کشف تخلف ایجاد تراکنش های صوری در خودپرداز
Self-Payment Fraud Detection on Automated Teller Machine

محمدحسین برخورداری پژوهشکده فناوری اطلاعات و ارتباطات
Mohammadhossein Barkhordari
Barkhordari@ictrc.ac.ir ،
پرستو بخشمندی
Parastoo Bakhshmandi
parastoo.bakhshmandi@gmail.com

.چکیده (فارسی)

در طول دهه گذشته حجم تراکنش‌های انجام شده روی ماشین‌های خودپرداز بصورت چشمگیری افزایش یافته است. با این حال، این سرویس بستر بسیار مناسبی برای فعالیت‌های متخلفانه می باشد. گزارش‌های وسیعی در خصوص استفاده نابجا از کارت‌های خودپرداز ارائه شده است، در حالیکه متدهای زیادی جهت جلوگیری و کشف تخلفات ارائه شده است.

در برخی کشورها بانک‌ها، ماشین‌های خودپرداز را تحت شرایط خاص و از پیش تعیین شده به مشتریان می فروشند و در این حالت درصدی از مبلغ تراکنش به عنوان کارمزد به آنها تعلق می گیرد تا در دسترس بودن سرویس را افزایش دهند. با این وجود برخی از دارندگان خودپردازها تراکنش‌های تخلفی را ایجاد می کنند تا بتوانند کارمزد بیشتری دریافت کنند. این مقاله سعی در کشف چنین تخلفاتی را با یک متد دو مرحله ای دارد. در مرحله اول مشتریان متخلف با قوانینی خاص شناخته می شوند. در مرحله بعدی، با ایجاد حلقه تراکنش و استفاده از الگوریتم کشف چرخه سایر مشتریانی که به کمک مشتری خاطی آمده اند نیز شناسایی می‌شوند. برای ارزیابی متد پیشنهادی، تراکنش‌های یک بانک مورد استفاده قرار گرفته است. نتایج بطور قابل ملاحظه ای حاکی از آن است که عمده تراکنش های جعلی شناخته شده اند.

واژگان کلیدی

کشف تخلف، کشف چرخه، کشف تخلفات خودپرداز ، انبار داده

طبقه بندی JEL .

چکیده (انگلیسی)

Over the past decade the amount of transactions and reported frauds on Automated Teller Machines (ATM) has significantly increased. Various types of frauds have been reported around misusing ATM cards and many methods have been deployed to detect and prevent them. In some countries, banks sell ATMs to investors under predefined circumstances and pay them in commission in order to increase the availability of the service but some ATM owners have been found to create fake transactions to obtain extra commissions. This paper attempts to detect such frauds using a two-stage method. In the first stage fraudulent

customers are detected by certain rules and in the second stage their accomplices are identified using transaction loop and cycle detection algorithm. Transactions of a bank have been used to evaluate the proposed method and all detected fraudsters by system were confirmed by bank fraud detection office.

Keywords:
Fraud Detection, Cycle Detection, ATM Fraud Detection, Data warehouse

طبقه بندیJEL.

مقدمه

امروزه بکارگیری کارت‌های اعتباری و خودپرداز برای امور مختلف مانند خرید کالاها و خدمات، یکی از متدهای پیشرو در اقتصاد دیجیتالی می باشد [1]. این کارت‌ها به افراد کمک می کنند تا بدون حمل پول نقد با خود و مواجه با ریسک های آن به خرید بپردازند. همچنین کارت‌های خودپرداز به خریداران کمک می کند تا وجه کالا یا سرویس را با کمترین جزئیات پرداخت کنند. در نتیجه به سبب این امتیازات ، بیشتر مشتریان از این کارت‌ها بجای پول نقد استفاده می کنند. استفاده از خودپرداز ها برای پرداخت قبض‌ها، حواله پول، خرید شارژ تلفن همراه، مشاهده لیست تراکنش‌ها و بسیاری خدمات دیگر سبب می شود تا مشتریان ترجیح دهند در هر زمان از روز یا شب بدون نیاز به مراجعه به شعب بانک و هدر دادن زمان، کارهای خود را انجام دهند. همچنین سرویس‌های خودپرداز ، دارای مزایایی مانند حفظ مشتری و نقدینگی بیشتر برای بانک‌ها می باشد. بانک‌ها می توانند از پرسنل خود برای سایر فعالیت‌ها استفاده کرده و یا تعداد این افراد در بسیاری از شعب کاهش داده و در نتی‌جه هزینه های خود را کاهش دهند.

برای اینکه رضایتمندی وجذب نقدینگی از مشتریان افزایش یابد ، بانک‌ها سعی در بهبود سرویسهای خود در شهرها دارند. در این راستا، بانک‌ها ماشین‌های خودپرداز خود را به سرمایه گذارانی با شرایط خاص می فروشند. چنانچه یک سرمایه گذار بتواند شرایط زیرساخت ارتباطی و امنیتی را برای مکان خودپرداز ایجاد کند، بانک مجوز خرید خودپرداز را به وی می‌دهد. مدل کسب و کار بین بانک و سرمایه گذاران، به بانک‌ها این اختیار را می دهد تا درصدی از تراکنش‌های روزانه خودپرداز را بعنوان کارمزد دارندگان خودپرداز اختصاص دهند.

در مقابل بسیاری از مزایا و سرویس‌هایی که کارت‌های خودپرداز برای مشتریان ایجاد می کند، زیر ساخت بسیار مناسبی برای وقوع تخلفات فراهم می آورد. سهم بزرگ کارت‌های خودپرداز درانجام تراکنش‌ها، منجر به بسیاری از متدهای تخلف می شود [2].این مسئله باعث می شود صادر کنندگان کارت و ذینفعان آن اقداماتی را در جهت کشف و مواجه با انواع تخلفات انجام دهند.

متدهای متعددی که جهت کشف تخلف ارائه شده اند ، در تصوی‌ر ۱ نشان داده شده اند. طبق دسته بندی اندرسون، ۸ دسته تخلف را می توان درنظر گرفت [3]. در این طبقه بندی تخلفات مربوط به خودپرداز ، بعنوان یک زیر شاخه از طبقه " استفاده از تکنولوژی، خودپرداز و ای‌نترنت " شناخته شده که می تواند به دسته های زیر تقسیم شود:

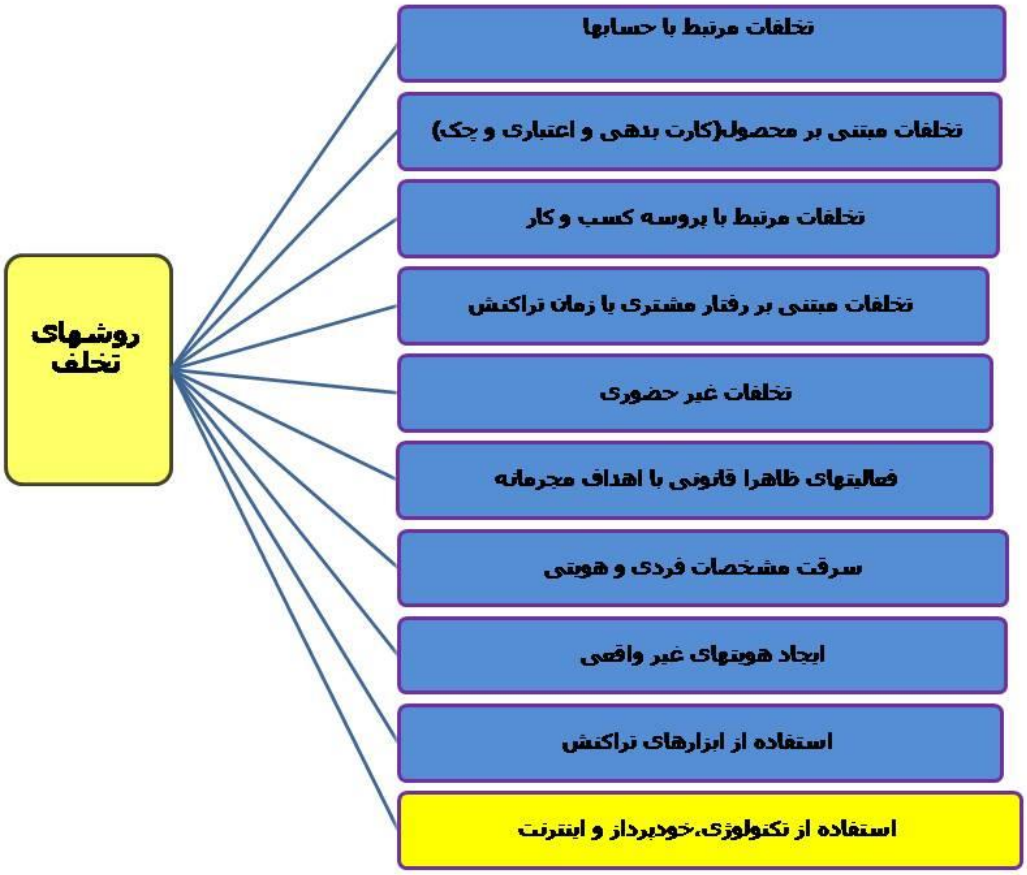
حملات فیزیکی: در این حملات، مهاجم سعی بر جابجایی یا تخریب فیزیکی دستگاه خودپرداز دارد.

نصب اشیاء غیرقانونی روی دستگاه خودپرداز : در این روش مهاجمین سعی در نصب اشیاء غیر قانونی به دستگاه خودپرداز داشته که هدف بدست آوردن اطلاعات کارت و گذر واژه می باشد.

دزدی گذرواژه: در این دسته بندی گذرواژه کارت توسط فرد مجرم به روش‌های گوناگون مانند نگاه به کاربران دستگاه خودپرداز از پشتشان دزدیده می شود.

تراکنش‌های مالی ایجاد شده بواسطه کاربر یا متد نامناسب: این دسته بندی بر تراکنش‌های مالی تمرکز داشته است که توسط کاربر یا متدهای غیر مجاز صورت می گیرد؛ مانند یادداشت‌های جعلی و استفاده از کارت‌های سرقتی.

ایجاد تراکنش های جعلی: برخلاف تمامی انواع تخلفات ذکر شده که مرتبط به شخص سوم می باشند،این نوع تخلف توسط صاحبان خودپرداز صورت می گیرد که از آنها تحت نام ایجاد تراکنش های جعلی می‌توان نام برد. این نوع از تخلف برای کسب کارمزد بیشتر صورت می گیرد. بر اساس مدل کسب و کار بانک، هرچه مبلغ تراکنش خودپرداز بیشتر باشد، کارمزد بیشتری به صاحب آن پرداخت می شود. این مسئله علت اصلی ایجاد تراکنش‌های جعلی توسط برخی از صاحبان خودپرداز می باشد. تصویر شماره ۱ روشهای تخلف را نمایش می‌دهد.



تصویر ۱-روشهای تخلف

در این مقاله، متدی جدید برای کشف تخلفات خود پرداز در خودپردازها ارائه شده است. در این سیستم در گام نخست، متخلفین توسط بکارگیری قوانینی که از خبرگان کسب شده شناسایی می شوند. شبکه تراکنشی این مشتریان ساخته شده و سپس با استخراج حلقه هایی در این شبکه ها، کاربران دیگری که در انجام تخلفات نقش داشته‌اند، شناسایی می شوند. با بکارگیری این متد بر روی تراکنش‌های یک بانک ، بسیاری از متخلفین شناسایی شده اند.

ادامه این مقاله به این ترتیب است که در بخش بعدی تعاریف و مطالعات مرتبط با حوزه کاری بصورت خلاصه مرور شده است. سپس در بخش سوم، متد پیشنهادی با اشاره به جزئیات ارائه شده است. نتایج حاصل از بکارگیری این متد بر روی داده عملی تراکنش‌های یک بانک در بخش چهارم ارائه و مورد بحث قرار گرفته است. در نهایت نتیجه گیری و برخی اشارات در خصوص کارهای آتی، در بخش پنجم ارائه شده است.

ادبیات موضوع

در این قسمت مطالعات مرتبط با کشف تخلفات خودپرداز به صورت مختصر بررسی شده اند

کشف تخلف خودپرداز

در این قسمت متدهای کشف تخلف خودپرداز مورد بررسی قرار گرفته است. تحقیقات وسیعی صورت گرفته تا از وقوع چنین جرایمی جلوگیری شود که می توان آنها را به ۵ دسته تقسیم کرد:

دسته اول حملات فیزیکی است. برای کشف چنین حملاتی، سنسورهای حرکتی برای کشف حرکات منجر به تخریب یا جابجایی خودپرداز ها بکار می روند.

همچنین در [13] سه راه برای غلبه بر حملات فیزیکی خودپرداز ها اشاره شده است: سطح مناسبی از امنیت برای مکان خودپرداز ها، استفاده از هشدار دهنده ها و سنسورها برای کشف حملات فیزیکی و در نهایت استفاده از تکنولوژی لکه جوهر[1]که باعث می شود هر پول جا بجا شده غیر قابل استفاده یا خراب می شود.

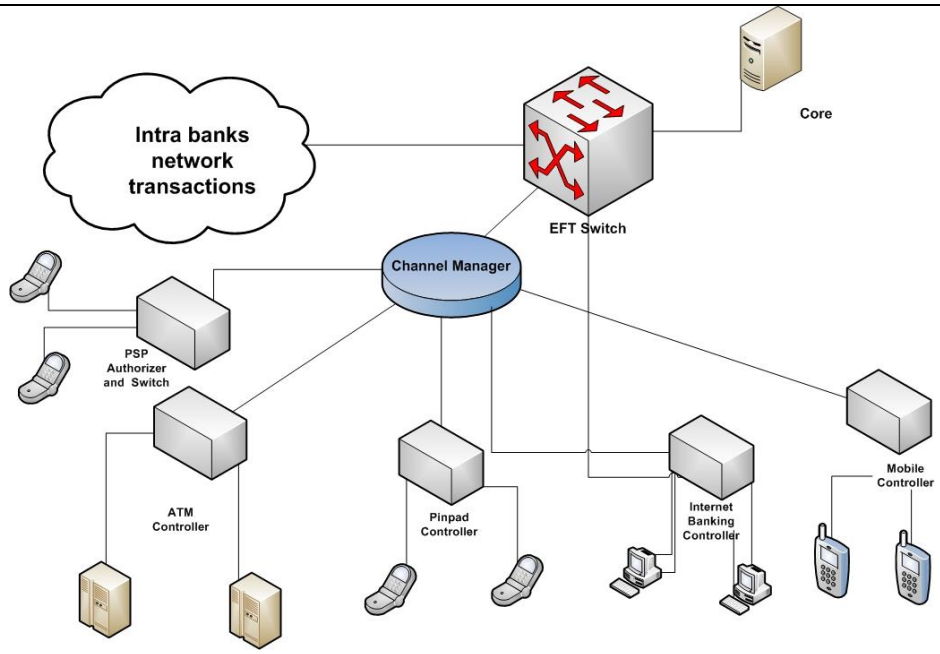
در دسته بعدی، متدهایی برای کشف اشیایی که بصورت غیر مجاز به خودپرداز نصب شده اند مثل دوربین ها و تولید کنندگان مجدد کارت ارائه شده اند [6]. همچنین در [12] یک سیستم برای کشف اشیاء غیر مجاز متصل به خودپرداز مانند دوربین هایی که قادر به ثبت کلمه گذر کاربران هستند ارائه شده است.

در دسته سوم متدهایی ذکر شده اند که از سرقت کلمه گذر جلوگیری می کنند. در [7] متدهای گوناگونی برای ورود کلمه گذر اشاره شده تا از سرقت آن توسط افرادی که از پشت سر نگاه می کنند جوگیری بعمل آید. در [12] سیستمی پیاده سازی شده است که در صورت افرادی در پشت سر و در حل پرسه زدن، به کاربر هشدار می دهد. در پایان آخرین دسته بندی مربوط به متدهایی است که به کشف تراکنشهای مالی می پردازند که توسط کاربران یا متدهای نا مناسب اجرا شده اند. برای مثال تعیین مشخصات دارندگان کارت بواسطه شاخص های بیومتریک [6,8,9]، تشخیص یادداشتهای جعلی [2]در محیط خودپرداز [6,7] و ضبط تصاویر چهره کاربران خودپرداز [5,10,11] در این دسته قرار داده شده اند.

سوییچ EFT[3]

در تصویر ۲ ، معماری بانکداری الکترونیک در محیط مورد بررسی نشان داده شده است:

[1] Ink stain
[2] forged note
[3] Electronic fund transfer



تصویر ۲- معماری سوییچ EFT

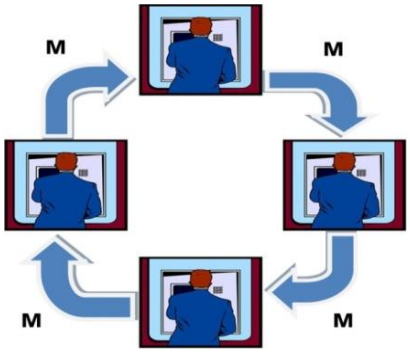
استاندارد استفاده شده برای تراکنش مالی ISO8583 است. این استاندارد ۳ ورژن داشته که در سالهای ۱۹۸۷،۱۹۹۳ و ۲۰۰۳ ارائه شده است. پیام‌ها در این استاندارد دارای ۱۲۸ فیلد می باشند که این فیلدهای حاوی اطلاعات تراکنش می باشند. برخی از این فیلدها عبارتند از مبلغ، تاریخ، زمان، کد دستگاه، کد عملیات، کد فرآیند و .. . در نتیجه تمام وسایل در شبکه بانکی باید با استاندارد ISO8583 همخوانی داشته و پیام را با این فرمت ارسال و دریافت نمایند. برای اطلاعات بیشتر می توان به [14,15,16] مراجعه کرد.

همانطور که در تصویر ۴ نشان داده شده است هر تراکنش بواسطه یک کانال پرداخت انجام شده و به نرم افزار کنترل کننده اش ارسال می شود. پس از بررسی پیام از لحاظ امنیتی و محتوایی ، پیام به سیستم مدیریت کانال پرداخت ارسال می گردد . علاوه بر کانال‌های کنترل پرداخت، این سیستم نیزمحتوا و امنیت پیام ارسال شده را کنترل می کند. پس از بررسی پیام ها توسط سیستم مدیریت کانال پرداخت، این پیام ها به EFT سوییچ مرکزی بانک ارسال می شود. در EFT سوییچ مرکزی بانک، چنانچه کارت توسط سایر بانک‌ها صادر شده باشد، پیام به شبکه الکترونیکی مدیریت پیام بین بانکی ارسال می شود. در غیر اینصورت، پیام به سامانه مرکزی بانک ارسال می شود. با روشی مشابه پاسخ پیام به مشتری ارسال می شود. معماری و گردش کار ارایه شده بسته به قوانین حاکمیتی یا قوانین بانک مرکزی می تواند متفاوت باشد.

ایجاد تراکنش های جعلی

همانطور که پیش از این اشاره شد، برخی از بانکها اقدام به فروش دستگاه های خودپرداز خود به برخی سرمایه گذاران در غالب یک سری شرایط مشخص می کنند. این بانک‌ها درصدی از تراکنش انجام شده توسط خودپرداز را به صاحب آن بعنوان کارمزد پرداخت می کنند. متاسفانه، برخی دارندگان خودپرداز تراکنش‌های جعلی انجام داده، تا سود خود را افزایش دهند که این مسئله تحت عنوان تخلف ایجاد تراکنش های جعلی شناخته شده است. در اینجا برای روشن شدن بهتر مسئله، مثالی ذکر شده است. برای مثال تصور کنید ۴ فرد دارای کارت بانکی یکسانی هستند. فرد اول مبلغ M برای فرد دوم حواله می کند و این فرد نیز همان مبلغ را برای فرد سوم حواله می کند. مجدداً در اقدامی مشابه فرد سوم همان مبلغ را برای فرد نخست

حواله می کند. بدین روش ۴ تراکنش با حجم 4*M بر روی خودپرداز صورت گرفته و صاحب خودپرداز دارای کارمزدی برای این تراکنشهای جعلی می شود. تصویر ۳ این فرآیند را نشان می دهد. این چرخه جعلی می تواند به کرات با مسیرهای کوتاه‌تر تکرار شود. در نتیجه این تراکنش‌های جعلی هزینه زیادی برای بانک داشته و آن را از مدل کسب و کار و هدف اصلی اش منحرف می سازد. در این مقاله تمرکز بر کشف انواع تخلفات می باشد.



تصویر ۳- حلقه انتقال

روش تحقیق

در این قسمت، متد پیشنهادی برای کشف تخلف ایجاد تراکنش های جعلی معرفی شده است. ابتدا اطلاعات تراکنش‌های خودپرداز ها به کنترل کننده خودپرداز سپس به سوییچ مرکزی بانک ارسال شده است.اطلاعات بصورت دوره ای از پایگاه‌داده سوییچ بانک استخراج شده و فرآیند ETL بر روی آن اعمال می شود. پس از این مرحله انباره‌داده ایجاد می شود.با حجم بالای تراکنش‌های بانکی، استفاده از انباره داده سرعت کشف تخلفات را بصورت چشمگیری ارتقاء می دهد.

فاز ۱

در این قسمت تمام داده EFT سوییچ مرکزی که برای فرآیندهای بعدی مورد نیازند، استخراج می شوند.

- تمامی تراکنش‌ها با کد دستگاه خودپرداز باید انتخاب شوند.
- از بین تمام تراکنش‌های مرحله قبلی، تمامی مواردی که دارای کد عملیات انتقال محلی هستند باید انتخاب شوند (همانطور که پیش از این اشاره شد، تراکنش‌های جعلی توسط انتقال محلی صورت می گیرند.)
- تمامی تراکنش‌های موفق انتخاب می شوند (تراکنشهایی با کد پاسخ ۰۰)
- در این مرحله ما دارای تراکنش‌هایی با فرمت ISO8583 هستیم لذا شماره دستگاه خودپرداز ، شماره کارت، حجم تراکنش، تاریخ و زمان انتخاب می شوند.
- موارد انتخاب شده در گام پیشین در جدولی با قالب جدول ۱ قرار داده می شوند.

ATM No	Card No	Deposit	Withdrawal	Date Time

جدول ۱ –قالب داده های ورودی

اگر پول به کارت واریز شود مقدار فیلد Deposit برابر با مبلغ مورد انتقال شده و در فیلد Withdrawal عدد صفر وارد می شود و در صورتیکه از کارت پولی انتقال یابد مقدار فیلدWithdrawal برابر با مبلغ مورد انتقال شده و در فیلد Deposit عدد صفر وارد می شود.

در این قسمت انبار و مکعب داده در جدول ۱ ساخته شده اند. ATM No، Card No وDate and Time بعنوان ابعاد درنظر گرفته شده اند. مبالغ Depositو Withdrawal به عنوان اندازه (measures) شناخته می شوند. تابع Sum بعنوان عملیات انبار داده انتخاب شده است. همچنین شاخصی (KPI) تحت عنوان نسبت حجم تراکنش (Θ) تعریف شده است. فرمول آن مطابق زیر تعریف شده است:

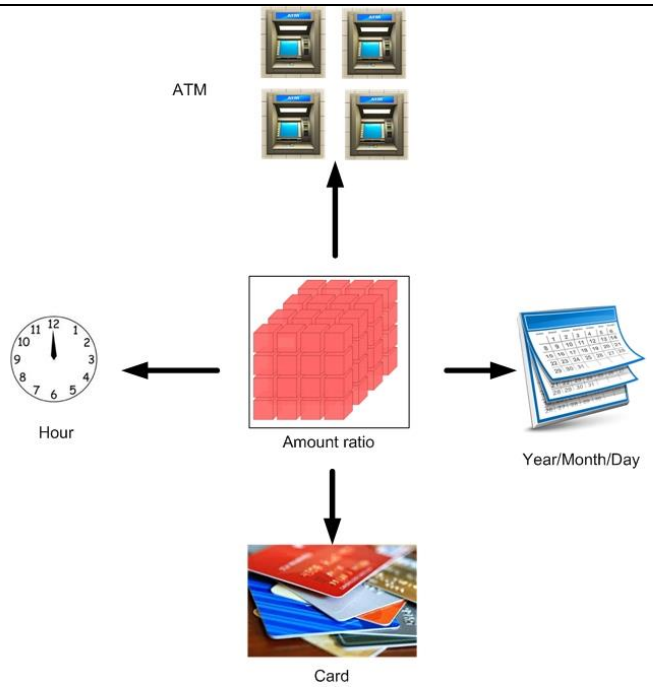
$$\Theta(\text{Card No}) = \frac{\text{Deposit}}{\text{Withdrawal}}$$

در این فرمول Deposit مبلغی را نشان می دهد که به کارت انتقال داده شده و Withdrawalمبلغی است که از کارت حواله شده است. نسبت حجم تراکنش $\Theta(\text{Card No})$ نشان دهنده نسبت Deposit به Withdrawal برای یک کارت است. جدول ۲ اطلاعاتی در خصوص ابعاد و اندازه‌ها نشان می دهد.

اندازه‌ها	Amount ratio
ابعاد	No, Card No , Time (Year, Month, Day, Hour) ATM

جدول ۲ - ابعاد و اندازه‌ها

شمای عمومی انبار داده در تصویر ۴ نشان داده شده است. همانطور که نشان داده شده است، بعد زمان بصورت سال، ماه، روز و ساعت در نظر گرفته شده است. این بعد برای کشف تخلف در محدوده های مختلف زمانی بکار می رود.



تصویر ۴: طراحی انباره داده

در این مقاله قوانین زیر برای کشف تخلف بکار می روند.

۱- کارتهایی با $\Theta=1$ ، Θ بین ۰،۹ و ۱،۱ یا Θ بین ۰،۸ و ۱،۲ احتمال بیشتری دارد که تراکنش جعلی تولید کند. هر چه ابعاد ریزتر شوند، احتمال ایجاد تراکنش جعلی افزایش می یابد. برای مثال، چنانچه یک مشتری در یک روز دارای حجم برداشت و واریز یکسان باشد، با احتمال زیاد این شخص در تخلف ایجاد تراکنش های جعلی مشارکت دارد.

۲- از آنجاییکه این احتمال وجود دارد که تخلف روی دو دستگاه خودپرداز یا بیشتر رخ دهد، بعد خودپرداز حذف شده و بررسی در خصوص نسبت حجم تراکنش مجدداً انجام می‌گیرد. هر ی از تراکنشی که به حدآستانه KPI رسیده باشد، بعنوان تراکنشی که احتمال دارد جعلی باشد، شناخته می شود. در این نوع از تخلفات مشتریان چندین دستگاه خودپرداز با یکدیگر مشارکت دارند تا تراکنش‌های جعلی بر روی خودپرداز ها صورت بگیرد.

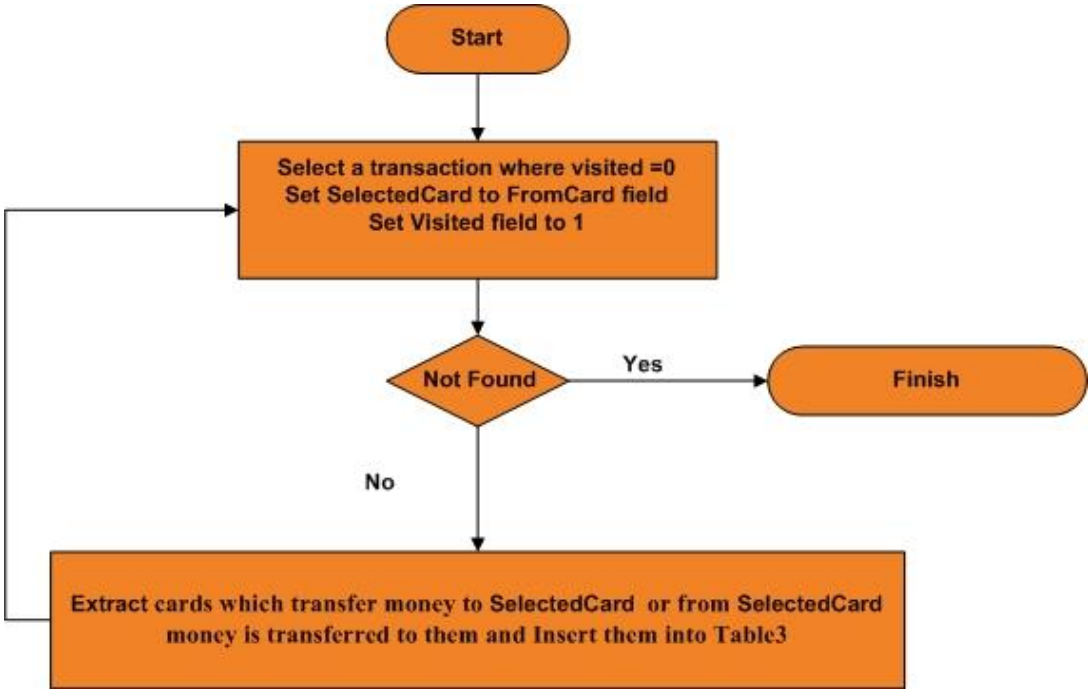
فاز دو

پس از استخراج عناصر داده از پایگاه‌داده‌های سوییچ مرکزی، یک شبکه محدود با تراکنش‌های مشتری ساخته می شود. در قسمت قبلی برخی از مشتریان که با احتمال زیاد، تراکنش‌های جعلی ساخته‌اند شناخته شده‌اند. اما نکته‌ای که در خصوص این نوع از تخلف مطرح است، این است که مشتریان، برای انجام چنین تخلفاتی احتیاج به سایر مشتریان دارند. همچنین برای یافتن سایر مشتریان که با یکدیگر برای ایجاد تراکنش‌های جعلی مشارکت دارند، تحلیل بیشتری مورد نیاز است. همانطور که پیش از این ذکر شد، برای افزایش حجم مبلغ تراکنش‌های خودپرداز برخی مشتریان وجهی را برای یکدیگر چندین بار ارسال می کنند. با تحلیل بیشتر، یک حلقه بین این مشتریان ایجاد می شود . جدول نتایج مشابه با جدول ۳ می باشد:

ATM No	FromCard	ToCard	Amount	DateTime	Visited

جدول ۳: فیلدهای ورودی

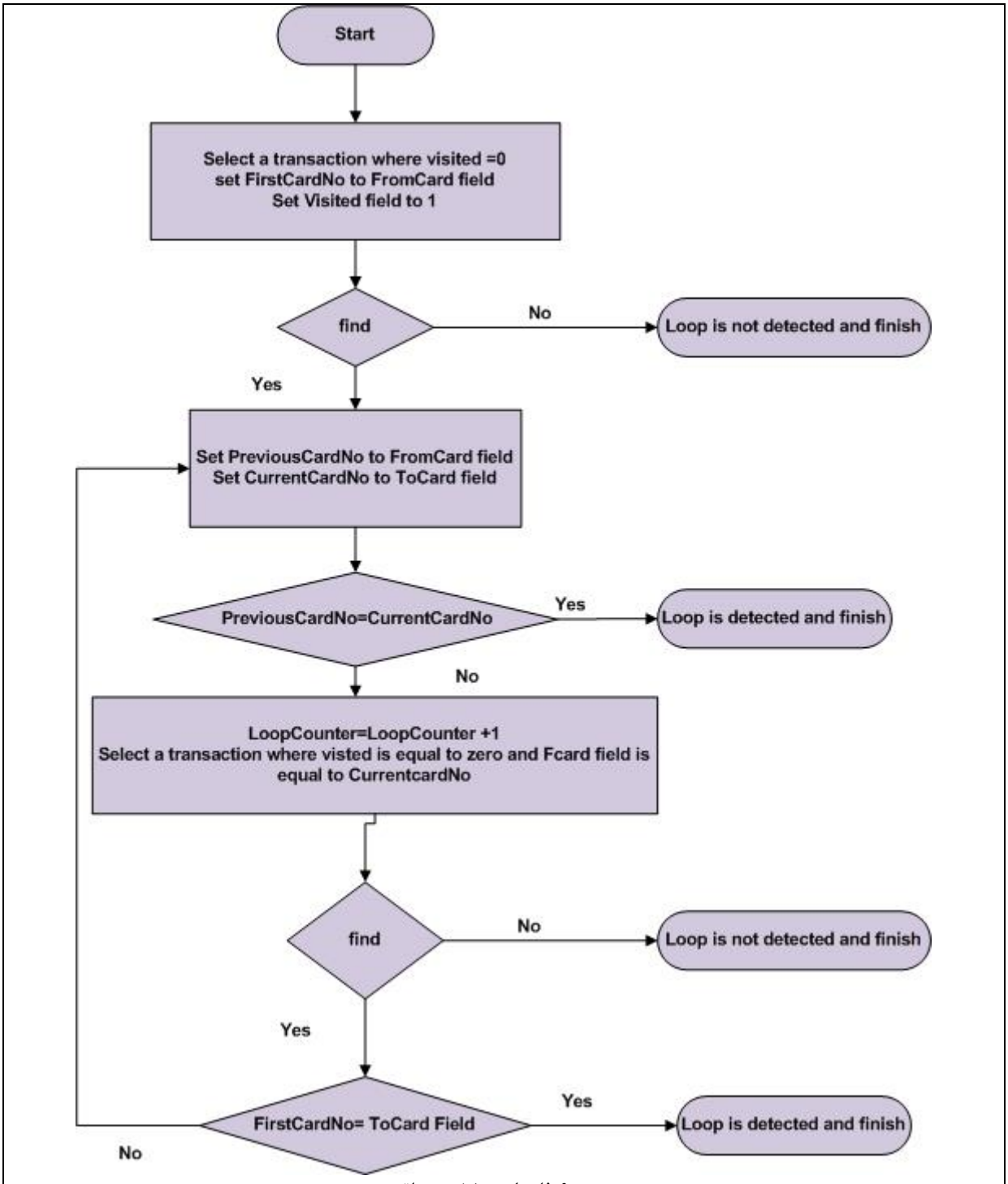
الگوریتم تصویر ۵ برای استخراج کارت های مرتبط استفاده می شود.
در ابتدا تمامی کارت‌هایی که ارتباطی با کارت مشکوک دارند، شناسایی می شوند. این کارت ها اقدام به ارسال وجه به کارتهای مشکوک کرده اند یا از کارت‌های مشکوک به آنها مبلغی ارسال شده است. تمامی تراکنش‌های مرتبط با این کارت ها استخراج می شوند.



تصویر ۵: فلوچارت استخراج کارتهای مرتبط

- Θ برای کارت های استخراج شده محاسبه می شود (همانطور که در فاز ۱ نشان داده شده است)
- تراکنش‌هایی که دارای Θ خارج از محدوده هستند از مجموعه تراکنش‌ها حذف می شوند.
- فیلد Visited برای تمامی تراکنش‌ها مقدار صفر می گیرد.

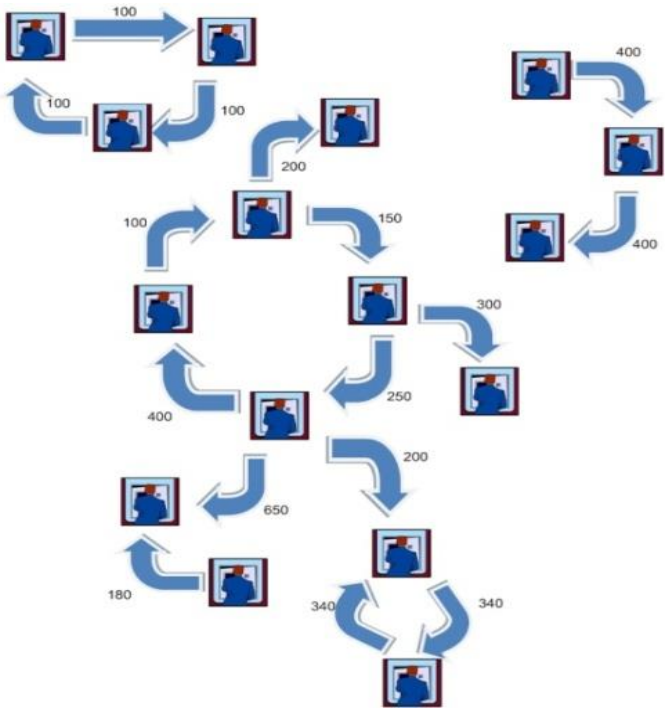
الگوریتم تصویر ۶ برای کشف حلقه بکار می روند.



تصویر ۶: فلوچارت تشخیص حلقه

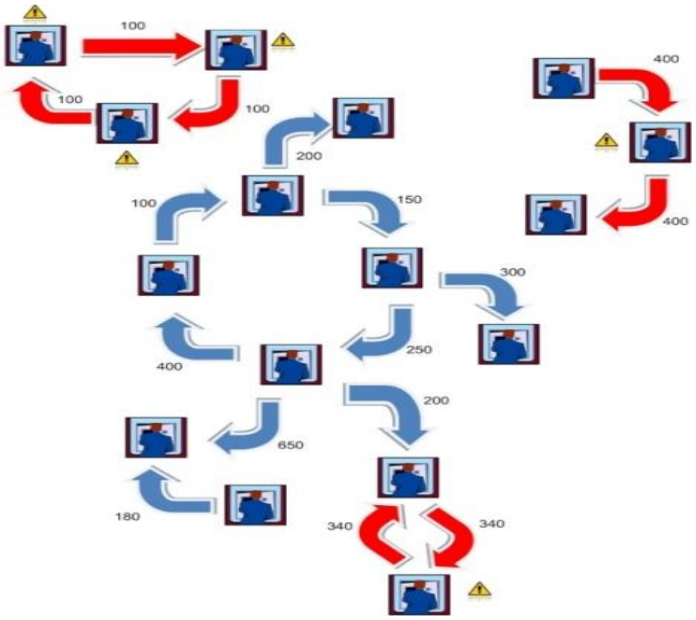
برای بهتر مشخص شدن موضوع، مثالی در شکلهای ۸،۹ و ۱۰ نشان داده شده است. فرض کنید شبکه‌ای برای تراکنش‌ها وجود داشته باشد. تصویر ۷ این شبکه را نشان می دهد که مبلغ هر تراکنش روی هر یال نشان داده شده است.

فاز اول از متد ارائه شده روی هر نود (کارت) اجرا شده و تمامی نودهایی که دارای ورودی و خروجی یکسان هستند استخراج می شوند ($\Theta = 1$). این نودها نودهای مشکوک هستند.



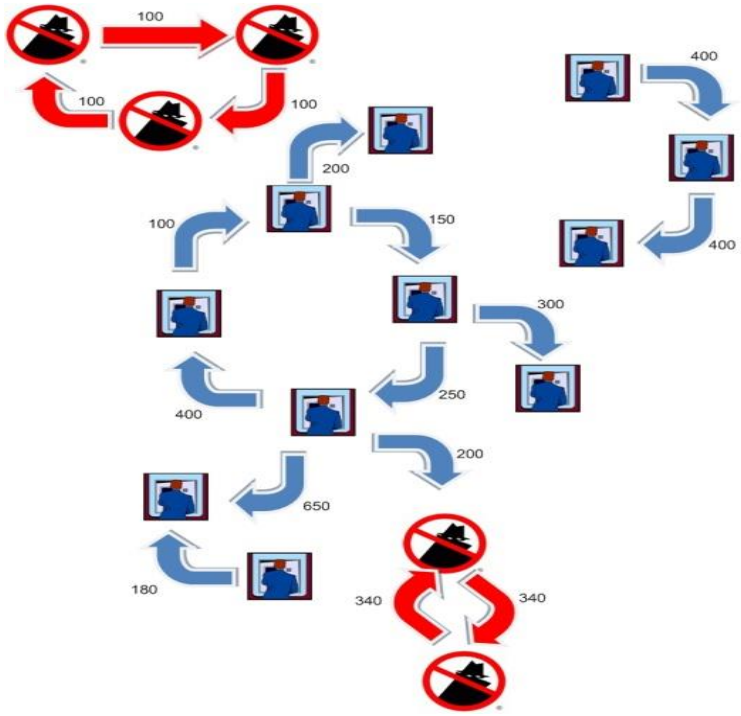
تصویر ۷: شبکه تراکنش ها

تصویر ۸ این فاز را نشان می دهد. در این شکل، ۵ دارنده کارت بعنوان عناصر مشکوک شناخته شده اند. اما همانطور که در تصویر ۹ می بینید تمامی آنها متخلف نیستند.



تصویر ۸: تشخیص نودهای مشکوک

پس از کشف نودهای مشکوک، فاز ۲ الگوریتم بر روی این نودها اجرا می شود. حلقه های کشف شده در تصویر ۱۰ نشان داده شده اند. همانطور که مشاهده می کنید برخی نودهای مشکوک از فاز پیشین بعنوان رفتار معمولی شناخته شده اند. ۲ حلقه مشکوک در اینجا شناخته شده اند. علاوه بر ایجاد حلقه، تمامی دارندگان کارت که در حلقه مشارکت دارند می بایست بازه از قبل تعیین شده ای از نسبت حجم تراکنش را داشته باشند. در تصویر ۹ بازه نسبت حجم تراکنش، مساوی یک قرار داده شده است. مشتریان کشف شده می توانند به اداره مبارزه با تخلفات بانک برای تحقیقات بیشتر معرفی شوند.



تصویر ۹:تشخیص حلقه

یافته‌ها و نتایج

جهت ارزیابی متد پیشنهادی، آن را بر روی تراکنش‌های یک بانک اعمال کردیم. برای این منظور ۹۲۷۰۲ تراکنش مورد بررسی قرار گرفت. تصویر ۴ نتایج فاز اول متد پیشنهادی را بر اساس ابعاد مختلفی نظیر شماره کارت، شماره دستگاه خودپرداز و زمان نشان می دهد. همانطور که در جدول ۴ شرح داده شده است، استفاده از فواصل مختلف برای بعد زمان می تواند بر تعداد تراکنش‌های مشکوک تاثیر بگذارد. در جدول ۴ بازه های متفاوتی برای Θ استفاده شده است. بر مبنای این بازه ها و تغییر در ابعاد، شماره کارت های مختلف و تراکنش های متفاوتی استخراج می شوند. زمانیکه بازه Θ و بعد زمان بزرگتر می شوند، شماره کارت ها و تراکنشهای بیتشری قابل استخراج هستند. اما چنانچه رنج Θ و بعد زمان کوچکتر شود احتمال تخلف بیشتر می شود. از آنجا که متد پیشنهادی از تکنیک‌های پایگاه داده و انبار داده استفاده می کند، بازده خوبی برای حجم زیادی از داده مانند داده های استخراج شده از تراکنش‌های بانکی دارد.

ابعاد			نسبت حجم تراکنش					
			Θ=1		0.9<Θ<1.1		0.8<Θ<1.2	
			کارتهای تشخیص داده شده	تراکنش های تشخیص داده شده	کارتهای تشخیص داده شده	تراکنش های تشخیص داده شده	کارتهای تشخیص داده شده	تراکنش های تشخیص داده شده
کارت	بازه پویا	سال	665	3819	848	7021	1039	11283
		ماه	758	2366	923	4291	1073	6287
		روز	804	2157	897	3059	947	3781
		ساعت	756	1836	897	2281	837	2672
	سال		607	1167	851	3486	1152	6494
	ماه		788	1578	1009	3451	1217	5047
	روز		844	2080	953	3057	1011	3746

	ساعت	770	1830	953	2291	865	2879

جدول ۴ – نتایج اولیه

جدول ۵ نتایج حاصل از فاز دوم متد پیشنهادی را نشان می دهد. همانطور که در این جدول نشان داده شده است کارت های مشکوک تشخیص داده شده اند و کارتهای مرتبط به کارت های مشکوک نیز همانطور که پیش از این شرح داده شد استخراج شده اند. سپس فیلتر بازه Θ بر آنها اعمال شده است. در نهایت فاز کشف حلقه بر روی کارتها اعمال شده است. جدول ۵ کارتهای مکشوفه، تراکنش‌ها و حلقه های تشخیص داده شده، طول میانگین حلقه و تراکنش‌ها را که بیش از 1000000 ریال هستند را نشان داده است.

ابعاد			نسبت حجم تراکنش													
			Θ=1					Θ=1					Θ=1			
			کارتهای تشخیص داده شده	تراکنش های تشخیص داده شده	حلقه های تشخیص داده شده	میانگین طول حلقه ها	مبالغ تراکنش بیشتر از10000000	کارتهای تشخیص داده شده	تراکنش های تشخیص داده شده	حلقه های تشخیص داده شده	میانگین طول حلقه ها	مبالغ تراکنش بیشتر از10000000	کارتهای تشخیص داده شده	تراکنش های تشخیص داده شده	حلقه های تشخیص داده شده	میانگین طول حلقه ها	مبالغ تراکنش بیشتر از10000000
ت کار	بازه خوشه	سال	638	823	107	2.06	83	740	1130	179	2.03	125	840	1346	222	2.03	173
		ماه	708	937	166	2.02	93	783	1166	205	2.02	127	876	1321	256	2.01	156
		روز	660	951	151	2.03	123	693	1042	181	2.03	138	723	1101	213	2.02	150
		ساعت	659	887	108	2	146	660	984	155	2.08	181	675	1054	183	2.09	182

سال	591	763	102	2.06	67	736	1205	219	2.12	171	902	1547	295	2.07	218	
۶	743	949	171	2.02	92	763	1382	242	2.02	172	853	1535	291	2.01	191	
روز	710	1014	167	2.08	155	746	1127	216	2.07	175	782	1214	260	2.06	194	
ساعت	673	904	110	2	145	683	1010	160	2.09	184	705	1094	194	2.09	185	

جدول ۵ – نتایج نهایی سیستم

کارتهای مکشوفه بطور قطع در تخلف ایجاد تراکنش های جعلی شرکت داشته اند. این کارتها، خودپرداز های مرتبط، تاریخ و زمان وقوع به قسمت کشف جرایم بانکی ارجاع داده می شود. آنها تراکنش‌ها و حلقه ها را مورد بررسی قرار می دهند و فیلترهایی را بر این تراکنشها اعمال می کنند. برای مثال، چنانچه مبلغ تراکنش در حلقه از 10000 ریال کمتر باشد، به احتمال زیاد این تراکنش مرتبط با عملیات تست سیستم بوده و تخلف محسوب نمیشود.همچنین چنانچه شمارنده حلقه برای یک کارت خاص بزرگتر از یک باشد، این کارت در تخلف ایجاد تراکنش های جعلی دخیل بوده است. با این دو قانون نتایج نهایی کسب شده در جدول ۶ نشان داده شده است. بر طبق مبلغ تراکنش‌های مشکوک برخی صاحبان خودپرداز باید جریمه ای را به بانک پرداخت کنند و برخی دیگر از ادامه فعالیت‌هایشان ممانعت خواهد شد.

9312	تراکنش های تشخیص داده شده بوسیله سیستم	نسبت حجم تراکنش
8928	تراکنش های تایید شده بوسیله اداره مبارزه با تخلفات بانک	

جدول ۶ – نتایج تایید شده بوسیله اداره مبارزه با تخلفات بانک

جمع بندی

در این مقاله گونه ای از تخلف بر روی خودپرداز هایی که به متقاضیان با شرایط از پیش تعریف شده ای تحویل داده می شد ، مورد بررسی قرار گرفت. بر اساس نوع تخلف، تمامی تراکنش‌ها باید مورد بررسی قرار گیرند و حلقه های تخلف باید استخراج شوند. در این مقاله به ۲ نوآوری اشاره شده است. بر اساس یافته های ما، پیش از این هیچ متدی برای کشف تخلفات صاحبان خودپرداز نبوده است. مورد بعدی اینکه سایر متدهای کشف حلقه از تکنیک‌های پایگاه داده و انباره داده برای کشف حلقه استفاده نکرده اند در نتیجه متد پیشنهادی بازده بیشتری داشته و می تواند برای داده های حجی‌م‌تر استفاده شود. متد پیشنهادی در فاز اول تراکنشهای مشکوک را استخراج کرده و در فاز دوم تراکنش‌های مرتبط را تشخیص داده و مجدداً تراکنش های مشکوک و استخراج شده را مورد بررسی قرار می دهد. در پایان نیز لیستی از حلقه های تخلف را ارائه می دهد. تخلفات ایجاد تراکنش های جعلی قطعاً در این حلقه ها قرار دارند.

جهت کارهای آتی ، متد پیشنهادی را می توان برای تحلیل ارتباطات [۴] در خصوص جلوگیری از پول شویی اعمال کرد. همچنین برای کشف تخلف روی کانال‌های دیگر پرداخت و صاحبان آنها مانند POS ها نیز می توان از متد پیشنهادی استفاده کرد.

منابع

[1] Weiner, S. E. (1999). Electronic payments in the US economy: an overview. Economic Review-Federal Reserve Bank of Kansas City, 84(4), 53-64.
[2] Chang-Tien, K. Y. L., & Sirirat, S. (2004). Survey of Fraud Detection Techniques in Networking, Sensing and Control. In *IEEE International Conference* (Vol. 2, pp. 749-754).
[3] Anderson, R. (2007). The credit scoring toolkit: Theory and practice for retail credit risk management and decision automation. Oxford University Press..
[4] Suhr, J. K., Eum, S., Jung, H. G., Li, G., Kim, G., & Kim, J. (2012). Recognizability assessment of facial images for automated teller machine applications. *Pattern Recognition*, *45*(5), 1899-1914.
[5] Tang, Y., He, Z., Chen, Y., & Wu, J. (2009, March). ATM intelligent surveillance based on omni-directional vision. In *Computer Science and Information Engineering, 2009 WRI World Congress on* (Vol. 4, pp. 660-664). IEEE.
[6] Sako, H., Watanbe, T., Nagayoshi, H., & Kagehiro, T. (2007, September). Self-defense-technologies for automated teller machines. In *Machine Vision and Image Processing Conference, 2007. IMVIP 2007. International* (pp. 177-184). IEEE.
[7] Kim, C. S., & Lee, M. K. (2010, January). Secure and user friendly pin entry method. In *2010 Digest of Technical Papers International Conference on Consumer Electronics (ICCE)*.
[8] Sako, H., & Miyatake, T. (2004, August). Image-recognition technologies towards advanced automated teller machines. In *Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on* (Vol. 3, pp. 282-285). IEEE.
[9] Negin, M., Chmielewski, T. A., Salganicoff, M., von Seelen, U. M., Venetainer, P. L., & Zhang, G. G. (2000). An iris biometric system for public and personal use. Computer, 33(2), 70-75.
[10] Duan, L. Y., Yu, X. D., Tian, Q., & Sun, Q. (2003, August). Face pose analysis from MPEG compressed video for surveillance applications. In Information Technology: Research and Education, 2003. Proceedings. ITRE2003. International Conference on (pp. 549-553). IEEE.
[11] Kim, G., Suhr, J. K., Jung, H. G., & Kim, J. (2010, December). Face occlusion detection by using b-spline active contour and skin color information. In Control Automation Robotics & Vision (ICARCV), 2010 11th International Conference on (pp. 627-632). IEEE.
[12] Sako, H. (2010, January). Technologies for developing an advanced intelligent ATM with self-defence capabilities. In IS&T/SPIE Electronic Imaging (pp. 75340E-75340E). International Society for Optics and Photonics.
[13] Mohammed, L. A. (2011). On The Design of Secure ATM System
[14]http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm? csnumber=31628
[15]http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm? csnumber=23632
[16]http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm? csnumber=35363

[۴] Link analysis