانشگاهی اهواز، شعبه طالقانی دزفول شاخص ۱۵۰۱۳۹۹

چکیده:

به دلیل پیشرفت سریع در فناوری تجارت الکترونیک، بیشتر تراکنش‌ها در بانکداری به صورت آنلاین انجام می‌شوند. از آنجا که در بانکداری ارائه‌دهندگان خدمات زیادی وجود دارند، کاربر باید عملکرد آنها را تحلیل کرده و بهترین را انتخاب کند، همچنین کارت‌های پرداخت نقدی به محبوب‌ترین روش پرداخت برای خریدهای آنلاین و معمولی تبدیل شده‌اند.

در این مقاله ما مفهوم سه سطح امنیت را معرفی می‌کنیم، سطح اول نام کاربری یا رمز عبور ایستا است و در سطح دوم از HMM[1] استفاده می‌شود و نشان می‌دهد که چگونه می‌توان از آن برای تشخیص تقلب‌ها استفاده کرد. یک مدل مارکوف پنهان ابتدا با رفتار عادی یک دارنده کارت، آموزش داده می‌شود. اگر یک تراکنش کارت پرداخت ورودی با احتمال کافی توسط آموزش‌دیده پذیرفته نشود، به عنوان یک تراکنش تقلبی در نظر گرفته می‌شود. در عین حال، ما سعی می‌کنیم اطمینان حاصل کنیم که تراکنش‌های واقعی رد نشوند و برای کاهش تراکنش‌های مثبت کاذب، ما رمز عبور پویایی را ارسال خواهیم کرد که می‌تواند به با سرعت از طریق خدمات وب به شماره تلفن همراه کاربر ارسال شود و او باید همان رمز عبور را برای دریافت تأییدیه از سمت بانک وارد کند و فرض کنید که به دلیل بار سنگین روی سرور، اگر کاربر رمز عبور را در تلفن همراه خود در زمان مقرر دریافت نکند، پس از یک فاصله زمانی کوتاه، برخی سوالات شخصی (یا سوالات امنیتی یا تصاویر) یا استفاده از کد رمز ریکپچا پرسیده خواهد شد که کاربر نهایی می‌تواند به آن‌ها پاسخ دهد.

---

[1] - مدل مارکوف پنهان

کلیدواژه‌ها: مدل مارکوف پنهان؛ نام کاربری/رمز عبور ثابت؛ سوال امنیتی؛ تصویر امنیتی؛ رمز عبور پویا؛ الگوریتم HMM؛ کپچا؛ ریکپچا.

۱- مقدمه

در هنگام انجام تراکنش آنلاین با استفاده از کارت پرداخت صادر شده توسط بانک، تراکنش ممکن است یا خرید آنلاین باشد یا انتقال وجه. خرید آنلاین می‌تواند با استفاده از کارت پرداخت یا کارت اعتباری صادر شده توسط بانک انجام شود و خرید مبتنی بر کارت می‌تواند به دو نوع تقسیم شود. کارت فیزیکی و کارت مجازی. در هر دو مورد، اگر کارت یا جزئیات کارت دزدیده شود، کلاهبردار می‌تواند به راحتی تراکنش‌های کلاهبرداری انجام دهد که منجر به خسارت قابل توجهی به دارنده کارت یا بانک خواهد شد. در مورد انتقال آنلاین وجه، کاربر از جزئیاتی مانند شناسه ورود، رمز عبور و رمز عبور تراکنش استفاده می‌کند. لذا اگر جزئیات حساب مورد سوء استفاده قرار گیرد، منجر به کلاهبرداری مجدد از دارنده کارت خواهد شد.

تقلب کارت پرداخت یک اصطلاح گسترده برای سرقت و تقلب است که با استفاده از کارت پرداخت یا هر مکانیزم پرداخت مشابه به عنوان منبع تقلبی از وجوه در یک معامله انجام می‌شود.

هدف ممکن است به دست آوردن کالا بدون پرداخت، یا به دست آوردن وجوه غیرمجاز از یک حساب باشد. تقلب با کارت پرداخت همچنین به سرقت هویت مرتبط است. تقلب با دزدی فیزیکی کارت یا نفوذ به داده‌های مرتبط با حساب آغاز می‌شود، از جمله شماره حساب کارت یا سایر اطلاعاتی که به طور معمول و ضروری در طول یک معامله قانونی برای یک فروشنده در دسترس خواهد بود. این نفوذ می‌تواند از طریق بسیاری از مسیرهای رایج اتفاق بیفتد و معمولاً می‌توان آن را بدون اطلاع دارنده کارت، فروشنده یا صادرکننده انجام داد. یک مثال ساده این است که یک کارمند فروشگاه یک رونوشت از رسیدهای فروش را برای استفاده بعدی تهیه می‌کند. رشد سریع استفاده از کارت‌های پرداخت در اینترنت، به ویژه نقص‌های امنیتی پایگاه داده را پرهزینه کرده است. در برخی موارد، میلیون‌ها حساب به خطر افتاده‌اند.

کارت‌هایی که به مفقود یا به سرقت رفته اند می‌توانند به سرعت توسط دارندگان کارت گزارش شوند، اما یک حساب یا کارت پرداخت که با خطر مواجه می شود می‌تواند توسط یک دزد برای هفته‌ها یا ماه‌ها قبل از هرگونه استفاده تقلبی نگهداری شود، که شناسایی منبع نقض امنیت را دشوار می‌کند. دارنده کارت ممکن است تا زمانی که صورت حسابی دریافت کند که ممکن است به ندرت ارسال شود، از استفاده غیرمجاز کارتش مطلع نشود.

۲- پیاده‌سازی

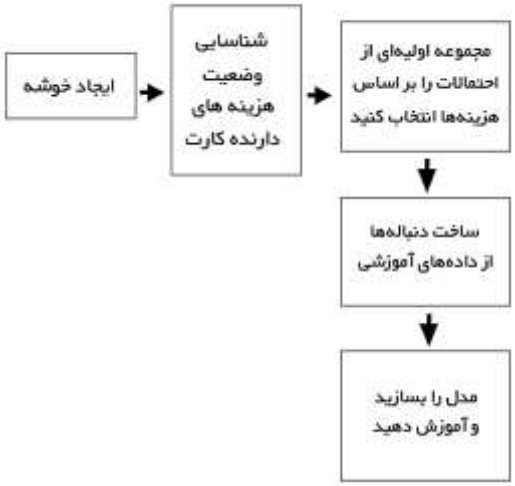
مدل مارکوف پنهان چگونه کار می‌کند؟

مدل مخفی مارکوف (HMM) الگوی خرج کردن هر کارت را پیگیری می‌کند و هر گونه ناهماهنگی با الگوهای

خرج کردن "معمولی" را شناسایی می‌کند. اگر یک تراکنش کارت پرداخت ورودی با احتمال کافی بالا توسط HMM آموزش‌دیده پذیرفته نشود [۵]. سپس یک هشدار صادر می‌کند که نشان می‌دهد مشکلی در استفاده از کارت پرداخت وجود دارد، اما در این مقاله به جای هشدار، می‌توانیم رمز عبور پویا را به تلفن همراه کاربر ارسال کنیم تا تعداد تراکنش های مثبت بی مورد را کاهش دهیم، یا از طریق کد رمزهای ریکپچا عملیات احراز هویت را تایید کنیم، لذا تراکنش های مثبت بی مورد به معنای هشدار یا اخطاری است که نشان می‌دهد حمله‌ای در حال انجام است یا حمله‌ای با موفقیت انجام شده است در حالی که در واقع چنین حمله‌ای وجود نداشته است.

در مدل مارکوف پنهان، که نیازی به امضای تقلب ندارد و با در نظر گرفتن عادت‌های خرج کرد دارنده کارت، قادر به تشخیص تقلب‌ها است. (دنباله پردازش تراکنش کارت توسط فرآیند تصادفی یک مدل مارکوف پنهان).

شکل (۱) نمودار جریان فرآیند برای آموزش مدل الگوریتم مارکوف پنهان را نشان می‌دهد.

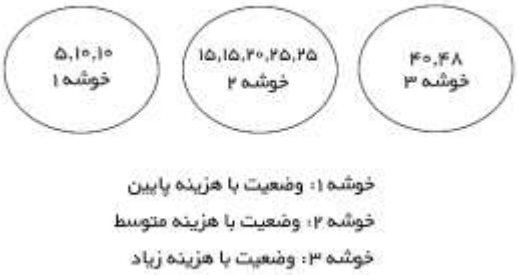


شکل (۱): نمودار جریان فرآیند برای آموزش الگوریتم مارکوف پنهان

ما اطلاعات کاربران را با عنوان دسته بندی کم‌خرج، دسته با خرج متوسط و پرخرج و خود نفوذگر تقسیم بندی می‌کنیم. اطلاعات وضعیت یا حالت هزینه‌کرد دارنده کارت فردی برای به‌دست آوردن یک تخمین اولیه از سایر اطلاعات وضعیت یا حالت آن‌ها استفاده می‌شود.

شماره تراکنش	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰
مقدار به هزار	۲۰	۲۵	۱۵	۵	۱۰	۲۵	۱۵	۲۰	۱۰	۸۰

جدول (۱) : جدول حالت تراکنش ها



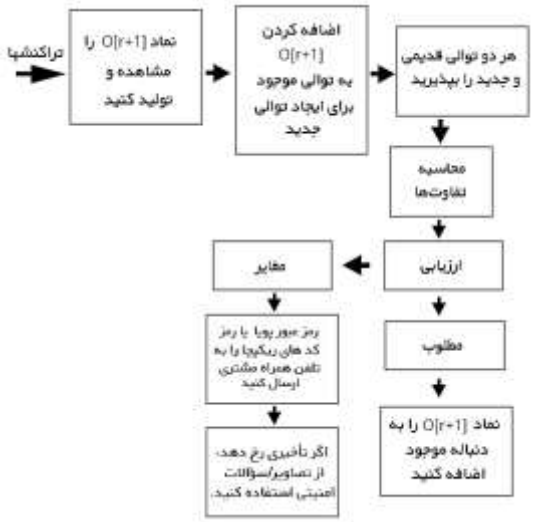
شکل(۲): خوشه بندی

۳-خوشه‌بندی

به عنوان مثال، اگر O1 ، O2، O3، O4 را در نظر بگیریم، یا دنباله‌های تراکنش‌های انجام شده توسط دارنده کارت، به طول r و اگر O[r+1] نمادی باشد که توسط جدیدترین تراکنش ایجاد شده است، برای تشکیل یک دنباله دیگر به طول r ، O1 را حذف کرده و O[r+1] را به دنباله اضافه می‌کنیم و در واقع یک دنباله جدید از O2، O3، O4، ...، O[r+1] ایجاد می‌کنیم. سپس تفاوت‌ها را بین هر دو توالی قدیمی و جدید محاسبه می کنیم تا مشخص شود آیا تراکنش واقعی است یا خیر. در واقع ما از این طریق واقعی بودن تراکنش را مورد بررسی قرار میدهیم. همانطور که در شکل (۲) نشان داده شده است. ما مقدار r را برابر با ۱۰ در نظر گرفته‌ایم. همانطور که در جدول (۱) نشان داده شده است، معاملات انجام شده توسط کاربر را نشان می‌دهد و برای این معاملات، ما سه خوشه ایجاد می‌کنیم. جایی که خوشه(۱) خوشه وضعیت با هزینه پایین، خوشه(۲) خوشه وضعیت با هزینه متوسط و خوشه(۳) خوشه وضعیت با هزینه بالا است.

همانطور که در شکل(۲) نشان داده شده است. بنابراین در مثال فوق، خوشه(۲) دارای بالاترین درصد تراکنش‌ها است. لذا می‌توانیم نتیجه بگیریم که کاربر در خوشه(۲) قرار دارد یا او در وضعیت هزینه متوسط قرار دارد.

اگر تراکنش جدیدی بیاید، دوباره خوشه‌ها تشکیل می‌شوند و تفاوت‌ها ثبت می‌شوند. اگر تفاوتی وجود نداشته باشد، تراکنش انجام می‌شود و اگر تفاوت هایی پیدا شود (یعنی مشخصات تغییر کند) باید رمز عبور پویا یا استفاده از کد رمزهای ریکپچا به تلفن همراه کاربر ارسال شود تا کاربر واقعی شناسایی شود. همانطور که در شکل(۲) نشان داده شده است.



شکل (۳): نمودار جریان فرآیند برای تشخیص تقلب از طریق مدل مارکوف پنهان

۴-رمز عبور پویا

در مورد رمز عبور پویا، شماره تصادفی در سمت سرور تولید می‌شود و از طریق وب سرویس‌ها به تلفن همراه مشتری ارسال می‌شود تا اطمینان حاصل شود که کاربر صحیح در آن لحظه از کارت استفاده می‌کند. او باید همان رمز عبور را برای دریافت تأییدیه از سمت بانک وارد کند و اگر به دلیل بار سنگین روی سرور، کاربر رمز عبور را در تلفن همراه خود در زمان مقرر دریافت نکند، پس از مدت زمانی کوتاه، برخی سوالات شخصی (سوالات یا تصاویر امنیتی) پرسیده می‌شود که کاربران می‌توانند به آنها پاسخ دهند و این سوالات یا تصاویر امنیتی باید با سوالات یا تصاویر امنیتی پر شده یا انتخاب شده توسط مشتری در زمان افتتاح حساب مطابقت داشته باشند.

۵- رمز کدهای ریکپچا یا آرکپچا:

کپچا[۲] نرم‌افزاری امنیتی است که برای تشخیص انسان از کامپیوتر و با هدف مقابله با ربات های مخرب اینترنتی به وجود آمد. در ابتدا، کپچا صرفا برای جلوگیری از اسپم استفاده می‌شد اما دیری نگذشت که حملات بات های مخرب اینترنتی شدت گرفت و حساب‌های کاربری، اطلاعات کاربران و غیره را هدف قرار داد. اما کپچا سپری قدرتمند برای محافظت از وب‌سایت‌ها و اطلاعات شخصی کاربران در مقابل ربات های اینترنتی است که با هدف جلوگیری از چنین آسیب‌هایی به وجود آمد.

کپچا به معنی آزمایش عمومی کاملا خودکار تورینگ[۳] به منظور تشخیص دادن انسان از کامپیوتر است. کپچاها آزمون‌های امنیتی بر پایه آزمایش تورینگ هستند که به سایت‌ها اضافه می‌شوند تا امنیت سایت را درمقابل حملات ربات‌های مخرب اینترنتی تامین کنند. تست‌های آنلاین کپچا از طریق ایجاد پرسش‌هایی قابل حل برای انسان ولی چالش برانگیز برای ربات‌ها، انسان‌ها را از ربات تشخیص می‌دهند.

در خصوص آرکپچا می توان گفت که آرکپچا سرویسی امن، سریع و حرفه‌ای است. ویژگی‌های اصلی آرکپچا در بخش امکانات، امنیت، سرعت، حریم خصوصی و پشتیبانی در مقایسه با سایر سرویس‌های کپچا به شرح زیر است:

- دارای امکانات کنترلی پیشرفته مانند تنظیم دستی و خودکار سختی چالش‌ها، کنترل محتوا و نوع چالش‌ها، نمایش آمار و گزارش استفاده‌ها و هشدار ترافیک نامتعارف.

- امنیت اولویت آرکپچا است. به کمک تایید دومرحله‌ای پاسخ‌ها، نویزهای هوشمند و آدرس‌دهی داینامیک تصاویر، امنیت را برای سرویس کپچا تامین می‌کند.

---

۲ - CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)

۳ - Turing Test

- به کمک بهینه‌سازی‌های انجام شده و استفاده از سرورها و CDN[۴] های داخلی (شبکه توزیع محتوا) ، سرعت و دسترس‌پذیری باکیفیت را تضمین می‌کند[10].

- رعایت حریم خصوصی کاربران برای آرکپچا مهم است. آرکپچا کم‌ترین اطلاعات ممکن را از کاربران می‌گیرد و از این اطلاعات برای هیچ گونه مقاصدی استفاده نخواهد شد.

شکل (۴): نمودار جریان عملکردی کد رمزهای ریپچا

نتیجه‌گیری

در این مقاله، ما رویکردی را پیشنهاد کردیم که بر روی تراکنش‌های آنلاین با استفاده از کارت پرداخت صادر شده توسط بانک تمرکز دارد، که این تراکنش می‌تواند خرید آنلاین یا انتقال باشد. جایی که سه سطح امنیت باید پیاده‌سازی شود، اولین سطح رمز عبور ایستا است، دومین سطح مدل مارکوف پنهان است و اگر HMM هرگونه تقلبی را تشخیص دهد، سطح سوم وارد عمل می‌شود که در آن باید از رمز عبور پویا و استفاده از کدهای ریکپچا استفاده شود، که به دنبال آن سوال امنیتی یا تصاویر امنیتی قرار دارد. چرا از تصاویر امنیتی استفاده می‌کنم؟ زیرا در برخی موارد دستگاه‌هایی که از آن‌ها تراکنش انجام می‌دهیم، صفحه‌کلیدهای الفبایی ندارند .

بنابراین در چنین مواردی پاسخ به سوالات امنیتی تایپ نخواهد شد. در نتیجه، اگر کاربر این امکان را داشته باشد که هر تصویری را از طریق صفحه لمسی یا به هر روش دیگری انتخاب کند، این می‌تواند کار کند محدودیت استفاده از سه سطح امنیتی ممکن است منجر به تأخیر در خرید آنلاین یا انتقال آنلاین مبلغ شود[7]. اما این تأخیرها ناچیز هستند زیرا ما بیشتر بر روی امنیت تمرکز داریم. چنین نظرسنجی ای به ما این امکان را می‌دهد که رویکردی امن برای شناسایی تراکنش‌های تقلبی کارت پرداخت ایجاد کنیم. با سرویس آرکپچا می‌توانیم از نرم افزار و محیط های نرم افزاری بانک در مقابل حملات ربات‌های مخرب و اسپم محافظت کنیم. سرویس آرکپچا با ارائه سوالات تصویری مختلف ربات‌ها را تشخیص داده و مانع از دسترسی آن‌ها به محیط های نرم افزاری بانک (همراه بانک، اینترنت بانک و ...) می‌شود.

---

[۴] - Content Delivery Network

منابع:

[1] Abhinav Srivastava,Amlan Kundu,Shamik Sural and Arun K Majumdar," Credit Card Fraud Detection Using Hidden Markov Model,"IEEE Transactions On Dependable And Secure Computing ,vol.5 No.1,January-March 2008.

[2]"Credit Card Fraud," http://en.wikipedia.org/wiki/Credit_card_fraud

[3] L.R Rabiner,"A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognotion," proc.IEEE, vol.77, no.2,pp. 257-286,1989

[4] Raj Jain,The Art of Computer Systems Performance Analysis,John Wiley and Sons,Chapter 3,2010.

[5] S.Benson Edwin Raj,A.Annie Portia, "Analysis on Credit Card Fraud Detection Methds", International Conference on ComputerCommunication and Electrical TechnologyICCCET2011,March 2011

[6]"Types of Credit Card Fraud,"http://www.monetos.co.uk/financing/creditcards/fraud-protection/types.

[6] navi mumbai Nerul, India, navi mumbai Nerul, India. "Banking Expert System"With credit card fraud detection using HMM algorithm. International Journal Of Engineering And Computer Science, Dec 2015

[7] https://mahanserver.net/blog

[8] https://iranhost.com/blog/captcha

[9] https://kerasno.com/best-captcha-plugins/

[10] https://mizbancloud.com/blog/best-iranian-cdn