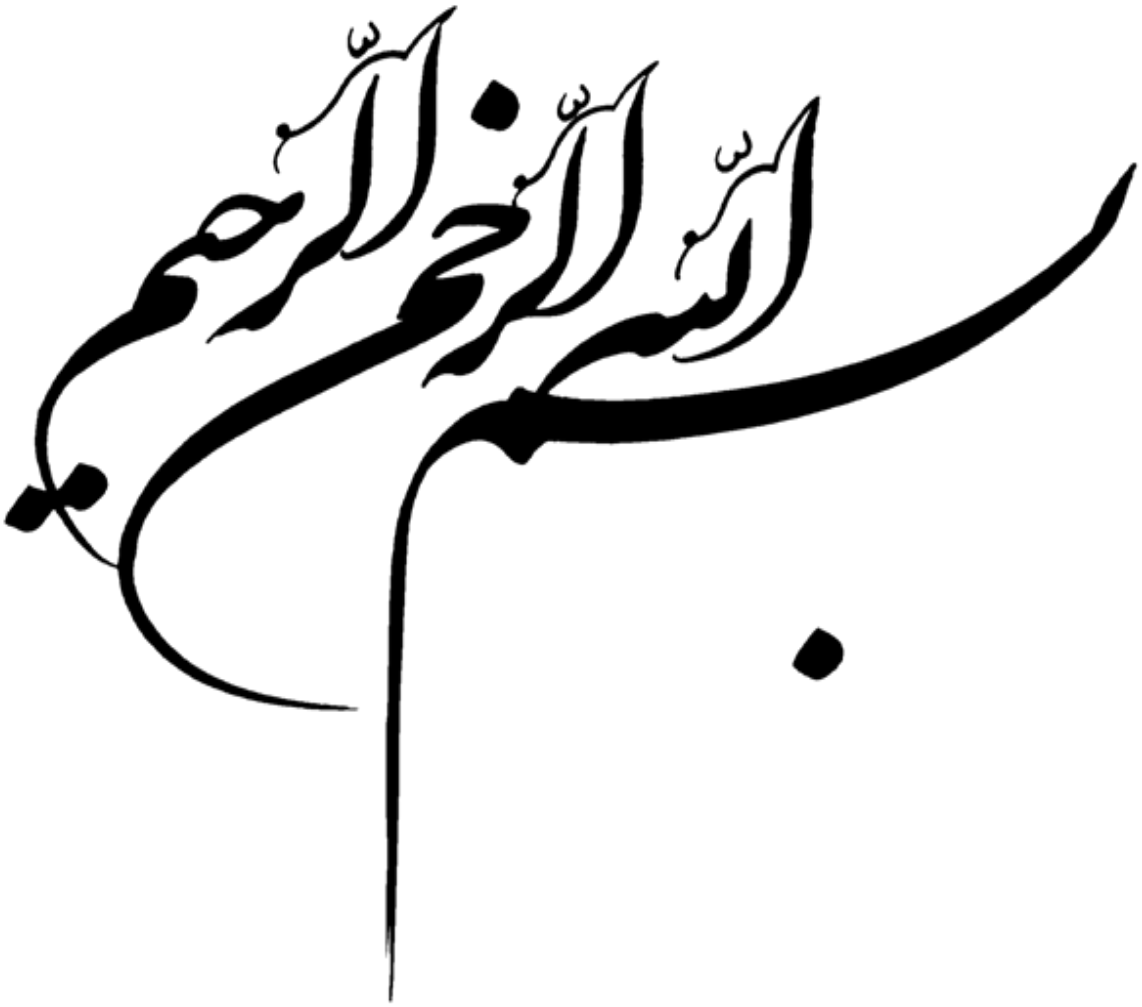
بسم الله الرحمن الرحیم

دانشگاه شاهد

دانشکده فنی و مهندسی

پایان‌نامه دوره کارشناسی ارشد مهندسی رشته فناوری اطلاعات–گرایش فناوری اطلاعات

ارائه‌ی راه حل جدید جهت افزایش کارایی و امنیت در پرداخت سیار

استاد راهنما:

جناب آقای دکتر محمدعلی دوستاری

نام دانشجو

آتنا لطفی

زمستان ۹۱

دانشگاه شاهد

دانشکده فنی و مهندسی

صورت جلسه هیئت داوران پایان نامه کارشناسی ارشد

جلسه دفاعیه پروژه کارشناسی ارشد مربوط به آقای/خانم **آتنا لطفی** به شماره دانشجویی**۸۹۷۵۲۸۰۰۲**در رشته **مهندسی فناوری اطلاعات** با عنوان "**ارائه راه حل جدید جهت افزایش کارآیی و امنیت در پرداخت سیار**" به ارزش **۶ واحد** در روز **۹۱/۱۱/۲** در دانشکده فنی و مهندسی با حضور افراد ذیل تشکیل شد، نتیجه به قرار زیر است :

☐ پروژه نامبرده با نمره ۱۸/۱۶ قابل قبول می‌باشد.

☐ پروژه نامبرده مردود می‌باشد.

☐ پروژه نامبرده به شرط انجام اصلاحات جزیی قابل قبول می‌باشد. نمرهٔ دانشجو متعاقباً اعلام می‌شود.

☐ نام استاد راهنمای اول دکتر درستکاری	دانشگاه : شاهد	امضاء	سهم استاد (به درصد): ۵۰
☐ نام استاد راهنمای دوم	دانشگاه :	امضاء	سهم استاد (به درصد):
☐ نام استاد مشاور اول	دانشگاه :	امضاء	سهم استاد (به درصد):
☐ نام استاد مشاور دوم	دانشگاه :	امضاء	سهم استاد (به درصد):
☐ نام داور اول دکتر حاج سید جوادی	دانشگاه : شاهد	امضاء	
☐ نام داور دوم دکتر علی نژاد یان ورجانی	دانشگاه : پژوهشگاه	امضاء	
☐ نام داور سوم	دانشگاه :	امضاء	
☐ نام داور چهارم	دانشگاه :	امضاء	
☐ نام نماینده معاونت پژوهشی ناصر محمدزاده		امضاء	

تذکر:تعیین سهم اساتید در صورت وجود بیش از یک استاد راهنما و مشاور ضروری است.

	اظهار نامه دانشجو	شماره: تاریخ:

اینجانب آتنا لطفی دانشجوی کارشناسی ارشد رشته مهندسی فناوری اطلاعات گرایش فناوری اطلاعات دانشکده فنی و مهندسی دانشگاه شاهد، گواهی می دهم که پایان نامه/ رساله تدوین شده حاضر با عنوان؛ «ارائه ی راه حل جدید جهت افزایش کارایی و امنیت در پرداخت سیار» به راهنمایی استاد محترم جناب آقای دکتر محمد علی دوستاری، توسط شخص اینجانب انجام و صحت و اصالت مطالب تدوین شده در آن، مورد تأیید است و چنان چه هر زمان، دانشگاه کسب اطلاع کند که گزارش پایان نامه/ رساله حاضر صحت و اصالت لازم را نداشته، دانشگاه حق دارد، مدرک تحصیلی اینجانب را مسترد و ابطال نماید هم چنین اعلام می دارد در صورت بهره گیری از منابع مختلف شامل؛ گزارش های تحقیقاتی، رساله، پایان نامه، کتاب، مقالات تخصصی و غیره، به منبع مورد استفاده و پدید آورنده آن به طور دقیق ارجاع داده شده و نیز مطالب مندرج در پایان نامه/ رساله حاضر تاکنون برای دریافت هیچ نوع مدرک یا امتیازی توسط اینجانب و یا سایر افراد به هیچ کجا ارایه نشده است. در تدوین متن پایان نامه/ رساله حاضر، چارچوب (فرمت) مصوب تدوین گزارش های پژوهشی تحصیلات تکمیلی دانشگاه شاهد به طور کامل مراعات شده و نهایتاً این که، کلیه حقوق مادی ناشی از گزارش پایان نامه/ رساله حاضر، متعلق به دانشگاه شاهد می باشد.

نام و نام خانوادگی دانشجو(دست نویس):.....

امضاء دانشجو:

تاریخ:

تقدیم به **پدر** و **مادر** عزیزم

که همواره خود را مدیون مهربانی‌هایشان

می‌دانم.

سپاس و ستایش بی حد و حصر پروردگاری را که همه عالم از پرتو نور کرمش تکوین یافته و هر چه هست به اشاره‌ی لطف اوست.

جای دارد از همکاری کلیه استادان و دوستان ارجمند به خصوص جناب آقای دکتر محمدعلی دوستاری، استاد راهنمای گرامی که در انجام این پایان نامه اینجانب را همراهی و راهنمایی نمودند؛ کمال تشکر و قدرانی را بنمایم.

آتنا لطفی

چکیده

با افزایش نفوذ تلفن همراه و توسعه تجارت سیار، استفاده از تلفن همراه به عنوان ابزار پرداخت روز به روز گسترش می‌یابد. با توجه به اهمیت امنیت در تجارت و پرداخت و به دلیل محدودیت‌های موجود در شبکه‌های بی‌سیم، پروتکل‌های پیشنهادی در حوزه پرداخت سیار می‌بایستی علاوه بر تامین امنیت از کارایی خوبی نیز برخوردار باشند. در این پایان نامه که در راستای اهداف فوق می‌باشد، دو پروتکل پرداخت منطبق با دو سناریوی ارتباطی مختلف، متناسب با نیازمندی‌های حوزه پرداخت سیار ارائه شده است. در طراحی این پروتکل‌ها از طرح کلید عمومی خودگواهی[1] مبتنی بر رمزنگاری خم بیضوی استفاده گردیده و همچنین طرحی جدید از امضای رقمی شانور[2] ارائه شده است. بکارگیری راه‌حل‌های پیشنهادی در این پروتکل‌ها، سبب کاهش بار محاسباتی و حافظه مصرفی می‌شود. پروتکل‌های ارائه شده، ویژگی-های محرمانگی، تصدیق اصالت، عدم انکار فرستنده، دست نخوردگی اطلاعات و گمنامی مشتری را برآورده می‌نمایند و در برابر حملاتی از جمله مردی در میان، تکرار، و ایفای نقش نیز مقاوم می‌باشند.

کلید واژه: سیستم پرداخت سیار، پروتکل پرداخت، رمزنگاری خم بیضوی، کلید عمومی خودگواهی، امضای رقمی شانور.

[1] Self-Certified
[2] Schnorr digital signature

فهرست مطالب

عنوان **صفحه**

فهرست جدول‌ها

عنوان **صفحه**

فهرست شکل‌ها

عنوان **صفحه**

فهرست علایم و نشانه‌ها

عنوان	علامت اختصاری
پرداخت سیار	MP
مرکز تولید کلید	KGC
پروتکل کلید اینترنت	iKP
پروتکل تراکنش الکترونیکی امن	SET
پروتکل طراحی شده توسط Kungpisdan-Srinivasan-Le	KSL
ارتباط حوزه نزدیک	NFC
شناسه فرکانس رادیویی	RFID
پروتکل تبادل کلید تصدیق اصالت	AKE
مرکز سیستمی مورد اعتماد	SA
توصیف سفارش	OD
اطلاعات سفارش	OI
اطلاعات پرداخت	PI
شناسه	ID
اطلاعات کارت اعتباری	CCI
شناسه تراکنش	TID
درخواست خرید	PReq
پاسخ خرید	PRes
درخواست مجوز	AuthReq
پاسخ مجوز	AuthRes

فصل ۱- مقدمه

۱-۱- پیشگفتار

پیشرفت و گسترش فناوری‌های سیار منجر به شکل‌گیری نوع جدیدی از تجارت الکترونیکی تحت عنوان تجارت سیار شده است. تجارت سیار، یک داد و ستد الکترونیکی در محیط بی‌سیم می‌باشد که در آن حداقل یکی از طرف‌های شرکت کننده در تراکنش از ابزار پرداخت سیار استفاده می‌کند. با وجود آن که زمان زیادی از ظهور این سیستم پرداخت نمی‌گذرد اما به دلیل مزایا و قابلیت‌هایی که این روش پرداخت فراهم می‌آورد و سبب تسهیل فرآیند پرداخت برای استفاده کنندگان می‌شود؛ بنابراین امروزه شاهد رشد روزافزون استفاده از ابزارهای سیار در مبادلات تجاری می‌باشیم. در نتیجه پرداخت سیار یک نیاز اجتناب ناپذیر جهت پرداخت هزینه‌ی کالاها و خدمات در دنیای امروز می‌باشد. انجام پرداخت سیار مستلزم استفاده از پروتکل‌های پرداخت می‌باشد؛ که این پروتکل‌ها می‌بایست متناسب با نیازمندهای حوزه‌ی پرداخت سیار طراحی شوند.

با توجه به اهمیت امنیت در تجارت و پرداخت، پروتکل‌های پیشنهادی در این حوزه می‌بایستی با دید همه جانبه نسبت به مباحث امنیتی در زمینه‌ی شبکه‌های سیار و محدودیت‌های موجود در ابزار پرداخت طراحی شوند. از جمله محدودیت‌های شبکه‌های بی‌سیم می‌توان به هزینه‌ی ارتباطی بالا، پهنای باند پایین و قابلیت اطمینان پایین تر آن نسبت به شبکه‌های ثابت اشاره نمود[۱], [۲]. بنابراین برای غلبه بر مشکلات مرتبط با بحث پرداخت سیار، توجه به دو بحث امنیت و کارایی در طراحی پروتکل‌های پیشنهادی یک ضرورت محسوب می‌شود.

در حوزه‌ی پرداخت سیار تاکنون تلاش‌های فراوانی در راستای ارائه‌ی پروتکل‌های پرداختی متناسب با نیازمندی‌های موجود در تجارت سیار صورت گرفته است که در بسیاری از این پروتکل‌ها جهت برقراری خواسته‌های امنیتی از سیستم‌های رمز کلید عمومی استفاده می‌شود. از مسائل مهم در این سیستم‌ها، نیاز به برقراری ارتباط بین کلید عمومی و هویت شخص- اصالت کلید عمومی- می‌باشد. برای حل این مسئله راه حل‌هایی پیشنهاد شدند. یک راه حل، سیستم‌های رمز کلید عمومی مبتنی بر گواهینامه می-باشد ولی این سیستم‌ها به دلیل نیاز به ساختار کلید عمومی و مدیریت و کنترل گواهینامه‌ها، جهت بکارگیری در بحث پرداخت سیار نامناسب می‌باشند. راه حل دیگر، سیستم رمز کلید عمومی مبتنی بر هویت [۳] است؛ که در آن کلید عمومی از مشخصه‌های هویتی شخص استخراج می‌شود و کلید خصوصی متناسب با کلید عمومی، توسط مرکز تولید کلید[1] و با استفاده از کلید اصلی[2] آن مرکز تولید می‌گردد. از جمله مزایای این طرح، رفع مشکلات سیستم رمز کلید عمومی مبتنی بر گواهینامه و عیب آن وابستگی تمامی کلیدهای خصوصی به کلید اصلی مرکز تولید کلید می‌باشد. سیستم‌های رمز کلید عمومی

[1] Key Generation Center(KGC)
[2] Master Key

خودگواهی برای مواجهه با مشکلات بیان شده در دو طرح فوق معرفی گردیدند. این سیستم‌های رمز، نه فقط خواسته‌های امنیتی موجود در سیستم‌های رمز کلید عمومی را فراهم می‌آورند بلکه عملکرد بهتری را نیز نسبت به دیگر طرح‌های کلید عمومی دارا می‌باشند. بنابراین استفاده از آن در بحث پرداخت سیار سبب بهبود فرآیند پرداخت می‌شود. البته می‌توان جهت طراحی پروتکل پرداخت سیار از سیستم‌های رمز متقارن نیز استفاده نمود. استفاده از سیستم‌های رمزمتقارن اگرچه سبب کاهش بار محاسبات تراکش پرداخت می‌شود ولی مستلزم به اشتراک گذاری مقادیر محرمانه بین طرفین شرکت کننده در پروتکل پرداخت می‌باشد که این خود، محدودیت‌هایی را در طراحی پروتکل پرداخت به وجود می‌آورد. بنابراین در طراحی پروتکل پیشنهادی از سیستم رمز کلید عمومی خودگواهی استفاده می‌شود.

هدف ما در این پایان نامه، ارائه پروتکل‌های پرداختی منطبق با دو سناریو ارتباطی مشتری محور و فروشنده محور می‌باشد؛ که در طراحی آن‌ها، از طرح کلید عمومی خودگواهی مبتنی بر رمزنگاری خم بیضوی استفاده می‌شود. همچنین از طرح‌های امضای رقمی و تصدیق اصالت شانور و نیز طرح رمز-امضا هم بهره گرفته شده است. بکارگیری راه حل‌های پیشنهادی در پروتکل ارائه شده سبب بهبود کارایی پروتکل پرداخت می‌شود. همچنین این پروتکل خواسته‌های امنیتی محرمانگی، تصدیق اصالت، عدم انکار فرستنده، جامعیت، دست نخوردگی اطلاعات و گمنامی مشتری را برآورده می‌نماید و از طرفی در برابر حملات مردی در میان، تکرار، و ایفای نقش نیز مقاوم می‌باشد.

۱-۲- ساختار پایان نامه

در فصل دوم، سیستم پرداخت سیار معرفی می‌شود. مزایا و محدودیت‌های این سیستم پرداخت بیان می‌گردد. در ادامه، به مروری کلی بر سیستم پرداخت سیار خواهیم پرداخت. به این منظور، ابتدا ویژگی‌های امنیتی لازم در یک سیستم پرداخت سیار توضیح داده می‌شود. سپس از دیدگاه‌ها و وجوه مختلف به دسته بندی پرداخت سیار خواهیم پرداخت و درنهایت، انواع چارچوب‌های مورد استفاده در پیاده سازی یک سیستم پرداخت سیار معرفی می‌گردد.

فصل سوم به دو بخش کلی تقسیم می‌شود که در بخش اول چند نمونه از پروتکل‌های پیشنهاد شده برای پیاده سازی یک سیستم پرداخت سیار معرفی می‌شود؛ که در این جا، پروتکل‌های پرداخت iKP، SET، KSL و Tellez را مورد بررسی قرار می‌دهیم. پروتکل iKP شامل سه نوع 1KP، 2KP و 3KP می‌باشد. از آنجایی که پروتکل 3KP بیشترین سطح امنیت را فراهم می‌کند در این جا تنها به جزئیات همین یک پروتکل از خانواده iKP می‌پردازیم. پروتکل بعدی، پروتکل SET می‌باشد. پروتکل SET مناسب برای شبکه‌ی ثابت است. لذا در ادامه‌ی آن پروتکل SET/A که مناسب برای محیط بی‌سیم می‌باشد و برگرفته از پروتکل SET است، معرفی می‌شود. پروتکل KSL، دو نسخه به نام‌های KSLv1 و KSLv2 دارد که شرح هر دو نسخه آورده شده است. در پایان به معرفی پروتکل‌های ارائه شده توسط Tellez و همکاران خواهیم پرداخت. در انتهای این بخش، مقایسه‌ای روی پروتکل‌های معرفی شده انجام می‌گیرد. در بخش دوم این فصل، به معرفی مفاهیم پایه‌ای که در پروتکل پیشنهادی از آن‌ها استفاده شده است خواهیم پرداخت. که این موارد عبارتند از: رمزنگاری خم بیضوی، سیستم رمز کلید عمومی خودگواهی، طرح رمز-امضا و طرح تصدیق اصالت و امضای شانور.

در فصل چهارم، پروتکل‌های پرداخت پیشنهادی ارائه می‌شود. در این فصل ابتدا موجودیت و نمادهای شرکت کننده در پروتکل‌ها معرفی می‌شوند. در ادامه مفروضات پروتکل‌ها بیان می‌گردد و همچنین راه حل‌های جدید برای امضای پیغام و همچنین امضا و رمز پیغام به صورت همزمان ارائه می‌شود. با توجه به این راه حل‌ها، دو پروتکل پرداخت ارائه می‌گردد و در ادامه جزییات مراحل این پروتکل‌ها شرح داده می‌شود. در پایان پروتکل‌های پیشنهادی را با توجه به ویژگی‌های امنیتی و حملات مورد بررسی قرار می‌دهیم.

فصل ۲- سیستم پرداخت سیار

۲-۱- مقدمه

جهت پیاده سازی هر سیستم باید به تمامی ویژگی‌ها و قابلیت‌های مورد انتظار از آن سیستم پرداخته شود؛ بنابراین سیستم پرداخت سیار نیز از این قاعده مستثنی نمی‌باشد و در زمان پیاده‌سازی آن بایستی به ویژگی‌ها و قابلیت‌های مورد انتظار از سیستم پرداخت توجه شود. در این فصل، بعد از ارائه‌ی تعریفی از پرداخت سیار، مزایا و محدویت‌های یک سیستم پرداخت سیار بیان می‌شود. در ادامه در مورد امنیت پرداخت که از ویژگی‌های اصلی در پیاده سازی سیستم پرداخت سیار می‌باشد و دوام و پیشرفت سیستم وابسته به آن است صبحت می‌شود. در واقع در بخش۲-۵-، به معرفی ویژگی‌های امنیتی مورد نیازی که یک سیستم پرداخت سیار باید فراهم نماید پرداخته می‌شود. این ویژگی‌ها شامل محرمانگی، جامعیت، تصدیق اصالت و عدم انکار می‌باشد. در پایان این بخش چند روش برای تحقق این فاکتورهای امنیتی معرفی شده است.

در بخش ۲-۶-، پرداخت سیار را از جنبه‌ها و دیدگاه‌های مختلف تقسیم بندی می‌نماییم. یک سیستم پرداخت الکترونیک از لحاظ نحوه‌ی انتقال پول به دو دسته، سیستم پرداخت مبتنی بر صورت حساب و سیستم پرداخت مبتنی بر توکن تقسیم بندی می‌شود. همچنین سیستم پرداخت بر اساس میزان پول منتقل شده در تراکنش پرداخت، به دو دسته پرداخت خرد و پرداخت کلان تقسیم می‌شود. دسته‌بندی دیگر در سیستم پرداخت سیار، بر اساس نوع محصولی است که در سیستم خرید می‌شود. محصول ممکن است از نوع دیجیتال باشد و یا محصول فیزیکی باشد. مسئله‌ی دیگری که در سیستم پرداخت سیار باید مد نظر قرار گیرد، تکنولوژی‌های مورد استفاده در پیاده سازی سیستم پرداخت می‌باشد که از جمله این تکنولوژی‌ها می‌توان به سرویس پیام کوتاه، NFC و RFID اشاره نمود. البته دسته بندی‌های دیگری نیز در این بخش معرفی می‌گردد.

نکته‌ی دیگری که در پیاده سازی سیستم پرداخت سیار حائز اهمیت است، ساختار و چارچوب پیاده سازی سیستم می‌باشد. به طور کلی ساختارهای موجود در پیاده سازی سیستم پرداخت سیار به دو دسته تقسیم می‌شوند. دسته‌ی اول، ساختاری است که مبنای آن همان شبکه‌ی ثابت می‌باشد؛ یعنی شبکه‌ی ثابت را تغییر داده تا جهت پرداخت در محیط بی‌سیم قابل استفاده گردد. دو نوع ساختار با نام‌های ساختار مبتنی بر پروکسی و ساختار مبتنی بر نماینده در این روش وجود دارد. ساختار دیگری که برای سیستم پرداخت سیار معرفی شده است، ساختار بدون پروکسی است. این ساختار از ابتدا مخصوص محیط بی‌سیم طراحی شد و در طراحی این ساختار، محدودیت‌های محیط بی‌سیم در نظر گرفته شده است. در بخش ۲-۷- به معرفی این ساختارها می‌پردازیم. در انتهای این فصل در بخش ۲-۸- سناریوی‌های پرداخت سیار را معرفی می‌نماییم.

۲-۲- پرداخت سیار

پرداخت سیار، یک پرداخت الکترونیکی در محیط بی‌سیم می‌باشد که در آن حداقل یکی از طرف‌های شرکت کننده در تراکنش از ابزار پرداخت سیار استفاده می‌کند؛ به عبارت دیگر، پرداخت سیار عبارت از پرداخت پول برای کالاها و خدمات و یا پرداخت صورت‌حساب‌ها با استفاده از یک وسیله‌ی سیار مانند تلفن همراه، کامپیوتر همراه و یا ابزارهای دیجیتال شخصی[1] با بهره‌گیری از فن‌آوری‌های بی‌سیم است. با استفاده از پرداخت سیار هم می‌توان به خرید کالاها و خدمات غیر فیزیکی مانند محتوای دیجیتال، مقاله، اخبار، موسیقی، بازی‌های کامپیوتری، نرم افزار، بلیط، هزینه پارکینگ، کرایه حمل، پرداخت صورت‌حساب و غیره اقدام نمود و هم کالاهای فیزیکی را از ماشین‌های فروشنده خودکار و یا از فروشگاه-های مجهز به POS[2] خریداری کرد[1], [۴].

۲-۳- مزاياي سيستم پرداخت سيار

سیستم پرداخت سیار نسبت به سیستم پرداخت با شبکه‌ی ثابت دارای مزیت‌هایی می‌باشد که در ادامه به معرفی این مزیت‌ها می‌پردازیم[۵]:

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

۲-۴- محدوديت‌هاي موجود در پياده سازي سيستم پرداخت سيار

به طور کلی دو دسته محدودیت برای پیاده‌سازی سیستم پرداخت سیار وجود دارد. یک دسته از این محدودیت‌ها مربوط به دستگاه سیار و دسته‌ی دیگر آن مربوط به ویژگی‌های محیط بی‌سیم است. در ادامه هر دسته از این محدودیت‌ها توضیح داده می‌شود.

۲-۴-۱- محدوديت‌هاي مربوط به دستگاه سيار

دستگاه سیار برای استفاده در پرداخت سیار دارای محدودیت‌های زیر می‌باشد[1], [3], [۶]:

- توان پردازش دستگاه سیار نسبت به کامپیوترهای شخصی کم‌تر است.
- دستگاه سیار بر خلاف کامپیوتر شخصی که از برق استفاده می‌کند، از باتری استفاده می‌کند؛ لذا زمان کوتاه تری نسبت به کامپیوتر شخصی می‌تواند کار کند.

[1] Personal Digital Assistanat
[2] Point Of Sale

- دستگاه سیار دارای محدودیت حافظه می‌باشد؛ که این امر بر روی استفاده از الگوریتم رمزنگاری تأثیر می‌گذارد.

رمز نگاری کلید عمومی دارای محاسبات بالایی می‌باشد. لذا در صورتی که بخواهیم این محاسبات را با دستگاه سیار انجام دهیم، زمان طولانی‌تری نیاز می‌باشد. علاوه بر آن لازم است برای ذخیره‌ی گواهی کلید عمومی حافظه کافی داشته باشیم. اگرچه هم اکنون وسیله‌های سیاری با قابلیت محاسبات بالا مانند تلفن‌های هوشمند و PDA تولید شده‌اند، ولی این ابزار هنوز در بین مردم فراگیر نشده‌اند. لذا لازم است تا در سیستم‌های پرداخت سیار که پیاده سازی می‌شوند این محدودیت‌ها در نظر گرفته شوند.

۲-۴-۲- محدوديت‌هاي مربوط به شبكه بي‌سيم

شبکه‌ی بی‌سیم دارای ویژگی‌های زیر می‌باشد که این موارد محدودیت‌هایی را هنگام پیاده سازی سیستم پرداخت سیار ایجاد می‌کند[۷], [۸]:

- شبکه بی‌سیم نسبت به شبکه ثابت پهنای باند کمتری دارد.
- امکان این که در شبکه بی‌سیم بسته‌ها گم شود بیشتر است.
- هزینه‌ی اتصال شبکه‌ی بی‌سیم در مقایسه با شبکه ثابت بیشتر است.
- امکان استراق سمع در شبکه‌ی بی‌سیم بالاتر از شبکه ثابت است.

لذا با توجه به محدودیت‌های ذکر شده، اجرای تراکنش پرداخت در شبکه‌ی بی‌سیم زمان بر است. علاوه بر این، از آن جایی که در محیط بی‌سیم شنود به طور راحت تر امکان پذیر می‌باشد؛ لذا لازم است تا رمزنگاری قوی‌ای مانند رمزنگاری کلید عمومی استفاده شود. از طرفی این رمز نگاری نیاز به قابلیت محاسباتی بالا و همچنین شبکه بی‌سیمی با سرعت بالا دارد که هر دوی این‌ها، هزینه‌ی بالایی را برای کاربران در بر خواهد داشت.

۲-۵- ويژگي‌هاي امنيتي مورد نياز در سيستم پرداخت سيار

در این جا به بررسی عوامل موثر بر قبول[۱] پرداخت‌های سیار پرداخته می‌شود. اعتماد یکی از مهمترین فاکتورهای لازم جهت پذیرش سیستم پرداخت سیار می‌باشد. اولین چیزی که مشتریان برای کسب اعتماد در مورد یک سیستم پرداخت در مورد آن سوال می‌کنند، پرسش درباره‌ی امنیت تراکنش‌های صورت گرفته می‌باشد. شش متغیر کلیدی جهت قبول پرداخت سیار عبارتند از: محرمانگی[۲]، تصدیق اصالت[۳]، عدم انکار[۴]، جامعیت داده[۵]، مجوز[۶] و اعتماد[۷]. این عوامل امنیتی در پذیرش سیستم‌های پرداخت

[1] adoption
[2] confidentiality
[3] authentication
[4] non-repudiation
[5] integrity of data
[6] authorization
[7] trust

سیار موثر می‌باشند و بر اعتماد کاربر جهت استفاده از دستگاه سیار به عنوان ابزاری جهت پرداخت تاثیر گذار می‌باشند[۱۱], [۱۰], [۹].

محرمانگی: اطلاعات نمی‌بایست برای افراد، فرآیندها یا دستگاه‌های غیر مجاز فاش شود؛ یعنی محرمانگی این اطمینان را می‌دهد که اطلاعات تنها توسط طرف‌های مجاز قابل دسترسی باشد. که این معمولا با استفاده از رمزنگاری مبتنی بر کامپیوتر حاصل می‌شود. عمده حملات به محرمانگی شامل: تحلیل ترافیک[۱]، شنود[۲] و حمله فردی در میان[۳] است.

- ✓ قدرت درک شده از محرمانگی یک تاثیر مثبت بر اعتماد مشتری در پرداخت‌های سیار خواهد داشت.

تصدیق اصالت: تصدیق اصالت تضمین می‌نماید که طرفین تراکنش متقلب نبوده و قابل اعتماد می‌باشند. قبل از این که تراکنش‌های تجاری بتوانند انجام شوند، موجودیت‌های شرکت کننده می‌بایست هویت طرف‌های دیگر را تایید نمایند و آن با استفاده از پروتکل‌های تصدیق اصالت مبتنی بر شبکه و پین قابل انجام می‌باشد. حملات تصدیق اصالت، تحلیل ترافیک، شنود و حمله فردی در میان است.

- ✓ قدرت درک شده از تصدیق اصالت یک تاثیر مثبت بر اعتماد مشتری در پرداخت‌های سیار خواهد داشت.

عدم انکار: این ویژگی این اطمینان را حاصل می‌کند که هیچ یک از طرفین نتواند پیغامی که ارسال کرده است را انکار نماید. که با استفاده از تکنیک‌های امضای رقمی این امر حاصل می‌شود.

- ✓ قدرت درک شده از عدم انکار یک تاثیر مثبت بر اعتماد مشتری در پرداخت‌های سیار خواهد داشت.

جامعیت داده: جامعیت به این معنی می‌باشد که اطلاعات و سیستم‌ها توسط طرف‌های خارجی و غیر مجاز تغییر نکرده یا خراب نشده باشند. اضافه کردن امضای رقمی امن روی پیغام، جامعیت داده‌ی تراکنش را فراهم می‌آورد. حملات به جامعیت شامل: ربودن جلسه[۴]، حملات تکرار [۵]و حمله فردی در میان است.

- ✓ قدرت درک شده از جامعیت داده یک تاثیر مثبت بر اعتماد مشتری در پرداخت‌های سیار خواهد داشت.

مجوز: روش‌های پرداخت سیار می‌بایست قادر به بررسی این موضوع باشند که آیا کاربر می‌تواند خریدهای درخواست شده را انجام دهد یا نه. که آن معمولا با استفاده از پین و کلمه عبور فراهم می‌شود.

- ✓ قدرت درک شده از مجوز یک تاثیر مثبت بر اعتماد مشتری در پرداخت‌های سیار خواهد داشت.

در شکل ۲-۱، عوامل کلیدی جهت برقراری اعتماد کاربر به پرداخت سیار نشان داده شده است و همچنین نتایج حاصل از این اعتماد که پذیرش پرداخت‌های سیار و قبول واقعی آن می‌باشد دیده می‌شود.

---

[1] traffic analysis
[2] eavesdropping
[3] man-in-the middle attack
[4] Session hijacking
[5] Replay Attack