



الف	معرفی طرح
۱	<p>عنوان طرح پیشنهادی</p> <p>مدل الگوریتم مارکوف پنهان و کاربرد آن در سیستم خبره بانکی با تشخیص و کشف تقلب در کارت های پرداخت</p> <p>Hidden Markov algorithm model and its application in an expert banking system by detecting and detecting fraud in payment cards</p>
۲	<p>محور طرح پیشنهادی</p> <p> <input type="checkbox"/> کارآمدی شعب (Branch 360) <input type="checkbox"/> ارزش گذاری مشتریان <input type="checkbox"/> چت ربات های هوشمند <input type="checkbox"/> شناسایی و مدیریت ریسک <input type="checkbox"/> تجربه مشتری </p> <p> <input type="checkbox"/> شناسایی، کشف و پیش بینی رفتار مشتری <input type="checkbox"/> کشف تقلب و رصد تراکنش های مشکوک <input type="checkbox"/> تشخیص تهدیدات و بهبود پروتکل های امنیتی </p> <p> <input type="checkbox"/> تحلیل کانالهای ارائه خدمات <input type="checkbox"/> شناسایی رفتارهای غیرمعارف <input type="checkbox"/> سایر (لطفا ذکر شود) </p>
۳	<p>در این بخش بایستی توضیحاتی برای پاسخگویی به سوالات زیر را مختصراً درج نمایید.</p> <p>✓ کشف تقلب با ارائه سه سطح امنیتی</p> <p>✓ 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 داده های مرتبط با حساب آغاز می شود، 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.</p> <p>✓ در این مقاله ما مفهوم سه سطح امنیت را معرفی می کنیم، سطح اول نام کاربری یا رمز عبور ایستا است و در سطح دوم از HMM استفاده می شود و نشان می دهد که چگونه می توان از آن برای تشخیص تقلبها استفاده کرد. یک مدل مارکوف پنهان ابتدا با رفتار عادی یک دارنده کارت، آموزش داده می شود. اگر یک تراکنش کارت پرداخت ورودی با احتمال کافی توسط آموزش دیده پذیرفته نشود، به عنوان یک تراکنش تقلبی در نظر گرفته می شود. در عین حال، ما سعی می کنیم اطمینان حاصل کنیم که تراکنش های واقعی رد نشوند و برای کاهش تراکنش های مثبت کاذب، ما رمز عبور پویایی را ارسال خواهیم کرد که می تواند 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 می تواند به آن ها پاسخ دهد. حداقل مدتی که نیاز دارند تا پس از دریافت اطلاعات و سخت افزار مناسب طرح را عملیاتی نمایند.</p> <p>✓ باتوجه به وجود زیرساخت های موجود در شبکه بانکی کشور و بالتبع وجود مهندسان و نخبگان عزیز در واحد انفورماتیک بانکها، با مشورت اساتید محترم این موارد قابل پیگیریو اجرا هستند.</p>
۴	<p>منافع و جنبه های کاربردی</p> <p>دقت در احراز هویت دارندگان کارت هنگام انجام تراکنش های بانکی و جلوگیری از سرقت اطلاعات در پرداخت های دروغین و کاذب در سطح شبکه بانک و ایجاد یک حصار کارآمد در مقابل نفوذگران و سوء استفاده گران از سیستم های پرداخت.</p>



کاربرگ معرفی طرح

رویداد دیتاتون بانک سپه

Association Rule Mining <input type="checkbox"/> Principal Component Analysis <input type="checkbox"/> Portfolio Optimization <input type="checkbox"/> سایر (لطفا ذکر شود) <input type="checkbox"/>	Support Vector Machine <input type="checkbox"/> Neural Network <input type="checkbox"/> k-nearest Neighbors <input type="checkbox"/> Clustering <input checked="" type="checkbox"/> Anomaly Detection <input checked="" type="checkbox"/>	Linear Regression <input type="checkbox"/> Logistic Regression <input type="checkbox"/> Decision Tree <input checked="" type="checkbox"/> Random Forests <input type="checkbox"/> Time Series Forecasting <input type="checkbox"/>	تعیین الگوریتمهای مورد استفاده	۵	
توضیح :					
Go <input type="checkbox"/> C/C++ <input checked="" type="checkbox"/> سایر (لطفا ذکر شود) <input type="checkbox"/>	Scala <input type="checkbox"/> Julia <input type="checkbox"/> Swift <input type="checkbox"/> SAS <input type="checkbox"/>	Python <input type="checkbox"/> R <input type="checkbox"/> MATHLAB <input type="checkbox"/> Java <input checked="" type="checkbox"/>	نرم افزارهای مورد نیاز	۶	
تعداد و نوع تراکنشهای بانکی در سیستم تصمیم گیری واحد در هنگام بررسی توسط مدل الگوریتم مارکوف پنهان یا HMM بعنوان ایجاد مجموعه اولیه داده ها و احتمالات پیش آمده جهت ساخت دنباله ها برای ایجاد خوشه مورد نیاز می باشد.			داده های مورد نیاز برای اجرای تحلیل	۷	
<input type="checkbox"/> تحقیقاتی	<input type="checkbox"/> افزایش سودآوری	<input type="checkbox"/> افزایش سهم بازار	<input checked="" type="checkbox"/> افزایش کیفیت یا ظرفیت	<input type="checkbox"/> مدیریت و کنترل	<input type="checkbox"/> سایر
توضیح : به دلیل پیشرفت سریع در فناوری تجارت الکترونیک، بیشتر تراکنشها در بانکداری به صورت آنلاین انجام میشوند. از آنجا که در بانکداری ارائه دهندگان خدمات زیادی وجود دارند، کاربر باید عملکرد آنها را تحلیل کرده و بهترین را انتخاب کند، لذا استفاده از بستر امن پرداخت الکترونیکی، برای همه مشتریان و کاربران شبکه بانکی و افرادی که روزانه از سیستم های پرداخت غیرحضوری بهره می برند، بسیار حائز اهمیت می باشد. لذا با روشهای ذکر شده در این مقاله می تواند منجر به ایجاد مسیری امن تر جهت پرداخت های غیرحضوری جهت ایجاد اطمینان خاطر بیشتر و جلوگیری از تراکنش های دروغین و کاذب ناشی از سرقت اطلاعات بکار برد.					
[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 Recognition,” 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”,					
			نمونه کارهای مشابه	۹	



<p>International Conference on ComputerCommunication and Electrical Technology ICCET2011, March 2011</p> <p>[6] "Types of Credit Card Fraud," http://www.monetos.co.uk/financing/creditcards/fraud-protection/types.</p> <p>[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</p> <p>[7] https://mahanserver.net/blog</p> <p>[8] https://iranhost.com/blog/captcha</p> <p>[9] https://kerasno.com/best-captcha-plugins/</p> <p>[10] https://mizbancloud.com/blog/best-iranian-cdn</p>		
	سایر موارد	۱۰

فرم (۲)

اعضای تیم								ب
نام	نام خانوادگی	سمت سازمانی	محل خدمت	آخرین مدرک تحصیلی	نقش در تیم	شماره تلفن همراه	پست الکترونیکی	
۱	علی	بشیری فرد	کارشناس	شعبه طالقانی دزفول شاخص ۱۵۰۱۳۹۹	کارشناسی مهندسی تکنولوژی نرم افزار کامپیوتر	عضو	۰۹۳۵۶۸۷۶۴۳۲ Alibashiri4446@Gmail.com	
۲								
۳								
۴								



کاربرگ معرفی طرح

رویداد دیتاتون بانک سپه

سایر ملاحظات:

- لطفاً در صورتی که پاسخ به برخی از بندها مقدور نمی‌باشد آن را خالی بگذارید؛ هر چند تکمیل بودن کاربرگ در نظر هیئت داوران تأثیرگذار خواهد بود.
- فایل خام این کاربرگ بر روی سایت شرکت نوآوران بوم گستر امید (امیدبوم) به نشانی <https://omidinofactory.ir/datathon> قرار دارد. شرکت کنندگان بایستی پس از بارگیری فایل فرم و تکمیل آن ، فایل را در همان سامانه بارگذاری نمایند.
- مهلت ارسال کاربرگ‌های تکمیل شده ۳۰ مهرماه ۱۴۰۳ می‌باشد.
- در صورت وجود مشکل با شماره پشتیبانی سایت شماره ۰۹۱۲۰۹۱۳۹۱۵ تماس حاصل فرمایید و جهت اخذ اطلاعات تکمیلی به کانال روبیکایی با نام

مراجعه فرمایند.



"دیتاتون بانک سپه" با کد QR

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

علی بشیری فرد^۱

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 تراکنش ها در بانکداری به صورت آنلاین انجام می شوند. از آنجا که در بانکداری ارائه دهندگان خدمات زیادی وجود دارند، کاربر باید عملکرد آنها را تحلیل کرده و بهترین را انتخاب کند، همچنین کارت های پرداخت نقدی به محبوب ترین روش پرداخت برای خریده های آنلاین و معمولی تبدیل شده اند.

در این مقاله ما مفهوم سه سطح امنیت را معرفی می کنیم، سطح اول نام کاربری یا رمز عبور ایستا است و در سطح دوم از HMM^۱ استفاده می شود و نشان می دهد که چگونه می توان از آن برای تشخیص تقلب ها استفاده کرد. یک مدل مارکوف پنهان ابتدا با رفتار عادی یک دارنده کارت، آموزش داده می شود. اگر یک تراکنش کارت پرداخت ورودی با احتمال کافی توسط آموزش دیده پذیرفته نشود، به عنوان یک تراکنش تقلبی در نظر گرفته می شود. در عین حال، ما سعی می کنیم اطمینان حاصل کنیم که تراکنش های واقعی رد نشوند و برای کاهش تراکنش های مثبت کاذب، ما رمز عبور پویایی را ارسال خواهیم کرد که می تواند 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 ریکیچا پرسیده خواهد شد که کاربر نهایی می تواند به آن ها پاسخ دهد.

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 می‌شود 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

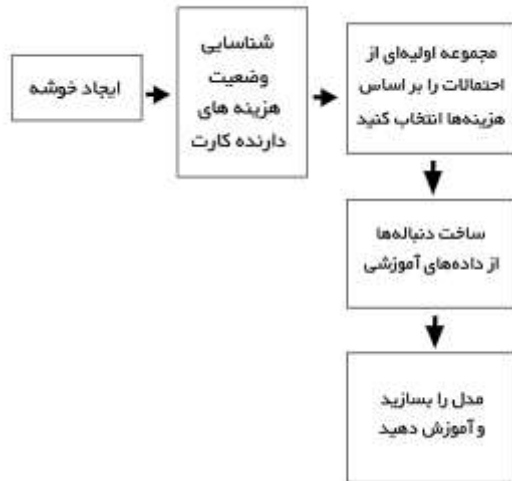
کلیدواژه‌ها: مدل مارکوف پنهان؛ نام کاربری/رمز عبور ثابت؛ سوال امنیتی؛ تصویر امنیتی؛ رمز عبور پویا؛ الگوریتم HMM؛ کپچا؛ ریکپچا.

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



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

ما اطلاعات کاربران را با عنوان دسته بندی کم خرج، دسته با خرج متوسط و پرخرج و خود نفوذگر تقسیم بندی می کنیم. اطلاعات وضعیت یا حالت هزینه کرد دارنده کارت فردی برای به دست آوردن یک تخمین اولیه از سایر اطلاعات وضعیت یا حالت آن ها استفاده می شود.

خرج کردن "معمولی" را شناسایی می کند. اگر یک تراکنش کارت پرداخت ورودی با احتمال کافی بالا توسط HMM آموزش دیده پذیرفته نشود [۵]. سپس یک هشدار صادر می کند که نشان می دهد مشکلی در استفاده از کارت پرداخت وجود دارد، اما در این مقاله به جای هشدار، می توانیم 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 ریکچا عملیات احراز هویت را تایید کنیم، لذا تراکنش های مثبت بی مورد به معنای هشدار یا خطاری است که نشان می دهد حمله ای در حال انجام است یا حمله ای با موفقیت انجام شده است در حالی که در واقع چنین حمله ای وجود نداشته است.

در مدل مارکوف پنهان، که نیازی به امضای تقلب ندارد و با در نظر گرفتن عادت های خرج کرد دارنده کارت، قادر به تشخیص تقلب ها 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 می دهد.

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

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



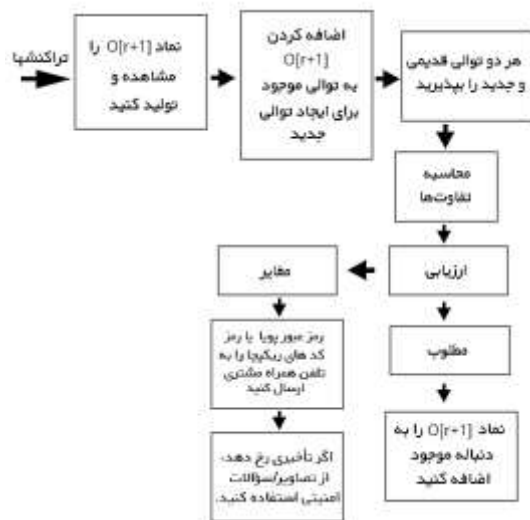
خوشه ۱: وضعیت با هزینه پایین
 خوشه ۲: وضعیت با هزینه متوسط
 خوشه ۳: وضعیت با هزینه زیاد

شکل (۲): خوشه بندی

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

۳- خوشه بندی

به عنوان مثال، اگر 01، 02، 03، 04 را در نظر بگیریم، یا دنباله های تراکنش های انجام شده توسط کاربر، 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 می کنیم و در واقع یک دنباله جدید از 02، 03، 04، ...، $O[r+1]$ ایجاد می کنیم. سپس تفاوت ها 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 می دهیم. همانطور که در شکل (۲) نشان داده شده است. ما مقدار ۲ را برابر با ۱۰ در نظر گرفته ایم. همانطور که در جدول (۱) نشان داده شده است، معاملات انجام شده توسط کاربر را نشان می دهد و برای این معاملات، ما سه خوشه ایجاد می کنیم. 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.



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 ربات‌های مخرب اینترنتی به وجود آمد. در ابتدا، کپچا صرفاً برای جلوگیری از اسپم استفاده می‌شد اما دیری نگذشت که حملات بات‌های 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 ربات‌های اینترنتی است که با هدف جلوگیری از چنین آسیب‌هایی به وجود آمد.

کپچا به معنی آزمایش عمومی کاملاً 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 در مقابل حملات ربات‌های مخرب اینترنتی تأمین 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 می‌توان 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.

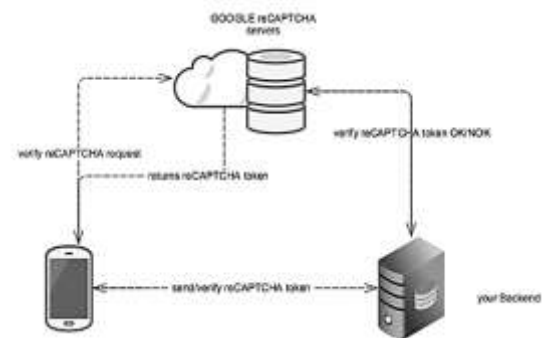
- امنیت اولویت آرکپچا است. به کمک تایید دومرحله‌ای پاسخ‌ها، نویزهای هوشمند و آدرس‌دهی داینامیک تصاویر، امنیت را برای سرویس کپچا تأمین می‌کند.

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، صفحه کلیدهای 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 نظرسنجی‌ای 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 محیط‌های 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 محیط‌های نرم افزاری بانک (همراه بانک، اینترنت بانک و ...) می‌شود.

- به کمک بهینه‌سازی‌های انجام شده و استفاده از سرورها و ^۴CDN 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 ریکپچا

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

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

منابع:

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

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

[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 Recognition," 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 Methods", International Conference on Computer Communication and Electrical Technology ICCET 2011, 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>