
بسم الله الرحمن الرحیم

دانشگاه شاهد

دانشکده فنی و مهندسی

پایان‌نامه دوره کارشناسی ارشد مهندسی فناوری اطلاعات– مهندسی فناوری اطلاعات

استفاده از کارت شناسایی هوشمند ملی جهت افزایش امنیت در پرداخت سیار

محسن مقصودلو

استاد راهنما:

دکتر محمدعلی دوستاری

زمستان ۱۳۹۲

تأییدیّه هیات داوران

(برای پایان نامه)

اعضای هیئت داوران، نسخه نهائی پایان نامه آقای:

را با عنوان:

از نظر فرم و محتوی بررسی نموده و پذیرش آن را برای تکمیل درجه کارشناسی تأیید می‌کند.

اعضای هیئت داوران	نام و نام خانوادگی	رتبه علمی	امضاء
۱- استاد راهنما			
۲- استاد مشاور			
۳- استاد مشاور			
۴- استاد ممتحن			
۵- استاد ممتحن			
۶- نماینده گروه			

چکیده

استفاده از تلفن‌های همراه به دلیل قابلیت حمل، در دسترس بودن و سهولت استفاده بسیار فراگیر شده است. حتی در کشورهای جهان سوم، اکثر شهروندان از تلفن همراه استفاده می‌کنند. در نتیجه سرویس‌های قابل توجهی بر روی تلفن‌های همراه ارائه شده است که سرویس‌های مالی و بانکی نمونه-هایی از آنها می‌باشند. زیرساخت‌های ارتباطی و بانکی کشورها تاثیر به سزایی در ارائه سرویس‌های پرداخت سیار دارند؛ بنابراین بعضی از سرویس‌ها در تعدادی از کشورها قابل ارائه نیستند و یا با محدودیت‌هایی همراه هستند. همچنین در بعضی از کشورها امکانات و زیرساختهایی وجود دارد که باعث توسعه هر چه بیشتر این سرویس‌ها می‌شود. کارت شناسایی هوشمند ملی، نمونه‌ای از این فرصت‌هاست که در آینده نزدیک بین شهروندان ایران توزیع خواهد شد. در این پایان نامه سیستم پرداختی بر پایه کارت شناسایی هوشمند ملی ارائه شده که سازگار با زیرساخت‌های بانکی و ارتباطی ایران است و از پردازنده‌ی کارت شناسایی هوشمند ملی جهت انجام محاسبات رمزنگاری استفاده می‌کند. همچنین یک روش احراز هویت جدید بر مبنای کارت هوشمند ارائه شده است که خطر حمله تروجان‌ها و بدافزارها را کاهش می‌دهد که سایر سیستم های پرداخت سیار ارائه شده در جهان نسبت به چنین حملاتی آسیب پذیر هستند. در ادامه راهکاری برای افزایش کارایی فرایند احراز هویت ارائه شده است. در انتها، این سیستم پرداخت نسبت به فاکتورهای امنیت، هزینه و سهولت استفاده مورد تحلیل قرار گرفته و برای اثبات عملی بودن طرح، نسخه‌ای از این سیستم پرداخت پیاده سازی شده است.

کلید واژه: پرداخت سیار، کارت شناسایی هوشمند ملی، زیرساخت کلید عمومی، تجارت الکترونیک.

فهرست مطالب

صفحه

فهرست جدول‌ها

عنوان **صفحه**

فهرست شکل‌ها

فصل ۱– مقدمه

۱–۱– پیشگفتار

اینترنت محدوده گسترده‌ای از خدمات مانند نامه‌های الکترونیکی، انتقال فایل، و غیره را ارائه می‌دهد. یکی از محبوب ترین خدمات ارائه شده در اینترنت تجارت الکترونیکی است. تجارت الکترونیک در حال تبدیل شدن به بزرگترین موج تکنولوژیکی است که راه و روش‌های کسب و کار را تغییر داده است. بانکداری الکترونیکی و کسب و کار در اینترنت حوزه‌هایی هستند که در سال‌های اخیر رشد بی سابقه‌ای داشته‌اند.

بانکداری اینترنتی، نحوه استفاده مشتریان از سرویس‌های بانکی را تغییر داده است. آنها مجبور نیستند برای برداشت از حساب بانکی یا انتقال بین حساب‌های بانکی به ترمینال‌های ماشین‌های خود پرداز مراجعه کرده و یا در صف بانک در یکی از شعب بانکی بایستند. آنها به وب سایت بانک‌ها که سرویس های اینترنتی همانند برداشت پول از حساب مشتریان را فراهم می‌کنند مراجعه می‌کنند. هر چند که مشتریان نمی‌توانند پول نقد فیزیکی در دستان خود داشته باشند، اما آنها قادر به انتقال پول به کارت‌های الکترونیکی و استفاده از این کارت‌ها برای خرید کالا یا خدمات در فروشگاه‌ها می‌باشند. علاوه بر این، مشتریان قادر به پرداخت صورتحساب و یا برنامه‌ریزی برای پرداخت صورتحساب ماهانه با استفاده از خدمات بانکداری الکترونیکی هستند.

با توجه به انجام کسب و کار در اینترنت، در واقع، تجارت الکترونیک شیوه‌های سنتی را شبیه سازی و بهبود می‌بخشد به صورتی که مردم، کسب و کار و برقراری ارتباط با یکدیگر را به شکل الکترونیکی انجام می‌دهند. به عنوان مثال، نامه های الکترونیکی (ایمیل) جایگزین خدمات پستی شده‌اند، که در آن مردم مجبور به انتظار طولانی مدت برای تحویل نامه‌ها نیستند و تنها در عرض چند دقیقه این کار را به صورت الکترونیکی انجام خواهند داد. بسیاری از ویژگی‌های ایمیل مشابه به نامه کاغذی می‌باشد مانند امضای فرستندگان (دیجیتال)، مهر زمانی و یا بازگشت نامه در صورتی که گیرنده نتوانسته باشد آن را دریافت کند. ایمیل علاوه بر کاهش زمان، هزینه‌های سند و تحویل آن را نیز کاهش می‌دهد.

با توجه به ویژگی‌های کسب و کار، بسیاری از وب سایت‌های تجارت الکترونیکی، مشتریانِ خود را قادر می‌سازند تا کالاها و خدمات ارائه شده در فروشگاه مجازی آنها را از راه دور (از رایانه های شخصی خودشان) جستجو کنند. در این فروشگاه‌ها نه تنها کالاهای فیزیکی از قبیل کتاب و یا رایانه های شخصی ارائه شده، بلکه محصولات الکترونیکی مانند موسیقی، تصاویر دیجیتالی، کلیپ‌های ویدئویی و یا رمان های الکترونیکی نیز موجود می‌باشد. مشتریان به سادگی محصولات و یا خدمات مورد نظر را انتخاب می-کنند و هزینه آن را طریق کارت اعتباری یا کارت نقدی الکترونیکی پرداخت می‌نمایند. مهم تر از همه، این فروشگاه‌های مجازی در ۲۴ ساعت شبانه روز و ۷ روز هفته باز هستند.

محبوب‌ترین نوع از روش‌های پرداخت الکترونیکی، پرداخت با کارت اعتباری است. مطابقِ این روش، پس از انتخاب کالاهای مورد نظر از فروشگاه آنلاین، مشتری می‌تواند از طریق سیستم پرداخت با کارت‌های

اعتباری که توسط فروشگاه فراهم گردیده است به سادگی با پر کردن شماره کارت اعتباری و اطلاعات مربوط از قبیل تاریخ تولد و یا ارائه آدرس، پرداخت صورتحساب را انجام دهد. این اطلاعات به شرکت ارائه دهنده‌ی کارت اعتباری مشتری، برای بررسی اعتبار منتقل می‌شود. اگر درخواست مورد تایید قرار گرفت، کالا (در مورد کالا های الکترونیکی) و رسید مربوط به پرداخت، در عرض مدت کمی به مشتری انتقال داده می‌شود. اکثرا، این نوع از سیستم‌های پرداخت است از پروتکل SSL استفاده می‌کنند.

سیستم‌های پرداخت کارت اعتباری مانند SET (تراکنش امن الکترونیکی) تراکنش‌های پرداخت امن تری نسبت به طرح‌های پرداخت مبتنی بر SSL فراهم می‌کنند. در SET، علاوه بر داشتن یک کارت اعتباری معتبر، مشتری نیازمند به نصب نرم افزار SET (که کیف پول SET نامیده می‌شود) بر روی کامپیوتر خود می‌باشد. بعد از جستجوی کالا و خدمات در فروشگاه آنلاین که پروتکل SET را پشتیبانی می‌کنند، کیف پول SET بر روی رایانه مشتری نصب و فعال می‌شود. پس از پر کردن اطلاعات لازم پرداخت، کیف پول SET عملیات رمزنگاری بسیار امن، مانند عملیات رمزنگاری کلید عمومی را برای تولید درخواست خرید انجام می‌دهد. این درخواست به فروشگاه و شرکت کارت اعتباری مشتری برای مجوز پرداخت، منتقل می‌شود. پس از اخذ موافقت، مبلغ درخواستی از حساب مشتری به حساب فروشگاه منتقل و سپس مشتری در پایان تراکنش کالاهای مورد درخواست و رسید پرداخت مربوطه را دریافت می‌کند.

به نظر می‌رسد پرداخت با کارت‌های اعتباری یک روش ساده پرداخت برای کالاها یا خدمات در اینترنت است، زیرا بسیاری از مردم دارای کارت‌های اعتباری هستند و به طور منظم از آنها برای خرید کالا یا خدمات در فروشگاه‌های فیزیکی استفاده می‌کنند. با این حال، سیستم‌های پرداخت کارت اعتباری، به ویژه در سمت فروشنده هزینه‌های عملیاتی بالایی دارند؛ در نتیجه، پرداخت با کارت اعتباری برای معاملات با ارزش کم مناسب نیست. روش دیگر، روش پرداختی است که مناسب برای معاملات کم ارزش است و پرداخت خرد[1] نامیده می‌شود . بیشتر سیستم‌های پرداخت خرد از عملیات رمزنگاری با محاسبات کم و انتقال پیام ساده به منظور کاهش هزینه های عملیاتی استفاده می‌کنند. از میلی‌سنت[2]، پِی‌ورد[3] و پِی‌فر[4] می‌توان به عنوان نمونه‌هایی از این سیستم پرداخت نام برد.

اخیراً، معاملات تجارت الکترونیک، می‌تواند در حرکت انجام شود. ظهور فناوری‌های ارتباطی بی سیم، توانایی دسترسی به اینترنت را به منظور انجام معاملات تجارت الکترونیک از طریق دستگاه‌های سیار مانند تلفن‌های همراه، PDA ها و یا لپ تاپ‌ها ارائه می‌دهد. چنین دستگاه‌های سیاری از طریق مودم یا کارت شبکه بیسیم به اینترنت متصل می‌شوند و یا از طریق خطوط ارتباطی تلفن همراه مبادلات خود را انجام می‌دهند. این ویژگی‌ها تا حد زیادی به کاربران سهولت در انجام تراکنش‌های تجارت الکترونیکی در هر زمان از راه دور را ارائه می‌دهد. انجام تراکنش‌های الکترونیکی که در آن حداقل یکی از شرکت-

[1] Micropayment
[2] Milicent
[3] PayWord
[4] PayFair

کنندگان درگیر، یک کاربر متحرک[1] باشد تجارت سیار[2] نامیده می‌شود. از مزایای سیستم‌های پرداخت سیار می‌توان به غلبه بر محدودیت‌های زمان و مکان در هنگام خرید نام برد.

همچنین در کشورهای مختلف با توجه به زیرساخت‌هایی که در اختیار دارند، فرصتهایی برای توسعه تجارت الکترونیک و یا پرداخت سیار وجود دارد. نمونه‌ی این فرصت در ایران کارت شناسایی هوشمند ملی است که قرار است در آینده نزدیک بین شهروندان پخش شود و فرصتی بزرگ برای صنایع مرتبط با آن ایجاد کرده است.

۱-۲- هدف از این مطالعه

هدف از این مطالعه طراحی و پیاده‌سازی یک سیستم پرداخت سیار مبتنی بر کارت شناسایی هوشمند ملی می‌باشد. در این مطالعه از تراشه کارت هوشمند به عنوان یک پردازنده امن برای انجام محاسبات رمزنگاری مبتنی بر کلید عمومی به جای پردازنده تلفن همراه و یا سیم‌کارت استفاده شده است؛ زیرا هم نسب به پردازنده تلفن همراه امن‌تر است و نسبت به سیم کارت‌ها هزینه معقول‌تری به اپراتورها تحمیل می‌کند.

همچنین در سیستم‌های پرداختِ ارائه شده قبلی، فرض بر این بوده است که تلفن همراه به عنوان ترمینال پرداخت، یک دستگاه امن است؛ در صورتی که این فرض، درست نمی‌باشد و همواره این دستگاه-ها به دلیل ساختار و کاربرد منحصر به فرد آنها در معرض خطر انواع ویروس‌ها و کدهای مخرب بوده‌اند. در نتیجه در این پایان‌نامه یک روش احراز هویت بر اساس کارت هوشمند و کاراکترهای گرافیکی ارائه شده است که ریسک حمله کدهای مخرب و تروجان‌ها را به سیستم پرداخت کاهش می‌دهد. از آنجا که کارایی، یک فاکتور مهم در روش‌های احراز هویت می‌باشد، روشی برای بهبود کارایی روش احراز هویت جدید، پیشنهاد شده است و کارایی دو روش با یکدیگر مقایسه شده است.

۱-۳- ساختار پایان نامه

در فصل دوم مشخصات یک سیستم پرداخت سیار که شامل مزایا و محدودیت های آن نیز می‌باشد شرح داده خواهد شد. همچنین این سیستم‌های پرداخت از نظر عوامل مختلف دسته‌بندی شده و ویژگی-های امنیتی جهت پذیرش پرداخت سیار به طور کامل شرح داده خواهد شد. در انتهای این فصل انواع چارچوب‌های استفاده شده در این نوع پرداخت‌ها معرفی شده است.

در فصل سوم به معرفی پروتکل‌های سیستم‌های پرداخت کنونی و مزایا و معایب آنها پرداخته شده است. این پروتکل‌ها به ۴ دسته‌ی کلی تقسیم شده‌اند. دسته‌ی اول پروتکل‌هایی هستند که برای سیستم-های غیر سیار و شبکه‌های ثابت طراحی شده‌اند. دسته دوم پروتکل‌هایی هستند که به دلیل بالا بودن

[1] Mobile user
[2] Mobile commerce(m-commerce)

توان محاسباتی الگوریتم‌های رمزنگاری کلید نامتقارن، مبتنی بر رمزنگاری متقارن هستند. دسته سوم از کیف پول الکترونیکی سمت سرور برای انجام محاسبات رمزنگاری کلید نامتقارن استفاده می‌کنند و دسته‌ی چهارم پروتکل‌هایی هستند از توانایی محاسباتی سیم کارت برای انجام عملیات رمزنگاری کلید عمومی استفاده می‌کنند.

با توجه به نقش کارت هوشمند در این پایان‌نامه، فصل چهارم به این موضوع اختصاص داده شده است. در این فصل در مورد تاریخچه‌ی کارت هوشمند، مزایا و کاربردهای آن، انواع کارت هوشمند و استانداردهای وابسته به آنها، ویژگی های سخت‌افزاری و ... توضیح داده شده است.

فصل پنجم به سیستم هویت الکترونیکی ملی می‌پردازد. در این فصل به مفاهیمی مانند دولت الکترونیک و جایگاه ثبت احوال در دولت الکترونیک می پردازد. همچنین سرویس‌های زیرساخت کلید عمومی سازمان ثبت احوال را معرفی کرده و در مورد هر یک از اجزای آن را توضیح می‌دهد.

در فصل ششم، سیستم پرداخت سیار مبتنی بر کارت شناسایی هوشمند ملی که نتیجه این مطالعه است آورده شده است. در ادامه این فصل روش جدید احراز هویت مبتنی بر کارت هوشمند و کاراکترهای گرافیکی بیان شده که خطر حمله کدهای مخرب و تروجان‌ها را کاهش می‌دهد. همچنین روشی برای افزایش بازدهی این روش احراز هویت پیشنهاد شده که حجم پردازش تصاویر گرافیکی را بین کارت و تلفن همراه تقسیم می‌کند. در انتهای این فصل یک نمونه اولیه از این سیستم پرداخت پیاده سازی شده و از نظر امنیت، کارایی، هزینه تولید و سهولت استفاده ارزیابی شده است.

در انتها و در فصل هفتم این مطالعه جمع‌بندی شده و پیشنهادات مطالعات آینده بیان شده است.

فصل ۲– سیستم‌های پرداخت سیار

۲–۱– مقدمه

جهت پیاده‌سازی هر سیستم باید به تمام ویژگی‌ها و قابلیت‌های آن سیستم توجه شود؛ بنابراین سیستم‌های پرداخت سیار نیز از این قاعده مستثنی نخواهند بود و در زمان طراحی و پیاده‌سازی آن بایستی به این ویژگی‌ها توجه شود. در این فصل، بعد از ارائه‌ی تعریفی از پرداخت سیار، مزایا و محدودیت‌هایی یک سیستم پرداخت سیار بیان می‌شود. در ادامه در مورد امنیت پرداخت که از ویژگی-های اصلی سیستم‌های پرداخت سیار است صحبت می‌شود. در بخش (۲-۵)، به معرفی ویژگی‌های امنیتی یک سیستم پرداخت سیار پرداخته می‌شود. این ویژگی ها شامل محرمانگی، جامعیت، تصدیق اصالت و عدم انکار می‌باشد. در پایان این بخش چند روش برای تحقیق این فاکتورهای امنیتی معرفی شده است.

در بخش (۲-۶)، پرداخت سیار را از جنبه‌ها و دیدگاه‌های مختلف تقسیم‌بندی می‌نماییم. یک سیستم پرداخت الکترونیک از لحاظ نحوه انتقال پول، به دو دسته‌ی پرداخت مبتنی بر حساب و سیستم پرداخت مبتنی بر توکن تقسیم می‌شود. همچنین سیستم پرداخت بر اساس میزان پول منتقل شده در تراکنش، به دو دسته پرداخت‌های خرد و پرداخت‌های کلان تقسیم می‌شود. دسته بندی دیگر در سیستم‌های پرداخت، بر اساس نوع محصولی است که در سیستم خرید و فروش می‌شود. محصول ممکن است از نوع دیجیتال و یا از نوع فیزیکی باشد. مسئله دیگری که باید در سیستم‌های پرداخت در نظر گرفته شود تکنولوژی‌های مورد استفاده در پیاده‌سازی آنها می‌باشد که از جمله این تکنولوژی‌ها می‌توان به سرویس-های پیام کوتاه، NFC[1] و RFID[2] اشاره نمود. همچنین دسته‌بندی‌های دیگری نیز در این فصل معرفی می‌گردد.

نکته‌ی دیگری که در پیاده‌سازی سیستم‌های پرداخت حائز اهمیت است، ساختار و چارچوب پیاده-سازی سیستم می‌باشد. به طور کلی ساختارهای موجود در پیاده‌سازی سیستم‌های پرداخت سیار به دو دسته تقسیم می‌شوند. دسته‌ی اول ساختاری است که مبنای آن همان شبکه ثابت است؛ یعنی معماری شبکه ثابت دچار تغییر شده تا جهت استفاده در محیط بیسیم به کار برده شود. در این قسمت، دو نوع ساختار با نام‌های ساختار مبتنی بر پروکسی و ساختار مبتنی بر نماینده ارائه شده است. چارچوب دیگری که برای سیستم پرداخت سیار معرفی شده است، ساختار بدون پراکسی است. این ساختار از ابتدا مختص استفاده در محیط بیسیم بوده و در طراحی این ساختار محدودیت‌های محیط بیسیم در نظر گرفته شده است. در بخش (۲-۷) به معرفی این ساختارها می پردازیم. در انتهای این فصل در بخش (۲-۸) سناریو های پرداخت سیار را معرفی خواهیم کرد.

[1] Near Field Communication
[2] Radio-Frequency-IDentification

۲-۲- پرداخت سیار

پرداخت سیار، یک پرداخت الکترونیکی در محیط بیسیم می‌باشد که در آن حداقل یکی از طرف‌های شرکت کننده در تراکنش به صورت سیار باشد؛ به عبارت دیگر، پرداخت سیار عبارتست از پرداخت پول برای کالا و خدمات و یا پرداخت صورتحساب با استفاده از یک وسیله‌ی سیار مانند تلفن همراه، کامپیوتر همراه و یا ابزارهای دیجیتال شخصی با بهره‌گیری از فن‌آوری‌های بیسیم است. با استفاده از پرداخت سیار هم می‌توان به خرید کالا و خدمات غیر فیزیکی مانند محتوای دیجیتال، مقاله، اخبار، موسیقی، بازی‌های کامپیوتری، نرم افزار، بلیط، هزینه پارکینگ، کرایه حمل و نقل، پرداخت صورت حساب و ... اقدام نمود و هم کالاهای فیزیکی را از ماشین‌های فروشنده خودکار و یا از فروشگاه های مجهز به POS خریداری کرد [۳][۱].

۲-۳- مزایای سیستم پرداخت سیار

سیستم پرداخت سیار نسبت به سیستم پرداخت با شبکه‌ی ثابت از مزیت‌هایی برخوردار می‌باشد که در ادامه به معرفی این مزیت ها می پردازیم[۴]:

- در هر زمان و هر مکانی می تواند به صورت بلادرنگ، تراکنش لازم برای خرید الکترونیکی انجام شود.
- دستگاه سیار نسبت به کامپیوتر شخصی اندازه و وزن کمتری دارد. لذا کاربر به راحتی می-تواند آن را به هر مکانی منتقل کند.
- دستگاه سیار یک وسیله شخصی است، لذا می‌توان آن را متناسب با نیازهای هر فرد، شخصی سازی شود.

۲-۴- محدودیت های موجود در استفاده و پیاده‌سازی سیستم های پرداخت سیار

به طور کلی دو دسته محدودیت برای پیاده سازی سیستم‌های پرداخت سیار وجود دارد. یک دسته از این محدودیت‌ها مربوط به دستگاه‌های سیار و دسته دیگر مربوط به ویژگی‌های محیط بیسیم است. در ادامه هر دسته از این محدودیت ها توضیح داده می شود.

۲-۴-۱- محدودیت های مربوط به دستگاه سیار

دستگاه‌های قابل حمل برای استفاده در پرداخت سیار از محدودیت‌های زیر رنج می‌برند[۵][۱]:

- توان محاسباتی دستگاه‌های قابل حمل در مقایسه با رایانه‌های شخصی کمتر است.
- دستگاه‌های قابل حمل بر خلاف رایانه‌های شخصی که از سیستم برق مستقیم استفاده می کنند از باتری استفاده می‌کنند؛ بنابراین زمان کمتری می‌توانند دستگاه مورد نظر را تغذیه کنند.

- دستگاه‌های قابل حمل، دارای محدودیت حافظه هستند که این امر در سرعت پردازش اطلاعات موثر است.

رمزنگاری بر پایه کلید عمومی، حجم محاسباتی بالایی را به دستگاه قابل حمل تحمیل می‌کند، بنابراین در صورتی که لازم شود از این محاسبات بر روی دستگاه های قابل حمل استفاده شود، زمان طولانی‌تری برای انجام پردازش، مورد نیاز می‌باشد. علاوه بر آن لازم است برای ذخیره گواهی کلید عمومی، حافظه کافی در اختیار داشته باشیم.

۲-۴-۲- محدودیت‌های مرتبط به شبکه‌های بیسیم

ویژگی‌های ذکر شده در زیر، محدودیت‌هایی را برای پرداخت سیار ایجاد می‌کنند[۷][۶].

- شبکه‌های بیسیم پهنای باند کمتری نسبت به شبکه ثابت دارا هستند.
- امکان استراق سمع در شبکه‌های بیسیم بیشتر از شبکه‌های ثابت می‌باشد.
- احتمال از دست رفتن بسته‌ها در محیط بیسیم بیشتر است.

با توجه به محدودیت‌های فوق الذکر راه حل‌های ارائه شده برای پرداخت‌های الکترونیکی در شبکه-های ثابت برای استفاده در پرداخت سیار مناسب نیستند.

۲-۵- عوامل امنیتی موثر در پذیرش پرداخت سیار

اولین عاملی که افراد برای استفاده از یک سرویس، مخصوصا در زمینه مالی و بانکی، به آن توجه می کنند، امنیت آن سیستم است. یک سیستم مالی و بانکی به هر میزان کاربردی و مفید باشد اما فاکتور امنیت را به اندازه کافی مورد توجه قرار نداده باشد مورد قبول واقع نمی‌شود. مقوله امنیت را می‌توان به دو بخش امنیت ذهنی[1] و عینی[2] تقسیم‌بندی کرد[۸]. امنیت عینی شامل بررسی ۶ متغیر کلیدی که در قبول پرداخت سیار تاثیر گذار است. این متغیرها عبارتند از: محرمانگی، تصدیق اصالت، عدم انکار، جامعیت داده، مجوز و اعتماد[۹]. این عوامل امنیتی در پذیرش سیستم‌های پرداخت سیار موثر هستند و بر اعتماد کاربر جهت استفاده از دستگاه سیار به عنوان ابزاری جهت پرداخت تاثیرگذار می‌باشند. هر یک از این عوامل در ادامه توضیح داده شده است.

آ) تصدیق اصالت[3]

قبل از این که تراکنش پرداخت صورت گیرد، موجودیت‌های شرکت‌کننده (معمولا فرستنده و گیرنده)، می‌بایست موجودیت یکدیگر را تائید نمایند. این مسئله باعث می‌شود تا شخص ثالث بدون مجوز

[1] Subjective
[2] Objective
[3] Authentication