مدل ترکیبی آنلاین برای پیشگیری و کشف جعل آنلاین

چکیده :

روند فعلی کسب و کار آنلاین را قادر می سازد خدمات بهتر و سریع تری برای کاربران فراهم کند و باعث سود بیشتر برای بازرگانان می گردد. در طرف دیگر، اینترنت محبوب ترین پلت فرم برای کلاهبرداران جهت ارتکاب جعل آنلاین و با سهولت تبدیل شده است . چند راه حل برای غلبه بر این جعل آنلاین ارائه شده است. اما، راه کامل و کارآمد این مشکل هنوز هم در حال پژوهش است. در این مقاله، ما مدل ترکیبی آنلاین (اهم) که به طور گسترده مانع از احتمال جعل آنلاین می شود، و امکان تشخیص و رفع آن را دارد پیشنهاد کرده ایم. روش اهم به طور انحصاری برای حراج، عدم تحویل / کالا و سرقت هویت ارائه شده است. اهم بیشتر در روش های دیگر جعل آنلاین قابل اجرا است. ما عملکرد این مدل را ارزیابی کرده و نشان داده ایم که اهم یک رویکرد آنلاین پیشگیری و کشف جعل قوی و بسیار موثر است.

کلمات کلیدی : جعل مزایده، جعل کارت اعتباری، جعل هویت. HMM

1. مقدمه

کسب و کار آنلاین روش کسب و کار مدرن است که با استفاده از بازاریابی مستقیم، فروش، و خدمات عمل می کند. رشد اینترنت دارای معنی خاصی در رشد تجارت الکترونیک است[1]. با توجه به گزارش های وزارت بازرگانی، و تحقیقات فورستر، خرده فروشی اینترنتی، در شرکت کامسور[2]، فروش آنلاین به سرعت در چند سال گذشته افزایش یافته است و نشان می دهد که چرا تجارت الکترونیک محبوب شده است.

افزایش رشد کسب و کار آنلاین و مصرف بیشتر از اینترنت (نشان داده شده در جدول 1 و 2) [2] ، و فعالیت های غیر قانونی به طور همزمان افزایش یافته است. رفتار جعل اینترنتی به طور کلی برای ردیابی و تعقیب آسان نیست. کلاهبرداران به راحتی می توانند اطلاعات خود را از قربانیان بدون تحمیل هزینه های قابل توجه مخفی کنند. یکی از دلایل اصلی برای جعل اینترنتی ناآگاهی کاربر در مورد مکانیسم حمله کلاه بردار از طریق رسانه اینترنت است. از آنجا که فقدان قانون و به تبع آن درایو در بسیاری از کشورها مانند کشورهای آسیایی وجود دارد، بسیاری از آسیایی ها

توسط کلاهبرداران قربانی می شوند [3]. مزایده جعلی ، عدم تحویل / کالا، جعل فرصت ، سرقت هویت، جعل در کارت اعتباری، جعل آنلاین طرح های سرمایه گذاری، اضافه پرداخت، انتقال پول: با توجه مرکز جرم ، جعل اینترنتی را می توان به شرح زیر [4] طبقه بندی کرد ، جعل اسپم / جعل چرخش، جعل خیریه، خودرو، و جعل کارت. در میان این جعل ها، سه جعل شایع تر هستند که عبارتند از: حراج جعلی آنلاین ، جعل عدم تحویل کالا و جعل هویت. جعل حراج آنلاین یکی از شایع ترین انواع کلاهبرداری اینترنتی (بخش 2) است. این فرآیند به شرح زیر است: اول، کاربران آیتم های مختلف وب سایت های خرید و فروش آنلاین را بازدید می کنند . سپس، خریداران علاقه مند می توانند برای آیتم حراج شده پیشنهاد ارائه بدهند. پس از برنده شدن، خریدار برای مورد حراج شده پرداخت انجام می دهد. جعل رخ می دهد و قربانی آیتم خریداری شده را دریافت نمی کند یا یک آیتم با ارزش کمتر از [5] آگهی دریافت می کند. دوم عدم تحویل / پرداخت کالا، که آن هم در بسیاری از مناطق جعل توسط بازاریابی اینترنت و وب سایت های خرده فروشی، که ارائه دهنده انواع محصولات و خدمات هستند ایجاد شده. قربانی ، که توسط یک سایت قانونی، به دنبال بازاریابی موثر است گمراه شده. سپس قربانیان با دادن اطلاعات کارت اعتباری خود و یا ارسال پرداخت توسط برخی از وسایل دیگر برای کالاها و خدمات ارائه شده توسط سایت های جعلی مورد کلاه برداری قرار می گیرند و هرگز کالاها به آن ها نمی رسد، و یا اگر برسد، ارزش محصول کمتر از قیمت واقعی [4] است. سوم سرقت هویت است. هنگامی که یک شخص تبدیل شدن به شخص دیگری را وانمود می کند و با استفاده از اطلاعاتی مانند جزئیات کارت اعتباری شخص برای ارتکاب جعل اقدام می کند [4].

در این مقاله، ما یک مدل برای جلوگیری و تشخیص آنلاین در جعل و عدم تحویل / پرداخت کالا به دلیل احتمال بالای جعل اینترنتی پیشنهاد کرده ایم . مدل ما مدل ترکیبی آنلاین (اهم) است که دو مرحله می باشد. یکی مانع جعل برای کاربران و سرورهای وب است. در مرحله دوم، اگر جعل در سیستم رخ دهد، جعل را تشخیص داده و به قربانی اطلاع می دهد. اهم قادر به جلوگیری و تشخیص جعل مانند حراج جعلی، بازاریابی اینترنتی و فروش جعلی ، جعل کارت و جعل هویت است.

این مقاله پنج بخش است. بخش 1 معرفی طبقه بندی جعل اینترنتی و توصیف دسته بندی آن: جعل حراج آنلاین ، عدم تحویل / جعل کالا، و جعل هویت. بخش 2 مرور برای جلوگیری از این جعل را نشان می دهد و فرمول مشکل در مورد این جعل است. در بخش 3 رویکرد اهم برای پیشگیری و تشخیص توصیف جعل و پیشنهاد الگوریتم پیشگیری اهم است. پس از آن، در بخش 4 رویکرد عملکرد اهم برای نشان دادن مزایای استفاده از مدل ما مورد بررسی قرار گرفت. بخش 5 نتیجه گیری و کارهای آینده با مراجع است.

Year	US online sales
2012 (Quarter 1)	$50,270,000,000
2011	$255,600,000,000
2010	$172,900,000,000
2009	$155,200,000,000
Year	Global online sales
2011	$763,200,000,000
2010	$680,600,000,000

جدول 1 - اطلاعات فروش آنلاین

Top consumer reasons for shopping online	Percentage of survey citing reason
Time saving	73
More variety	67
Easy to compare prices	59
No crowd	58
Lower prices	55
Spend less on gas	40
Less taxes	30
Other	3

جدول 2 - دلایل مصرف کننده بالا

2. کار مرتبط و فرمولاسیون مسئله

در حال حاضر ما در بخش مورد بحث انواع مختلفی از جعل اینترنتی را داریم. 1. در این بخش، ما به طور خلاصه حل و فصل جعل آنلاین و تدوین و فرموله کردن مشکل به دلیل جعل در بالا را دسته بندی کرده ایم.

1.2. کار مرتبط

در زمینه در حراج جعل [3] پیشگیری و تشخیص، وانگ و همکاران طراحی مکانیزم یک برنامه هزینه شیل-بازدارنده (SDFS) [6]. اما، این مکانیسم به دلیل مناقصه تبانی، مناقصه های متعدد و غیره بعدها، وانگ و همکاران قادر به کاهش جعل حراج نیست. ثابت کرد که هیچ تقارن بدون مناقصه shill و با تجزیه و تحلیل مناقصه shill و در چند دور حراج آنلاین انگلیسی وجود دارد [7]. در جعل در حراج، پیشگیری اتفاق می افتد به بهترین استراتژی، اما گاهی اوقات، این استراتژی نمی تواند کار کند بنابراین ما باید به اتخاذ طرح های تشخیص جعل حراج. برای جلوگیری از کاربران صادقانه از تبدیل شدن به قربانی، پورتر و سوهام یک استراتژی برای مقابله با سایه تلاش و مناقصه کاذب [8] ارائه شده است. آنها تخمین زده اند برنده احتمال برای شناسایی احتمال جعل.

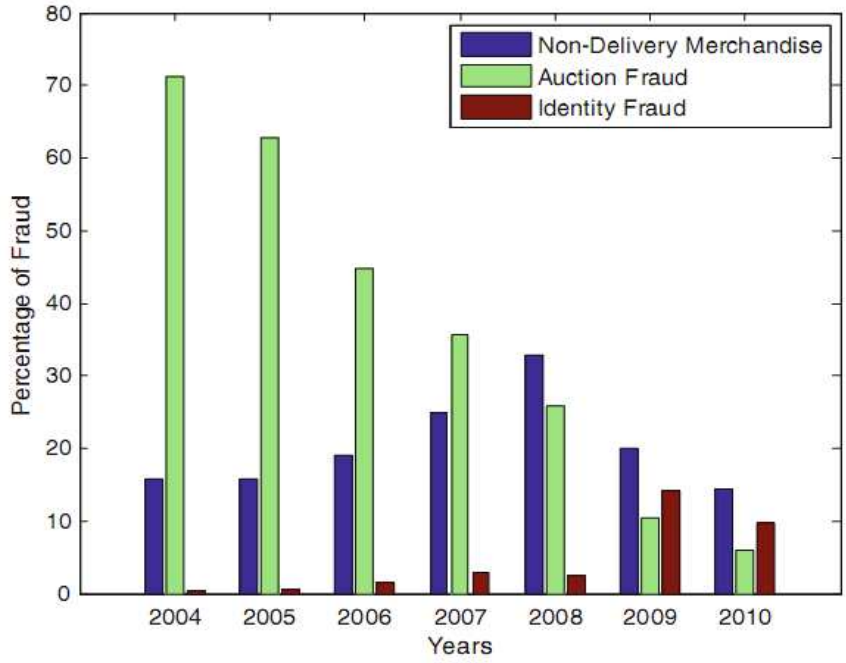
بعدها، برای تشخیص مناقصه تبانی، Trevathan و همکاران پیشنهاد یک الگوریتم [9]. " نمره تبانی " برای تشخیص افتادن تبانی توسط یک فروشنده کنترل می شود. تجزیه و تحلیل می گیرد با توجه به سه استراتژی: (1) متناوب استراتژی مناقصه، (2) متناوب استراتژی حراج، و (3) استراتژی ترکیبی. در زمینه سرقت هویت، یک مدل ترکیبی است نیتین راکش و همکاران ارائه شده است. در کاهش مشکل در سیستم پرداخت آنلاین با استفاده از مدل ترکیبی [10]. این مدل ترکیبی از دو مدل: مدل احراز هویت تلفن همراه و مدل HMM پیشنهاد شده توسط آبهیناو استاوا و همکاران [11]؛ با توجه به این، مدل پنهان مارکوف می توان مورد استفاده برای شناسایی کلاهبرداری های آنلاین با بررسی الگوی رفتار کاربران.

2.2. فرمولاسیون مسئله

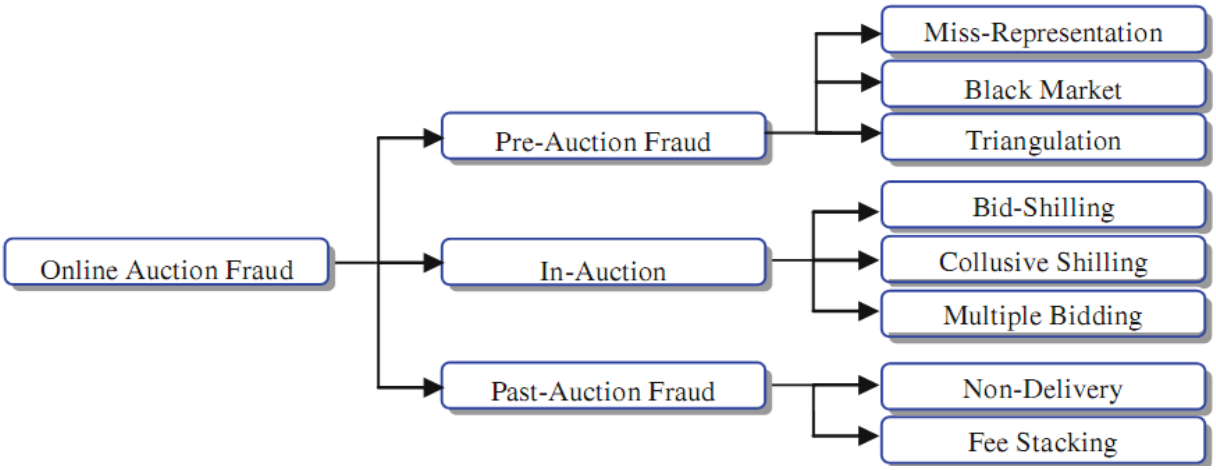
بر اساس گزارش سالانه IC^3 از سال 2004-2010 [12]، روشن شده است که جعل آنلاین ، عدم تحویل / کالا، و سرقت هویت انواع روش های مکرر جعل هستند. گزارش 7 سال ما و مطالعه یک آمار برای این سه جعل که از سال 2004-2010 ایجاد شده (شکل 1). نشان می دهد که حراج آنلاین و عدم تحویل / کالا در همه 7 سال بسیار مکرر انجام شده است ، اما پس از سال 2008، روش جعل دیگر به عنوان مثال، سرقت هویت نمایان شده است.

حراج جعلی: این یکی از شایع ترین جعل ها در اینترنت است. بر اساس این گزارش جرم و جنایت در سال 2011 توسط IC^3 [12]، در کل به دلیل حراج جعلی بیش از 8،288،098.73 دلار در 4،066 شکایت انجام شده است.

شکل 2 نشان می دهد که حراج جعلی آنلاین را می توان به سه بخش طبقه بندی کرد: اول جعل پیش حراج است. این قبل از فرایند مناقصه شروع می شود و برای کالای مورد حراج رخ می دهد. علاوه بر این، سه نوع جعل که جعل از سمت نمایندگی، جعل در بازار سیاه ، و جعل مثلث را شامل می شود. دوم حراج جعلی است؛ این مورد در طول فرایند مناقصه اتفاق می افتد ، و غیر قابل پیش بینی است. علاوه بر این، این سه نوع جعل که شیلینگ، شیلینگ تبانی و مناقصه های متعدد هستند. بخش سوم حراج جعلی آنلاین جعل پس از حراج است. این مورد پس از تکمیل فرایند حراج فرایند. علاوه بر این، متشکل از دو نوع جعل است. یکی عدم تحویل است، و دوم هزینه انباشته است. در این مقاله، تمرکز ما بر روی جلوگیری و تشخیص جعل در حراج می باشد.



شکل. 1 آمار جعل آنلاین



شکل. 2 طبقه بندی حراج جعلی آنلاین [3]

1. پیشنهاد شیلینگ: در این حالت، فروشنده مناقصه بالاتری برای آیتم خود قرار می دهد. به طور کلی، شیلینگ توسط فروشندگان انجام و یا برخی از انجمن فروشندگان (دوست یا عضو خانواده) انجام شده است. به عنوان یک نتیجه، پیشنهاد شیل و درایوها تا قیمت مورد نظر فروشنده افزایش می یابد و باعث می شود سود بالا توسط گمراه کننده به فروشنده برسد چرا که خریداران واقعی نیز با پیشنهاد بالاتر در تلاش برای خرید آیتم مورد نظر هستند. [6]

2. تبانی شیلینگ: این زمانی رخ می دهد گروه های متعدد شیلینگ در فرایند مزایده [3] شروع می شود. این رفتار برای تشخیص پیچیده تر است.

3. مناقصه های چندگانه: زمانی اتفاق می افتد که یک خریدار در مکان مناقصه های متعدد (برخی از بالا و برخی از کم) در مورد مشابه با استفاده از نام مستعار متفاوت شرکت کند. مناقصه متعدد با همان خریدار باعث می شود قیمت به شدت افزایش یابد، که خریداران بالقوه دیگر مناقصه را می ترساند. سپس، پس از گذشت چند دقیقه از حراج، همان خریدار از مناقصه خارج شده، و تنها پیشنهاد بسیار پایین تر برای آن آیتم ارائه می دهد [3].

عدم تحویل/پرداخت محصولات: در این نوع جعل، وضعیت کاربر و چیزی که او خریداری کرده و یا دریافت کرده، پس از آن موردی که او خریداری کرده است را دریافت نمی کنند. بر اساس گزارش جرم و جنایت 2011 اینترنت توسط IC3 از کل سال شکایت برای پرداخت غیر تحویل/ کالا، جعل بیش از 22404 مورد بوده است.

کلاهبرداری سرقت هویت: با توجه به IC[3]، سرقت هویت می تواند به عنوان استفاده غیر مجاز از اطلاعات یک شخص مانند هویت شخصی، جزئیات کارت اعتباری، و غیره برای ارتکاب جعل و یا دیگر جرایم تعریف شود. برای ارتکاب این نوع جعل، مجعل دزد هویت فرد دیگری است و نقش آن شخص را بازی می کند ، این کار برای کسب اطلاعات افزایش اعتبار و مزایای دیگر از طرف آن شخص است. در این حالت، قربانی از بسیاری از عوارض جانبی رنج می برد زیرا مجعل می تواند شماره شناسایی یا کارت اعتباری شماره خود را / او را با ارتکاب جعل و یا جنایات از طرف قربانی استفاده کند.

3. مدل ترکیبی موجود

به منظور جلوگیری و تشخیص حراج آنلاین ، عدم تحویل / کالا و سرقت هویت جعلی، این بخش رویکرد اهم را نشان می دهد. نگاهی اجمالی از رویکرد اهم در شکل 3 نشان داده شده است. شکل 3 نشان می دهد که آن شامل سه ماژول است به عنوان مثال، کاربران، سرور اهم، و وب سایت. کار این ماژول در زیر تعریف شده است.

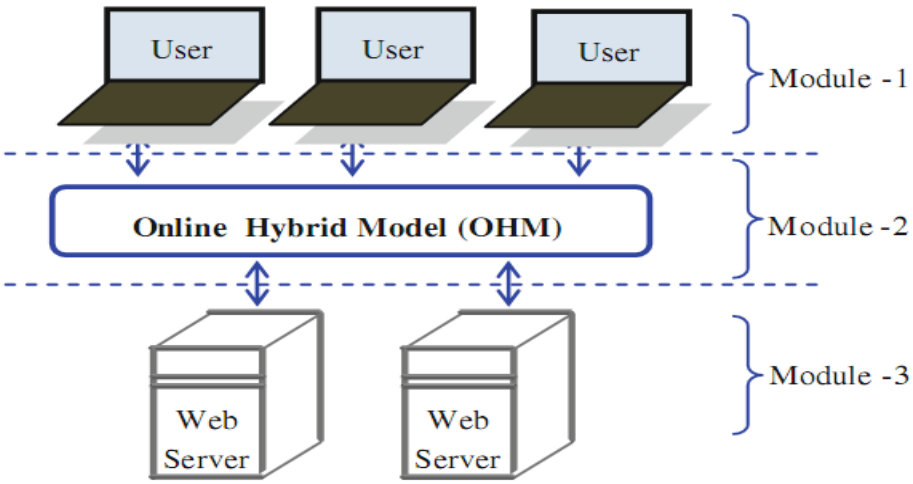
1. کاربران : آن ها می توانند دو نوع خریدار یا فروشنده باشند. هر کاربر، زمانی که می خواهد با تجارت الکترونیکی وب در هر گونه فرایند حراج و یا خرید کالا شرکت کند ، لازم است که آن ها اهم را بررسی کنند.

2. اهم : این رویکرد اعتبار کاربر و وب سرور است و همچنین به طور منظم بر روند تعامل بین کاربر و وب سرور نظارت دارد. پس از احراز هویت، مسائل مربوط به گواهی اهم (OC) که گواهی وب سرور و کاربران است و به کاهش جعل آنلاین کمک می کند. این مورد برای کاربران و سرورهای وب الزامی است.

3. وب سرور: این ماژول پلت فرم و مدیریت روش برای حراج و خدمات خرده فروشی مانند خرید و فروش کالا را فراهم می کند. صحت یک وب سرور نیز توسط اهم با صدور یک OC به وب سرور مشخص می شود. هر یک از سایت های تجارت الکترونیک که برخورد با مسائل پولی دارند باید یک گواهی امضا دیجیتالی از مقامات دریافت کنند. این برای یک وب سرور و برای نمایش OC در وب سایت الزامی است.

1.3. روش اهم

در رویکرد اهم طبقه بندی در دو بخش است: اول اهم برای پیشگیری است و دوم اهم برای تشخیص است. ما هر دو آن ها را یک به یک مورد بحث قرار داده ایم.



شکل 3 . روش اهم

1. اهم برای پیشگیری: این رویکرد تأیید و احراز هویت مراحل برای جلوگیری از کلاهبرداری های آنلاین را فراهم می کند. این طرح پیشگیری جعل شامل سه بخش به شرح زیر:

a تأیید هویت کاربر: برای تأیید هویت کاربر، اهم ویژگی های زیر را در مراقبت و همراه با فرم ثبت نام بیان می کند.

1. آدرس کاربر و عکس: آدرس کاربران که در حال حاضر ساکن آن محل است. عکس فعلی کاربر برای شناسایی.

2. اطلاعات تلفن همراه: با در نظر گرفتن اطلاعات تلفن همراه، OHM تایید آدرس کاربران با ردیابی محل تلفن همراه و سپس انطباق آن با آدرس ارائه شده توسط کاربر را انجام می دهد. تفاوت بین دو آدرس باید پایین تر از حد معیینی باشد. در غیر این صورت، ثبت نام کاربر رد خواهد شد. اهم نیز تایید می کند که تلفن همراه باید یک دوره زمانی مشخص فعال باشد.

3. شناسایی (ID) اثبات: شناسه منحصر به فرد برای یک کاربر است. آن می توانید از میان ID پاسپورت / منحصر به فرد کشور / ID شماره مجوز رانندگی ، و غیره انتخاب شده باشد ، اهم نیاز به این شناسه جهت تصدیق آدرس دائمی برای کاربران دارد.

4. اعتبار / اطلاعات کارت: اهم نیاز به هر یک از اطلاعات مربوط به کارت به جز رمز عبور دارد(که توسط کاربر برای انجام معامله نهایی استفاده می شود). اهم این جزئیات و آخرین اظهارات معامله بانک با مکان خود را نیز تایید می کند. اگر اگر آخرین بار کارت 1 ماه قبل استفاده شده باشد، تفاوت بین محل سکونت معامله و مکان فعلی باید کمتر از فاصله آستانه باشد. هنگامی که مکان فعلی بیش از حد آستانه باشد، کارت را رد کرده. و با جزئیات کارت اعتباری، دوباره آدرس و شماره تلفن کاربران را تایید می کند.

5. رفتار کاربر: اهم الگوی رفتار کاربران با اتخاذ مدل پنهان مارکوف می شود ، و در صورتی که علامت نباشد، ثبت نام کاربران را لغو می کند.

6. صدور گواهی نامه: پس از تأیید صحت کامل کاربر، اهم مسائل گواهی اهم (OC) را به کاربران و یک نسخه به وب سایت می فرستد.

b. وب سرور احراز هویت: اعتبار وب سرور اهم با در نظر گرفتن مراحل زیر است:

1. گواهی تایید امضای دیجیتال اهم که اطمینان می دهد که این یک وب سرور ثبت شده است.

2. تایید معاملات گذشته از وب سرور اهم و بازخورد کاربران مختلف از آن سرور. بر اساس این دو، OHM تولید یک رتبه بندی برای آن سرور انجام می دهد.

3. سپس، OHM تولید OC برای آن سرور انجام می دهد که شامل رتبه بندی از وب سرور است.

2. اهم برای تشخیص: این طرح تشخیص جعل که به طور انحصاری برای حراج جعلی است طراحی شده ، در طول فرایند مزایده تنها است است. چرا که پس از خروج کاربران و وب سرور، ممکن است شانس جعل مثل پیشنهاد شیلینگ ، شیلینگ تبانی و مناقصه های متعدد وجود داشته باشد [3].

اهم به طور منظم فرآیند حراج با اتخاذ SDFS ، باعث کاهش سود اضافی به دست آمده توسط مناقصه شیل و فروشنده می شود [6]. در مکانیزم SDFS، اتهام هزینه به ورود و خروج هزینه به فروشنده. فروشنده مجموعه تنها یک پیشنهاد شروع یا یک قیمت رزرو می تواند ارائه دهد. هزینه ورود قیمت رزرو اولیه است ، در حالی که هزینه خروج هزینه کمیسیون محاسبه شده است و بر تفاوت میان قیمت برنده مناقصه و قیمت رزرو است. اگر قیمت رزرو بیش از حد بالا باشد، هزینه آن از هزینه ورود بالاتر است. اگر قیمت رزرو بسیار پایین باشد، تفاوت بین قیمت رزرو و قیمت فروش بالا خواهد بود، و هزینه آن از هزینه کمیسیون بالاتر است. بنابراین، SDFS مرزهای تعیین قیمت صادقانه فروشندگان را تعیین می کند. نرخ کمیسیون سرور ، در پلت فرم حراج متفاوت است. در کل، SDFS مهار کننده رفتار شیلینگ است. که ارائه دهنده هزینه شیل و-بازدارنده است. و نظارت بر رفتار مناقصه (1) پیشنهاد افزایش می یابند: زمانی که پیشنهاد برای یک آیتم را به طور ناگهانی افزایش می دهد (2) پیشنهاد استراتژی متناوب: وقتی که دو مناقصه معادل آن در همان حراج بیش از زمان آستانه پیشنهاد شوند (3) استراتژی متناوب حراج، که در آن مناقصه معادل مناقصه در مزایده های مختلف است [9].

2.3. الگوریتم برای احراز هویت کاربر

این الگوریتم زمانی که اعتبار کاربر برای دسترسی به خدمات ارائه شده توسط وب سرور باشد ارائه می شود. برای این کار، نیاز به ورودی، و سپس اعتبار بخشی کاربر با صدور OC است.

Initial Condition:User for registration
Local variable:location_threshold, time_threshold,
mobile_location, mobile_use_time, address[ID], photo[ID]
Final Condition:Authentication or Rejection of user
User Authenticate {
a.Input: permanent_address, current_address, photo,
mobile_number, user_identification_proof,
card_detail;/* provide by user */

b.Verify: If [{(current_location - mobile_location) B
location_threshold} &&(mobile_use_time C time_threshold)]/*
mobile_location is traced by GPS, location_
threshold, time_threshold decide by OHM, mobile_use_time
obtain by mobile number information */
Then
If (permanent_address == address[ID])/* address[ID] is
the address written on ID proof*/
Then
If (photo == photo[ID])/* photo[ID] is the photo on ID
proof*/
Then Call: card_verification();/* function written just
below this algorithm */
If (card_verfication() == true)
Then If (user_behavior_pattern C behavior_pattern_
threshold)/*behavior_pattern obtain by HMM, behavior_
pattern_threshold decided by OHM */
Then OHM issues OC with username and password and stores in
OHM_DB;
Else
Authentication failed;
c. Exit.}
card_verification(permanent_address, current_address,
mobile_number)/* Function to validate car detail and user's
detail */
{Verify: If [(average_location - current_location) B
card_location_threshold)]/* average_location and card_

location_thresold are the local variables obtain by taking
last 5 card transactions */
Then If [(permanent_address == address[card]) &&
(mobile_number == mobile_number[card])] mobile_number
[card],address[card]/*obtain by the mobile number and
address registered for that card */
Then Return true;
Else
Return false;}

3.3. الگوریتم برای وب سرور احراز هویت

این الگوریتم با توجه به HMM و بازخورد کاربر با تایید امضای دیجیتال از وب سرور احراز هویت ارائه شده است. برای این کار، نیاز به ورودی، و سپس اعتبار بخشی کاربر با صدور OC است.

Initial Condition: Digital signature certificate, HMM
behavior pattern
Local variable: feedback_and_behavior_threshold, OHM_
Rank
Final condition: Authentication or Rejection of web
server
Web Authentication{
a.Input: digital_signature_certificate/* provide by webserver
*/
b.Verify: If (digital_signature_certificate == true)
Then
If (feedback_and_behavior[HMM] C feedback_behavior_
threshold)

/* feedback behavior[HMM] obtain by HMM, feedback behavior
threshold decide by OHM */
Then Issues OC with OHM_Rank and store in OHM_DB;
Else
Authentication failed;
c.Exit}

4. ارزیابی اهم

در این بخش، ما عملکرد اهم برای دو مورد زیر را بررسی می کنیم.

مورد 1. هنگامی که کاربران مجعل است: برای پیشگیری از فعالیت های کلاهبرداری انجام شده توسط کاربر غیر مشروع، OHM آدرس فعلی ، شماره تلفن همراه، آدرس دائم، عکسID ، و جزئیات کارت کاربر را تایید می کند (با توجه به الگوریتم بخش 2.3). هنگامی که یک کاربر جعلی برای دسترسی به سرور وب برای ارتکاب جعل تلاش می کند و هر یک از اطلاعات نادرست را وارد می کند، پس از آن اهم آن را تشخیص می دهد و کاربر را authentication می نماید. در نتیجه، کاربر را OC می کند و کاربر برای دسترسی به وب سرور قادر نخواهد بود.

مورد 2. هنگامی که یک وب سرور جعلی است: اهم توسط وب سرور با ارائه یک رتبه اهم در OC مانع کاربران می شود ، (با توجه به الگوریتم در بخش 3.3). با دیدن OC، کاربر می تواند تصمیم بگیرد که آیا این وب سرور معتبر است یا نه. در جدول 3، ما اثر اهم در جعل های مختلف اینترنت با توضیح علت را نشان داده ایم.

Internet fraud	Effect of OHM	Reasons
Online in-auction fraud • Multiple bidding • Bid shilling • Collusive shilling	Reduces	Due to unique OHM ID, Thru-in auction OHM process
Non-delivery/ merchandise	Reduces	By providing OC to authenticated Web servers
Identity theft	Reduces	By verifying user's details with card detail

جدول 3 - اثرات OHM بر تقلب آنلاین

5. نتیجه گیری و کارهای آینده

در این مقاله، ما روش اهم را برای پیشگیری و تشخیص جعل در اینترنت را پیشنهاد کرده ایم. اجرای رویکرد اهم برای موارد ارزیابی زیر کارآمد است : در حراج جعلی آنلاین ، عدم تحویل / کالا، و سرقت هویت و یا سرقت کارت جعلی. با استفاده از اهم، هر دو کاربر و وب سرور می توانند خود را از قربانی شدن کلاهبرداری های آنلاین نجات دهند. اهم برای تشخیص جعل های مختلف دیگر مانند اسپم / جعل چرخش، جعل در کارت جعلی، و غیره موثر است بنابراین، اهم یک رویکرد آنلاین پیشگیری و کشف جعل قوی و بسیار موثر است. در آینده روش اهم در زمان واقعی و موقعیت های آنلاین جعلی به منظور بررسی پاسخ موثر تر است.