



بنگاه ملی فناوری اطلاعات
بنک مرکزی جمهوری اسلامی ایران



شرکت ملی انفورماتیک
Mahdigreen Corporation

اولین همایش بین المللی بانکداری الکترونیک و نظام های پرداخت
تهران - ۳۰ بهمن و اول اسفند ۱۳۹۰ - مرکز همایش های برج میلاد



بانکداری الکترونیک
و نظام های پرداخت

ebps/90-213

سیستم بومی پرداخت *iWallet*

سیستمی کاربردی جهت پرداختهای الکترونیکی خرد در ایران

مهدی محمدی، کارشناس ارشد فن آوری اطلاعات و مدیریت دانشگاه امیرکبیر، mahdigreen@gmail.com

چکیده:

لازمه تحقق تجارت الکترونیک از نوع شخص به شخص، وجود سیستم پرداخت الکترونیک کارآمد می باشد، اما متأسفانه هیچ یک از سیستمهای فعلی پرداخت الکترونیک ایران، از تجارت نوع P2P و C2C پشتیبانی ننموده و یا کاربردی نیستند؛ لذا کمبود سیستم بومی پرداخت الکترونیک که در گام نخست بر بستر بانکی موجود، نقاط ضعف سیستمهای پرداخت الکترونیک فعلی را پوشش دهد و در گام بعدی، مسیر تحقق تجارت الکترونیکی را هموار سازد، به شدت احساس می شود.

از اینرو در این مقاله به معرفی سیستم پرداخت بومی *iWallet* (Internet Wallet) جهت پرداختهای P2P خواهیم پرداخت. این سیستم بر بستر بانکی موجود، محیطی ساده و در عین حال امن جهت پرداختهای P2P فراهم می آورد.

با بکارگیری این سیستم، هر وبلاگ می تواند محیطی جهت فروش محصولات و خدمات آنلاین گردد، همچنین بستر مناسب جهت راه اندازی حراجیهای آنلاین مهیا می گردد.

مقدمه:

هر یک از مدل‌های تجاری رایج در دنیا، سیستم پرداخت الکترونیک خاص خود را طلب می نماید، به عنوان مثال سیستم پرداخت الکترونیک مناسب برای تجارت B2B لزوماً جهت تجارت B2C مناسب نمی باشد.

از سیستمهای پرداخت الکترونیک رایج در ایران می توان از موارد زیر نام برد:

کارت‌های اعتباری (عابر بانک)، بانکداری الکترونیک (حواله اینترنتی)، انتقال وجه از طریق ATM و پرداخت الکترونیک قبوض نام برد.

البته هیچ یک از این سیستمها، مناسب همه مدل‌های تجارت الکترونیک نمی باشند. در جدول ۱ رابطه بین سیستم های پرداخت الکترونیک رایج در ایران و مدل‌های مختلف تجارت نشان داده شده است.

| سیستم پرداخت / مدل تجارت | کارتهای اعتباری (عابر بانک) | بانکداری الکترونیک (حواله اینترنتی) | انتقال وجه از طریق ATM | پرداخت الکترونیک قبوض |
|--------------------------|-----------------------------|-------------------------------------|------------------------|-----------------------|
| B2B | × | √ | × | × |
| B2C | √ | × | √ | × |
| C2C- P2P | × | × | √ | × |
| B2A | × | × | × | × |
| C2A | √ | × | × | √ |

(جدول ۱) - مقایسه سیستمهای پرداخت و مدلهای تجارت الکترونیک

موانع موجود در سیستمهای پرداخت الکترونیک ایران

- موانع قانونی و بوروکراسی: مدیران فروشگاههای مجازی جهت دریافت MerchantID میبایست علاوه بر ارائه جواز فعالیت، شرایط سختگیرانه عقد قرارداد با بانک را پذیرفته و چند میلیون سفته نزد بانک به امانت گذارند.
- موانع فنی: اتصال به درگاه پرداخت الکترونیک و انطباق آن با فروشگاههای مجازی نیازمند کدنویسی و تنظیمات امنیتی می باشد که تخصص خاص خود را می طلبد.
- محدود بودن به مدل تجاری B2C: از میان سیستمهای پرداخت الکترونیک فقط سیستم انتقال وجه از طریق ATM و حواله اینترنتی به نوعی از تجارت P2P و C2C پشتیبانی می نماید.

سیستم پرداخت بومی (iWallet) Internet Wallet

جدول ۱ نشان می دهد که هیچ یک از سیستمهای فعلی پرداخت الکترونیک ایران، از تجارت نوع P2P و C2C پشتیبانی نمی کنند و یا کاربردی نیستند؛ لذا در طراحی سیستم پرداخت بومی *iWallet* سعی شده است در گام نخست بر بستر بانکی موجود، نقاط ضعف سیستمهای پرداخت الکترونیک فعلی را پوشش دهد و در گام بعدی، مسیر تحقق تجارت الکترونیکی را هموار سازد.

این سیستم بر بستر بانکی موجود، محیطی ساده و در عین حال امن جهت پرداختهای P2P فراهم می آورد. با بکارگیری این سیستم، هر وبلاگ می تواند محیطی جهت فروش محصولات و خدمات آنلاین گردد، همچنین بستر مناسب جهت راه اندازی حراجی های آنلاین مهیا می گردد.

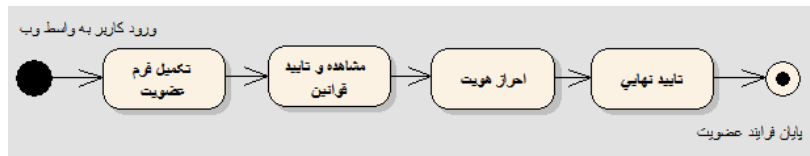
معرفی سیستم iWallet

در طراحی این سیستم که اساس آن بر سیستم های پرداخت حساب مرکزی بنا نهاده شده است سعی شده است با تجمیع ویژگی های مثبت سیستم های فعلی و در نظر داشتن شرایط کنونی ایران، از قبیل بستر بانکی، فرهنگ IT و شرایط اقتصادی، سیستمی بومی جهت پرداخت های P2P (شخص به شخص) ارائه گردد.

پروتکلها:

ایجاد حساب جدید

فرآیند عضویت در سیستم و ایجاد حساب کاربری ساده و محدود به چهار مرحله می باشد که در شکل ۱_ به تصویر کشیده شده است.



(شکل ۱) - عضویت

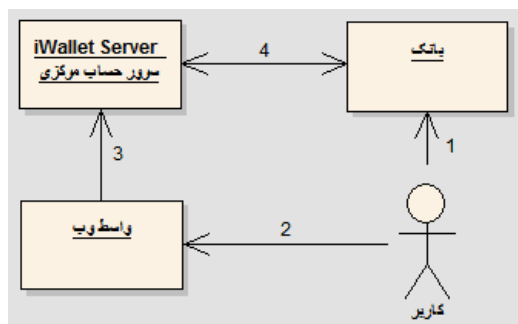
- ۱- **تکمیل فرم عضویت:** کاربر می بایست اطلاعاتی همچون نام، آدرس پستی، شماره تماس، آدرس ایمیل و شماره حساب بانکی نزد یکی از بانکهای جمهوری اسلامی ایران را به سیستم ارائه نماید.
- ۲- **قوانین و مقررات:** در این مرحله کاربر لیستی از قوانین و مقررات مربوط به عضویت و استفاده از سیستم را مشاهده می نماید. پس از قبول این قوانین و مقررات مرحله دوم عضویت به پایان می رسد.
- ۳- **احراز هویت:** در این مرحله مدیر سیستم، اطلاعات ورودی کاربر را بررسی نموده و از طریق تلفن، موبایل و یا شماره حساب بانکی، هویت کاربر را احراز می نماید.
- ۴- **تایید نهایی:** در این مرحله کاربر از طریق پیام کوتاه (SMS)، تلفن و یا ایمیل از فعال شدن حساب خود آگاه می شود.

متدهای واریز پول به حساب

جهت واریز پول به حساب کاربری و در حقیقت شارژ نمودن کیف پول اینترنتی کاربر می تواند از متدهای متفاوتی بهره گیرد که در ادامه به تفصیل مرور خواهند شد.

حواله بانکی

به کمک این متد کاربر می‌تواند کیف پول اینترنتی خود را از طریق حواله بانکی شارژ نماید. شکل ۲ سناریو این متد را به تصویر کشیده است.



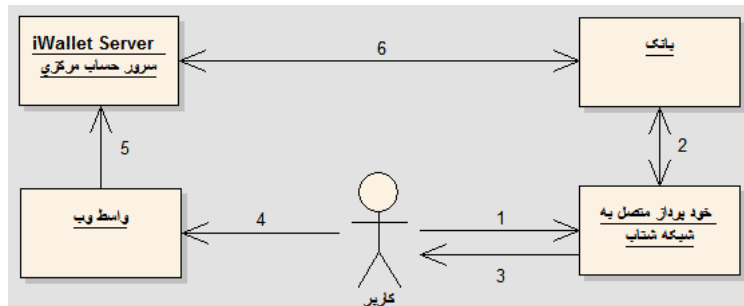
(شکل ۲) - حواله بانکی

- ۱- کاربر، مبلغ مورد نظر را به شماره حساب بانکی سیستم کیف اینترنتی، واریز می‌نماید (حواله بانکی)
- ۲- کاربر شماره فیش را در واسط وب وارد می‌نماید.
- ۳- شماره فیش به سرور *iWallet* جهت بررسی و تایید ارسال می‌گردد.
- ۴- با بهره‌گیری از بستر بانکداری الکترونیک موجود، سرور *iWallet* صحت و سقم شماره فیش را بررسی می‌نماید و در صورت تایید، کیف پول اینترنتی کاربر را شارژ می‌نماید.

کارت عابر بانک (انتقال وجه از طریق خودپرداز)

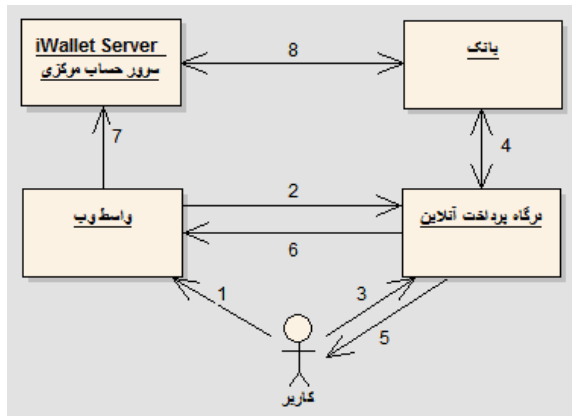
این متد برای کاربران این امکان را فراهم می‌نماید که بطور ۲۴ ساعته بدون نیاز به مراجعه به شعب بانک و تنها با مراجعه به یکی از دستگاه‌های خودپرداز متصل به سیستم شتاب از طریق امکان انتقال وجه (کارت به کارت) کیف پول اینترنتی خود را شارژ نمایند.

شکل ۳ مراحل عمل را به تصویر کشیده‌است.



(شکل ۳) - انتقال وجه از طریق خودپرداز

- ۱- کاربر به دستگاه خودپرداز مراجعه می‌نماید، مبلغ مورد نظر و شماره کارت متعلق به سرور *iWallet* را وارد می‌نماید.
- ۲- دستگاه خودپرداز با اتصال به شبکه شتاب وجه مورد نظر را از حساب بانکی کاربر کسر و به حساب بانکی سرور *iWallet* اضافه می‌نماید.
- ۳- شماره تراکنش (شماره فیش) به کاربر ارائه می‌گردد.
- ۴- کاربر شماره فیش را در واسط وب وارد می‌نماید.
- ۵- اطلاعات جهت بررسی و تایید در اختیار سرور *iWallet* قرار می‌گیرد.
- ۶- پس از بررسی صحت شماره فیش، از طریق بانکداری الکترونیک، کیف پول اینترنتی کاربر شارژ می‌گردد.



(شکل ۴) - پرداخت اینترنتی

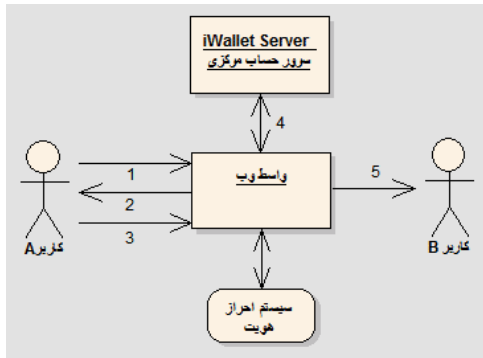
کارت اعتباری (کارت عابر بانک)

علاوه بر متدهای ذکر شده کاربران قادرند کیف پول اینترنتی خود را از طریق درگاه پرداخت آنلاین سامان، پاریسان، ملت و دیگر درگاه‌های موجود، شارژ نمایند. شرح عملیات در شکل ۴_ به تصویر کشیده شده است

- ۱- کاربر وارد واسط وب می‌شود و درخواست شارژ از طریق درگاه پرداخت آنلاین می‌دهد.
- ۲- کاربر به درگاه پرداخت بانگ مورد نظر هدایت می‌شود (Redirect)
- ۳- کاربر اطلاعات کارت اعتباری (عابر بانک با امکان پرداخت اینترنتی) خود را از قبیل شماره کارت، تاریخ انقضاء و مبلغ مورد نظر را وارد می‌نماید
- ۴- درگاه پرداخت با اتصال به شبکه شتاب، وجه مورد نظر را از حساب بانکی کاربر کسر و به حساب بانکی سرور *iWallet* اضافه می‌نماید.
- ۵- شماره رسید دیجیتالی به کاربر ارائه می‌گردد
- ۶- کاربر به واسط وب هدایت می‌گردد (Redirect)
- ۷- اطلاعات در سرور *iWallet* ذخیره می‌گردد.
- ۸- صحت اطلاعات از طریق اتصال به API درگاه بررسی می‌گردد، در صورت صحت اطلاعات، کیف پول اینترنتی کاربر شارژ می‌شود.

کارت‌های Prepaid

در صورت نیاز سیستم قابلیت شارژ توسط کارتهای پیش پرداخت را نیز دارا می‌باشد.



متدهای برداشت از حساب

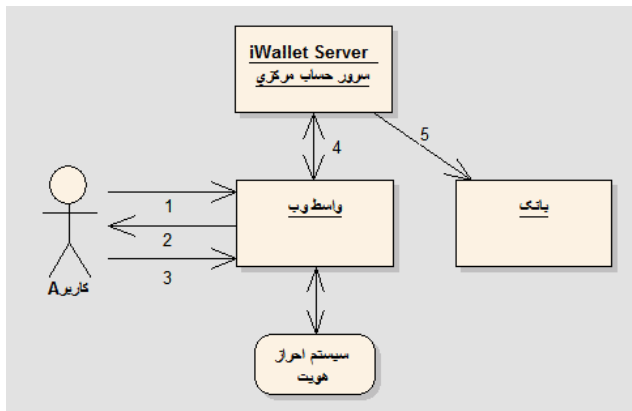
- انتقال پول به شخص دیگر

در حقیقت رسالت اصلی سیستم *iWallet* فراهم نمودن امکان انتقال وجه از کاربر A به کاربر B از طریق اینترنت می‌باشد. مراحل انتقال وجه در شکل ۵ آمده است.

(شکل ۵) - انتقال پول به شخص دیگر

- ۱- کاربر A پس از ورود به واسط وب تقاضای انتقال وجه از کیف پول اینترنتی خود به کیف پول اینترنتی کاربر B می‌نماید.
- ۲- واسط وب با کمک سیستم احراز هویت اقدام به احراز هویت کاربر A می‌نماید، لذا کد امنیتی ۱۰ رقمی را از طریق پیام کوتاه (SMS) یا ایمیل به کاربر A ارسال می‌نماید.
- ۳- کاربر A کد دریافتی را در واسط وب وارد می‌نماید.
- ۴- در صورت مثبت بودن فرایند احراز هویت، اطلاعات به سرور *iWallet* ارسال می‌گردد و از کیف پول اینترنتی کاربر A مبلغ مورد نظر کسر و به کیف پول اینترنتی کاربر B اضافه می‌گردد.
- ۵- کاربر B از طریق پیام کوتاه (SMS) و یا ایمیل از تراکنش انجام شده مطلع می‌گردد.

- واریز پول به حساب بانکی کاربر



کاربر می‌تواند پولهای کیف پول اینترنتی خود را به حساب بانکی خود منتقل نماید. این سرویس به صورت آنی صورت نمی‌پذیرد و نیاز به ۱ روز کاری زمان دارد. مراحل انجام فرآیند در شکل ۶ آمده است.

(شکل ۶) - واریز پول به حساب بانکی کاربر

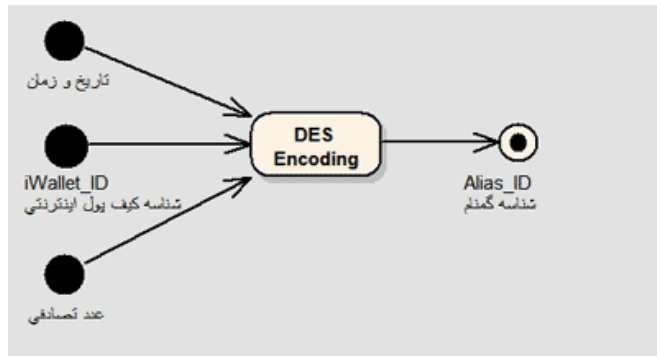
- ۱- کاربر پس از ورود به واسط وب، درخواست برداشت مبلغ مورد نظر و واریز آن به حساب بانکی خود را به ثبت می‌رساند.
- ۲- واسط وب با کمک سیستم احراز هویت اقدام به احراز هویت کاربر A می‌نماید، لذا کد امنیتی ۱۰ رقمی را از طریق پیام کوتاه (SMS) یا ایمیل به کاربر A ارسال می‌نماید.
- ۳- کاربر A کد دریافتی را در واسط وب وارد می‌نماید.
- ۴- اطلاعات به سرور مرکزی ارسال می‌گردد.
- ۵- وجه مورد نظر از حساب کاربر کسر و به حساب بانکی وی واریز می‌گردد.

پرداخت گمنام

اگر کاربر A می‌تواند هنگام انتقال پول از کیف اینترنتی خود به کیف اینترنتی کاربر B، گزینه پرداخت گمنام را انتخاب نماید، مشخصات و شماره کیف اینترنتی وی از دید کاربر B پنهان می‌ماند، در حقیقت کاربر B فقط شماره تراکنش را می‌بیند.

دریافت گمنام

کاربر B جهت دریافت پول از کاربر A می‌بایست شماره کیف پول اینترنتی خود را در اختیار کاربر A قرار دهد، اما در حقیقت هویت کاربر B در شماره کیف وی نهفته است، لذا جهت تحقق دریافت گمنام، کاربر B می‌بایست شناسه گمنام کیف خود را در اختیار کاربر A قرار دهد.

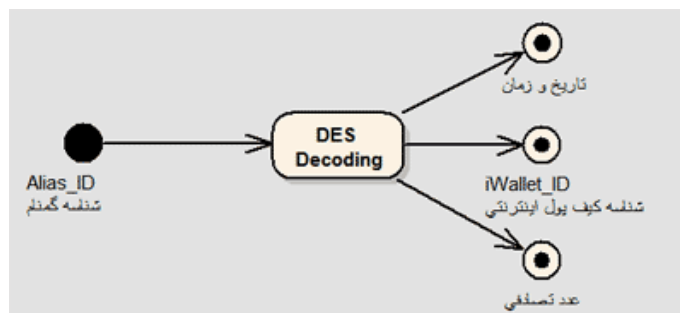


هر کاربر با مراجعه به واسط وب می‌تواند به تعداد مورد نیاز شناسه گمنام دریافت نماید. در حقیقت این شناسه‌های گمنام، شناسه مستعار (Alias) می‌باشد. (شکل ۷)

(شکل ۷) - تولید شناسه مستعار (گمنام)

پس از ثبت دستور پرداخت توسط کاربر A، سرور *iWallet* با رمز گشایی شناسه مستعار (Alias_ID) شماره اصلی کیف کاربر B را استخراج می‌نماید. (شکل ۸)

نکته: متغیرهای زمان و عدد تصادفی جهت بالا بردن امنیت و تضمین گمنامی مورد استفاده قرار می‌گیرد.



(شکل ۸) - استخراج شماره اصلی کیف از روی شناسه مستعار

سیستم احراز هویت

همانطور که در شکل ۵ و ۶ نشان داده شده است، سیستم احراز هویت در کنار واسط وب به انجام وظیفه می پردازد. عملیات های سیستم *iWallet* به دو دسته حساس و معمولی تقسیم می شوند. انتقال وجه به حساب شخص دیگر، برداشت پول از کیف پول اینترنتی و تغییر رمز از جمله عملیات های حساس می باشند اما ورود به حساب، چک نمودن موجودی و مشاهده گزارشات مالی، از عملیات های معمولی به شمار می آیند. سیستم احراز هویت هنگام انجام عملیات هایی از نوع حساس فعال می گردد و اقدام به شناسایی دقیق کاربر می نماید اما در موارد دیگر همچون ورود به سیستم، مشاهده موجودی، غیر فعال می باشد. این سیستم از طریق *email-Server* و یا *SMS-Server* کد تصادفی ده رقمی را به کاربر ارسال می نماید سپس کاربر با وارد نمودن این کد در واسط وب هویت خود را به اثبات می رساند. نکته: نحوه ارسال کد (از طریق پیام کوتاه و یا ایمیل) توسط کاربر در هنگام عضویت مشخص می شود.

بررسی نیازمندی های سیستم پیشنهادی

مدلهای پرداخت الکترونیک می بایست نیازمندیهای خاصی را برآورده نمایند تا بتوانند جایگزین سیستم های پرداخت سنتی شوند، اهم این نیازمندی ها عبارتند از:

(۱) امنیت

در *iWallet* امنیت از دو منظر مورد توجه قرار گرفته است

- از منظر ارتباطات: استفاده از ارتباط امن (SSL) تا حد قابل قبولی امنیت ارتباط را تضمین می نماید.
- از منظر نفوذ پذیری: معماری سه لایه در طراحی و پیاده سازی سیستم، خطر نفوذ پذیری سیستم را به حداقل می رساند و از طرفی اگر به هر نحوی رمز کاربر لو رود، سیستم احراز هویت از انجام تراکنش توسط نفوذگر جلوگیری می نماید.

(۲) گمنامی (Anonymity)

با استناد به امکان دریافت گمنام و پرداخت گمنام که در بخش پروتکل ها به تفصیل شرح داده شد می توان ادعا نمود سیستم *iWallet*، از ویژگی گمنامی برای هر دو طرف پرداخت پشتیبانی می نماید.

۳) سهولت استفاده

پروسه دریافت و پرداخت بسیار ساده و کوتاه می‌باشد به گونه‌ای که کاربر با ارائه شماره مشخصه کیف پول اینترنتی طرف مقابل می‌تواند وجه مورد نظر را به کیف وی انتقال دهد و از طرف دیگر گیرنده وجه بلافاصله از انجام تراکنش مطلع می‌گردد. همچنین سیستم احراز هویت با توجه به انتخاب کاربر از سیستم SMS و یا ایمیل بهره می‌گیرد، علاوه بر این، سیستم احراز هویت، فقط در مواقعی که عملیات از نوع عملیات حساس است مورد استفاده قرار می‌گیرد، لذا سیستم احراز هویت اثر منفی بر ویژگی سهولت استفاده از *iWallet* ندارد.

۴) قابلیت ردیابی

در سیستم *iWallet* حتی اگر تراکنش به صورت گمنام انجام شده باشد، در صورت لزوم با ارائه شماره تراکنش، تمامی اطلاعات پرداخت از جمله مشخصات طرفین پرداخت، میزان و تاریخ پرداخت، از بانک اطلاعاتی *iWallet* قابل دستیابی می‌باشد.

مزایا و کاربردها

استفاده از *iWallet* نیاز به نصب هیچ نرم افزار جانبی ندارد، فقط کافیسست که کاربر در این سیستم عضو شود سپس قادر خواهد بود با از طریق سیستم بانکی موجود به کیف اینترنتی خود پول واریز نماید و یا پول به کیف اینترنتی شخص دیگری انتقال دهد.

از ویژگی‌های این سیستم می‌توان به موارد زیر اشاره نمود:

- ۱) مناسب جهت اشخاص و شرکت‌های کوچک که شرایط دریافت MerchantID از بانک را ندارند.
- ۲) مناسب برای اشخاصی که قصد فروش محصولات و خدمات در سایت شخصی و یا وبلاگ خود دارند.
- ۳) سیستمی ساده و کاربردی بر پایه سیستم بانکی موجود ایران

کاربرد سیستم محدود به حوزه پرداخت P2P نمی‌باشد، دو مورد از کاربردهای سیستم *iWallet* در زیر آمده‌است.

۱) فروشگاه‌های آنلاین

با توسعه سیستم *iWallet* و طراحی یک سری API ویژه مدیران سایتهای استاتیک و داینامیک و همچنین وبلاگ‌ها، می‌توان امکان فروش آنلاین (B2C) را فراهم نمود.

۲) حراجی‌های آنلاین

از آنجایی که سیستم *iWallet* از پرداخت P2P به معنای واقعی آن پشتیبانی می‌نماید لذا بستری مناسب جهت راه‌اندازی حراجی آنلاین را فراهم می‌آورد.

جمع بندی و نتیجه گیری

با توجه به ویژگی‌های منحصر به فرد سیستم *iWallet* مانند قابلیت پیاده سازی، بر بستر بانکی فعلی ایران، از طرفی و از طرفی دیگر، فقدان سیستم پرداخت از نوع P2P، می‌توان نتیجه گرفت طراحی و پیاده سازی این سیستم می‌تواند گام موثری در راستای تحقق تجارت الکترونیک در ایران باشد.

منابع

- [1] Abrazhevich, D. (2001) Electronic Payment Systems: Issues of User Acceptance, In Stanford-Smith, B. and Chiozza, E. (Eds.), *E-work and E-Commerce*. IOS Press.
- [2] Yu, H.C., Hsi, K.H. and Kuo, P. J. (2002) 'Electronic payment systems: an analysis and comparison of types', *Technology in Society*, 24
- [3] Hurwicz, M. (2001) 'The Return of Micropayments', *Web Techniques*, 12, 2001.
- [4] Kniberg, H. (2002) 'What Makes a Micropayment Solution Succeed', Masters Thesis, Institution for Applied Information Technology, Stockholm, Sweden.
- [5] Simpson, B. (2004) 'What's Next for Electronic Payments?', *Collections & Credit Risk*, 9(3)
- [6] Shon, T.H. and Swatman, P.M.C. (1998) 'Identifying Effectiveness Criteria for Internet Payment Systems', *Internet Research: Electronic Networking Applications and Policy*, 8(3), pg 202-218.
- [7] Liao, Z. and Wong, W.K. (2004) 'The Sustainability of a Smartcard for Micro e-Payments', Australian Conference of Information Systems 2004, Tasmania, Australia.
- [8] Schwartz, E.I. (2001) 'Digital cash payoff', *Technology Review*, 104(10), pg 62-68.
- [9] Truman G. E., Sandoe, K. and Rifkin, T. (2003) 'An empirical study of smart card technology', *Information and Management*, 40(6)
- [10] Chau, P. and Poon, S. (2003) 'Octopus: An E-Cash Payment System Success Story', *Communications of the ACM*, 46(9)

- [11] Camenisch, J., Piveteau, J., and Stadler M. (1996) 'An efficient fair payment system', Proceedings of the 3rd ACM Conference on Computer and Communications Security, New Delhi, India.
- [12] Dai, X. and Grundy, J. (2006) 'NetPay: An off-line, decentralized micro-payment system for thin-client applications', Accepted for *Electronic Commerce Research and Applications*.
- [13] Herzberg, A. (2003) 'Payments and banking with mobile personal devices', *Communications of the ACM*, 46(5)
- [14] Juang, W.S. (2006) 'D-cash: A flexible pre-paid e-cash scheme for date-attachment', Accepted for *Electronic Commerce Research and Applications*.
- [15] Peha, J.M. and Khamitov, I. M. (2004) 'PayCash: a secure and efficient internet payment system', *Electronic Commerce Research and Applications*, 3(4)