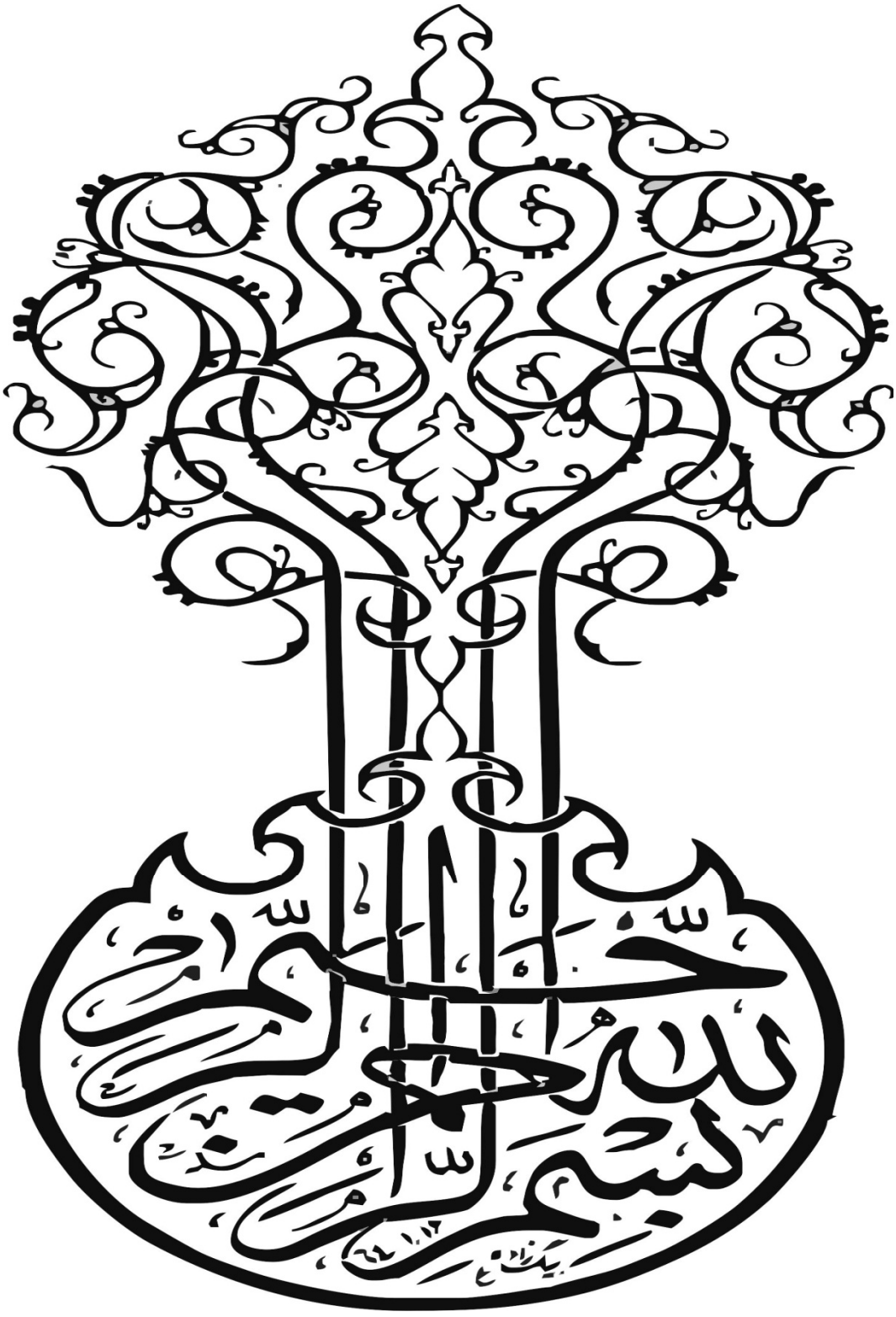

بسم الله الرحمن الرحيم

دانشکده: فنی و مهندسی

گروه علمی: مهندسی فناوری اطلاعات و ارتباطات

پایان‌نامه

برای دریافت درجه کارشناسی ارشد

در رشته: مهندسی کامپیوتر (نرم افزار)

عنوان پایان‌نامه:

تحلیل امنیتی راه‌حل‌های پرداخت الکترونیکی مبتنی بر تلفن‌همراه

استاد راهنما:

دکتر رضا عسکری مقدم

استاد مشاور:

دکتر صمد مومن بالله

نگارش:

محمد وحید علی‌زاده دیزج

آبان ۱۳۸۹

بسمه تعالی

تصویب پایان‌نامه

پایان‌نامه تحت عنوان: تحلیل امنیتی راه حل های پرداخت الکترونیکی مبتنی بر تلفن‌همراه که در مرکز تهران تهیه و به هیات داوران ارائه گردیده است مورد تایید می باشد. تاریخ دفاع: نمره: درجه ارزشیابی:

اعضای هیات داوران:

نام و نام خانوادگی	هیات داوران	مرتبه علمی	امضاء
۱-	-	-	-
۲-	-	-	-
۳-	-	-	-
٤-	-	-	-
٥-	-	-	-

چکیده:

توسعه روز افزون شبکه‌های بی‌سیم و محبوبیت گسترده دستگاه‌های دستی فرصتی عالی برای فعال کردن دستگاه‌های تلفن همراه به عنوان یک روش پرداخت جهانی که شامل تراکنش‌های مالی روزانه است ، را فراهم آورده است. متاسفانه برخی مسائل مانند: خواص پاسخگویی، حفاظت از حریم خصوصی، انکار کردن، محدودیت شبکه‌های بی‌سیم و دستگاه‌های تلفن‌همراه مانع پذیرش گسترده پرداخت‌همراه می شود. اخیراً، پروتکلهای پرداخت تلفن همراه زیادی بر اساس کلید عمومی ارائه شده اند. با این حال، قابلیت‌های محدود تلفن‌های همراه و شبکه‌های بی‌سیم این پروتکل‌ها را برای شبکه تلفن همراه نامناسب می سازند. علاوه بر این، این پروتکلها برای حفظ جریان سنتی داده‌ها در پرداخت طراحی شده اند، به همین علت در معرض حمله هستند و میزان مخاطره کاربر را افزایش می دهند. در این مقاله، ما پروتکل پرداخت تلفن همراه MPCP۲ (Mobile Pay Center Protocol۲) را که بر اساس مدل مشتری محور است و از عملیات کلید متقارن استفاده می کند، پیشنهاد می کنیم. پروتکل پیشنهادی علاوه بر کم کردن عملیات محاسباتی و کم کردن ارتباطات در بین گروه های درگیر، به حفاظت کامل از حریم خصوصی پرداخت کننده پرداخته و مانع از انکار طرفین می شود همچنین امکان حمله تکرار را بسیار کم می کند. با توجه به محدودیت های شبکه‌های بی‌سیم و تلفن‌های همراه، این مقاله پروتکل موافقت کلید VAM (Vahid Alizadeh Dizaj-Askari Moghaddam-Momenebellah) را برای تولید کلید نشست مشترک بین دو گروه ، پیشنهاد داده است.

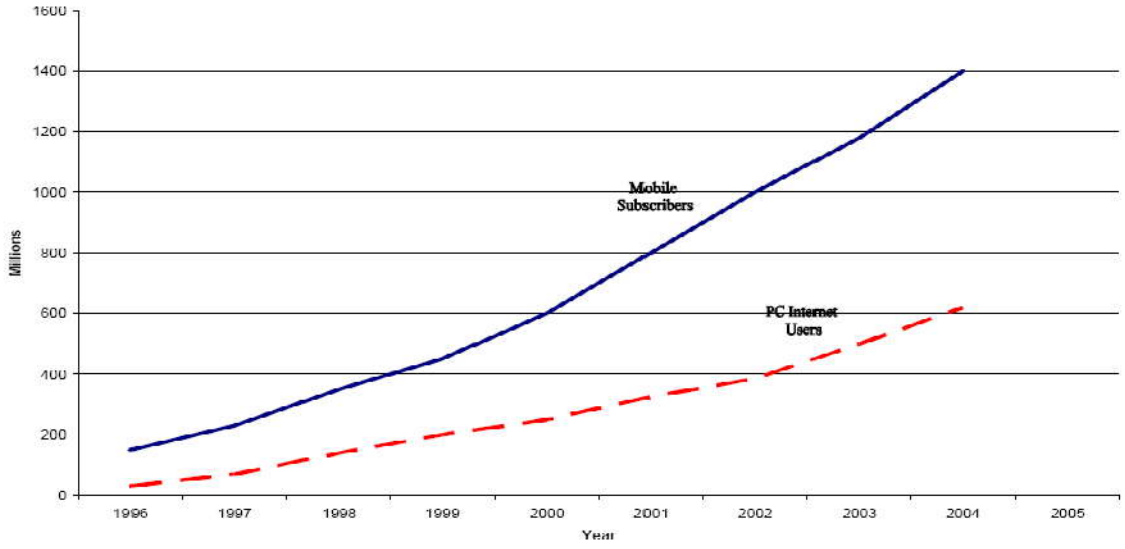
فهرست مطالب:

فهرست جدول:

فصل اول

مقدمه

گسترش شبکه‌های کامپوتری و افزایش استفاده از کامپیوترهای شخصی بستر بسیار مناسبی برای رشد تجارت الکترونیکی و برنامه های ارتباطی فراهم کرده است با افزایش کارایی، توان و حافظه این دستگاه ها برنامه های پیچیده‌تر و کاراتری برای استفاده ایجاد شده‌اند اما با وجود این امکانات این سیستم‌ها هنوز محدودیت دارند از جمله آنکه کاربران ناچارند مقابل آنها نشسته و به طور فیزیکی به شبکه متصل شوند.



شکل ۱-۱ : مقایسه میزان استفاده از کامپیوترهای شخصی و دستگاه‌های سیار [۲]

میزان استفاده از کامپیوترهای شخصی در جهان به سرعت رو به افزایش است به موازات آن آمارها نشان می‌دهد که دستگاه‌های سیار بیشتری مورد استفاده قرار می‌گیرند. این مطلب در شکل قبل نشان داده شده است. ظهور دستگاه‌های سیار و شبکه‌های بی‌سیم یک مسیر جدید در حوزه تجارت الکترونیکی با عنوان " تجارت سیار[۱] " ایجاد کرده است.

[۱] M-Commerce(Mobile Commerce)

به منظور بررسی در مورد تجارت سیار و پرداخت الکترونیکی ابتدا لازم است که بعضی از مفاهیم به طور دقیق تعریف شوند.

تجارت الکترونیکی: عبارت است از تبادل محصول یا کالا و یا یک ارزش مالی به وسیله ابزارهای الکترونیکی روی شبکه های با قابلیت دسترسی باز. این تعریف عمدتاً به معنی ارتباط از طریق اینترنت برای همه یا قسمتی از پردازش تراکنش می باشد. [۲۹]

پرداخت الکترونیکی: عبارت است از فراهم آوردن وسیله پرداخت برای محصولات و سرویس‌ها از طریق شبکه ارتباط عمومی به نحوی که کلیه اطلاعات مربوط به پرداخت بوسیله این شبکه ارسال شده و نیاز به هیچ ارتباط خارجی (فکس، تلفن و یا پست) نباشد. [۲۹]

تجارت سیار: عبارت است از انجام تراکنش‌های تجاری و یا تبادل اطلاعات مالی بوسیله یک دستگاه سیار و از طریق شبکه بی‌سیم. [۲۹]

پرداخت سیار: عبارت است از فرآیندی که دو طرف را قادر می سازد تا ارزش‌مالی یک محصول یا سرویس را با استفاده از یک دستگاه سیار مبادله کنند. [۲۹]

دستگاه سیار: عبارت است از کلیه دستگاه‌های بی‌سیم، انواع PDA [۱]ها، کامپیوترهای شخصی قابل حمل و گوشی‌های تلفن همراه. [۲۹]

شبکه بی سیم: عبارت است از انواع شبکه‌های WiFi، شبکه‌های ماهواره‌ای، رادیویی، مادون قرمز و شبکه‌های تلفن همراه. [۲۹]

در چند سال گذشته رشد نمایی استفاده از دستگاه‌های تلفن همراه با افزایش کاربران اینترنت، چشم اندازهای اقتصادی گسترده‌ای از ترکیب این دو بوجود آمده است در سال ۲۰۰۸ میلادی در حدود ٤۰۰ میلیون نفر به مشترکان تلفن در جهان افزوده شده است که انتظار می رود این رقم در سال ۲۰۱۰ به یک میلیارد و ٦۷٦ میلیون عضو ثابت برسد. [۳۰] همچنین پیش بینی شده است تراکنش‌های پرداخت سیار از

[۱] Personal Data Assistant

۷۸ میلیون به ۱۷۵ میلیون خواهد رسید. حجم پرداخت سیار در سال ۲۰۰۸ بالغ بر ۳۰۰ میلیون دلار بوده است و تخمین زده می شود این رقم در سال ۲۰۱۰ به ۱۰ میلیارد دلار برسد. [۳۰]

این رشد بخاطر افزایش گسترده ارائه سرویس‌ها و محتوا از طریق تلفن همراه، ورود راه حل‌های پرداخت جدید به بازار و به دنبال آن افزایش تقاضای مشتریان خواهد بود. خصوصیات کلیدی که باعث گسترش و استقبال از تجارت الکترونیکی سیار شده است در زیر توضیح داده شده اند.

حضور در همه جا و همه وقت[۱] : مزیت همه جا، همه وقتِ تجارت سیار، یعنی دسترسی به اطلاعات به صورت بلا درنگ و بدون توجه به مکان فیزیکی کاربر

قابلیت دسترسی[۲] : استفاده از دستگاه تلفن همراه امکان دسترسی در هر زمان و هر کجا را به کاربر می دهد در عین حال این امکان برای کاربر وجود دارد که دسترسی افراد خاص را برای برقراری ارتباط با او محدود کند.

شخصی سازی[۳] : گوشی ها ابزارهای بسیار کارای شخصی هستند که قابلیت ذخیره اطلاعات و دسترسی به داده ها و خدمات را به طور مستقل و شخصی برای هر فرد فراهم می کنند.

مکان یابی[٤] : توجه به اینکه کاربر در هر لحظه کجاست و فراهم کردن اطلاعات مرتبط با آن محل یک ارزش یکتا است که فقط برای محیط سیار قابل تصور است.

راحتی[٥] : استفاده کنندگان از دستگاه های سیار به استفاده از دستگاه خود و دسترسی به داده‌ها و اینکه همیشه همراه آنها باشد عادت می کنند. بنابراین برنامه های پیشرفته و جدید برای این دستگاه‌ها بیشتر مورد توجه دارندگان آنها قرار می گیرد.

---

[۱] Ubiquity

[۲] Reachability

[۳] Personalization

[٤] Localization

[٥] Convenience

دسترسی به اینترنت[۱] : اتصال فوری به اینترنت از طریق تلفن همراه پیش از این به واقعیت پیوسته است و با ورود سرویس‌های GPRS سرعت گرفته است. با استفاده از GPRS بدون روشن کردن یک کامپیوتر شخصی یا برقراری تماس می توان ساده‌تر و سریع‌تر به اطلاعات روی وب دسترسی پیدا کرد بنابراین دستگاه‌های سیار به روشی برتر برای دسترسی به اطلاعات بدل خواهند شد.

در عین حال فاکتورهایی هم وجود دارند که می توانند گسترش و رشد تجارت الکترونیکی سیار را کند کرده و یا محدود نمایند این عوامل در زیر آورده شده اند.

قابلیت کار با همه سیستم‌ها[۲] : به خاطر تنوع انواع سیستم‌های عامل و قابلیت گوشی‌ها و دستگاه‌های سیار فراهم کردن سرویسی که همه را در بر بگیرد نیازمند سرمایه گذاری زیاد از طرف فراهم کنندگان محتوا می باشد این امر می تواند منجر به عدم رغبت بعضی از سرویس دهندگان به ارائه سرویس در این محیط شود.

قابلیت استفاده[۳] : فراهم کنندگان محتوا برای اینترنت از صفحه های نمایش بزرگ و قابلیت های چند رسانه ای استفاده می کنند محدودیت‌های تلفن‌های همراه می تواند جاذبه برای انتقال سرویس به آن را کم کند.

امنیت[٤] : نگرانی در مورد امنیت تجارت الکترونیکی روی اینترنت هنوز هم وجود دارد این نگرانی ها به محیط سیار نیز منتقل شده است ولی به دلیل خصوصیات خاص این محیط تهدیدها و در نتیجه عدم اطمینان در این محیط بیش از اینترنت مطرح می باشد.

با این حال با رشد نفوذ تلفن‌های همراه و توسعه تجارت سیار، پرداخت سیار یک سرویس تنها نیست بلکه یک نیاز اجتناب ناپذیر برای پرداخت هزینه کالاها و گسترش تجارت سیار خواهد بود. این

---

[۱] Internet Access

[۲] Interoperability

[۳] Usability

[٤] Security

امر مستلزم پیاده‌سازی پروتکل‌های بی‌سیمی است که بتوانند مکانیزم‌های پرداخت از راه دور را به خوبی روش‌های رو در رو با استفاده از یک دستگاه واحد مدیریت نماید. این خدمات می‌توانند یک دستگاه تلفن همراه را به یک ابزار تجارت که می تواند جایگزین ATM[۱] و کارت های اعتباری شود، تبدیل کنند. البته نباید ریسک‌ها و مشکلات امنیتی خاص این محیط را نادیده گرفت. براساس تحقیقات انجام گرفته توسط Forrester مسائل امنیتی مانع اصلی برای حدود ۵۲ درصد کسانی است که هیچ نوع تراکنش تجاری با تلفن همراه انجام نمی دهند. [۳۱]

امن کردن اطلاعات پرداخت روی اینترنت و شبکه های موبایل کار پر زحمت ولی ممکنی است. با دقت کافی، توجه به جزییات، انتخاب و استفاده از ابزارهای مناسب می توان حریم‌های خصوصی و جامعیت را هم برای داده های مشتریان و هم برای سایر داده‌ها فراهم نمود. همیشه باید توجه داشت که هر راه حل امنیتی نیاز به توجه و نظارت دائمی دارد.

پرداخت الکترونیکی یک قدم بسیار بزرگ در بین تغییرات مستمر روش‌های پرداخت بوده است. از زمانی که سیستم‌های پرداخت با کارت‌های اعتباری و سایر انواع کارت ابداع شد واریزهای الکترونیکی از / به حساب نیز به نوعی وجود داشته است. چیزی که باعث می‌شود تا یک مکانیزم پرداخت به صورت الکترونیکی انجام شود آن است که بر خلاف پول ، صورت حساب یا سکه‌ها که ارزش مالی دارند ، هیچ روش نقدی در این نوع پرداخت استفاده نمی‌شود و بر اساس اطلاعات مبادله شده در یک تراکنش ، حساب‌های مناسبی که حاوی پول نمادین هستند بین بانک‌ها و موسسات مالی ایجاد شده و تبادلات میان آنها انجام می‌شود. بر این اساس به نظر می‌رسد یکی از جامع‌ترین تعاریف برای پرداخت الکترونیکی از طرف گروه ePSO باشد. مطابق این تعریف پرداخت الکترونیکی عبارت است از فراهم کردن وسیله پرداخت برای محصولات و سرویس‌ها از طریق شبکه ارتباط عمومی (خصوصا اینترنت) به نحوی که کلیه اطلاعات مربوط به پرداخت بوسیله این شبکه ارسال شده و نیاز به هیچ ارتباط خارجی (فکس ، تلفن یا پست) نباشد.

[۱] Automated Teller Machine

امروزه پرداخت الکترونیکی بخش بسیار کوچکی از پرداخت‌های انجام شده را در بر می‌گیرد. بر اساس آمارهای Federal Reserve Bank of St.Louis در سال ۱۹۹۵ در حدود ۸۰٪ از خریدهای جرئی در آمریکا نقدا انجام می‌شده است و ۹۶٪ از تراکنش‌های بین تجار با چک‌های کاغذی صورت می‌گرفته است. حتی بعد از یک دهه استفاده از سیستم‌های پرداخت الکترونیکی ، تعداد چک‌های کاغذی که هنوز مورد استفاده قرار می‌گیرد بسیار قابل توجه است (۲۰۰ میلیون چک در روز). با این حال حجم کلی تراکنش‌های مالی مبادله شده به روش نقدی و چک بخش کوچکی از کل تراکنش‌های مالی را تشکیل می‌دهد. به عبارت دیگر پرداخت الکترونیکی که از نظر تعداد کمتر از ۵ درصد کل تراکنش‌ها را در بر می‌گیرد ، از نظر حجم ۸۸٪ تراکنش‌ها را شامل می‌شود.

به پیشبینی گروه Forrester Research ، میزان فروش برخط در آمریکا از ۹۷.۵ میلیارد دلار در سال ۲۰۰۲ به ۲۲۹ میلیارد دلار د رسال ۲۰۰۸ خواهد رسید که تنها ده درصد از کل پردخت کاملا برخط خواهد بود. در سال ۲۰۰۳ بانک‌ها بیشترین سرمایه گذاری را روی توسعه سیستم‌های پرداخت داشته اند. سهم آنها ۱.٤۸ میلیارد دلار ، فروشندگان ۱۰۰ ملیون دلار و سایر موسسات ۲۰۰ ملیون دلار بوده است.

پرداخت تلفن همراه عبارت است از هر تراکنشی که میان دستگاه‌های تلفن‌همراه به اجرا درآید و میان گروه‌ها[۱] مبادله مستقیم یا غیر مستقیم ارزش پولی[۲] صورت گیرد. ویژگی جالب پرداخت تلفن همراه این است که دستگاه تلفن همراه می تواند به عنوان وسیله ای برای تمام حالت‌های پرداخت، استفاده شود. افراد خوش بین بر این باورند که اقتصاد جهان شاهد گذار تلفن همراه از یک وسیله ارتباطی ساده به یک مکانیزم پرداخت خواهد بود[٤و۹و۱۰و۱۲و۱۷].

این روزها، پروتکل‌های پرداخت تلفن همراه زیادی ارائه شده است و بیشتر آنها بر اساس زیر ساخت کلید عمومی هستند که برای شبکه‌های بی‌سیم نامناسب است. برخی از آنها اطلاعات کارت اعتباری گروههای درگیر در تراکنش را در تلفن همراه او ذخیره می کنند یا بدون محافظت در تراکنش از آن استفاده می کنند. همین موضوع است که آنها را در معرض خطر قرار می دهد. بیشتر این پروتکل‌های

[۱] Parties

[۲] Fiscal

پرداخت برای حفظ جریان سنتی داده‌های پرداخت طراحی شده‌اند (متقاضی[۱]، فروشنده[۲]، بانک فروشنده)، یعنی تراکنش بین متقاضی و فروشنده انجام می شود. بنابر این، احتمال حمله‌هایی مثل تغییر تراکنش یا میزان آن از طرف فروشنده وجود دارد. همچنین خطر بدست آوردن اطلاعات کارت بدهی[۳] یا اعتباری[٤] متقاضی که ممکن است منجر به دسترسی غیر مجاز به حساب او شود، افزایش می یابد. علاوه بر این، اطلاع‌رسانی از طرف بانک متقاضی به متقاضی بعد از انجام موفقیت‌آمیز تراکنش وجود ندارد. کاربر مجبور است به سایت بانک خود رجوع کرده و بعد از وارد شدن به آن مانده حساب خود را چک کند [۲و٦و۹و۱۰و۱۱و۱۳و۱٤و۱۵و۱۸و۱۹و۲۰].

علاوه بر این، در طراحی برخی از پروتکل‌های تلفن‌همراه نگرانی در مورد حفظ حریم شخصی مشتری دیده نمی شود. اطلاعات شخصی مشتری از جمله هویت مشتری و جزئیات تراکنش نه تنها برای فروشنده، بلکه برای دروازه‌پرداخت[۵] و بانک‌ها نیز آشکار می شود [۳و۹و۱۰و۱۱و۱٤و۱۹].

به علاوه، پروتکل موافقت کلید دیفی هلمن دارای محاسبات سنگینی است. بنابراین، برای تولید کلید نشست مشترک استفاده نشد. برای یک دستگاه تلفن همراه با منابع محدود خوب نیست که چنین محاسبات سنگینی را برای تولید یک کلید نشست مشترک انجام دهد. بعلاوه، در دیفی هلمن اگر هر کدام از گروه‌ها کلید خصوصی خود را $(p-۱)/۲$ انتخاب کنند، آنگاه پارامتر عمومی هر کدام از این دو گروه $(p-۱)$ خواهد بود. بنابراین، اگر پارامتر عمومی $(p-۱)$ باشد، یک مزاحم می تواند خیلی بی‌دردسر فرض کند که کلید خصوصی هر کدام $(p-۱)/۲$ است. کلید $(p-۱)/۲$ در این پروتکل کلید خصوصی ضعیفی است [۲۲و۲۳و۲٤و۲۵و۲٦و۲۷و۲۸].

---

[۱] Client

[۲] Seller

[۳] Debit Card

[٤] Credit Card

[۵] Payment Gateway

با توجه به این مشکلات، اولین هدف این مقاله ایجاد یک پروتکل خصوصی پرداخت تلفن‌همراه می‌باشد که شامل اپراتور شبکه تلفن‌همراه بوده و از عملیات کلید متقارن استفاده می کند. دومین هدف پیشنهاد پروتکل موافقت کلید برای تولید کلید نشست مشترک بین دو گروه با محاسباتی کمتر از دیفی هلمن می باشد. بقیه این مقاله به صورت زیر طراحی شده. در فصل اول مقدمه‌ای از بحث بیان می‌گردد. فصل دوم شامل بررسی بحث از دیدگاه امنیت است. در فصل سوم پروتکل‌های موجود پرداخت الکترونیکی مورد بررسی قرار می‌گیرند. در فصل ٤ دو پروتکل پیشنهادی مطرح می‌شوند. سرانجام فصل ۵ نتیجه گیری ما از این پایان‌نامه می باشد.

فصل دوم

امنیت در پرداخت الکترونیکی

۲-۱ امنیت پرداخت‌ها و تراکنش‌ها

ظهور شبکه‌های بی‌سیم و موبایل تجارت الکترونیکی را به تجارت سیار گسترش دادند. تجارت سیار بر بستر زیر ساخت‌های شبکه موجود که شامل شبکه‌های سیمی هم شدند. بنابراین مسایل امنیتی در آن با مسائل امنیت شبکه بسیار نزدیک و در بعضی موارد یکسان می‌باشد. بدون درک کامل امنیت و موارد مربوط به آن تجارت سیار محقق نخواهد شد.

امروزه سرمایه‌های اطلاعاتی هسته مرکزی سیستم‌های تجارت الکترونیک هستند.بنابراین حفاظت این سرمایه‌ها یک انتخاب نیست بلکه یک نیاز اصلی برای موفق شدن است. موفقیت در حفاظت از داده و حریم‌های خصوصی نتیجه معیارهای مناسب امنیتی می‌باشد.در عین حال حفاظت از یک سیستم تجارت الکترونیکی نمی‌تواند با یک روش امنیتی تنها به نتیجه برسد. این مهم است که ترکیب مناسبی از سیاست‌ها و شیوه‌ها و ابزارهای مطمئن را برای ایجاد یک محیط امن شبکه‌ای بشناسیم.

اکثر سازمان‌ها از مشکل دسترسی غیرمجاز به داده‌های شخصی با اطلاع هستند.ولی تعداد کمی یک برنامه امنیتی خوب برای سیستم‌هایشان پیاده سازی کرده‌اند و به رغم افزایش آگاهی از نیازهای امنیتی ، اغلب آن‌ها با مسئله کمبود مهارت‌های امنیتی مواجه هستند. این فصل به بررسی امنیت پیغام‌ها و تراکنش‌ها روی یک شبکه باز بدون در نظر گرفتن رسانه انتقال دهنده می‌پردازد و در آن موارد زیر مختصرا بررسی می‌شوند.

حملات امنیتی: هر عملی که امنیت اطلاعاتی را که سازمان مالک آن است به خطر بیندازد.

مکانیزم‌های امنیتی: یک مکانیزم که برای تشخیص و ممانعت از یک حمله امنیتی طراحی شده است.

سرویس‌های امنیتی: یک سرویس که امنیت سیستم پردازش داده و انتقال داده را بهبود می‌بخشد. سرویس‌ها ، خاص مقابله با حمله‌های امنیتی هستند و از یک یا چند مکانیزم امنیتی برای فراهم کردن سرویس استفاده می‌کنند [۳۰].