چارچوبی برای ارزیابی و انتخاب سیستمهای بهینه پرداخت الکترونیکی امن و ناشناخته

محمدرضا ثنایی[۱] ، ادریس عباس زاده[۲]

[۱]استاد ومدیرگروه مدیریت فناوری اطلاعات، دانشکده مدیریت و حسابداری،دانشگاه آزاد واحد قزوین

[۲]دانشجوی دکتری مدیریت فناوری اطلاعات، دانشگاه آزاد واحد قزوین

mohamadrezasanaei@gmail.com

نویسنده مسئول: محمدرضا ثنایی (edris_abbaszadeh@yahoo.com)

چکیده: سیستم های پرداخت الکترونیکی دارای اهمیت بالایی درنظام سیستمهای اطلاعات دیجیتالی امروز هستند. امنیت و ناشناختگی یک ترکیب تعیین کننده ای را دراین حیطه ایجاد می کند. اولا پول الکترونیکی در حقیقت یکسری اطلاعات دیجیتالی است که می تواند به هنگام انتقال از طریق شبکه و یا در سیستمهای پردازنده و ذخیره سازی اطلاعات شنود و کپی برداری شود . افزون برآن ، استفاده کنندگان به طور اتوماتیک دنباله ای از تمامی فعالیتهایشان را دردنیای دیجیتالی باقی می گذارند که ناشناسی پرداختها را از بین می برد. در این تحقیق چارچوبی برای ارزیابی سیستمهای مختلف پرداخت الکترونیکی از نظر امنیت و ناشناختگی ارائه شده و جداول تصمیم گیری مورد نیاز به طور دقیق تهیه شده است. معیارهای مختلف مورد نیاز تعریف شده اند. بر اساس چارچوب فوق مقایسه ای بین چندین سیستم موجود صورت گرفته و رتبه بندی آنها از جنبه های مختلف امنیتی انجام شده است .

کلمات کلیدی: پرداختهای مبتنی بر پول الکترونیکی ، ناشناختگی ، امنیت در پرداخت ، سکه های الکترونیکی ، Trusted third party

۱. مقدمه

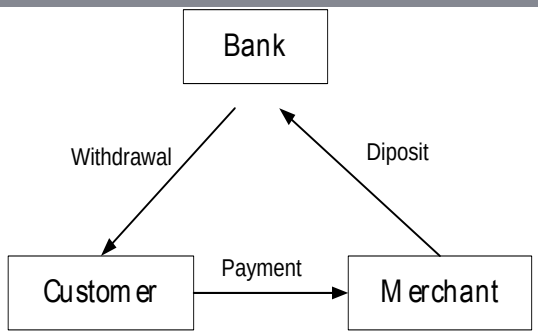
بیشتر فعالیتهای فیزیکی ما به معادل الکترونیکی اش تغییر یافته است . یک فعالیت بسیار مهم تجارت الکترونیکی و پرداختها ، نقش حساس و بحرانی را درآن ایفا می کنند. امنیت همواره مهم بوده است . تلاشهای اساسی صورت گرفته برای اینکه تولید پول تقلبی سخت وهزینه بر باشد. متدهای پرداخت الکترونیکی حتی نیاز به امنیت بیشتری دارند . مثل سکه دیجیتالی که براحتی قابل کپی و تکرار است.

دردنیای الکترونیکی هرفرد به طور اتوماتیک یک سری فعالیتهایش را باقی می گذارد . ضمانت کردن محرمانگی در دنیای دیجیتال بسیار سخت تر از دنیای فیزیکی است . مانند زندگی ما که دردنیای الکترونیکی توسعه یافته است ، تکنیکهای افزودن محرمانگی به طور سریعی سود بخش خواهد بود.

واضح است با پدیدار شدن جامعه الکترونیکی ترکیب جدیدی از امنیت و محرمانگی هم به صورت تکنیکی و هم به صورت غیر تکنیکی ایجاد شده است. تحقیقات تکنیکی درمورد امنیت اطلاعات و محرمانگی نقش بسیار مهمی را درتوسعه یک دنیای الکترونیکی با بهترین سطح امنیت ومحرمانگی را بازمی کند.

مدل پرداخت الکترونیکی

شکل زیر یک مدل عمومی از یک سیستم پرداخت الکترونیکی را ارائه می دهد. نقشهای مختلفی دراین سیستم وجود دارد. تراکنشهای متفاوتی بین این نقشها اجرا می‌شوند.



شکل۱ : مدل عمومی از یک سیستم پرداخت الکترونیکی

سناریوهای E- commerce

دو نوع اجزا درمحیط تجارت الکترونیکی وجود دارد. کسب وکار و مشتری (مصرف کننده) چندین سناریوی تجارت الکترونیکی اصلی می توانـد تعریـف شود. که درترکیبهای مختلف به شرح زیر بیان می شود:

B2C (Business-to-Consumer)
B2B (Business-to-Business)
C2C / P2P (Consumer -to-Consumer)
B2G (Business-to-Government)
M- Commerce (Mobile Commerce)

مشخصات امنیتی درپرداختهای الکترونیکی [۱]

جدول زیر نمونه هایی از مهمترین مشخصات امنیتی مورد نیاز برای هر طرح پرداخت الکترونیک است ، به علاوه سـایر مشخصـه هـایی کـه سـودمندی مشـتری ، فروشنده و موسسات مالی رانشان می دهد.

جدول ۱: مشخصات امنیتی در پرداختهای الکترونیکی

مشخصات	سیاستهای ممکنه
جامعیت دراتباطات Communication Integrity	طرح باید مطمئن باشد که ارتباطات بین مشتری ، فروشنده و موسسه مالی مصون از تغییرات است .
قابلیـــــــت اعتمـــــــاد درارتباطـــــــات Communication Confidentiality	طرح باید مطمئن باشد که ارتباطات بین مشتری ، فروشنده وموسسه مالی مصون از استراق سمع است .
تصدیق مشتری Customer Authentication	مشتری باید تصدیق شود ، براین اساس که تعیین شود که وی مجوز پرداخت را دارد. این بـرای جلـوگیری از استفاده متقلبانه از کارت یا وسایل پرداخت است .
تصدیق عامل Agency Authentication	عامل باید تصدیق شود براین اساس که از سایتهای تقلبی جلوگیری شود که مخصوصـا ایجـاد شـده انـد ، تـا جزئیات پرداخت را برای اهداف متقلبانه ، ضبط و نگهداری کند.
عدم انکار پرداخت Non Repudiation of Payment	سیستم باید مطمئن باشد که مشتری نمی تواند منکر شود که تراکنش مبنی بر استرداد پرداخت ، واقع شده است . این مورد اطمینان به عامل را باعث می شود.
قابلیـــــت اعتمـــــاد بـــــه جزئیـــــات پرداخـــــت Payment Detail Confidentiality	جزئیات پرداخت نباید برای فروشنده ، قابل دسترسی باشد. فروشنده فقـط بایـد ایـن جزئیـات را بدانـد چـه چیزی خریداری شده است . این مورد محرمانگی بر اساس Need – to – Know را حفظ می کند.
قابلیـــــت اعتمـــــاد بـــــه جزئیـــــات خریـــــد Purchase Detail Confidentiality	طبیعت کالا یا سرویس خریداری شده نباید برای بانک یا موسسه مالی در تائید پرداخت در دسترس باشد.

اعتبار سنجی پرداخت Validation of Payment	دستورات پرداخت باید توسط بانک یا موسسه مالی ، محرز شوند تا وجوه پرداخت گردد یا اعتبار افزوده شود.
جلوگیری از استفاده دوباره از مقادیر Prevention of Reuse of Value	وقتی یک طرح از توکن یا سکه دیجیتالی استفاده می کند ، باید از پرداخت توکنهای کپی شده درعوض کالا و سرویس جلوگیری کند. واین عمل به طور عادی به وسیله مراجعه به موسسه ای که سکه ها را تولید می کند جهت اطمینان از مجوز و اطمینان از اینکه که مقادیر قبلا مطالبه نشده است صورت می گیرد.
دسترسی منصفانه(به قاعده) Equity Of Access	اسباب پرداخت باید مطمئن باشد که تمامی مشتری ها قادرخواهند بود حداقل یکبار از متد پرداخت انتخاب شده استفاده کنند.
پردازش سریع Quick Processing	طرح باید پروتکلهای ساده پیغام رسانی رابه کار گمارد که قادر به پردازش سریع توسط تکنولوژی های مورد استفاده توسط فروشنده وموسسه مالی باشند اگر پاسخهای تصدیق پرداخت دریک زمان قابل قبول دریافت نشود ، عاملها با احتیاط به چنین طرحی نزدیک می‌شوند.

ناشناختگی ومحرمانگی برای پرداختهای الکترونیکی

ناشناختگی (Anonymity): وضعیتی است که امکان شناسایی مجموعه ای از موضوعات ، مجموعه چیزهای ناشناخته وجود نداشته باشد . به بیان دیگر ناشناختگی روی پنهان سازی هویت یک شخص تاکید دارد .

تکنیکهای فراهم کننده ناشناختگی

تکنیکهای مختلفی برای رسیدن به حد مطلوبی از ناشناختگی در پرداختهای الکترونیکی وجود دارد که هرکدام با استفاده از روش خاصی آن را فراهم می کنند.

۱. امضا کور (Blind Signature)

Chaum اولین کسی بود که معادل دیجیتالی پول فیزیکی را ارائه داد. سیستم وی بر اساس امضاء کور بود [۳] .

۲. امضا گروهی (Group Signature)

در یک امضا گروهی ، اعضای گروه می توانند از طرف گروه (بنام گروه) امضا کنند. یک طرح امضا گروهی نیاز به مدیر گروه دارد. هرکس می تواند امضا را توسط کلید عمومی گروه تشخیص و اعتبار دهد ولی هیچ کس نمی تواند به جای مدیر گروه تعیین که کدام عضو داده را امضا کرده است .

۳. امضا کور گروهی(Group Blind Signature)

Lysyanskaya یک طرح E-cash برای بانکهای توزیع شده ارائه داد[4] که براساس تکنیک امضا کور می باشد که مفاهیم امضا کور و امضا گروهی را به هم پیوند می دهد

۴. تکنیک Cut-And- Choose

این تکنیک یک روش اصلی درتئوری اعداد صحیح است . ما می توانیم از روش ریاضی برای توصیف این تکنیک استفاده کنیم.

آلیس مجموعه A را به دو بخش A1={j1,…jk}, A2=A-A1 تقسیم می کند.

Bob به صورت تصادفی A1 یا A2 را انتخاب می کند.

آلیس بخش باقی مانده را برمی دارد.

در این تکنیک آلیس می تواند حدس بزند که کدام بخش توسط Bob انتخاب شده است . آلیس ۵۰ درصد شانس داردکه بخش انتخابی Bob را در هر دوره از پروتکل حدس بزند . شانس وی در دو دوره می تواند ۲۵ درصد باشد و شانس وی برای N دفعه می تواند 2-N باشد. بعد از ۱۶ دوره مقدار صحیح برای حدس آلیس ، یک از ۶۵۵۳۶ می باشد. بنابراین آلیس نمی تواند هیچ حدسی بزند که آن Zero- Knowledge نامیده می شود. Mishael Rabin اولین کسی بود که از تکنیک Cut-And- Choose استفاده کرد [۵] .

چهار چوب پیشنهادی مقایسه سیستمهای مختلف از جنبه های امنیتی و ناشناختگی

در ادامه چارچوبی را که جهت ارزیابی و انتخاب سیستمهای بهینه پرداخت الکترونیکی امن و ناشناخته پیشنهاد داده ایم ارائه می نماییم این چارچوب شامل اجزاء اصلی زیر می باشد:

تعریف معیارهای ارزیابی

تعریف کاربرد ها و سرویسهای امنیتی مورد نیاز در سیستمهای پرداخت الکترونیکی

تعریف نیازهای فنی جهت ارائه سرویسهای امنیتی

تعریف ماتریس سرویس - نیازمندی

تعریف ماتریس روشها - نیازمندی ها

تعریف ماتریس روشها – سرویس ها

تشکیل جداول تصمیم گیری

۱ .تعریف معیارهای ارزیابی

هر کدام از سیستمهای پرداخت الکترونیکی موجود جنبه های مختلفی از امنیت و ناشناختگی را فراهم می آورند . برای بررسی و ارزیابی قابلیتهای هریک از سیستمها ، در اینجا معیارهای اساسی را تعریف می نماییم که بر مبنای آنها می توان قابلیتهای امنیت و ناشناختگی روشهای مختلف و تفاوتهای بین آنها را بیان نمود .

معیارهای اصلی موثر در عملکرد سیستمهای فوق عبارتند از :

پیچیدگی محاسباتی : سیستم پرداخت دارای محاسبات بغرنج و بسیار پیچیده ریاضی نبوده و قدرت محاسباتی متعادلی را نیاز داشته باشد.

اندازه پایگاه داده مورد نیاز : در پرداختهای الکترونیکی که بر اساس e-cash کار می کنند ، نگهداری سکه ها و مشخصات آنها در کاربردهایی مانند جلوگیری از خرج دوباره و پیگیری اختلاس کننده نقش مهمی را ایفا می کند. لذا سیستم پرداخت باید بنحوی طراحی شود که پایگاه داده ای که وظیفه نگهداری این سکه ها را دارد از نظر حجم به طور معقول و منطقی رشد نموده و اطلاعات ضروری حفظ و نگهداری شود.

Single Point Of Failure بودن بخشی از سیستم : درسیستم پرداخت آیا بخشی وجود دارد که خرابی آن باعث از کار افتادن کل سیستم شود یا در کارایی سیستم تاثیر مستقیم بگذارد؟

میزان پراکندگی اطلاعات در سطح شبکه : در سیستمهای پرداخت الکترونیکی که اطلاعات در سطح شبکه توزیع شده اند ، پراکندگی بیش از حد اطلاعات می تواند روی کارایی سیستم تاثیر نامطلوبی بگذارد .لذا اطلاعات باید در حد متعادی پراکنده شوند.

وابستگی اعتماد به اجزا سیستم : به این معنی است اعتماد یا عدم اعتماد به اجزایی از سیستم تا چه حد روی محبوبیت سیستم تاثیر می گذارد

امکان جلوگیری از اختلاس: جلوگیری از اختلاس یکی از مهمترین سرویسهای امنیتی است که بیشتر سیستمهای پرداخت الکترونیکی آن را ارائه می دهند .لذا سیستمی مقبول خواهد بود که بتواند این سرویس را با کمترین هزینه و بهترین کیفیت ارائه دهد.

امکان جلوگیری از خرج دوباره: عدم استفاده مجدد از ابزار خرید نیز از مشخصه های امنیتی مهم در سیستمهای پرداخت الکترونیکی می باشد.لذا سیستم پرداخت الکترونیکی که طراحی می کنیم حتی الامکان باید دارای این ویژگی مهم باشد.

قابلیت عدم انکار جزئیات پرداخت : سیستم باید مطمئن باشد که مشتری نمی تواند منکر تراکنش پرداخت شود.

در ادامه با استفاده از معیارهای فوق بر ارزیابی سیستمهای مختلف خواهیم پرداخت.

۲. تعریف کاربرد ها و سرویسهای امنیتی مورد نیاز در سیستمهای پرداخت الکترونیکی

در چهار چوبی که ارائه می دهیم ابتدا انواع کاربردها و سرویسهای امنیتی را که در سیستمهای پرداخت مد نظر است معرفی کرده و سیستمها را ارزیابی می نماییم .

کاربردها و سرویسهای امنیتی اصلی در سیستمهای پرداخت عبارتند از:

عدم انکار پرداخت از طرف مشتری

تصدیق مشتری

فراهم آوردن ناشناختگی

جلوگیری از اختلاس

پیگیری اختلاس کننده

جلوگیری از خرج دوباره

پیگیری دوباره خرج کننده

سیستمهای مختلف پرداخت بر اساس نوع کاربردی که دارند ممکن است بخشی از این سرویسها را ارائه دهند.

۳. تعریف نیازهای فنی جهت ارائه سرویسهای امنیتی

هر کدام از سیستمهای پرداخت الکترونیکی سرویسهای قابل توجهی را ارائه می دهند لذا بر اساس سرویسی که ارائه می دهند، نیازمندی های خاص خودشان را نیز دارا خواهند بود. در این بخش نیازمندی های فنی سیستمهای پرداخت را متذکر می شویم که شامل نیازمندی های زیر است:

الف) نیازمندی های اساسی

نیازهای اساسی عموما شامل همه روشها می شود و سیستمهای پرداخت الکترونیکی بر اساس کاربردهایی که دارند چندین مورد از آنها را به طور ویژه ای نیاز دارند. این نیازمندی ها شامل موارد زیر می باشد:

- عملکرد Online : بعضی از سرویسهایی که سیستمها ی پرداخت ارائه می دهند نیاز دارند که در پروسه پرداخت ، موجودیتهای پرداخت همواره به صورت Online با شند.

- عملکرد Offline : بر اساس ساختار بعضی سیستمهای پرداخت ، سرویسهایی که ارائه می دهند میتوانند به صورت Offline نیز باشد.

- نیاز به TTP[1] : بعضی از سیستمها ی پرداخت ، در امر پیگیری نیاز به یک شخص ثالث معتمد دارند تا بتوانند ناشناختگی کنترل شده را فراهم آورند.

- فسخ ناشناختگی : یکی دیگر از نیازهای اساسی در سیستمهای پرداخت الکترونیکی که ناشناختگی کنترل شده را فراهم می آورند امکان فسخ ناشناختگی است.

لا زم به توضیح است که ممکن است این نیازمندی ها در رابطه با هم باشند. یعنی برای رفع یک نیازمندی نیاز به یک نیازمندی اساسی یا نسبی دیگری احساس شود.

ب) نیازمندی های نسبی

نیازهای نسبی نیازهایی هستند که نسبت به سرویسهای امنیتی و ناشناختگی که سیستمهای پرداخت ارائه می دهند تغییر می کنند و لزوما همه سیستمها آنها را شامل نمی شوند و در کاربردهای مختلف اهمیت خود را نشان می دهند.لازم به توضیح است که در ماتریسهای ارزیابی موجود در بخشهای بعدی، نیازهای نسبی بر اساس اهمیت در هر کدام از کاربردها ، وزن دهی شده اند. نیازهای نسبی شامل موارد زیر است:

علامت گذاری سکه ها

نگهداری سکه های خرج شده

نیازمندی به یک تکنیک/پروتکل ویژه

۴.تعریف ماتریس سرویس - نیازمندی

با توجه سرویسهای امنیتی و ناشناختگی که سیستمهای مختلف پرداخت الکترونیکی ار ائه می دهند و نیازمندی مختلف هر کدام از این سرویسها دارا می باشند . ماتریس سرویس – نیازمندی را تعریف می کنیم که در جدول ۲ قابل مشاهده است.

۵. تعریف ماتریس روشها - نیازمندی ها

نیازمندی های اساسی و نسبی روشهای مختلف را به طور جداگانه مورد بررسی قرار داده وآنها را رتبه بندی نمودیم۲ . ماتریس نیازمندیها/ روشها را درجدول۳ قابل مشاهده است.

[1] Trusted third party

[2] هرکدام از سیستمها ی پرداخت اشاره شده در این بخش، به طور دقیق مورد مطالعه قرار گرفته و در لیست منابع به طور جداگانه ذکر شده اند.

ردیف	→ نیازمندی ها/ روشها ↓	عملکرد Online	عملکرد Offline	نیاز به TTP	اساسی فسخ ناشناختگی	علامت گذاری سکه ها	نگهداری سکه های خرج شده	نسبی (وزن از ۱۰) نیازمندی به یک تکنیک/پروتکل ویژه
۱	[۴]طرح E-Cash برای جلوگیری از اختلاس (Chen & zhang)	√	--	√	√	10	3	10
۲	[۴] طرح E-Cash عادلانه (Chen & zhang)	--	√	√	√	10	3	10
۳	[۱]سیستم E-Cash ناشناخته(Helger & lipmaa)	√	--	--	×	3	10	10
۴	[۱] سیستم ناشناخته ارتباطی(Marni & Jakobsson)	√	--	--	--	0	0	5
۵	[۶] سیستم ناشناخته ارتباطی Neuman & medrinsky	√	--	×	--	0	10	5
۶	[۷] سیستم ناشناخته ارتباطی(Simon)	--	√	--	--	0	10	5
۷	[۸] شبکه mix (chaum)	√	--	×	--	0	5	10
۸	[۵] سیستم Offline E-Cash غیر قابل پیگیری (Wang & zhang)	--	√	--	√	10	10	10
۹	[۹] مکانیزم پیگیری بدون نیاز به TTP (Kugler & Vogt)	--	√	--	√	10	10	10

جدول ۲: ماتریس سرویسهای امنیتی - نیازمندی ها

نیازمندی ها/سرویسهای امنیتی ← ↓	اساسی				نسبی (وزن از ۱۰)		
	عملکرد Online	عملکرد Offline	نیاز به TTP	فسخ ناشناختگی	مارک گذاری سکه ها	نگهداری سکه های خرج شده	نیازمندی به یک تکنیک/پروتکل ویژه
عدم انکار	×	×	×	√	0	10	5
تصدیق مشتری	√	×	×	--	0	0	5
فراهم آوردن ناشناختگی	√	√	×	--	3	5	10
جلوگیری از اختلاس	√	--	×	√	7	2	5
پیگیری اختلاس کننده	√	√	√	√	10	10	2
جلوگیری از Double Spending	√	--	×	×	3	10	0
پیگیری Double Spender	--	√	√	√	10	10	0

√ : نیازمندی مزبور را شامل می باشد. × : حالت بی تفاوت -- : سرویس مورد نظر قطعا نیازمندی مزبور را شامل نمی شود.

جدول۳ : ماتریس روشها - نیازمندی ها

√ سرویس مزبور را شامل می باشد. × : حالت بی تفاوت -- : روش مورد نظر قطعا سرویس مزبور را شامل نمی شود.

۶.تعریف ماتریس روشها - سرویس ها

حال که نیازمندی ها و سرویسهای سیستم های مختلف مشخص شده اند ، روشهای مختلف را از جنبه های کاربردی مورد ارزیابی قرار دادیم که بر اساس جنبه های استفاده هرکدام از سیستم ها ممکن است درکاربردهای مختلف، مشابه هم نباشند. جدول ۴ حاوی جزئیات هر روش نسبت به کاربرد مربوطه بوده و در نهایت براساس جداول و معیارهای موجود ، سیستم هایی به عنوان سیستم بهینه معرفی خواهند شد. (در این جدول از ۹ سیستم بررسی شده ۵ مورد را به طور نمونه ذکر کرده ایم)

۷.ارائه چارت تصمیم گیری برای انتخاب روشهای نهایی

ردیف	سرویسها/روشها ←	ایده اصلی	عدم انکار	تصدیق مشتری	فراهم آوردن ناشناختگی	جلوگیری از اختلاس	پیگیری اختلاس کننده	جلوگیری از Double Spending	پیگیری Double Spender	مسائل و مشکلات
۱	طرح E-Cash برای جلوگیری از اختلاس (Chen & zhang)	استفاده از امضا کور گروهی جهت جلوگیری از اختلاس.	√	√	√ در زمان اختلاس ، مجرم از مارک شدن سکه اطلاع ندارد.	√ با استفاده از مارک گذاری سکه ها	√	--	--	اعتماد به TTP
۲	طرح عادلانه E-Cash (Chen & zhang)	استفاده از امضا کور گروهی جهت جلوگیری از اختلاس	√	√	√ فقط بانک تشخیص می دهد که سکه ها مارک شده اند.	√ با استفاده از مارک گذاری سکه ها	√	--	--	اعتماد به TTP
۳	سیستم E-Cash ناشناخته (Helger & lipmaa)	استفاده از امضا کور جهت فراهم آوردن ناشناختگی استفاده کننده.	--	--	√ ناشناختگی استفاده کننده	-- بنا را بر اعتماد به مشتریان مشروع گذاشته است	--	--	--	رشد بی رویه پایگاه داده در صورت فراهم آوردن جلوگیری از Double Spending در نگهداری سکه های خرج شده
۴	سیستم ناشناخته ارتباطی (Marni & Jakobsson)	استفاده از شبکه Mix جهت فراهم آوردن ناشناختگی	--	√	√ ناشناختگی استفاده کننده (خریدار)	--	--	--	--	پراکندگی اطلاعات روی سرورهای Mix و گسترش لیستهای داخلی
۵	سیستم ناشناخته ارتباطی Neuman & medrinsky	فراهم آوردن ناشناختگی ارتباطی با استفاده از سرورهای پول (CS)	√	--	√ ناشناختگی برای سکه	--	--	√ زمانی که گیرنده سکه ها را با cs بررسی میکند	--	اعتماد به CS (Currency Server) زیرا خودش قادر به خرج کردن سکه ها می باشد.

جدول ٤ : ماتریس روشها-سرویسها

بنا بر چارچوبی که برای مقایسه سیستمهای پرداخت الکترونیکی ارائه می دهیم ، ارائه چارت تصمیم گیری برای انتخاب روشهای نهایی یکی دیگر از فعالیتهایی است صورت می دهیم.

۸.تشکیل جداول تصمیم گیری نهایی

تا کنون تمامی ملزومات ارزیابی سیستمهای پرداخت الکترونیکی فراهم آورده ایم .حال می خواهیم نحوه تصمیم گیری نهایی را در خصوص انتخاب سیستمهای بهینه داشته باشیم. برای این کار نیاز به جداول تصمیم گیری خواهیم داشت که این جداول بر اساس چارت تصمیم گیری بخش ۳-۷رسم می گردند

۹ جدول تصمیم گیری سرویسها / روشها

در این جدول ارزیابی نهایی را بر اساس سرویسهایی که روشها ارائه می دهند انجام می دهیم. بدین گونه که هرکدام از روشهایی که بیشترین سرویس امنیتی و ناشناختگی را داشته باشند، انتخاب خواهند شد.جدول شماره ۵ شامل این نوع ارزیابی می باشد.

جدول ۵ : ارزیابی نهایی سرویسها / روشها

ردیف	سرویسها/روشها ← ↓	عدم انکار	تصدیق مشتری	فراهم آوردن ناشناختگی	جلوگیری از اختلاس	پیگیری اختلاس کننده	جلوگیری از Double Spending	پیگیری Double Spender	ارزیابی نهایی
۱	طرحE-Cash برای جلوگیری از اختلاس (Chen & zhang)	√	√	√	√	√	--	--	Ok
۲	طرح عادلانه E-Cash (Chen & zhang)	√	√	√	√	√	--	--	Ok
۳	سیستم E-Cash ناشناخته (Helger & lipmaa)	--	--	√	--	--	--	--	No
۴	سیستم ناشناخته ارتباطی (Marni & Jakobsson)	--	√	√	--	--	--	--	No
۵	سیستم ناشناخته ارتباطی medrinsky & Neuman	√	--	√	--	--	√	--	No
۶	سیستم ناشناخته ارتباطی(Simon)	√	--	√	√	√	√	√	Ok
۷	شبکهMix (Chaum)	√	--	√	--	√	.--	--	No
۸	سیستمOffline E-Cash غیر قابل پیگیری (Wang & zhang)	√	--	√	--	√	--	√	OK
۹	مکانیزم پیگیری بدون نیاز به TTP (Kugler & Vogt)	√	√	√	√	√	√	√	Ok

۱۰ جدول تصمیم گیری نهایی روشها /نیازمندی ها

در این جدول ارزیابی نهایی را بر اساس نیازمندی هایی که هر کدام از روشهای ارائه شده دارند، انجام می دهیم. بدین گونه که هرکدام از روشهایی کـه کمتـرین نیازمندی اساسی و کوچکترین وزن در نیازمندی های نسبی را داشته باشند ، انتخاب خواهند شد.

لازم به توضیح است که ورودی این جدول آن روشهایی می باشند که در ارزیابی نهـایی جـدول تصـمیم گیـری روشـها / سرویسـها مـورد تائیـد مـی باشـند. همانگونه که می بینید از نه سیستم بررسی شده پنج مورد آن در این جدول شرکت کرده اند. جدول شماره ۶ شامل این نوع ارزیابی می باشد.

ردیف	→ نیازمندی ها/ روشهای تائید شده ↓	عملکرد Online	عملکرد Offline	نیاز به TTP	اساسی فسخ ناشناختگی	علامت گذاری سکه ها	نسبی (وزن از ۱۰) نگهداری سکه های خرج شده	نیازمندی به یک تکنیک/پروتکل ویژه	ارز یابی نهایی
۱	طرح E-Cash برای جلوگیری از اختلاس (Chen & zhang)	√	--	√	√	10	3	10	No
۲	طرح عادلانه E-Cash (Chen & zhang)	--	√	√	√	10	3	10	No
۳	سیستم ناشناخته ارتباطی(Simon)	--	√	--	--	0	10	5	Ok
۴	سیستم Offline E-Cash غیر قابل پیگیری (Wang & zhang)	--	√	--	√	10	10	10	No
۵	(Kugler & Vogt) مکانیزم پیگیری بدون نیاز به TTP	--	√	--	√	10	10	5	Ok

جدول۶: ارزیابی نهایی روشها / نیازمندیها

با توجه به جداول فوق ، سیستم های offline به دلیل عدم نیاز به اتصال به بانک درزمان پرداخت وعدم درگیر کردن بانک ، سیستم کارایی می باشد ولی به خوبی سیستم های online نمی توانند از مسائلی مانند اختلاس و double Spending وغیره پیشگیری کنند.

دربعضی از سیستم های ذکر شده نیاز به یک معتمد (TTP) جهت جلوگیری از اختلاس واخاذی داریم که وجود TTP دارای مزایای و معایب خاص خود است .

خلاصه و نتیجه گیری

کاملا واضح است که محرمانگی استفاده کننده دراینترنت درمعرض خطر است . سیستمهای پرداخت الکترونیکی هر کدام اقدامات تکنیکی خاصی را ارائه می‌دهد که می تواند محرمانگی استفاده کننده را که یک خرید الکترونیکی روی اینترنت انجام می دهد ، گارانتی کند. ما معتقدیم که چنین اقدامات تکنیکی برای افزودن اهداف مشروع و مدیریتی جهت حفظ محرمانگی استفاده کننده ضروری است . این تحقیق یک بررسی کاملی از سیستم های پیشرفته موجود انجام می دهد. لذا سیستم های بسیاری وجود دارند که تفاوتهای اندکی با هم دارند، بنابراین هنوز هم به نظر می رسد که برای انجام تحقیقات درآینده برای ایجاد سیستم های پیشرفته پرداخت ، جا داریم . درحقیقت طرحهای بسیاری با مشخصه های جالب توجهی وجود دارد. ولی هیچکدام از طرحها به طور حقیقی همه آن مشخصه ها را باهم ترکیب نکرده اند ، تا اینکه آنها را کارا و عملی سازند. برای مثال قابل توجه وجالب خواهد بود اگر سیستم پرداختی طراحی شود که قابلیت فسخ و قابلیت بازبینی را باهم ترکیب کند. در نهایت این تحقیق روی پروتکلهای پرداخت الکترونیکی با ناشناختگی مشتری و سیستم های ارتباطی ناشناخته با ناشناختگی آغازگر تمرکز دارد.لذا با وجود سیستمهای مختلف پرداخت الکترونیکی باید یک چارچوب مشخص و مناسبی موجود باشد تا بتواند ارزیابی کاملی از سیستمهای پرداخت ، با توجه جنبه های مختلف امنیت و ناشناختگی داشته باشد و سیستمهای بهینه را جهت استفاده در محیطهای پرداخت انتخاب نماید.تحقیق موجود سعی کرده این چارچوب را با توجه به تمامی جنبه های امنیتی و ناشناختگی در سیستم های پرداخت الکترونیکی به طور بهینه ای ارائه دهد.

مراجع

[1] S.Aghdami and S.khorsandi, "Secure and Anonymous TTP- based Electronic Payment Systems and Making Anonymity and Security Via Multi-User interfaces and Passwords In Proceedings of the 3d International confrence on Information Security Applications (ICIME 2010), april 2010

[2] Donal O'Mahony, Michael Peirce, and Hitesh Tewari, "Electronic Payment Systems for E-Commerce", Artech House , 2001,Second edition.

[3] David Chaum," Blind Signatures for Untraceable Payments", Rivest, and Alan T, Sherman, editors, Advances in Cryptology,2000

[4] Xiaofeng Chen, Fangguo Zhang and et.al , " A New Approach to Prevent Blackmailing in E-Cash" ,Information and Communications University (ICU), 2002.

[5]H. Wang Y. Zhang,"Untraceable Off-line Electronic Cash Flow in E-Commerce",Department of Maths & Computing University of Southern Queensland Toowoomba QLD 4350 Australia ,2001.

[6] Gennady Medvinsky and Clinord Neuman," NetCash: A design for prac-tical electronic currency on the Internet", In Proceedings of the 1st ACM Conference on Computer and Communications Security,2001

[7] Daniel R. Simon," Anonymous Communication and Anonymous Cash",In Neal Koblitz, editor, Advances in Cryptology { CRYPTO'96, Lecture Notes in Computer Science, LNCS 1109,2002

[8] David Chaum," Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM,1999

[9] Dennis Kugler and Holger Vogt," Auditable Tracing with Unconditional Anonymity", In Proceedings of the Second International Workshop on Information Security Applications (WISA 2001), September 2001.