کارگاه‌های آموزشی مرکز اطلاعات علمی

آموزش نرم‌افزار Word برای پژوهشگران

روش تحقیق کمی

آموزش مهارت‌های کاربردی در تدوین و چاپ مقالات ISI

بررسی و مقایسه سیستم های پرداخت الکترونیکی برای مبالغ پائین

آرش رحمان

استادیار، گروه مهندسی کامپیوتر (نرم افزار) دانشکده فنی و مهندسی واحد رودهن دانشگاه آزاد اسلامی
عضو باشگاه پژوهشگران جوان دانشگاه آزاد اسلامی واحد رودهن
arashrahman@yahoo.com

چکیده- اجرای تجارت الکترونیکی مستلزم فراهم شدن شرایطی است که از آنجمله در نظر گرفتن مسائل امنیتی، محرمانگی، حقوقی، استفاده از سیستم های پرداخت الکترونیکی و غیره است. در این مقاله سیستم های رایج در امر پرداخت های الکترونیکی برای مبالغ پائین مورد بررسی و بحث قرار گرفته است. همچنین این سیستم ها بر حسب ویژگی های مطرح تحلیل و مقایسه شده اند و نقاط ضعف و قوت هر کدام مشخص شده است. نتایج نشان می دهد که در امر تجارت الکترونیک، انتخاب یک سیستم از میان سیستم های مطرح شده با در نظر گرفتن ملاحظات و ویژگی های مطرح شده و مورد درخواست امکان پذیر بوده و سیستم های مطرح شده با در نظر گرفتن بستر مناسب، سیاست های حاکم، امکانات در دسترس، موجودیت های معتبر و شرایط (امنیتی، حقوقی و محرمانگی) مد نظر، قابل استفاده، بهره برداری و توسعه اند.

کلید واژه- سیستم های پرداخت الکترونیکی[1]، سیستم های پرداخت الکترونیکی برای مبالغ پائین[2]

۱- مقدمه

در سیستم های پرداخت الکترونیکی برای مبالغ پایین مبالغی که در معاملات رد و بدل می شوند از حد خاصی (مثلاً ۵۰ یا ۱۰۰ تومان) تجاوز نمی کنند، در پروتکل های مربوط به اینگونه سیستم ها از ابزارهای امنیتی نسبتاً ضعیف تر استفاده می شود تا کارایی و سرعت عملکرد در این گونه سیستم ها بالا رفته و ترافیک در شبکه به حداقل برسد. استفاده از ابزارهای امنیتی نسبتاً ضعیف در اینگونه سیستم ها بدلیل آن است که ضرر و زیانی که در صورت بروز تقلب و حمله در اینگونه سیستم ها حادث گردد چندان جدی نیست.

در این مقاله در ابتدا ویژگی های مطرح در این سیستم های بیان شده است، سپس متداول ترین این سیستم ها مورد بررسی و بدنبال آن بر حسب ویژگی های مطرح شده مورد مقایسه قرار گرفته اند. در انتها نیز از بحث نتیجه گیری شده است.

۲. ویژگی های سیستم های پرداخت الکترونیکی

یک سیستم ایده آل در پرداخت های الکترونیکی شایسته است دارای کلیه ویژگی های زیر باشد، لکن بدلیل امکان افزایش پیچیدگی های سیستم و در نتیجه غیر عملی شدن آن ها، معمولاً زیر مجموعه ای از این ویژگی ها برای یک سیستم پرداخت الکترونیکی در نظر گرفته می شود. این ویژگی ها عبارتند از [۱۰، ۵، ۳، ۲]:

۱ .۲ . اقتصادی[3]

مهمترین ویژگی ها در این قسمت عبارتند از:

۱ . ۱ . ۲. اندازه پرداخت[4]

سیستم های پرداخت الکترونیکی از نظر مبلغ پرداختی به سه دسته تقسیم شده اند:

الف) سیستم های پرداخت الکترونیکی برای مبالغ بالا[5]

اینگونه سیستم ها مبالغ $۱۰ به بالا را در بر می‌گیرند. به‌لحاظ اینکه اینگونه سیستم ها معمولاً در

مبالغ رد و بدل شده محدودیتی ندارند، عمدتاً قابل ملاحظه هستند. در این حالت به علت وجود احتمال بالای حمله به سیستم توسط افراد مختلف و به جهت سودجوئیهای مالی، نیاز به ابزارهای امنیتی قوی می باشد تا پروتکل را از امکان تقلب و حمله مصون نماید.

ب) سیستم های پرداخت الکترونیکی برای مبالغ کوچک[۶]

اینگونه سیستم ها مبالغ بین $ ۰/۱ تا $ ۱۰ را در بر می گیرند ابزارهای امنیتی برای پروتکل اینگونه سیستم ها معمولاً ضعیف تر از سیستم های پرداخت الکترونیکی برای مبالغ بالا است

ج) سیستم های پرداخت الکترونیکی برای مبالغ پایین[۷]

اینگونه سیستم ها مبالغ زیر ۱ سنت[۸] را در برمی‌گیرند. در اینگونه سیستم ها مبالغ رد و بدل شده از حد خاصی (مثلاً ۱۰۰ تومان) تجاوز نمی کنند. بدلیل اینکه ضرر و زیان ایجاد شده در صورت بروز تقلب و حمله در اینگونه سیستم ها جدی نیست، پروتکل های مربوطه از ابزارهای امنیتی ضعیف تری استفاده می نمایند تا کارایی و سرعت عملکرد را بالا برده و ترافیک را به حداقل رسانند.

۲ . ۱ . ۲ . سادگی کار[۹]

اعمال لازم به انجام توسط کاربر شایسته است حداقل باشد، تا کاربر بدون نیاز به وارد شدن به جزئیات بتواند خرید و پرداخت را انجام دهد و عضویت یا ترک سیستم برای کاربر ساده باشد. با این وجود کاربر بایستی بتواند تا با کمک ابزارهایی که در اختیارش گذاشته می شوند، از مراحل انجام پذیرفته بصورت قدم به قدم اطلاع حاصل نماید.

۲ . ۲ . ویژگی های فنی[۱۰]

۱ . ۲ . ۲ . شرکت کنندگان در یک سیستم پرداخت الکترونیکی[۱۱]

۱ . ۱ . ۲ . ۲ . مشتری[۱۲]: کاربری است که عمل پرداخت را انجام می دهد.

۲ . ۱ . ۲ . ۲. فروشنده[۱۳]: دریافت کننده پرداخت یا فروشنده است.

۳ . ۲ . ۲ . ۲ . صادرکننده[۱۴]: معمولاً تحت عناوین بانک یا تأمین کننده سرویس[۱۵] برای مشتری، در یک سیستم تجارت الکترونیکی مطرح می گردد. بیشتر فعل و انفعالات آن با مشتری است.

۴ . ۲ . ۲ . ۲. حصول کننده[۱۶]: معمولاً تحت عناوین بانک یا تأمین کننده سرویس برای فروشنده، در یک سیستم تجارت الکترونیکی مطرح می گردد. بیشتر فعل و انفعالات آن با فروشنده است.

۵ . ۲ . ۲ . ۲. دلال یا واسطه[۱۷]: دلال ترکیبی ازحصول کننده و صادرکننده است که هنگامیکه در پروتکلی نیاز به اشتراک گذاری بخش سومی بین مشتری و فروشنده باشد، مورد استفاده قرار می گیرد.

۶ . ۲ . ۲ . ۲ . رویت کننده[۱۸]: شخص ثالثی است که سعی بر بدست آوردن اطلاعات تراکنش ها دارد.

۷ . ۲ . ۲ . ۲. گواهی نامه[۱۹]:بسیاری از سیستم های پرداخت الکترونیکی در جهت تأیید و تصدیق رسمی یک بخش اعم از مشتری یا فروشنده به مرجعی رسمی متکی اند که گواهی تصدیق و یا تأیید مشتری یا فروشنده را صادر می نماید. گواهی نامه ها می توانند شامل دستورالعمل های صادر کننده (مرجع رسمی) برای هر فروشنده ای باشند که می خواهد مبالغ پرداختی از کاربران را نقد کند، معمولاً صدور گواهی نامه توسط مرجع رسمی با ثبت[۲۰] اطلاعات در خواست کننده گواهی نامه همراه است. یک گواهی نامه معمولاً پس از صادر شدن توسط صادرکننده آن امضای دیجیتال می شود.

۲ . ۲ . ۲ . مدلهای پولی[۲۱]

یک سیستم پرداخت الکترونیکی می تواند به یکی از سه روش زیر عمل نماید:

۱ . ۲ . ۲ . ۲ . روش اعتباری[۲۲]: در این روش مبلغ پرداختی توسط مرکزی اعتباری پرداخت و سپس آن مبلغ از اعتبار کاربر کم شده و در زمان خاصی مبلغ واقعی توسط کاربر (یا از طریق حساب بانکی وی) به آن مرکز پرداخت می گردد.

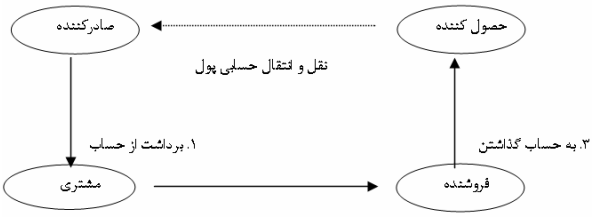
۲ . ۲ . ۲ . ۲. روش چک[۲۳]: در این روش همانند چکهای فیزیکی مبلغ پرداختی توسط یک مدرک معتبر به فروشنده ارسال می گردد، سپس مدرک فوق همانند چک فیزیکی از طریق حساب بانکی خریدار نقد می شود.

۳ . ۲ . ۲ . ۲ . روش پول نقد[۲۴]: در این روش کاربر (خریدار) قبلاً مبلغی را پرداخته و در مقابل آن پول الکترونیکی دریافت نموده است. این پول در موقع خرید به فروشنده ارسال می شود. پول (یا اصطلاحاً سکه) الکترونیکی از طریق سرویس دهندگان مالی قابل خرید بوده و در هر زمان ممکن است دوباره با پول فیزیکی تعویض گردد.

۳ . ۲ . ۲. مدلهای پرداخت

مهمترین مدلهای پرداخت در سیستم های پرداخت الکترونیکی عبارتند از:

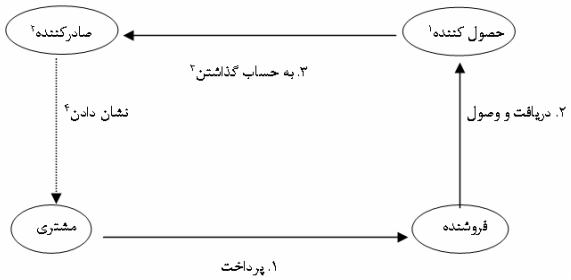
۱ . ۳ . ۲ . ۲. مدل شبه پول مستقیم[۲۵]: شمای کلی این مدل در شکل ۱ مشخص شده است:



شکل ۱: شمای کلی مدل شبه پول مستقیم

در این سیستم ها مدل پول نقد استفاده می شود. در این سیستم ها مشتری مبلغی را از حسابی که نزد صادر کننده دارد برداشت کرده و این پول را که بصورت الکترونیکی[۲۶] در آمده است به فروشنده پرداخت می کند. فروشنده هم در خـواست به حساب گذاشتن[۲۷] این پول را از حصول کننده می نماید. در انتهای کار هم حصول کننده در خواست نقل و انتقال حسابی پول را از صادرکننده می نماید.

۲ . ۳ . ۲ . ۲. مدل مبتنی بر حساب مستقیم[۲۸]: شمای کلی این مدل در شکل ۲ مشخص شده است.

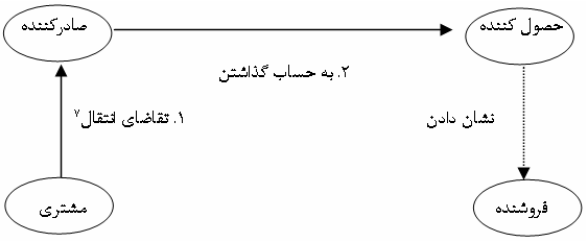


شکل ۲: شمای کلی مدل مبتنی بر حساب مستقیم

اینگونه سیستم ها شباهت زیادی با سیستم های چک دارند. در اینگونه سیستم ها مشتری چکی را به فروشنده می فرستد که فروشنده این چک را به حصول کننده ارائه می نماید. سپس حصول کننده تقاضای بازخرید[۲۹] کردن آن را از صادرکننده می نماید. سپس تکمیل پرداخت توسط وی به مشتری اطلاع داده می شود.

سیستم های مبتنی بر حساب مستقیم یا سیستم های چک (گاهی وقت به این نام نامیده می شوند) مدل پولی Notational را استفاده می نمایند.

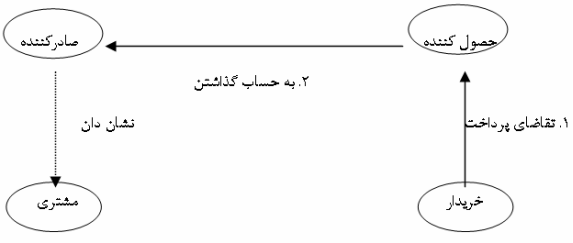
۳ . ۳ . ۲ . ۲ . مدل مبتنی برحساب از طریق خریدار[۳۰]: شمای کلی این مدل در شکل ۳ نشان داده شده است.



شکل ۳: مدل مبتنی بر حساب از طریق خریدار

در این مدل، مشتری در خواست انتقال وجه از حساب خود را به حساب فروشنده که در نزد حصول کننده است را می دهد. این مدل درست شبیه انتقال بانکی مرسوم است. در این مدل پس از قرار گرفتن پول در حساب فروشنده که در نزد حصول کننده است، فروشنده (از طرف حصول کننده) متوجه ورود مبلغ به حساب خود میشود.

۴ . ۳ . ۲ . ۲. مدل مبتنی بر حساب از طریق فروشنده[۳۱]: شمای کلی این مدل در شکل ۴ نشان داده شده است.



شکل ۴: شمای کلی مدل مبتنی بر حساب از طریق فروشنده

در این مدل فروشنده در خواست برداشت پول از حساب مشتری را که در نزد صادرکننده است را به حصول کننده که خود نزد آن حساب دارد، می دهد. درست مثل برداشتن پول از یک حساب بانکی، در این

مدل فروشنده فقط متوجه خارج شدن پول از حسابش می شود.

۲ . ۲ . ۴ . تعیین اعتبار[۳۲]

تقسیم بندی سیستم های پرداخت الکترونیکی از لحاظ تعیین اعتبار بصورت زیر است:

۱ . ۴ . ۲ . ۲. بلادرنگ[۳۳]: در تعیین اعتبار بلادرنگ مشتری و/یا فروشنده با یک بخش سوم نظیر صادرکننده و/یا حصول کننده تعیین اعتبار پرداخت را انجام می دهد. در این حالت بخش سوم می بایست بصورت بلادرنگ نتیجه را اعلام نماید. این نوع تعیین اعتبار معمولاً خاصه سیستم هایی است که نیازمند امنیت بالا است.

۲ . ۴ . ۲ . ۲. غیر بلادرنگ[۳۴]: به منظور جلوگیری از ایجاد ترافیک در زمان خاص و در گره خاص در شبکه می‌توان تعیین اعتبار غیربلادرنگ را مطرح نمود. بخصوص در مورد سیستم هایی که با مبالغ پایین سر و کار دارند، تعیین اعتبار بهتر است بصورت غیر بلادرنگ انجام گیرد.

۳ .۴ . ۲ . ۲. شبه بلادرنگ[۳۵]: تعیین اعتبار شبه بلادرنگ در مورد سیستم هایی مطرح می شود که برخی از فعل و انفعالات در آنها نیازمند ارتباط بلادرنگ با موجودیت سوم، و برخی فعل و انفعالات نیازمند ارتباطات غیر بلادرنگ است.

۵ . ۲ . ۲ . مکانیزم های امنیتی[۳۶]

در ذیل برخی از مکانیزم های امنیتی مطرح شده است.

۱ . ۵ . ۲ . ۲ . جمله رمز[۳۷] : در این مکانیزم کلمه رمز میان ارزیابی کننده[۳۸] و مجاز کننده[۳۹] به اشتراک گذاشته می شود. رمز نگاری کلید اشتراکی[۴۰] مکانیزمی در این زمینه است.

۲ . ۵ . ۲ . ۲. امضاء[۴۱]: بخش ارزیابی کننده نیازمند امضای دیجیتال بخش مجاز کننده است. امضاء شامل پیام و رمزنگاری کلید عمومی است و به عنوان عاملی برای جلوگیری از انکار شدن معامله توسط یکی از دو طرف عمل می نماید.

۳ . ۵ . ۲ . ۲. امضاء کور[۴۲]: تکنیکهای امضای کور در جهت جلوگیری از ردیابی کردن[۴۳] و تأمین اختفاء[۴۴] در یک تجارت الکترونیکی مورد استفاده قرار می گیرند. به عنوان نمونه در یکی از این تکنیکها شماره سریال سکه ها از حالت اولیه خود خارج می شوند (کور می شوند)، که این کار با ضرب کردن در یک ضریب تصادفی می تواند انجام گیرد. سکه های کور درون یک پیام جا گرفته، پیام با کلید خصوصی کاربر بطور دیجیتالی امضاء شده و سپس با کلید عمومی بانک رمز شده و برای بانک فرستاده می‌شود. پیام ارسالی فقط توسط بانک می تواند رمزگشایی شود. زمانیکه بانک پیام را دریافت می کند، امضاء را چک نموده و مقدار خرید شده را از حساب صاحب امضاء کم می کند. بانک سکه ها را با کلید خصوصی امضاء می کند. بعد از امضای سکه های کور شده آنها را به کاربر برمیگرداند که با کلید عمومی کاربر رمز شده اند. کاربر می‌تواند پیام را رمز گشایی کرده و آنها را با تقسیم کردن بر ضریب کورکننده به حالت اولیه خود بازگرداند. با توجه به اینکه بانک شماره سریال های موجود بر روی سکه ها را نمی بیند تضمین می کند که هیچ راهی برای پیگیری اینکه چه کسی این سکه ها را خریده است، وجود ندارد. به این ترتیب اختفاء کامل تأمین می شود.

۴ . ۵ . ۲ . ۲. زنجیره پراکنده شده[۴۵]: پرداخت های متوالی به یک فروشنده می تواند بوسیله زنجیره پرداخت ها شکل گیرد. مانند سیستم payword که در آن کاربر زنجیره مبلغ پرداختی را به ترتیب عکس با انتخاب تصادفی آخرین مبلغ پرداختی W_n ایجاد می نماید. سپس $w_i = h(w_i+1)$ را برای $i= \dots , 0$ n-1, n-2,محاسبه می کند. در اینجا w. ریشه زنجیره مبلغ پرداختی است.کاربر مبالغ پرداختی را به ترتیب w_1 سپس w_2 و به همین ترتیب الی آخر خرج می کند. در این سیستم فروشنده آخرین مبلغ خرج شده توسط مشتری را در نزد خود نگاه می‌دارد. i امین پرداخت مشتری به فروشنده که شامل w_i است را فروشنده با استفاده از w_{i-1} ارزیابی می نماید.

۲.۳. نیازمندیها[۴۶]

خصیصه های مرتبط با نیازمندیها در سیستم های پرداخت الکترونیکی شامل موارد زیر است:

۱.۳.۲. تراکنش[۴۷]

تراکنش های مالی بایستی شرایطACID بانکهای اطلاعاتی را پشتیبانی کنند. این شرایط عبارتند از:

۱.۱.۳.۲. اتمی بودن[۴۸]: در مورد خاصیت فوق دو نکته قابل ذکر است:

الف) انتقال وجوه[۴۹]: چنانچه از حساب مشتری مبلغی برداشته و به حساب فروشنده گذاشته شود، هر دو مبلغ بایستی با هم مطابقت داشته باشند.

ب) انتقال کامل[۵۰]: ارائه وجوه مبتنی بر سند (نظیر چک) و پرداخت آن بایستی پشت سر هم صورت گیرد. یعنی یا هر دو با هم صورت گیرند و یا هیچ کدام از آن دو انجام نگیرد.

۲.۱.۳.۲. سازگاری[۵۱]: توافق همه قسمتها نسبت به مقدار پرداختی، علّت پرداخت و جابجا شدن مبلغ انتقالی از یک حساب به حساب دیگر بایستی صحیح[۵۲] باشد.

۳.۱.۳.۲. ایزوله بودن[۵۳]: تراکنش ها بایستی بصورت غیر وابسته و بصورت ایزوله از هم انجام بگیرند که این کار با انجام تراکنش ها بصورت ترتیبی و یا به کمک مکانیزم های کنترل همزمانی میسر می گردد.

۴.۱.۳.۲. ماندگار بودن[۵۴]: در این زمینه سه نکته لازم به ذکر است:

الف- وقتی که تراکنش به اتمام[۵۵] رسید، بایستی قابل احیا[۵۶] باشد.

ب- اگر تراکنشی به اتمام نرسیده بود، ولی چیزی روی دیسک نوشته بود، بایستی هیچ اثری روی پایگاه داده ها نداشته باشد، به عبارت دیگر آثار وجودش پاک شود. انگار که اصلاً شروع نشده است.

ج- امکان مراجعه به فایل های تاریخچه[۵۷] و شروع تراکنش از نقطه ای که در آنجا بدلایلی توقف کرده بود، وجود داشته باشد.

۲.۳.۲. امنیت[۵۸]

در مورد امنیت مواردی مطرح گردیده است که در زیر به توضیح هر یک پرداخته شده است:

۱.۲.۳.۲. غیر قابل خرج کردن دوباره پول[۵۹]: امکان خرج دوبار پول در سیستم های پرداخت الکترونیکی بخصوص وقتی که از مدل پرداخت سکّه[۶۰] استفاده می‌شود نبایستی وجود داشته باشد.

۲.۲.۳.۲. غیر قابل جعل کردن پول[۶۱]: با اتخاذ پروتکل های امنیتی بایستی تا آنجا که امکان دارد امکان جعل غیر قانونی پول الکترونیکی را منتفی نمود.

۳.۲.۳.۲. تجاوز نکردن از حد قابل خرج[۶۲]: با اتخاذ پروتکل های مناسب، بایستی امکان خرج پول توسط مشتری را بیشتر از حد تعیین شده، در یک معامله الکترونیکی منتفی نمود.

۴.۲.۳.۲. انکار نکردن[۶۳]: یکی از دو طرف معامله نبایستی امکان انکار معامله را داشته باشد. احراز هویت و استفاده از امضاءهای دیجیتال یکی از راههای متداول برای دستیابی این مقصود است.

۵.۲.۳.۲. سخت افزارهای مقاوم در برابر دستکاری کردن[۶۴]: استفاده از سخت افزارهای مقاوم در مقابل دستکاری غیر قانونی اشخاص، یکی از موارد مهم امنیتی است.

۳.۳.۲. محرمانگی[۶۵]

در ارتباط با محرمانگی در یک تجارت الکترونیکی ویژگی های زیر مطرح است:

۱.۳.۳.۲. محرمانگی[۶۶]: میدان دید افراد نسبت به آنچه در یک تجارت الکترونیکی بین مشتری و فروشنده رد و بدل می شود در بسیاری از جاها بایستی محدود شود. استفاده از تکنیک های رمزنگاری نامتقارن و امضای آنچه می خواهد از یک طرف به طرف دیگر فرستاده شود، با کلید عمومی طرف مقابل، یکی از راهکارهای حصول محرمانگی است.

۲.۳.۳.۲. اختفاء[۶۷]: مشخصه فرد در یک تجارت الکترونیکی بایستی مخفی نگاه داشته شود. استفاده از نام مستعار برای خرید از یک فروشنده و تکنیک های استفاده از امضای کور به عنوان راهکارهایی در این زمینه توصیه شده است.

۳.۳.۳.۲. غیر قابل پیگیری[۶۸]: مشخصه افرادی که در یک تجارت الکترونیکی مشارکت می کنند نبایستی

قابل پیگیری بوده و یا حداقل پیگیری آن هزینه ای را در بر بگیرد که برای افراد عادی قابل پرداخت نباشد.

۴ . ۳ . ۲ . درون سازگاری (تعامل پذیری)[۶۹]

در ارتباط با درون سازگاری در یک تجارت الکترونیکی ویژگی های زیر مطرح است:

۱ . ۴ . ۳ . ۲. خردکردن[۷۰]: این خصیصه در مورد سیستم های پرداخت مبتنی بر پول نقد[۷۱] مطرح است، که بر اساس آن جایگزین کردن یک تراکنش با ارزش بالا به چندین تراکنش با ارزش پایین تر امکان پذیر است.

۲ . ۴ . ۳ . ۲ . دوسویه بودن[۷۲]: بر اساس این خصیصه نه تنها فروشنده می تواند پرداخت[۷۳] را دریافت نماید، بلکه مشتری نیز می تواند پرداخت را دریافت نماید. سیستم های مبتنی بر چک معمولاً دارای این خصیصه اند، اما سیستم های مبتنی بر کارت های اعتباری فاقد این ویژگی اند.

۳ . ۴ . ۳ . ۲ . امکان دوباره خرج کردن[۷۴]: دریافت کننده پول دیجیتال بایستی بدون دخالت بخش سوم (بانک) قادر به انتقال آن به شخص دیگری باشد. سیستم های مبتنی بر کارت های اعتباری بدلیل اینکه مجبور به ارتباط با بانک اند، فاقد این خصیصه اند.

۴ . ۴ . ۳ . ۲. تطابق و تقبل[۷۵]: نتیجه پرداخت الکترونیکی یک بانک، بایستی توسط بانک های دیگر قابل قبول باشد، و نیاز به بانک مشابه نداشته باشد. این خصیصه بیشتر در ارتباط با توسعه سیستم های پرداخت الکترونیکی مطرح می شود.

۵ . ۴ . ۳ . ۲. پشتیبانی از گردش پول[۷۶]: اعتبار و ارزش یک سیستم پرداخت الکترونیکی وابسته به تعداد کاربرانی است که آن را قبول می کنند. بدین ترتیب است که اعتبار آن افزایش می یابد. لذا دست به دست شدن پول و یا گردش پول در سطح جهانی بیشتر مد نظر است.

۶ . ۴ . ۳ . ۲ . انعطاف پذیری[۷۷] : یک سیستم پرداخت الکترونیکی شایسته است که روشهای مختلف پرداخت را، از قبیل؛ پرداخت توسط کارتهای اعتباری، پرداخت توسط چک و پرداخت توسط پول نقد را حمایت نماید، و کاربر را محدود به یک روش خاص ننماید.

۵ . ۳ . ۲ . قابل تغییر سایز بودن[۷۸]

سایز (تعداد کاربران و تاجران) یک سیستم پرداخت الکترونیکی نبایستی توسط سرویس دهندگان که عمده فعالیتهای فرایند را بعهده دارند، محدود شود. همچنین افزایش تعداد کاربران یا تاجران در سیستم نبایستی کارایی سیستم را پائین آورد.

۶ . ۳ . ۲. اقتصاد خرد[۷۹]

در این ارتباط دو مورد توضیح داده شده است.

۱ . ۶ . ۳ . ۲ . هزینه پایین[۸۰]: هزینه اجرای یک تراکنش پرداخت بایستی به قدر کافی از لحاظ اقتصادی پایین باشد. همچنین پروتکل پرداخت بایستی متناسب با سایز پرداخت[۸۱] در نظر گرفته شود.

۲ . ۶ . ۳ . ۲. کارایی و یا اثربخشی[۸۲]: سرعت و کارایی یک سیستم پرداخت بایستی در حد مطلوب باشد. لازم به ذکر است چنانچه تعداد معاملات با مبالغ پایین زیاد باشند و پروتکل اجرایی ساده نباشد، آن گاه بدلیل وجود ترافیک در یک گره[۸۳]، کارایی سیستم پایین خواهد آمد.

۷ . ۳ . ۲ . اقتصاد عمومی[۸۴]

در این ارتباط موارد ذیل مطرح است.

۱ . ۷ . ۳ . ۲. عملیاتی[۸۵]: منظور از عملیاتی بودن یک سیستم پرداخت الکترونیکی این است که این سیستم مرحله آزمایش خود را می گذرانده است (این سیستم قبل از مرحله آزمایش به صورت فرضیه مطرح شده است) و وارد مرحله عملیاتی و اجرائی شده است.

۲ . ۷ . ۳ . ۲. کاربر پسندبودن[۸۶]: برای یک فروشنده میزان جذب و تحت تأثیر قرار دادن مشتریان توسط یک سیستم پرداخت دیجیتال بسیار حائز اهمیت است، چراکه باعث جذب مشتری به فروشنده شده و تعداد مشتریان فروشنده را افزایش می دهد.

۳ . ۷ . ۳ . ۲. خطر در سطح پایین[۸۷]: منظور خطرات مربوط به از دست دادن های مالی (پول و یا جنس) است، که شایسته است کم و کنترل شده باشد، چه در مورد مشتری و چه در مورد فروشنده.

۴ . ۷ . ۳ . ۲. قابل اطمینان بودن[۸۸]: با توجه به حساسیت موجود در امر تجارت، یک سیستم پرداخت

الکترونیکی بایستی همواره در دسترس بوده و احتمال وجود خطا و خرابی در آن به صفر نزدیک شود.

۵ . ۷ . ۳ . ۲. معتبر بودن درطی زمان[۸۹]: ذخیره[۹۰] و بازیابی[۹۱] پول الکترونیکی بایستی به آسانی امکان پذیر بوده و با گذشت زمان نامعتبر نشود.

۶ . ۷ . ۳ . ۲ . پرداخت بدون وقفه[۹۲]: پرداخت بایستی بصورت اتوماتیک (بدون اینکه برای تأمین نمودن اطلاعات کاربر دچار وقفه ای شود) صورت گرفته و بعد از زمانی اندک برای تأیید مجدد کاربر، نمایش داده شود.

۷ . ۷ . ۳ . ۲. تأخیر کم[۹۳]: تراکنش پرداخت بایستی سریع بوده و تأخیری در انجام عملیات خرید وجود نداشته باشد.

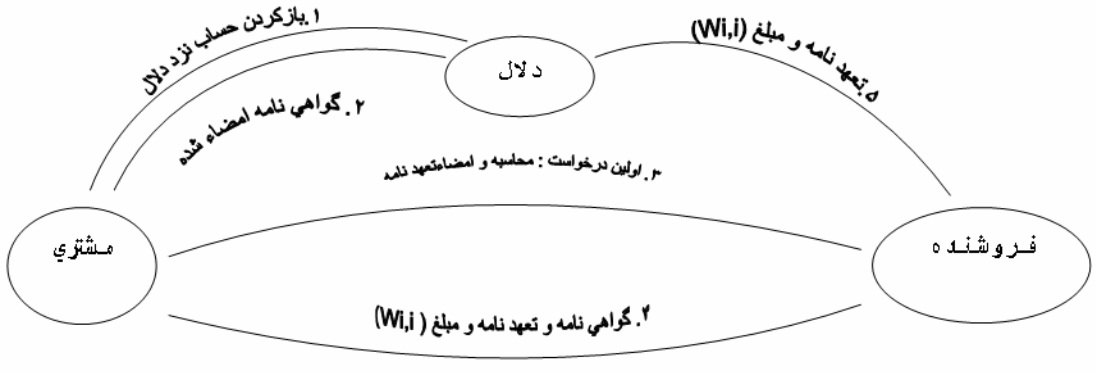
۸ . ۷ . ۳ . ۲ . عدم وابستگی سخت افزاری[۹۴]: کاربران نبایستی نیازمند به استفاده از سخت افزارهای ویژه باشند.

۹ . ۷ . ۳ . ۲. هزینه پایین تراکنش[۹۵]: هزینه انجام تراکنش ها در یک سیستم پرداخت الکترونیکی بایستی پایین باشد.

۳. سیستم های پرداخت الکترونیکی برای مبالغ پائین

۳,۱. سیستم پرداخت Payword

مراحل تراکنش های این سیستم در شکل ۵ مشخص شده است [۱۳، ۱].



شکل ۵: مراحل تراکنش ها در سیستم Payword

در مرحله آغازین تراکنش خرید، کاربر بر روی یک اتصال[۹۶] برای دستیابی به صفحه وب فروشنده کلیک می‌نماید. در این مرحله جستجوگر[۹۷] مشخص می کند که این اولین تقاضا برای فروشنده از طرف این خریدار در آن روز است. سپس برای اولین درخواست، کاربر یک تعهدنامه را برای زنجیره جدید خاص کاربر[۹۸] و خاص فروشنده[۹۹] برای مبالغ پرداختی $W_1, W_2, \ldots, W_n$ محاسبه و امضاء می‌نماید. در این مرحله کاربر زنجیره مبالغ پرداختی را به ترتیب عکس و با انتخاب تصادفی آخرین مبلغ پرداختی W_n ایجاد می نماید و سپس $W_i = h(w_i+1)$ را برای $i=n-1, n-2, \ldots,0$ محاسبه می نماید، که در اینجا W_0 ریشه زنجیر مبلغ پرداختی است و خود مبلغ پرداختی نیست. (می توان فرض کرد که هر مبلغ پرداختی دقیقاً ۱۰ تومان ارزش دارد) در این پروتکل تعهدنامه شامل ریشه(W_0) است و هیچ مبلغ پرداختی W_i ($i>0$) را شامل نمی شود. کاربر این تعهدنامه را به همراه گواهی نامه اش به فروشنده تقدیم می کند، که در مرحله بعد فروشنده امضاءها را بررسی می نماید.

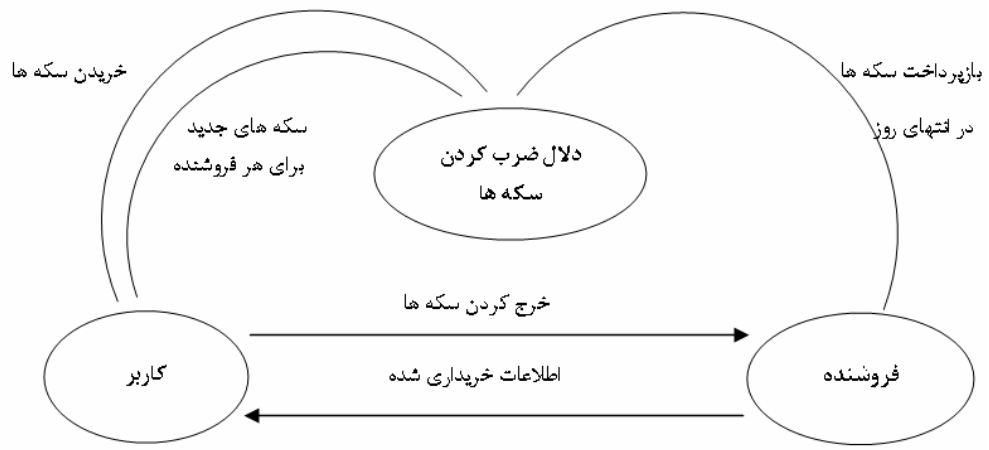
i امین پرداخت (برای $i= 1, 2, \ldots$) از کاربر به فروشنده شامل زوج (W_i, i) است، که فروشنده می تواند آنرا با استفاده از W_{i-1} ارزیابی نماید. این پرداختها نیاز به محاسبه ای توسط کاربر ندارد و فقط یک عمل درهم سازی توسط فروشنده را لازم دارد. در انتهای هر روز فروشنده آخرین مبلغ دریافت شده ($W_{i/i}$) از هر کاربر را به دلال گزارش می دهد و تعهدنامه متناظر هر کدام را نیز می فرستد. دلال، i تومان از حساب کاربر بر می دارد و به حساب فروشنده واریز می نماید.

مهمترین هدف سیستم Payword بهینه کردن و کمینه کردن ارتباط با دلال است این سیستم برای

زمانیکه یک کاربر درخواست های مکرر را از یک فروشنده می نماید، بسیار کارا و در بقیه حالات نسبتاً کارا می باشد. ضمناً عملیات مربوط به کلید عمومی که مورد نیاز فروشنده است، فقط ارزیابی امضاءها را شامل می گردد که تقریباً کارا است.

۳,۲. سیستم پرداخت MicroMint

مدل MicroMint به همراه موجودیت های این مدل در شکل ۶ نشان داده شده است [۹، ۱۳].



شکل ۶: مدل سیستم MicroMint

اعتبار سکه های الکترونیکی، در گرو بانکی است که آنها را به طور دیجیتالی امضاء و یا ضرب نموده است. MicroMint روشی را اتخاذ نموده است که در آن سکه زدن توسط دلال ها صورت پذیرفته و تولید سکه (سکه زدن[۱۰۰]) برای سایر افراد بجز دلال ها محاسبات بسیار سخت و غیر ممکنی را در بر داشته باشد. هر چند ارزیابی سکه ها توسط هر کسی که صورت گیرد، کاملاً سریع و کارا است.

یک سکه MicroMint یک K-Way hash function collision است. در یک عمل هشنیگ در ارتباط با مقدار ورودی x مقدار y تولید می شود: H(x) = y، (one-way hash function) . بدین ترتیب تابع H مقدار x را به مقدار با طول معین y نگاشت[۱۰۱] می کند.

طبق تعریف هنگامیکه دو ورودی مختلف یک خروجی را تولید نمایند یک برخورد تابع هش اتفاق می افتد[۱۰۲].

$H(X_1) = H(X_2) = y$

بدست آوردن دو مقدار متفاوت که به یک مقدار نظیر y نگاشت شوند، بسیار مشکل است.

یک k- way hash function collision وقتی اتفاق می‌افتد که k تا ورودی متفاوت به یک خروجی مشابه اشاره[۱۰۳] کند:

$H(X_1) = H(X_2) = H(X_3) \ldots = H(X_K) = y$

بنابراین اگر K برابر ۴ باشد، یک سکه، یک Four-way hash function collision خواهد بود. اگر فرض شود که هر سکه دقیقاً ۱۰ تومان ارزش داشته باشد. سکهٔ C شامل چهار مقدار ورودی است که برخورد آنها در هنگامیکه تابع هش به کار برده شود، یک مقدار یکسان y را نگاشت می نماید.

$C = \{X_1, X_2, X_3, X_4\}$

در این سیستم در طی مراحل زیر یک سکه به راحتی ارزیابی می شود:

۱ـ انجام دادن چهار عملیات هش روی X_i ها، برای بدست آوردن مقدار مشابه y

$H(X_1) = H(X_2) = H(X_3) = H(X_4) = y$

۲ـ اطمینان حاصل کردن از اینکه X_i ها مقادیر متفاوتی هستند.

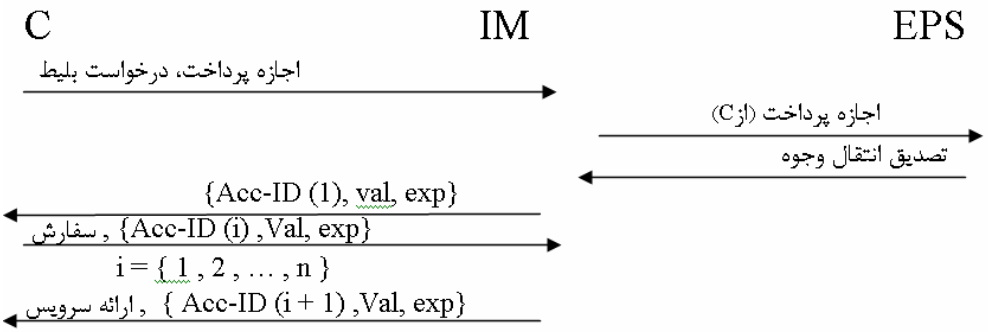
۳ـ ارزیابی سکه ها فقط در جهت تائید اعتبار سکه ها به کار برده می شود و به عنوان عاملی برای تشخیص دوباره خرج کردن[۱۰۴] نیست.

یک عملیات خرید در این سیستم، بوسیله ارسال سکه (ها) به همراه درخواست خرید، به یک فروشنده شکل می گیرد (شکل ۳,۶). اگر فرض کنیم ارزش هر سکه دقیقاً ۱ سنت باشد به علت آنکه تعداد معینی از آن می‌تواند جهت خرید استفاده شود، پس خرد کردن سکه ها[۱۰۵] در این سیستم منتفی است.

۳,۳. سیستم پرداخت SubScrip

در شکل ۷ پروتکل کلاسیک سیستم SubScrip مشاهده می شود [۷].

مشتری (C) دارای حسابی با Eps می باشد، بطوریکه پشتیبانی مالی مشتری توسط Eps صورت می گیرد. بنابراین مشتری با مراجعه به IM تقاضای بلیط[۱۰۶] می نماید و اجازه پرداخت دریافت شده از Eps را به او می دهد. IM با ارسال اجازه پرداخت دریافت شده از مشتری به Eps، وجود پول در حساب مشتری که در نزد Eps است را چک می‌کند. Eps پس از دریافت اجازه پرداخت و معتبر شناختن آن، مشتری و حسابش را تصدیق می نماید.



شکل ۷: پروتکل سیستم کلاسیک SubScrip

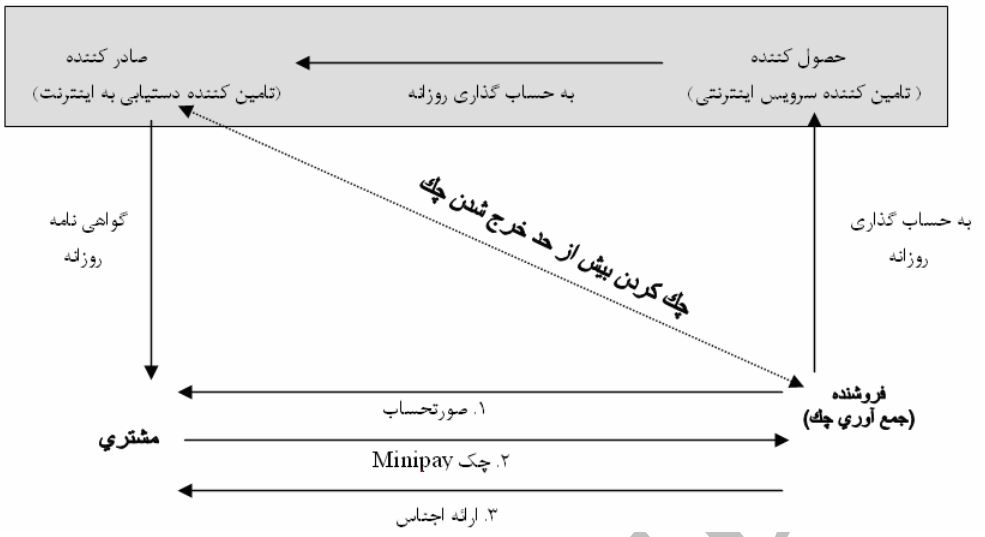
در این مرحله انتقال وجه از Eps به IM شکل گرفته و وجه مذکور در حساب تخصیص یافته به مشتری (توسط IM) قرار می گیرد. حال بلیط توسط IM شکل گرفته و به مشتری فرستاده می شود. مشتری سفارش خود را به همراه بلیط دریافت شده به IM فرستاده، آنگاه IM، حساب مشتری را بطور محلی چک می کند، تا ببیند که آیا معتبر است یا خیر.

سپس متناسب با سرویسی که به مشتری ارائه می‌دهد، مبلغ مورد نظر را از موجودی مشتری کم نموده و یک شناسه حساب جدید برای مشتری تولید می نماید. بدین ترتیب بلیط جدیدی با شناسه حساب و مقدار جدید شکل گرفته و به همراه سرویس درخواست شده برای مشتری فرستاده می شود. مشتری می تواند باقی مانده حساب خود را در خریدهای بعدی از فروشنده، تا قبل از تاریخ انقضاء خرج نماید. همچنین مشتری می تواند بلیط دریافتی را به همراه آدرس فروشنده تا نیاز بعدی خرید، در دیسک سخت رایانه خود ذخیره نماید.

در این پروتکل با وجود آنکه از مکانیزم های رمزنگاری[۱۰۷] و امضای دیجیتال[۱۰۸] استفاده نشده است، در عین حال امکان دستکاری مشتری در بلیط وجود ندارد، چراکه که کلیه مقادیر در پایگاه داده ها نزد فروشنده ثبت شده است. در عین حال این امکان وجود دارد که رباینده ای در هنگامیکه بلیط از فروشنده به سمت مشتری فرستاده می شود آن را استراق سمع نماید، که در اینصورت می تواند آن را جهت گرفتن سرویس مورد استفاده قرار دهد. و این از خطرات موجود در این سیستم است.

لازم به ذکر است که شناسه حساب (ACC-ID) فقط در نزد یک فروشنده منحصر به فرد معتبر می باشد.

۳ . ۴ . سیستم پرداخت Mini-Pay



شکل ۸: مراحل تراکنش پرداخت در سیستم Minipay

تراکنش پرداخت در این سیستم که در شکل ۸ مشخص شده است، شامل مراحل زیر است [۸ , ۵].

الف ـ مشتری در هر روز گواهی نامه تأیید شده و پول قابل خرج روزانه اش[۱۰۹] را در زمان Login از صادرکننده (IAP) دریافت می نماید.

ب ـ با کلیک کردن مشتری بر روی وب سایت فروشنده یک سفارش پرداخت[۱۱۰] تولید و توسط مشتری امضاء می شود. سفارش پرداخت امضاء شده به همراه گواهی نامه امضاء شده توسط صادرکننده به فروشنده ارسال می‌شود.

ج ـ فروشنده گواهی نامه و امضاء روی آن را ارزیابی نموده، کلید عمومی مشتری را از آن استخراج کرده و دستورالعمل مربوط به محدودیت خرید غیربلادرنگ[۱۱۱] در گواهی نامه را چک می کند.

د ـ اگر محدودیت خرج روزانه مشتری به اتمام رسیده باشد، فروشنده فوراً اطلاعات درخواست شده را بر گردانده و سفارش پرداخت را بصورت غیربلادرنگ ذخیره می‌نماید.

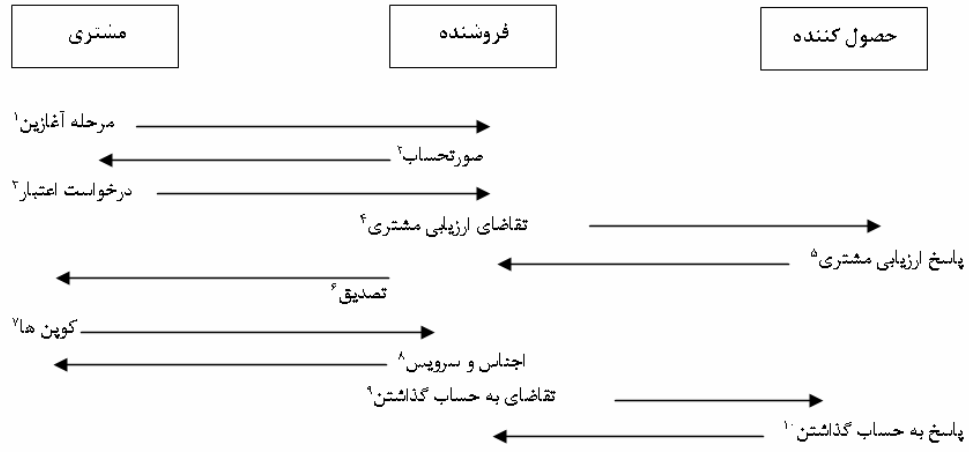
ه ـ اگر محدودیت خرج روزانه مشتری به اتمام رسیده باشد، فروشنده با صادرکننده ارتباط برقرار می نماید تا مجدداً سفارش پرداخت را تصدیق کند. صادرکننده می‌تواند عمل تصدیق یا عدم تصدیق را انجام دهد.

ی ـ در انتهای هر روز فروشنده مجموع سفارشات پرداخت را برای عمل به حساب گذاری[۱۱۲] به حصول کننده ارسال می کند. حصول کننده همگی سفارشات پرداخت های فروشندگان را جمع آوری و برای به حساب گذاری به صادرکننده ارسال می نماید.

ر ـ هر روز در زمان Login که مشتری به صادرکننده (IAP) خود مراجعه می کند، بالانس حسابها و مجموع خریدهای روز قبلش را امضاء می نماید.

۳,۵. سیستم پرداخت Mykro- ikp

در این سیستم مراحل تراکنش شبیه شکل ۹ و شامل موارد زیر است [۹ , ۵]:



شکل ۹: تراکنش های مطرح در سیستم M- 3kp

الف- مرحله آغازین: در این مرحله مشتری تراکنش پرداخت را آغاز می نماید. مشتری شناسه خود، ریشه زنجیره مبالغ پرداختی ارزش هر کوپن، مجموع کوپن ها در زنجیره، کلید عمومی گواهی نامه اش و یک عدد تصادفی را به فروشنده می فرستد.

ب- مرحله ارسال صورتحساب[113]: پاسخ فروشنده شامل شناسه فروشنده، شماره تراکنش (شناسه تراکنش)، تاریخ و زمان حال است که به صورت آشکار[114]، و پیغام خلق شده توسط فروشنده به مشتری و یک عدد تصادفی است که این دو بصورت امضای دیجیتال شده (پنهان) به مشتری فرستاده می شوند (پیغام خلق شده شامل مقدار و شرح مال التجاره است).

ج- درخواست اعتبار[115]: مشتری درخواست خود را که شامل تعداد کوپن ها (مجموع کوپن ها)، ارزش هر کوپن و شماره حساب خود (که SLIP نامیده می شود) است و با کلید عمومی حصول کننده رمز شده است را به فروشنده می فرستد.

د- درخواست ارزیابی[116]: درخواست تصدیق اعتبار مشتری بوسیله حصول کننده است.

ه- پاسخ به ارزیابی[117]: حصول کننده یک پاسخ امضاء شده که شامل اعتبار یا عدم اعتبار مشتری است را برای فروشنده ارسال می کند. پاسخ مثبت نشان دهنده تضمین اعتبار مشتری توسط حصول کننده است.

ی- تصدیق[118]: فروشنده پاسخ امضاء شده حصول کننده و همان عدد تصادفی اول (که توسط مشتری فرستاده شده بود) را برای مشتری می فرستد. وجود عدد تصادفی اول در تصدیق نشان دهنده پذیرفته شدن پاسخ تصدیق است.

ر- پرداخت های مبالغ کم[119]: در این مرحله مشتری می تواند تراکنش های پرداخت خود را به دفعات تا زمانیکه کوپن هایش تمام شود، به انجام رساند.

ز- درخواست به حساب گذاشتن[120]: در این مرحله فروشنده از حصول کننده تقاضای بازپرداخت می نماید.

ژ- پاسخ به درخواست[121]: پیغامی امضاء شده است که از جانب حصول کننده به فروشنده ارسال می گردد که نشان دهنده موفقیت یا عدم موفقیت باز پرداخت تراکنش های پرداخت است.

۳.۶. سیستم پرداخت Millicent

یکی از مطرح ترین سیستم های پرداخت برای مبالغ پایین است که از مدل پولی خاصی بنام گواهی نامه موقت[122] استفاده می کند. جزئیات این مدل در ذیل شرح داده شده است [۱۸، ۶، ۵].

در بررسی پروتکل ها مشخصه های زیر تعریف شده اند:

۱) Vendor - id: یک شناسه منحصر بفرد (یا نام) فروشنده است.
۲) props: هر داده ای که مشخصات مشتری را بیان کند (می تواند شامل نام مشتری باشد).
۳) Value: ارزش هر گواهی نامه است.
۴) exp: تاریخ انقضاء گواهینامه است.

۵) request: تقاضای مشتری است.

۶) reply: پاسخ فروشنده به مشتری است.

(معمولاً هر پاسخ با یک درخواست مطابقت دارد.)

رمزگواهی نامه مدیر: فقط برای فروشنده یا دلالی که گواهی نامه را تولید می کند، شناخته شده است.

۷) id# : از دو جزء تشکیل شده است:

الف - id-Series#: شناسه ای است که رمزگواهی نامه مدیر را مشخص می کند.

ب - id-Sequence #: شناسه ای است منحصر بفرد که شماره سریال را در بر می گیرد.

id# = id-Series#, id-Sequence#

۸) رمز مشتری مدیر: رمزی است که برای تولید رمز مشتری بکار می رود و فقط برای فروشنده و دلال (واسطه) شناخته شده است.

۹) Cust-id# : از دو جزء تشکیل شده است:

الف- Cust-id-Series#: شناسه ای است که رمز مشتری مدیر را مشخص می کند.

ب- Cust-id-Sequence#: شناسه ای منحصر بفرد است که به همراه cust-id-series#، مشتری را مشخص می کند.

cust-id# = cust-id-series#, cust-id-sequence#

customer-secret = H (cust-id#, master-customer-secret)

یک گواهی نامه با ترکیب تمامی فیلدهایی که در بالا عنوان شده اند، تولید می شود.

id-material = Vendor-id, id# , cust-id#

Cert-material = props, value, exp

Scrip-body = id-material, cert-material

Cert = H (scrip-body, master-scrip-secret)

Cert مشخص کننده اعتبار واقعی بودن بدنه گواهی نامه است.

Scrip = Scrip-body, cert

پروتکل های مطرح در این سیستم بصورت زیر است:

الف- پروتکل اول: حالت نا امن[۱۲۳]

در این حالت هیچگونه امنیت و حفاظتی صورت نمی گیرد.

Customer ⟶ Vendor: Scrip, request

Vendor ⟶ Customer: Scrip´, reply

ب- پروتکل دوم: حفظ اعتبار و محرمانگی[۱۲۴]

Customer ⟶ Vendor: Vendor-id, cust-id#, {scrip, request} Customer-secret

Vendor ⟶ Customer: Vendor-id, cust-id#, {scrip´, cert, reply} Customer-secret

Customer– secret در جهت تأمین محرمانگی[۱۲۵] واحراز هویت[۱۲۶] بکار برده می شود.

لازم به ذکر است که امکان رمزنگاری[۱۲۷] در سطح پایین تر برای بالا بردن کارایی وجود دارد. بطور مثال برخی از قسمتهای scrip´ می تواند به شکل آشکار[۱۲۸] فرستاده شود.

هر دو پیغام شامل cust-id# و Vendor-id آن هم بصورت آشکار است، و این اجازه را به دریافت کننده می‌دهد تا رمز مشتری را تولید نماید.

ج- پروتکل سوم حفظ اعتبار بدون محرمانگی[۱۲۹]

Customer ⟶ Vendor: Scrip, request, H (scrip, request, Customer- secret)

Vendor ⟶ Customer: Scrip´, reply, H (scrip´, cert, reply, Customer- secret)

گرچه همه پیغام ها به شکل آشکار فرستاده می شوند، اما بوسیله امضایی که روی رمز مشتری بنا نهاده شده است، حفاظت می شوند. در اینجا از رمزنگاری استفاده نمی شود. تعداد عملیات هشنیگ برای فروشنده در این حالت عبارتند از:

۱) برای چک کردن گواهی نامه قدیمی[۱۳۰]

۲) برای تولید مجدد رمزمشتری

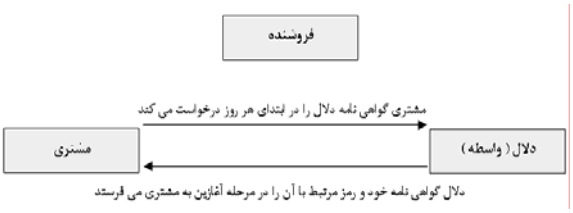
۳) برای چک کردن امضاء مشتری

۴) برای تولید گواهی نامه جدید

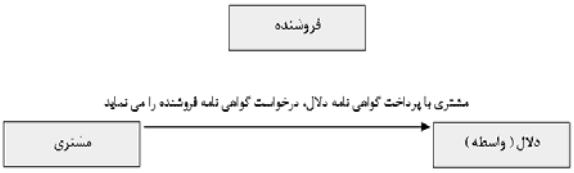
۵) برای امضاء کردن پاسخ

هر دو پیغام شامل cust-id# و Vendor-id به شکل آشکار (موجود در scrip´ و scrip) است که کاربرد آن در استخراج رمز مشتری توسط دریافت کننده آن است.

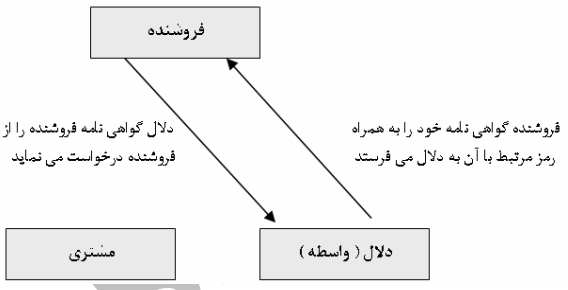
در اشکال زیر تعاملات و تراکنش های مطرح فیمابین مشتری، فروشنده و دلال نشان داده شده است.



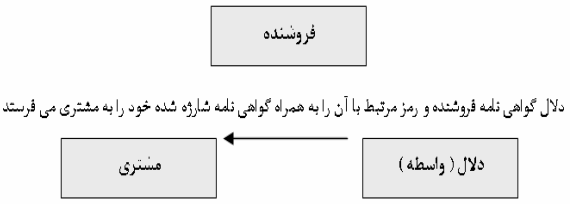
شکل ۱۰- الف: تراکنش های بین دلال و مشتری در مرحله آغازین



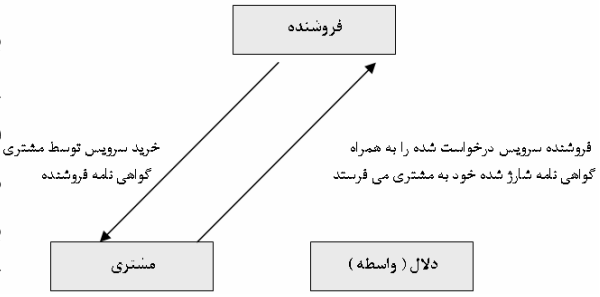
شکل ۱۰-ب: ادامه تراکنش های بین دلال و مشتری پس از مرحله آغازین



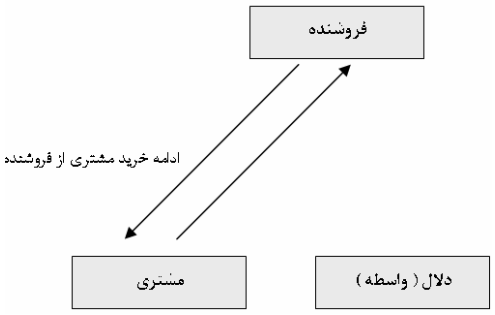
شکل ۱۱: تراکنش های بین دلال و فروشنده



شکل ۱۲: تراکنش های بین دلال و مشتری



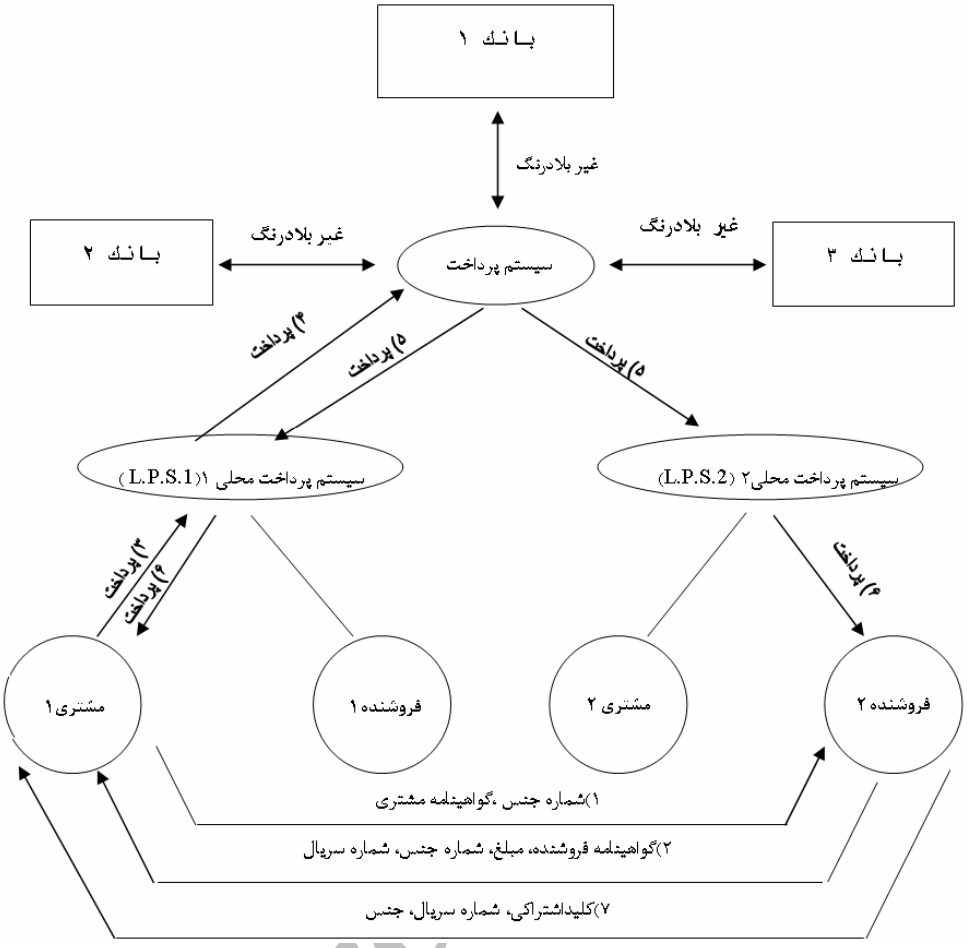
شکل۱۳: تراکنش های بین مشتری و فروشنده



شکل ۱۴: ادامه تراکنش های خرید بین مشتری و فروشنده

۳,۷. سیستم پرداخت Micro-Pay

این سیستم یک پروتکل مناسب جهت پرداخت الکترونیکی برای مبالغ پایین و برای خرید اطلاعات الکترونیکی و غیر الکترونیکی را مطرح ساخته است [۳,۴] بویژه با گسترش سرویس دهنده های ISP[۱۳۱] در ایران این سیستم می تواند با در نظر گرفتن ملزوماتی اندک در جهت انجام معاملات الکترونیکی مورد استفاده قرار گیرد. بعنوان نمونه، اگر سرویس دهنده ای بخواهد در ایران از طریق شبکه اینترنت تصاویر ماهواره ای یا روزنامه خود را به قیمت هر یک ۵۰ و یا ۱۰۰ تومان در اختیار کاربران شبکه قرار دهد، این پروتکل بسیار سودمند خواهد بود. در این پروتکل از تابع هش[۱۳۲] (H) استفاده شده است تا برای ورودی مانند M یک چکیده H(M) با طول ثابت (معمولاً ۱۲۸ بیت) را بوجود آورد. تابع هش بایستی دارای این خصوصیت باشد که امکان پیدا کردن دو ورودی مانند M و L که نتیجه هشنیگ آنها یکسان باشد، غیر ممکن باشد[۱۳۳]. همچنین در این سیستم در جهت ایجاد امضای الکترونیکی[۱۳۴] از الگوریتم های رمزنگاری نامتقارن و متقارن[۱۳۵] استفاده شده است. نمای {T}priv-x جهت ایجاد امضای الکترونیکی روی T با استفاده از کلید خصوصی عنصر x بکار می رود که طبیعتاً افرادی که به کلید عمومی x یعنی pub-x دسترسی دارند می توانند اصالت امضای فوق را احراز نمایند. همچنین E_K نشاندهنده رمزنگاری متقارن است که در آن K کلید به اشتراک گذاشته شده بین خریدار و فروشنده یا هر دو موجودیت دیگر می تواند باشد. در شکل ۱۵معماری و تراکنشهای مطرح در این سیستم مشاهده می شود.



شکل۱۵: معماری و تراکنش های سیستم Miro-Pay

۳،۷،۱. بررسی موجودیت های پروتکل در سیستم Micro- Pay

الف- مشتری[۱۳۶]: همانطور که در قسمت های قبل توضیح داده شد، مشتری موجودیتی است که در یک تجارت الکترونیکی تقاضای جنس یا اطلاعاتی را از فروشنده می‌کند.

ب- فروشنده[۱۳۷]: همانطور که در قسمت های قبل توضیح داده شد، فروشنده موجودیتی است که سرویس یا اطلاعاتی را به مشتری ارائه می کند.

ج- سیستم پرداخت[۱۳۸]: در این پروتکل ارتباط مالی تمامی قسمت ها با بانک ها از طریق سیستم پرداخت شکل می گیرد. سیستم پرداخت می تواند یک شرکت معتبر باشد که با تمامی بانک ها حساب دارد. همچنین این سیستم می‌تواند نزد تمامی بانک ها اعتبار مالی داشته باشد (وجود سیستم های پرداخت یکی از ملزومات پیاده سازی پروتکل در ایران است). لازم به ذکر است که صدور گواهی نامه های رسمی برای فروشنده ها، مشتریان و سیستم های پرداخت محلی[۱۳۹]، می تواند از طریق همین سیستم های پرداخت صورت بگیرد.

اگر حساب یک سیستم پرداخت محلی (که می تواند یک ISP باشد) از X مقدار کمتر باشد، سیستم پرداخت ´X تومان از بانک مربوط به آن سیستم پرداخت محلی پول به حساب وی می ریزد. بنابراین فرض بر این است که هر سیستم پرداخت محلی با حداقل یک بانک مرتبط و نزد آن حساب دارد. فرض دیگر اینکه برداشتن پول از حساب سیستم پرداخت محلی از بانک توسط سیستم پرداخت، می‌تواند بصورت غیربلادرنگ[۱۴۰] باشد، بطوریکه اگر حساب یک سیستم پرداخت محلی از x مقدار کمتر شد، سیستم پرداخت پیامی در این زمینه برای سیستم پرداخت محلی بفرستد و این موضوع را اطلاع دهد و سپس سیستم پرداخت محلی چک مربوط به مبلغ مورد نظر را صادر و به سیستم پرداخت ارائه دهد

تا آن ضمن مراجعه غیربلادرنگ با بانک آن را نقد کند. چنانچه امکان ارتباط بلادرنگ[۱۴۱] برای وصول پول با بانک وجود داشته باشد، باز هم سیستم پرداخت می تواند با ارسال پیامی به سیستم پرداخت محلی مجوزی از آن برای برداشت پول از حسابش از بانک را دریافت کند. طبیعی است که این مجوز را باید به بانک ارائه نماید. این نوع ارتباطات می توانند بصورت بلادرنگ شکل بگیرند. همچنین اگر حساب یک سیستم پرداخت محلی[۱۴۲] (ISP) از y مقدار بیشتر شد، سیستم پرداخت ´y تومان به بانک مربوط به آن سیستم پرداخت محلی (ISP) پول به حسابش واریز می نماید.

د- سیستم های پرداخت محلی[۱۴۳]: مشتریان و فروشندگان نزد سیستم پرداخت محلی (local p.s.) های خود) حساب دارند، که با توجه به اینکه مبالغ پرداخت چندان بالا نیست(در سطح Micro Payment است) این فرض می تواند درست باشد. البته سیستم های پرداخت محلی نزد سیستم های پرداخت حساب دارند و برقراری حساب ها می تواند بصورت غیربلادرنگ و یا مراجعه حضوری شکل بگیرد.

سیستم های پرداخت محلی می توانند دو سرویس را تأمین نمایند:

الف) سرویس دسترسی به اینترنت

ب) سرویس پرداخت

این دو نوع سرویس می تواند از پورت های جداگانه شکل بگیرد. در این صورت این امکان وجود خواهد داشت که شخصی از جایی دیگر به اینترنت وصل شود، ولی نزد سیستم پرداخت محلی دیگر حساب داشته باشد. بنابراین سیستم پرداخت محلی خود را می تواند برای پرداخت استفاده نماید. بدین ترتیب سیستم های پرداخت محلی می‌توانند سرویس رایگان پرداخت را فراهم نمایند. توجه شود که سیستم های پرداخت محلی می توانند سرویس دهندگان ISP باشند.

ه- **بانک ها**: بانک ها همان موجودیت هایی هستند که ارتباط مالی همگان با آنها برقرار است. در این پروتکل سیستم پرداخت با تمامی بانک ها حساب و با همگی آنها ارتباطات مالی دارد. در این پروتکل امکان ارتباط غیربلادرنگ بین آنها فرض شده است.

برای اینکه مشتری۱ بتواند جنس از فروشنده۲ خریداری نماید، سه مرحله کاری بایستی شکل گرفته باشد (برای حفظ پیچیدگی کار و نشان دادن مراحل تراکنش، بصورت کاملتر، فرض بر این است که مشتری۱ می خواهد از فروشنده ۲ خرید نماید):

۱) مشتری۱ حسابی نزد سیستم پرداخت محلی۱ باز کرده و پولی در آن واریز نموده است. بدین ترتیب رسیدی در این رابطه دریافت کرده است. اینکار می تواند با مراجعه حضوری مشتری۱ به سیستم پرداخت محلی۱ عملی گردد.

۲) همانطور که قبلاً ذکر شد، فروشنده۲ بایستی نزد سیستم پرداخت محلی۲ حساب داشته باشد. این حساب می تواند بصورت غیربلادرنگ (مثلاً مراجعه حضوری) شکل بگیرد.

۳) فرض بر این است که مرجعی رسمی که در اینجا خود سیستم پرداخت فرض شده است. گواهی نامه[۱۴۴] صادر می‌نماید. این گواهی نامه شامل کلید عمومی درخواست کننده، مشخصات صاحب گواهی (نام مشتری یا نام فروشنده یا شناسه آنها) و شامل تاریخ انقضاء گواهی نامه است.

Cert-Info = ID-PS, ID-User, Au, pub-U, E
Cert = cert-Info, {H (cert-Info)}priv-ps

ID-PS: شناسه سیستم پرداخت

ID-User: شناسه استفاده کننده گواهی نامه که می تواند مشتری و یا فروشنده باشد.

AU: آدرس استفاده کننده گواهی نامه یا آدرس الکترونیکی استفاده کننده گواهی نامه

pub-U: کلید عمومی استفاده کننده گواهی نامه

E: تاریخ انقضاء گواهی نامه

گواهی نامه با کلید خصوصی سیستم پرداخت درجهت حفظ تمامیت و احراز هویت امضاء دیجیتال می شود.

مراحل مختلف تراکنش در این سیستم در شکل ۱۵ نشان داده شده است.

الف- مراحل تقاضا: با نگاهی به شکل ۱۵ مراحل ۱ و ۲ را در نظر می گیریم. در مرحله ۱ مشتری به کمک مرورگر[۱۴۵] خود صفحه تار جهان گستر[۱۴۶] فروشنده را شناسایی کرده و پس از بررسی صفحه مربوطه جهت گرفتن سرویس یا جنس، شناسه جنس[۱۴۷] و گواهی نامه

خود را برای فروشنده می فرستد. در مرحله ۲ هم فروشنده گواهی نامه خود[۱۴۸]، مبلغ جنس[۱۴۹]، شناسه جنس و شماره معامله[۱۵۰] را برای مشتری می فرستد. بدین ترتیب تقاضای پرداخت پول جنس را می نماید. در نظر گرفتن شماره سریال معامله که در شروع کار (مرحله تقاضا) فروشنده به مشتری می فرستد، برای این است که در انتهای تراکنش برای هر دو (مشتری و فروشنده) مشخص شود که کدام معامله صورت پذیرفته است.

1) Customer Send to Merchant: ID-goods, Cert-p_1
2) Merchant Send to Customer: Serial-number, ID-goods, Amount, Cert-M_2, {H(Serial-number, Amount, ID-goods)} priv-M_2

ب- مراحل پرداخت: مراحل ۳ تا ۶ به مراحل پرداخت و وصول پول و واریز پول به حساب فروشنده تعلق می گیرد. در تمامی مراحل پرداخت بین موجودیت های نشان داده شده در شکل ۱۵ رد و بدل پیام انجام می گیرد، با این تفاوت که در هر مرحله پرداخت توسط یکی از موجودیت ها امضاء دیجیتال صورت می پذیرد.

پرداخت شامل اجزاء زیر است:

Payment = ID-P, ID-M, Serial-number, ID-goods, Amount

توجه شود که شناسه مشتری[۱۵۱] و شناسه فروشنده[۱۵۲] هر کدام عددی چند رقمی (مثلاً ۱۰ رقمی) بایستی در نظرگرفته شوند، که مثلاً ۴ رقم اول آن برای تشخیص سیستم پرداخت محلی و رقم های بعدی آن در جهت تشخیص مشتری و یا فروشنده از بین مشتریان یا فروشندگان یک سیستم پرداخت محلی به کار رود.

بدین ترتیب مراحل ۳ تا ۶ عبارتند از:

3) Payment, {H(payment)}priv-p1
4) Payment, {H(payment)}priv-local p.s.1
5) Payment, {H(payment)}priv-payment system
6) Payment, {H(payment)}priv-local p.s.2
   Payment, {H(payment)}priv-local p.s.1

ج- مرحله وصول جنس: در این مرحله فروشنده پس از دریافت پرداخت ازسیستم پرداخت محلی مربوط به خود (که در نزد آن حساب دارد) جنس مورد نظر را برای مشتری می‌فرستد. در این مرحله چنانچه فرستادن جنس به صورت الکترونیکی مد نظر باشد، فروشنده می تواند از رمزنگاری کلید اشتراکی[۱۵۳] استفاده نماید.

7) Merchant Send to Customer: E_K (Goods), {K}pub-p1, {H(serial-number, K)}priv-M

۴. مقایسه و تحلیل

در جدول ۱ تفاوت ها و شباهت های سیستم های پرداخت الکترونیکی مذکور مشخص شده است [۵ ، ۳]. از میان سیستم های مذکور سه سیستم Mykro-ikp، Payword، MicroMint و Micor-Pay در وضعیت پیشنهاد[۱۵۴] و سیستم های Mini-Pay و Millicent در وضعیت آزمایش عمومی[۱۵۵] اند. همه سیستم های مذکور از لحاظ سایز پرداخت[۱۵۶] برای مبالغ کم[۱۵۷] بنا نهاده شده اند. مدل پرداخت در سیستم های Millicent، Mykro-ikp، MicroMint و Paywordبصورت شبه پول مستقیم[۱۵۸]، در سیستم Mini-Pay بر مبنای حساب مستقیم[۱۵۹] و در سیستم Micro-Pay از نوع مدل مبتنی بر حساب از طریق خریدار[۱۶۰] است. تعیین اعتبار[۱۶۱] در اکثریت سیستم ها بصورت غیر بلادرنگ[۱۶۲] است، با این تفاوت که دو سیستم Mini-Pay، Millicent و Micro-Pay دارای تعیین اعتبار شبه بلادرنگ[۱۶۳] است؛ چراکه در سیستم Millicent اکثریت تراکنش هایی که بین فروشنده و مشتری و برخی تراکنش های مربوط به دلال (واسطه) می تواند بصورت بلادرنگ انجام گیرد. در سیستم Mini-Pay نیز محدودیت خرج کردن پول توسط مشتری می تواند بصورت بلادرنگ توسط فروشنده ارزیابی شود. همچنین در سیستم Micro-Pay برداشت پول از حساب مشتریان در سیستم های پرداخت محلی و یا برداشت پول از حساب سیستم های پرداخت محلی در سیستم های پرداخت و واریز آن به حساب فروشندگان و یا سیستم های پرداخت محلی، می تواند بصورت بلادرنگ[۱۶۴] یا غیر بلادرنگ انجام پذیرد. بطور کلی اکثریت سیستم های پرداخت برای مبالغ کم دارای تعیین اعتبار غیر بلادرنگ هستند که این امر گرچه خطرات[۱۶۵] زیادی را ممکن است در عملیات تراکنش های مالی بهمراه داشته باشد، ولی خود منجر به کاهش ترافیک شبکه در یک زمان خاص می گردد.

کنترل محرمانگی[۱۶۶] در اکثریت سیستم های مذکور در نظر گرفته نشده است به نحویکه تمامی

سیستم های فوق فاقد خاصیت های اختفاء[۱۶۷] و غیر قابل ردیابی کردن[۱۶۸] هستند، گرچه در برخی از این سیستم ها نظیر Mini-Pay و Millicent امکان توسعه و حرکت به سمت محرمانگی با استفاده از مکانیزم های خاص امکان پذیر است.

بلحاظ مکانسیم های امنیتی، در سیستم Millicent کلمات رمز[۱۶۹] و توابع هشنیگ[۱۷۰] و سطوح امنیتی مختلف در نظر گرفته شده است. این سیستم از لحاظ امنیتی می تواند به عنوان یک سیستم کارا طراحی و پیاده سازی شود. در سیستم MicroMint نیز استفاده از توابع هش تدارک دیده شده است، در ضمن امکان استفاده از رمزنگاری کلیدعمومی[۱۷۱] با توسعه پروتکل امکان پذیر شده است. این سیستم برای تولید سکه ها از برخورد[۱۷۲] توابع هش استفاده می نماید. در سیستم Payword هم از توابع هش و زنجیره[۱۷۳] مبالغ پرداختی و امضای دیجیتال[۱۷۴] استفاده شده است. سیستم Minipay علاوه بر استفاده از مکانیسم توابع هش و امضای دیجیتال از مکانیسم تولید گواهی نامه[۱۲] هم استفاده می نماید. ضمناً این سیستم با استفاده از تعیین اعتبار بلادرنگ محدودیت خرید[۱۷۵] مشتری را چک می نماید و از لحاظ مکانیسم های امنیتی نمونه ای از سیستم های کارا در این دسته است. در سیستم Micro-Pay نیز استفاده از امضای دیجیتال و تابع هشینگ در جهت تمامیت و احراز هویت، و رمزنگاری متقارن و نامتقارن بصورت ترکیبی در جهت حفظ محرمانگی در نظر گرفته شده است.

دراکثریت سیستم های پرداخت برای مبالغ کم به علت استفاده از ارزیابی های غیربلادرنگ ریسک برای هر دو طرف معامله یعنی مشتری و فروشنده وجود دارد. هزینه تراکنش ها در اکثریت این سیستم ها به علت استفاده از مبالغ کم در سطح پایین است. از میان سیستم های مذکور فقط سیستم Minipay هزینه سرباری را به علت ارتباطات و رمزنگاری در نظر گرفته شده در بر دارد.

برخی از سیستم های مذکور نیازمند وجود نرم افزارهای خاص به منظور قرارگرفتن به عنوان میانجی[۱۷۶] بین مرورگر مشتری و وب سرور فروشنده اند. از آنجمله می‌توان سیستم های Millicent،Minipay و Payword را نام برد.

اکثریت سیستم های مورد مقایسه فوق مدل پولی پول نقد[۱۷۷] را استفاده می نمایند. بجز سیستم Minipay و Micro-Pay که از چک الکترونیکی استفاده می کند.

اکثریت سیستم های مذکور دارای خاصیت توسعه پذیری اند. با توجه به هزینه تراکنش ها و مکانیسم های امنیتی در نظرگرفته شده پروتکل های اکثریت آنها قابل اطمینان[۱۷۸] است.

با نگاهی به جدول ۲ در قسمت درون سازگاری[۱۷۹] و خواص آن تفاوت های میان این سیستم ها آشکار می گردد. بر این اساس کلیه سیستم های مذکور فاقد خاصیت دوسویه بودن[۱۸۰] و خرج مجدد پول[۱۸۱] اند. برخی از این سیستم ها گردش پول[۱۸۲] در سطح جهانی و برخی گردش پول محلی را پشتیبانی می کنند. در برخی با توسعه پروتکل ها خواص تطابق و تقبل[۱۸۳] و گردش پول در سطح جهانی ممکن می گردد.

تأمل در قسمت امنیت از جدول مذکور تفاوت های آشکار خواص امنیتی در سیستم های مورد مقایسه را مشخص می نماید. بلحاظ خاصیت جلوگیری از خرج دوباره پول[۱۸۴] سیستم MicroMint فاقد این خاصیت است و مابقی سیستم های مذکور این خاصیت را پشتیبانی می نمایند. ضمناً تمامی سیستم های مذکور دارای امکان جلوگیری از جعل پول[۱۸۵] هستند.

در اکثریت سیستم های مذکور انجام پرداخت بصورت اتوماتیک (بدون ایجاد وقفه در گرفتن اطلاعات از کاربر) است و تأخیر بسیار کمی را در عملیات خرید ایجاد می‌نمایند. تقریباً تمامی سیستم های مذکور بجز سیستمهای MicroMint و Micro-Pay وابسته به سخت افزار ویژه اند. ضمناً در اکثریت سیستم های فوق پول الکترونیکی به گذشت زمان نامعتبر می گردد.

۵- نتیجه گیری

سیستم های رایج در امر پرداخت های الکترونیکی برای مبالغ پائین مورد بررسی و بحث قرار گرفت. همچنین این سیستم ها بر حسب ویژگی های مطرح تحلیل و مقایسه شدند و نقاط ضعف و قوت هر کدام به

همراه مزایا و معایب آنها مشخص شد. انتخاب یک سیستم از میان این سیستم ها در امر تجارت الکترونیک با در نظر گرفتن ملاحظات و ویژگی های مطرح شده و مورد درخواست امکان پذیر می‌باشد. نتیجه گرفته شد که اکثریت سیستم های مطرح شده قابل توسعه بوده و با در نظر گرفتن بستر مناسب، سیاست های حاکم، امکانات در دسترس، موجودیت های معتبر و شرایط (امنیتی، حقوقی و محرمانگی) مد نظر قابل انتخاب و استفاده و بهره برداری اند.

جدول ۱: مقایسه بین سیستم های پرداخت بررسی شده [۵ ، ۳].

نام سیستم/ خواص	Micro-Pay	Mykro-ikp	Mini-Pay	Payword	MicroMint	Millicent
منشاء تاریخی	Arash Rahman	Waidnre, M.et al.from IBM	A. Herzberg, IBM, Haifa	Rivest and Shamir	Rivest and shamir	M. Maneasse, S. Glassman of Digital Equipment.
وضعیت	طرح پیشنهادی سال ۱۳۸۱ شمسی	طرح پیشنهادی سال ۱۹۹۷	اتمام آزمایش سال ۱۹۹۸	طرح پیشنهادی سال ۱۹۹۵	طرح پیشنهادی سال ۱۹۹۶	آزمایش عمومی بعد از دسامبر ۱۹۹۷
سایز پرداخت	پرداخت مبالغ کم	پرداخت مبالغ کم	پرداخت مبالغ کم	پرداخت مبالغ کم	پرداخت مبالغ کم	پرداخت مبالغ کم
مدل پولی	چک الکترونیکی (Notational)	پول الکترونیکی (Token)	چک الکترونیکی (Notational)	پول الکترونیکی (Token)	پول الکترونیکی (Token)	پول الکترونیکی (Token)
مدل پرداخت	مبتنی بر حساب از طریق خریدار	احتمالاً شبه پول مستقیم	مبتنی بر حساب مستقیم	شبه پول مستقیم	شبه پول مستقیم	شبه پول مستقیم، پول محلی، مشتری در نزد واسطه حساب منعقد می‌کند .
تعیین اعتبار	شبه بلادرنگ، برداشت پول از حساب مشتریان در سیستم های پرداخت محلی و یا برداشت پول از حساب سیستم های پرداخت محلی در سیستم های پرداخت و واریز آن به حساب فروشندگان و یا سیستم های پرداخت محلی، می تواند بصورت بلادرنگ یا غیر بلادرنگ انجام پذیرد.	غیر بلادرنگ	شبه بلادرنگ، ارتباط با بانک با چک شدن محدودیت خرید بصورت بلادرنگ انجام می گیرد.	غیر بلادرنگ	غیر بلادرنگ	شبه بلادرنگ، اکثریت واکنش هایی که شامل مشتری و فروشنده می شوند بصورت بلادرنگ و برخی از آنها که دلال را شامل می شود هم بصورت بلادرنگ می‌تواند باشد .
کنترل محرمانگی	فاقد خاصیت اختفاء و قابل ردیابی کردن است.	موجود نیست	فاقد خاصیت اختفاء است و قابل ردیابی کردن است، همه پرداخت ها امضاء می شوند، نیاز به استفاده از ساختارهای SSL دارد.	فاقد خاصیت اختفاء است و قابل ردیابی است و چندان محرمانگی ندارد.	موجود نیست	توسعه پذیر به سمت محرمانگی فاقد خاصیت اختفاء است، قابل رد یابی است.
مکانیسم امنیتی	استفاده از امضای دیجیتال و تابع هشینگ در جهت تمامیت و احراز هویت، و رمزنگاری متقارن و نامتقارن بصورت ترکیبی در جهت حفظ محرمانگی	زنجیره مبالغ، امضاء دیجیتال و رمزنگاری کلید عمومی	امضاء دیجیتال، استفاده از گواهی نامه و توابع هش	زنجیره مبالغ پرداختی، امضاء دیجیتال	استفاده از کلید عمومی، توابع هش و برخورد	استفاده از کلمه رمز، استفاده از توابع هش، استفاده از امنیت عمومی در سطوح مختلف
لازمه امر	وجود سیستم پرداخت به عنوان یک مرجع رسمی معتبر برای صدور گواهی نامه و سیستم های پرداخت محلی که در نزد سیستم پرداخت اعتبار داشته باشند.	حصول کننده بایستی پاسخ ارزیابی مشتری را به فروشنده بفرستد .	نیاز به نرم افزار Mini Pay برای فروشنده و مشتری است .	نرم افزار Payword Wallet بین جستجوگر مشتری و وب سرور فروشنده بصورت نماینده عمل می کند.	ضرب کردن سکه ها توسط واسطه صورت می پذیرد و میان مشتری و فروشنده عمل می نماید .	نرم افزار سرور فروشنده (Millicent Wallet) میان جستجوگر فروشنده و وب سرور بازرگان بصورت نماینده عمل می نماید .
خطر	برای مشتری، اما در سطح بسیار کم	خیلی کم	مشتری و فروشنده اما خیلی ضعیف	مشتری و فروشنده	?	مشتری
هزینه ها	کم	کم	کم، رمزنگاری و ارتباطات کمی سربار ایجاد می نماید.	کم	کم	کم

جدول ۲: مقایسه بین سیستم های پرداخت برای مبالغ پائین [۵ ، ۳].

سیستم / نیازمندیها	MilliCent	MicroMint	Payword	Mini-Pay	Mykro-ikp	Micrp-Pay
سیستم پول الکترونیکی (Token)	بله	بله	بله	خیر	بله	خیر
امنیت						
جلوگیری از خرج دوباره پول	بله	خیر، اما امکان تشخیص خرج دوباره پول برای دلال وجود دارد.	بله	-	بله	-
جلوگیری از جعل کردن	بله	بله	بله	بله	بله	بله
جلوگیری از بیش از حدخرج شدن	-	-	**بله**	خیر، محدویت خرج بیش از حدپول می‌تواند شکل بگیرد.	بله	-
جلوگیری از انکار کردن	بله	-	بله	بله	-	بله
اختفاء	خیر	امکان پذیر	خیر	خیر	خیر	خیر
غیرقابل ردیابی	خیر	امکان پذیر	خیر	خیر	خیر	خیر
درون سازگاری						
خردکردن	خیر، اما تغییر ممکن است.	خیر، سایزپرداخت به گونه ای مناسب درنظر گرفته می شود که نیازی به خردکردن پول نیست.	خیر، سایزپرداخت به گونه ای مناسب درنظر گرفته می شود که نیازی به خردکردن پول نیست.	-	خیر، سایزپرداخت به گونه ای مناسب درنظر گرفته می‌شود که نیازی به خردکردن پول نیست.	خیر، سایزپرداخت به گونه ای مناسب درنظر گرفته می شود که نیازی به خردکردن پول نیست.
دوسویه بودن	خیر	خیر	خیر	خیر	خیر	خیر
خرج مجددپول	خیر	خیر	خیر	خیر	خیر	خیر
تطابق و تقبل	پول محلی	خیر	امکان پذیر	بله	امکان پذیر	امکان پذیر
پشتیبانی از گردش پول	بله ، بوسیله دلالان امکان پذیراست.	خیر	امکان پذیر	بله	امکان پذیر	امکان پذیر
توسعه						
توسعه پذیری	بله	بله	بله ، چون غیربلادرنگ است.	بله	بله	بله
عملیات غیربلادرنگ	بله ، قسمتی	بله	بله	بله ،بیشتراوقات	بله	بله

پیامدهای اقتصادی					
خیر،پیشنهاد است	خیر،پیشنهاد است	خیر،آزمایشی است	خیر، پیشنهاد است	خیر، پیشنهاد است	خیر، آزمایشی است
-	-	امکان پذیر	-	امکان پذیر	امکان پذیر
برای مشتری، اما در سطح بسیار کم	خیلی کم	بله، اجناس ممکن است فرستاده نشوند.	بله	بله	خیر
خیلی کم	خیلی کم	بله، مشتری ممکن است پول را بیش از حدخرج کند.	بله اما خیلی کم	بله	بله
بله	بله	بله	-	قسمتی	بله
بله	بله	بله	بله	-	بله
سادگی کار					
بله	بله	پرداخت بصورت اتوماتیک انجام می‌شود.	بله	بله	بله
بله	بله	بله	بله	بله	بله
بله	بله	بله	بله	بله	بله
خیر	خیر	خیر	خیر	خیر	خیر
بله	بله، امکان پذیراست	بله، امکان پذیراست	-	بله، امکان پذیراست	بله، امکان پذیراست
خیر	بله	بله	بله	خیر، برای جلوگیری از جعل و تقلب سخت افزارهای ویژه لازم است.	بله

ادامه جدول ۲

منابع

[۱] شهرام بختیاری،"طراحی و پیاده سازی سیستم پرداخت الکترونیکی در اینترنت"، گزارش اول، پژوهشکده الکترونیک، دانشگاه صنعتی شریف، ۱۳۷۹.

[۲] شهرام بختیاری، "پرداخت مبالغ کم از طریق اینترنت"، پژوهشکده الکترونیک، دانشگاه صنعتی شریف، ۱۳۷۹.

[۳] آرش رحمان، " تجزیه و تحلیل و طراحی سیستم های پرداخت الکترونیکی برای مبالغ پائین"، تز کارشناسی ارشد، دانشگاه آزاد اسلامی واحد جنوب، زمستان ۱۳۸۰.

[۴] آرش رحمان، شهرام بختیاری، "طراحی یک سیستم پرداخت الکترونیکی برای مبالغ پایین"، کنفرانس ملی مهندسی برق، دانشگاه آزاد اسلامی واحد نجف آباد، تهران، ایران. اسفند ۱۳۸۶.

[5] R.Weber, "Electronic Payment Systems Features",

URL:http://medoc.informatik.tu-muenchen.de/Chablis/mstudy/x-a-marketpay.html, 1998.
[6] S. Glassman, M. Manasse, M. Abadi, p. Gauthier, and P. Sobalvarro, "The Millicent protocol for Inexpensive Electronic Commerce White papers", 2000.
[7] A. furche, G. Wrightson, "Subscrip An efficient protocol for pay-per-view payments on the Internet, 1996.
[8] A. Herzberg and H. Yochai, "Minipay: Charging per Click on the web", 1998.
[9] Y. Karaaslan, "DVA-Seminar SS2000-Micropayment Systems, Millicent, ikp, MicroMint", 2000.
[10] Lucas de Carvalho Ferreira, Ricardo Dahab, Brasil, "A Scheme for Analyzing Electronic Payment Systems", 1998.
[11] Ronald L.Rivest, "Electronic Lottery Tickets as Micropayments", 1997.
[12] Ellis chi, "Evaluation of Micropayment", 1997.
[13] R.L.Rivest and A.Shamir, "Payword and Micropayment: Two Simple Micropayment Schems", MIT Labratory for Computer Science, NOV 1995.
[14] Paul J.M.Havinga, Gerard j.m.Smit, Arne Helme, "Survey of Electronic payment methods And Systems", 1997.
[15] Anthony Leong, "A Survey of Electronic payments Systems", 2000.
[16] N.Asokan, phil janson, Michael Steiner, Michael Waidner, "Electronic Payment Systems ", IBM Research Division, Zurich Research Laboratory, 1998.
[17] Thomi Pilioura, " Electronic Payment Systems on open Computer Networks: A Survey, 1998.
[18] Bob Palmer, "Closer Look: the Millicent Micropayment System", CEO of Digital Equipment Corporation, 2000.
[19] Dr.Philip M.Hallam Baker, "Electronic payment schemes", 1995.
[20] Li Gong, "Collisionful keyed hash functions with Selectable Collisions", 1994.
[21] R.j.Anderson and t.m.A.Lomas, "Fortifying key negotiation schemes with poorly chosen passwords", 1994.
[22] "How does ecoin Micropayment System work", URL:
http://www.ecoin.net/help/operation.htm
[23] "Internet keyed payment protocols (ikp)", URL:http://www.zurich.ibm.com:80/technology/security/extern/ecommerce/ikp-overview.htm
[24] "What is Ecommerce?", URL: http://www.ecommerce.com

زیرنویس ها

[1] .Electronic Payment Systems
[2] . Electronic Micropayment Systems
[3] Economical
[4]. Payment Size
[5]. Macro Payment Systems
[6]. Small Payment Systems
[7]. Micro Payment Systems
[8]. Fraction of cont
[9]. Ease of Use
[10]. Technical
[11]. participants
[12]. Payer
[13]. Payee
[14]. Issuer
[15]. Service provider
[16]. Acquirer
[17]. Broker
[18]. Observer
[19]. Certificate
[20]. Register
[21]. Money Models
[22]. Credit base
[23]. Notational
[24]. Cash based or token based
[25]. Direct Cash Like
[26]. Token
[27]. Deposit
[28]. Direct Account Based
[29]. Redeem
[30]. Indirect push Account Based
[31]. Indirect pull Account Based
[32]. Validation
[33]. Online
[34]. Offline
[35]. Semi-Online
[36]. Security Mechanisms
[37]. pass phrase
[38]. Verifier
[39]. Authorizer
[40]. Shared key
[41]. Signature
[42]. Blind Signature
[43]. Traceability
[44]. Anonymity
[45]. Chained Hash
[46]. Requirements
[47]. Transaction
[48]. Atomicity
[49]. Transfer of Funds
[50]. Complete Transfer
[51]. Consistency
[52]. Correct
[53]. Isolation
[54]. Durability
[55]. Commit

[56]. Recoverable
[57]. Log files
[58]. Security
[59]. No Double Spending
[60]. Token
[61]. No Counterfeiting
[62]. No Overspending
[63]. Non-Refutability
[64]. Hardware Tamper Resistance
[65]. Privacy
[66]. Confidentiality
[67]. Anonymity
[68]. Untraceability
[69]. Interoperability
[70]. Divisibility
[71]. Token based
[72]. Bidirectionality
[73]. payment
[74]. Respendability
[75]. Acceptability
[76]. Multicurrency Support
[77]. Flexibility
[78]. Scalability
[79]. Micro Economy
[80]. Low Cost
[81]. payment size
[82]. Efficiency
[83]. Bottle neck
[84]. General Economy
[85]. Operational
[86]. Large User Base
[87]. Low Risk
[88]. Reliability
[89]. Conservation
[90]. Store
[91]. Retrieve
[92]. Unobstusiveness
[93]. Low Latency
[94]. Hardware Independence
[95]. Low Transaction Costs
[96]. Link
[97]. Browser
[98]. User-Specific
[99]. Vendor-Specific
[100]. Mints Coins
[101]. Map
[102]. A Hash Function Collision
[103]. MAP
[104]. Double spending
[105]. Divisibility
[106]. Ticket
[107]. Encryption
[108]. Digital Signature
[109]. Daily Spending
[110]. Payment Order
[111]. Offline
[112]. Clearing and Deposit
[113]. Invoice
[114]. Clear
[115]. Credit Request
[116]. Authorization Request
[117]. Authorization Response
[118]. Confirm
[119]. Micropayments
[120]. Clear Request
[121]. Clear Response
[122]. Scrip
[123]. In the clear (insecure)
[124]. Authentic and private

[125]. Privacy
[126]. Authenticity
[127]. Encryption
[128]. Clear
[129]. Authentic but not private
[130]. Scrip
[131]. Internet Service Provider
[132]. Hash Function
[133]. Collision-freeness
[134]. Digital Signature
[135]. Unsymmetric and Symmetric Encryption
[136]. Customer or Payer
[137]. Merchant or Payee
[138]. Payment System
[139]. Local Payment System
[140]. Offline
[141]. Online
[142]. Local Payment System
[143]. Local payment systems
[144]. Certificate
[145]. Browser
[146]. Web Page
[147]. ID-goods
[148]. Cert-M
[149]. Amount
[150]. Serial-number
[151]. ID-P
[152]. ID-M
[153]. Shared Key Encryption
[154]. Proposal
[155]. Public Trial
[156]. Payment Size
[157]. Micropayment
[158]. Direct Cash Like
[159]. Direct Account base
[160]. Indirect Push Account Based
[161]. Validation
[162]. Offline
[163]. Semi-offline
[164]. Online
[165]. Risks
[166]. Privacy Control
[167]. Anonymous
[168]. Untraceable
[169]. Passphrase
[170]. Hash Function
[171]. Public Key Encryption
[172]. Collision
[173]. Chained
[174]. Signature
12. Certificate
[175]. Spending Limits
[176]. Proxy
[177]. Token
[178]. Reliable
[179]. Interoperability
[180]. Bidirectionality
[181]. Respendability
[182]. Multi Currency
[183]. Acceptability
[184]. Double Spending
[185]. Counterfeiting

کارگاه‌های آموزشی مرکز اطلاعات علمی

آموزش نرم‌افزار Word برای پژوهشگران

روش تحقیق کمی

آموزش مهارت‌های کاربردی در تدوین و چاپ مقالات ISI