



دانشگاه گیلان

پردیس بین الملل

پایان نامه کارشناسی ارشد

طراحی مدل امن ارتباط مشتری و بانک و بالعکس
با استفاده از زیرساخت کلید عمومی برای شبکه‌های سلولی

از

مونا پورقاسم

استاد راهنما:

دکتر رضا ابراهیمی آقانی

اسفند ماه ۱۳۹۱

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

دانشکده پردیس بین الملل
گروه مهندسی فناوری اطلاعات - تجارت الکترونیک

طراحی مدل امن ارتباط مشتری و بانک و بالعکس با استفاده از زیرساخت کلید عمومی برای شبکه‌های سلولی

از
مونا پورقاسم

استاد راهنما:
دکتر رضا ابراهیمی آتانی

اسفند ماه ۱۳۹۱

تقدیم به:

پدر و مادر عزیزم برای همه خوبی هایشان

و به همسر مهربانم بخاطر همه همراهی هایش

تشکر و قدردانی:

شکر خداوند متعال را بجای آورده که توفیق نصیب من کرد تا این پایان نامه را به سرانجام برسانم و با سپاس از استاد ارجمندم جناب آقای دکتر رضا ابراهیمی آتانی که با صبر و توصیه های ارزشمند خود مسیر انجام این پایان نامه را آسان نموده و از حمایت های بیدریغ ایشان بهره مند شدم. از داوران محترم سرکار خانم دکتر راهبه نیارکی و جناب آقای دکتر هاشم صابری که زحمت داوری این پایان نامه را بر عهده داشتند، صمیمانه تشکر و قدر دانی دارم. همچنین از جناب آقای مهندس فرزاد توکلی به دلیل کمک های بی دریغشان تشکر می نمایم. اما تقدیر ویژه ام از همسر مهربانم خواهد بود بخاطر حمایت های مداوم و دلگرمی های ایشان.

فهرست مطالب

۱	فصل ۱: مقدمه
۲	۱-۱- مقدمه
۳	۲-۱- هدف
۴	۳-۱- ساختار کلی پایان نامه
۵	فصل ۲: مروری بر ادبیات فنی
۶	۱-۲- مقدمه
۷	۲-۲- تجارت همراه
۷	۱-۲-۲- روند پیشرفت تجارت
۸	۲-۲-۲- پیشینه تجارت همراه
۸	۳-۲-۲- لزوم حرکت به سمت تجارت همراه
۱۰	۳-۲-۳- روند تکامل شبکه های سلولی
۱۰	۱-۳-۲- تعریف شبکه های سلولی
۱۱	۲-۳-۲- شبکه های نسل اول
۱۲	۳-۳-۲- شبکه های نسل دوم
۱۲	۱-۳-۳-۲- WAP
۱۵	۲-۳-۳-۲- SMS
۱۶	۳-۳-۳-۲- USSD
۱۶	۴-۳-۳-۲- کانال صوتی
۱۶	۴-۳-۲- شبکه های نسل ۲.۵
۱۷	۱-۴-۳-۲- GPRS
۱۸	۲-۴-۳-۲- EDGE
۱۸	۵-۳-۲- شبکه های نسل سوم
۱۸	۶-۳-۲- شبکه های نسل چهارم
۱۹	۴-۲- امنیت
۱۹	۱-۴-۲- حمله ها و تهدیدات امنیتی
۲۱	۲-۴-۲- فاکتورهای امنیتی در انتقال پیام
۲۳	۳-۴-۲- مکانیزم های امنیتی
۲۷	۴-۴-۲- زیر ساخت کلید عمومی
۲۷	۱-۴-۴-۲- مروری بر PKI

۲۸ گواهی نامه ۲-۴-۴-۲
۲۹ صدور گواهی نامه ۳-۴-۴-۲
۳۰ گواهی نامه X.509 ۴-۴-۴-۲
۳۱ چرخه حیات گواهینامه ۵-۴-۴-۲
۳۲ کارت SIM ۵-۴-۲
۳۳ جمع بندی ۵-۲

فصل ۳: کارهای انجام شده

۳۴	
۳۵ مقدمه ۱-۳
۳۶ امضای الکترونیکی در کشور ۲-۲
۳۷ مرکز دولتی صدور گواهی الکترونیکی ریشه ۱-۲-۳
۳۷ مراکز صدور گواهی الکترونیکی (CA) ۱-۱-۲-۳
۳۷ مرکز صدور گواهی الکترونیکی میانی بازرگانی ۲-۱-۲-۳
۳۸ سطوح اطمینان در زیرساخت کلید عمومی کشور ۲-۲-۳
۳۸ اجزای زیرساخت کلید عمومی ۳-۲-۳
۴۰ انتشار و وظایف مخزن ۴-۲-۳
۴۰ ملزومات الگوریتم های رمزنگاری ۵-۲-۳
۴۱ دستورالعمل طراحی و ارزیابی الگوریتم های رمزنگاری بومی ۶-۲-۳
۴۲ پروتکل مدیریت گواهیهای الکترونیکی ۷-۲-۳
۴۳ امضای همراه ۳-۳
۴۴ مدل های مبتنی بر WAP ۴-۳
۴۴ مدل سرور WAP ۱-۴-۳
۴۵ مدل دروازه WAP ۲-۴-۳
۴۶ مدل رمزگذاری دوبل ۳-۴-۳
۴۷ مدل های مبتنی بر اینترنت ۵-۳
۴۷ راه حل مبتنی بر سرور ۱-۵-۳
۴۸ سرویس امضای همراه ۲-۵-۳
۵۰ واحد برنامه کاربردی امضای همراه (MSAU) ۳-۵-۳
۵۲ سرویس امضا همراه مستقل از اپراتور شبکه همراه ۴-۵-۳
۵۵ آنالیز امنیتی مدل سرویس امضای همراه مستقل از اپراتور شبکه همراه ۱-۴-۵-۳
۵۶ جمع بندی ۶-۳

فصل ۴: مدل پیشنهادی

۵۷

۵۸	۱-۴- مقدمه
۵۸	۲-۴- نحوه عملکرد امضای همراه
۶۰	۱-۲-۴- SHA1
۶۱	۲-۲-۴- RSA
۶۲	۳-۴- انتخاب الگوریتم رمزنگاری متقارن:
۶۳	۱-۳-۴- زبان پیاده سازی J2ME
۶۵	۲-۳-۴- نتایج پیاده سازی
۶۹	۳-۳-۴- الگوریتم رمزنگاری Sosemanuk
۷۰	۴-۴- معرفی معماری مدل پیشنهادی
۷۱	۱-۴-۴- اجزا و نقشهای موجود در سیستم
۷۵	۲-۴-۴- جریان تراکشن ها
۷۵	۳-۴-۴- نیازمندیهای امنیتی و آنالیز آن
۷۶	۱-۳-۴-۴- پردازش گواهینامه
۷۷	۲-۳-۴-۴- ثبت نام کاربر همراه در بانک
۷۷	۳-۳-۴-۴- درخواست امضای همراه و تولید آن
۷۹	۴-۴-۴- ویژگی های امنیتی در تبادل اطلاعات
۷۹	۵-۴-۴- شبیه سازی
۸۰	۱-۵-۴-۴- طراحی
۸۰	۲-۵-۴-۴- انتخاب زبان و محیط مناسب
۸۰	۳-۵-۴-۴- محیط توسعه Gemalto Developer Suit
۸۹	۵-۴- جمع بندی

فصل ۵: جمع بندی و پیشنهادها

۹۰

۹۱	۱-۵- مقدمه
۹۱	۲-۵- جمع بندی
۹۲	۳-۵- نوآوری
۹۳	۴-۵- پیشنهادها

۹۴

مراجع

فهرست شکل‌ها

- شکل (۱-۲) عناصر اصلی شبکه‌های سلولی [8]..... ۱۱
- شکل (۲-۲) معماری WAP [12]..... ۱۳
- شکل (۳-۲) جریان عادی اطلاعات [۹]..... ۲۰
- شکل (۴-۲) حمله وقفه [۹]..... ۲۰
- شکل (۵-۲) حمله استراق سمع [۹]..... ۲۰
- شکل (۶-۲) حمله ایجاد تغییر [۹]..... ۲۰
- شکل (۷-۲) حمله جعلی سازی [۹]..... ۲۱
- شکل (۸-۲) نحوه امضای یک پیام دیجیتال [۱۹]..... ۲۶
- شکل (۹-۲) نحوه اعتبار سنجی امضای دیجیتال [۱۹]..... ۲۶
- شکل (۱۰-۲) فیلدهای معمول در گواهینامه [12]..... ۲۸
- شکل (۱۱-۲) سلسله مراتب گواهی نامه [12]..... ۳۰
- شکل (۱۲-۲) تصویر کلی از PKI [۱۸]..... ۳۲
- شکل (۱-۳) ساختار سلسله مراتبی زیرساخت کلید عمومی کشور [۳۴]..... ۳۹
- شکل (۲-۳) مدل سرور WAP [42]..... ۴۵
- شکل (۳-۳) تصدیق صحت WTLS/TLS [42]..... ۴۵
- شکل (۴-۳) نمودار مدل رمزگذاری دوبل [43]..... ۴۶
- شکل (۵-۳) روند کلی تولید امضای همراه در مکانیزم مبتنی بر سرور [52]..... ۴۸
- شکل (۶-۳) سرویس امضای همراه [24]..... ۵۰
- شکل (۷-۳) معماری برنامه کاربردی خدمت همراه [53]..... ۵۱
- شکل (۸-۳) نقش‌های موجود در سیستم [54]..... ۵۳
- شکل (۹-۳) روند امضای همراه [54]..... ۵۴
- شکل (۱-۴) نمودار خطی زمان-طول پیام ۴ رمز دنباله ای..... ۶۸
- شکل (۲-۴) نمودار میله ای زمان-طول پیام ۴ رمز دنباله ای..... ۶۸
- شکل (۳-۴) جریان تراکنش مدل پیشنهادی..... ۷۱
- شکل (۴-۴) حداقل اجزای سرویس امنیت در سرویس دهنده بانک..... ۷۳
- شکل (۵-۴) اجزا و تجهیزات تلفن همراه..... ۷۴
- شکل (۶-۴) نحوه تبادل داده بین برنامه کاربردی دستگاه تلفن همراه و برنامه SIM کارت..... ۷۴

- شکل (۷-۴) جریان تراکنش و پیغام ها مابین مشتری، بانک و PKI ۷۵
- شکل (۸-۴) محیط توسعه Gemalto ۸۱
- شکل (۹-۴) مراحل ایجاد Java card [62] ۸۱
- شکل (۱۰-۴) مراحل ایجاد Java card [62] ۸۲
- شکل (۱۱-۴) پروژه ایجاد شده در GEMALTO ۸۳
- شکل (۱۲-۴) شمایی از برنامه و همچنین تابع رمزنگاری عدد ورودی ۸۵
- شکل (۱۳-۴) شبیه سازی انجام شده Stream رمز نگاری شده ۸۶
- شکل (۱۴-۴) شبیه سازی انجام شده مربوط به برقراری ارتباط با سرور ۸۶

فهرست جدول‌ها

- جدول (۱-۲) آخرین وضعیت شبکه تلفن همراه در کشور [۶] ۹
- جدول (۲-۲) فهرست برخی از کشورها بر اساس تعداد تلفن همراه در حال استفاده [3] ۱۰
- جدول (۳-۲) مشخصه های کارت هوشمند [23] ۳۳
- جدول (۱-۴) اطلاعات تلفن‌های همراه مورد آزمون ۶۶
- جدول (۲-۴) زمان اجرای الگوریتم‌ها ۶۷

طراحی مدل امن ارتباط مشتری و بانک و بالعکس با استفاده از زیرساخت کلید عمومی برای شبکه‌های سلولی مونا پورقاسم

در دنیای امروز استفاده از شبکه های کامپیوتری و مخابراتی، از ملزومات زندگی بشر محسوب می‌شود. در این میان ابزارها و ادوات همراه به دلیل در دسترس بودن، جایگاه ویژه‌ای یافته‌اند. این ویژگی علاوه بر بوجود آوردن تسهیلات فراوان همانند انجام تراکنش های مالی در هر مکان و زمان، حساسیت هایی را در زمینه تامین امنیت این دستگاه‌ها برانگیخته است.

زیرساخت کلید عمومی (PKI) یکی از الزامات اجتناب ناپذیر تراکنش های اطلاعاتی در کاربرد های تجاری و دولتی می باشد. چرا که، تمامیت پیام، احراز هویت کاربر و انکار ناپذیری تراکنش ها را با استفاده از امضای دیجیتال تضمین می‌نماید. چنانچه امنیت امضای دیجیتال تضمین گردد، از نظر قانونی می‌تواند معادل امضای دست نوشته شده در نظر گرفته شود. با توجه به گسترش سریع دستگاه‌های تلفن همراه، که مبتنی بر کارت های SIM/USIM، می باشند، این دستگاه ها را می توان به عنوان دستگاه‌های ایده‌آل برای ایجاد امضای دیجیتال در نظر گرفت. علاوه بر این، با بکارگیری امضای همراه، توسعه برنامه‌های کاربردی مبتنی بر این امضا برای ارائه دهندگان خدمات و برنامه‌های کاربردی همراه ساده می‌گردد. در تراکنش‌هایی همچون برخی از مراودات بانکی که احراز هویت مشتری از اهمیت بالایی برخوردار است، استفاده از این زیرساخت می تواند نقش بسزایی در ایجاد امنیت داشته باشد.

در این پایان نامه یک مدل امن به منظور ارتباط بین مشتری و بانک با استفاده از تلفن همراه و بر بستر اینترنت در شبکه های سلولی پیشنهاد شده است. که در آن از رمز نگاری متقارن برای ایجاد محرمانگی و از PKI به منظور احراز اصالت کاربران استفاده می شود. مدل پیشنهادی علاوه بر امنیت و کارایی با توجه به امکانات موجود شبکه تلفن همراه در کشور طراحی شده است. این مدل به گونه ای طراحی شده که با پیشرفت های شبکه تلفن همراه سازگاری لازم را داشته باشد.

واژه‌های کلیدی: زیرساخت کلید عمومی، امنیت، رمزنگاری، شبکه های سلولی

Abstract

Customer relationship and bank security model, using a public key infrastructure for cellular networks

Mona Pourghasem

In today's world the use of computer networks and telecommunications is essential for human life. Among these, mobile tools and devices due to availability, has been found a special place. This feature in addition to provide numerous facilities in every place and time, such as financial transactions, are raised the sensitivity in the field of security of these devices.

Public key infrastructure (PKI) is one of the unavoidable requirements information transactions in the commercial and governmental applications. Because, it is guaranteed message integrity, user authentication and transactions undeniable by using the digital signature. If security of digital signature is ensure, legally can be considered equivalent to a handwritten signature. Due to the rapid development of mobile devices, which are based on the SIM/USIM cards, these devices can be considered as an ideal device for creating digital signatures. Furthermore, with the use of mobile signatures, the development of applications based on this signature will be simple for service providers and mobile applications. In the transactions, such as some of bank exchanges, which client authentication is very important, the use of this infrastructure can have a significant role in security.

In this thesis a secure model has been proposed in order to establish a connection between customer and bank by using mobile phone and on the internet at the cellular networks. In which the symmetric encryption is used to provide confidentiality and PKI is used for authentication of user's authenticity. The proposed model in addition to security and efficiency is designed due to the existing mobile network facilities in the country. The model is designed in a way that would be have consistent with advances in mobile networks.

Keywords: Public key infrastructure, security, cryptography, cellular networks

فصل ۱:

مقدمه

۱-۱- مقدمه

در دهه‌ی اخیر نیازمندی‌های ارتباطی مردم به واسطه گسترش و نفوذ اینترنت و تلفن همراه تغییر نموده است؛ به طوری که مشترکان شبکه‌های مخابراتی خواهان ارائه‌ی خدماتی متنوع، همانند خدمات بانکی و یا دولتی با کیفیت مطلوب بر روی شبکه‌های عمومی می‌باشند. آمارها حاکی از آن است که سرعت رشد استفاده از تلفن همراه در شبکه‌های سلولی به مراتب بیشتر از سایر شبکه‌های سیمی می‌باشد و این به دلیل قابلیت ویژه‌ی تلفن همراه، که همان سادگی حمل و استفاده در هر مکان و زمان است؛ می‌باشد. به دلیل همین ویژگی ادوات مورد استفاده در شبکه‌های سلولی، حوزه جدیدی تحت عنوان "تجارت همراه" در "تجارت الکترونیکی" ایجاد شده است. از طرف دیگر بخش قابل توجهی از تجارت، عملیات و تراکنش‌هایی است که به واسطه‌ی بانک‌ها و موسسات مالی صورت می‌پذیرد.

سیستم‌های بانکداری همراه، این فرصت را فراهم می‌سازند تا مشتریانی که از این خدمات استفاده می‌نمایند بتوانند به راحتی به فعالیت‌های بانکی خود دسترسی داشته باشند. در بانکداری همراه از تکنولوژی‌های ارتباطی مختلفی استفاده می‌گردد که از آنجمله می‌توان به SMS^۱، IVR^۲ و WAP^۳ اشاره نمود. مشکلات تکنولوژی‌های ذکر شده همچون، قابلیت اعتماد ضعیف، سرعت نسبتاً پایین و هزینه‌ی زیاد از یک طرف و همچنین سیر تکاملی سیستم‌های تلفن همراه که در جهت بهبود سرویس دهی می‌باشد از طرف دیگر، تغییرات زیادی را در ارائه‌ی سرویس‌های همراه بوجود آورده است. به همین دلیل امروزه با ارائه نسل ۲.۵ به بعد در شبکه‌های تلفن همراه که همان GPRS^۴ و تکنولوژی‌های پس از آن در شبکه‌های نسل سوم و چهارم است، شاهد ارائه خدمات تحت وب بر روی شبکه‌های سلولی می‌باشیم. استفاده از وب، به دلیل سهولت استفاده و کاربر پسند بودن، همچنین امکان رهگیری فعالیت‌های انجام شده و هزینه بسیار کمتر در مقایسه با سایر روش‌ها، برتری ویژه‌ای دارد و به همین دلیل چنانچه بتوان فاکتورهای امنیتی را تامین نمود، می‌توان آن را به عنوان بستری مناسب، برای ارتباط بین مشتری و بانک مورد استفاده قرار داد.

اهمیت موضوع تامین امنیت، در تراکنش‌هایی که توسط دستگاه تلفن همراه انجام می‌شوند به دلیل این است که این تراکنش‌ها به طور ذاتی در بسترهای ناامنی همچون شبکه‌های بی‌سیم انجام می‌پذیرد و کاربران تنها هنگامی حاضرند تراکنش‌هایی چون تراکنش‌های مالی را بر روی تلفن همراه خود انجام دهند، که از امنیت آن اطمینان کامل داشته باشند.

با توجه به اینکه انجام تراکنش‌های مالی بین بانک‌ها و موسسات مالی و مشتری، بخش مهمی از تجارت همراه به شمار می‌رود؛ حفظ امنیت و اطمینان، از نگرانی‌های بزرگ در تجارت همراه به شمار می‌رود. چرا که علاوه بر

^۱ Short Message Service (SMS)

^۲ Interactive Voice Response (IVR)

^۳ Wireless Application Protocol (WAP)

^۴ General Packet Radio Service (GPRS)

مسائل امنیتی در شبکه‌های سیمی، برخی از مسائل خاص امنیتی با توجه به محدودیت‌های موجود در شبکه‌های تلفن همراه باید لحاظ گردد. در واقع حفظ امنیت و اطمینان از هویت طرفین در زمان انجام تراکنش‌ها به صورت آنلاین، از ضروریات این موضوع به شمار می‌آید. در این خصوص از پروتکل‌ها و تکنولوژی‌های مختلفی استفاده می‌گردد. استفاده از زیرساخت کلید عمومی در شبکه‌های سلولی به این دلیل که احراز و تصدیق هویت در آن توسط مرکز تصدیق هویت کاربر که یک مرجع قانونی است، انجام می‌پذیرد از قابلیت اطمینان بیشتری نسبت به سایر روش‌ها برخوردار است.

زیر ساخت کلید عمومی کلیه فاکتورهای لازم به منظور استفاده از امضای دیجیتال را فراهم می‌آورد. امضای دیجیتال در زمینه‌هایی مانند تجارت الکترونیک و دولت الکترونیک از زمانی که برخی از ویژگی‌های جالب توجه از قبیل یکپارچگی، احراز هویت و انکار ناپذیری را فراهم می‌کند، بحثی اساسی می‌باشد. به همین دلیل، امروزه تعداد بسیار زیادی از برنامه‌های کاربردی مختلف نیاز به استفاده از امضای دیجیتال و سرویس‌های انکار ناپذیری دارند. هدف از امضای دیجیتال این است که صحت و تمامیت اسناد الکترونیکی را در راه معادل سازی آن با امضایی که در اسناد کاغذی نوشته شده است تضمین نماید.

چنانچه امضای دیجیتال با استفاده از ادوات همراه تولید شود، "امضای همراه" نامیده می‌شود. امضای همراه به عنوان یک روش جهانی برای استفاده از یک دستگاه همراه به منظور تایید شهروندان در ادامه انجام تراکنش پیشنهاد گردیده است. علاوه بر این، یکی از مزیت‌های این پدیده آن است که امضایی که در یک دستگاه همراه تولید شده، ممکن است در هر مکان و هر زمان مورد استفاده قرار گیرد. بنابراین می‌توان گفت امضای همراه طراحی شده تا ارائه دهندگان نرم افزارهای کاربردی مجبور به توسعه راه‌حل‌های متعدد برای طیف وسیعی از دستگاه‌های همراه، سیستم عامل‌های ادوات همراه و فناوری‌های امضای دیجیتال که برای دستگاه‌های تلفن همراه وجود دارد، نباشند.

در این پایان نامه، یک مدل امن ارتباط بین مشتری و بانک و بالعکس با استفاده از زیر ساخت کلید عمومی بر روی شبکه‌های سلولی پیشنهاد گردیده و تلاش شده است با بررسی جامع روش‌ها و استانداردهای موجود، بهترین گزینه‌ها برای ارائه این سرویس ارائه گردد. همچنین در طراحی این مدل پیشنهادی سعی بر آن شده که با پیشرفت‌های شبکه تلفن همراه سازگاری لازم لحاظ گردد.

۱-۲- هدف

هدف از این پایان نامه طراحی یک مدل امن برای ارتباط بین مشتری و بانک با استفاده از زیرساخت کلید عمومی (PKI) برای شبکه‌های سلولی می‌باشد. که در آن سعی بر آن شده تا راهکاری عملیاتی برای اجرایی نمودن آن با توجه به وضعیت گذار از شبکه‌های نسل دوم به سوم در کشور ارائه گردد. در این طراحی خدمات امنیتی محرمانگی داده، تمامیت داده، احراز اصالت، انکارناپذیری و سایر ویژگی‌های افزون امنیتی در نظر گرفته شده است.

۱-۳- ساختار کلی پایان نامه

جهت بررسی موارد فوق، در ادامه فصول مختلفی از نظر خواهد گذشت که در اینجا به معرفی عناوین آنها پرداخته می شود:

- فصل دوم به بررسی ادبیات فنی می پردازد. در این فصل، پس از مروری بر تجارت همراه، روند تکامل شبکه های سلولی مطرح خواهد شد. همچنین فاکتورهای امنیتی بیان شده و معرفی زیرساخت کلید عمومی مورد مطالعه قرار می گیرد. در خاتمه نیز به تعریف و جزئیات SIM کارت به عنوان یک بستر مناسب برای احراز اصالت پرداخته می شود.
- در فصل سوم کارهای انجام شده در خصوص زیر ساخت کلید عمومی در کشور بیان شده و همچنین مدل های موجود که در خصوص استفاده از این زیر ساخت بر روی شبکه های سلولی پیشنهاد شده اند، مورد مطالعه قرار می گیرد. در بررسی این مدل ها به بیان مزایا و محدودیت های هر کدام نیز پرداخته می شود.
- فصل چهارم بر اساس آنچه در فصول قبل بیان شد، فاکتورهای لازم در خصوص نحوه عملکرد امضا با استفاده از کلید عمومی، که در طراحی مدل پیشنهادی مورد استفاده قرار می گیرد ارائه و معماری مدل تشریح و مورد ارزیابی قرار می گیرد. همچنین به جهت اطمینان از عملیاتی بودن آن، سرویس بخش های مربوط به کاربر شبیه سازی می گردد.
- در نهایت در فصل آخر (فصل پنجم)، به جمع بندی مسئله و فعالیت های صورت گرفته در خصوص موضوع مورد بحث پرداخته و نوآوری های حاصل شده از طراحی مدل پیشنهادی مطرح می گردد. همچنین، در ادامه نیز پیشنهاداتی در ارتباط با ادامه تحقیقات در آینده تبیین می گردد.

فصل ۲:

مروری بر ادبیات فنی

۲-۱- مقدمه

گسترش و نفوذ ادوات و ابزارهای همراه، تغییرات زیادی را در نیازمندی های جوامع بشری بوجود آورده است. تلفن‌های همراه، دستیاران دیجیتال شخصی (PDA)^۱ و تلفن های هوشمند، امروزه به یک ابزار ضروری برای انجام بسیاری از کارها تبدیل شده اند. به دلیل کوچک و نسبتا ارزان بودن، این ابزارها می توانند نه تنها برای ایجاد تماس های صوتی و تصویری و یا ارسال و دریافت پیام های متنی و چندرسانه ای مورد استفاده قرار گیرند؛ بلکه می توانند در نقش یک کامپیوتر رومیزی نیز ظاهر شوند [1].

استفاده از ابزارهای همراه به عنوان یک کامپیوتر رومیزی، برگرفته از مفهوم محاسبات فراگیر^۲ است که اولین بار توسط مارک وایسر^۳ در سال ۱۹۹۹ مطرح گردید. محاسبات فراگیر مدل تعاملی بین انسان و کامپیوتر می باشد به گونه ای که داخل هر شی در محیط اطراف ما یک کامپیوتر تعبیه شده و عملیات محاسبات و پردازش اطلاعات را انجام می دهد [2]. به دنبال گسترش این مفهوم، استفاده از سایر ابزارها به عنوان کامپیوتر بیش از پیش مورد استقبال و توجه قرار گرفت. این موضوع تا جایی پیش رفت که در حال حاضر ۹۸.۸ درصد ریزپردازنده‌های تولید شده در کارخانه‌ها، به صورت ریز پردازنده تعبیه شده و در سایر دستگاه ها و ابزارها مورد استفاده قرار می‌گیرد و تنها ۱.۲ درصد ریز پردازنده‌ها برای استفاده در کامپیوترهای سنتی تولید می‌شوند [3]. همچنین، پیشرفت سریع تکنولوژی‌های ارتباطی و به دنبال آن تکنولوژی های بی سیم و شبکه های تلفن همراه باعث افزایش محبوبیت ادوات و ابزارهای همراه در بین مردم گردیده است. از ویژگی های برجسته و منحصر به فرد تلفن همراه دسترسی همیشگی و متحرک بودن آن می باشد. تلفن همراه همواره و همه جا با کاربر، همراه است. تلفن‌های همراه از شبکه‌های سلولی برای برقراری ارتباط استفاده می‌نمایند. از مهمترین تراکنش ها بر روی این نوع شبکه ها، ارتباط با بانک ها و سایر موسسات مالی می‌باشد.

در این فصل، برای دستیابی به یک مدل امن با کارایی و پذیرش کافی، پس از مروری بر تجارت همراه، روند تکامل شبکه‌های سلولی مطرح خواهد شد. در ادامه، فاکتورهای امنیتی بیان شده و معرفی زیرساخت کلید عمومی مورد مطالعه قرار می گیرد. در انتها نیز به تعریف و جزئیات SIM کارت به عنوان یک بستر مناسب برای احراز اصالت پرداخته خواهد شد.

¹ Personal Digital Assistant (PDA)

² Ubiquitous Computing

³ Mark Weiser

۲-۲- تجارت همراه

امروزه با گسترش فناوری های الکترونیکی، و بالاخص فناوری های ارتباطی، انجام بسیاری از امور زندگی دستخوش تغییرات زیادی شده است. انجام امور تجاری نیز از این امر مستثنی نبوده و با پیشرفت تکنولوژی، روش های نوین جایگزین روش های سنتی انجام معاملات و بانکداری شده اند. در ادامه برای روشن شدن این تغییرات مروری مختصر، بر سیر تکاملی تجارت خواهیم داشت.

۲-۲-۱- روند پیشرفت تجارت

- تجارت سنتی (T-commerce)¹: به طور معمول، انجام هر گونه امور تجاری با استفاده از تلفن، نمابر و امکانات معمولی بانک ها، تحت عنوان "تجارت سنتی" شناخته می شود.
- تجارت الکترونیکی (E-commerce)²: به انجام امور تجاری که با استفاده از فناوری های جدید (به خصوص امکاناتی که به واسطه ی گسترش اینترنت فراهم آمده اطلاق می شود. از جمله e-mail, chat, ... که بدون محدودیت زمانی، تحت استاندارد های خاص انجام می پذیرد که از معتبرترین این استانداردها می توان به استاندارد بین المللی EDIFACT³ اشاره نمود. یکی از مهمترین الزامات در این گونه تجارت، الزام به استفاده از امضای دیجیتال در انجام معاملات می باشد.
- تجارت همراه (M-commerce)⁴: انجام امور تجاری، با استفاده از فناوری موبایل، تحت ضوابط تجارت الکترونیکی، بدون محدودیت زمانی و همچنین مکانی از ویژگی های این تجارت محسوب می شود.

با این تعاریف و با توجه به ویژگی های برتر تجارت همراه نسبت به انواع دیگر، همچون در دسترس بودن، سهولت استفاده، کم حجم بودن و قابلیت حمل ادوات همراه و امکان استفاده در هر مکان و هر زمان، اینگونه به نظر می رسد که استفاده از تجارت همراه در آینده جایگاه خاصی در جهان داشته باشد. در ادامه به بررسی بیشتر این تجارت خواهیم پرداخت.

¹ Traditional commerce

² Electronic commerce

³ Electronic Data Interchange For Administration, Commerce and Transport (EDIFACT)

⁴ Mobile commerce