ششمین همایش ملی تجارت و اقتصاد الکترونیکی

ارائه یک معماری امنیتی برای سیستم های پرداخت الکترونیکی سیار جهت استفاده در تراکنش های مالی درسیستم های بانک داری و تجارت الکترونیک

مصطفی اخوان صفار [1]

عضو هیات علمی دانشگاه پیام نور- دانشکده مهندسی فن آوری اطلاعات و ارتباطات

چکیده

یکی از بخش های اصلی در هر سیستم تجارت الکترونیکی بحث پرداخت ها و تراکنش های مالی است.امروزه شاهد بروز سیستم ها ی نوین تجارت الکترونیک تحت عنوان سیستم های تجارت الکترونیک سیار می باشیم.همگام با گسترش و تکامل روز افزون شبکه های بیسیم و دستگاه های سیار ،کارایی و امنیت در این سیستم ها و بخصوص سیستم های پرداخت سیار اهمیت ویژه ای پیدا کرده است.ما در این مقاله یک معماری امنیتی جدید برای سیستم های پرداخت سیار مثل بانکداری سیار یا همان سیستم بانکداری از طریق تلفن همراه و سیستم های تجارت الکترونیکی سیار ارائه می کنیم. در واقع در این طرح یک سیستم تصدیق هویت چند عامله ارائه می گردد.معماری این طرح از یک سیستم رمزگزاری سبک که ترکیبی از سیستم های رمزنگاری کلید عمومی و کلید متقارن می باشد،تشکیل شده است. استراتژی ارائه شده برای ورود به تراکنش های سیار ،تمامی ویژگی های لازم در سیستم های امن مانند محرمانگی،تصدیق هویت،صحت و عدم انکار را محقق می سازد.در مقایسه با برخی از سیستم های پردخت سیار ،سیستم پیشنهادی یک مکانیزم امن سبک وزن است که برای تبادلات مالی دو سویه در دستگاه های تلفن همراه که دارای منابع محدود می باشند،بسیار مناسب می باشد.

کلمات کلیدی: تجارت الکترونیک سیار، امنیت،رمزنگاری،تراکنش های مالی الکترونیکی.

---

[1] تلفن: ۰۹۱۳۳۵۶۷۴۳۳

آدرس پست الکترونیکی:akhavansaffar@gmail.com و آدرس کامل

۱.مقدمه

استفاده از شبکه های بیسیم و دستگاه های تلفن همراه با سرعتی چشم گیر روز به روز در حال افزایش می باشد.در چنین شرایطی محافظت از داده هایی که از طریق سیستم های بیسیم ردوبدل می شوند بعنوان یک مسئله حیاتی ،مطرح گردید. در این مقاله یک معماری امنیتی مفید برای سیستم های پرداخت بانکی سیار پیشنهاد می گردد.ما در این مقاله بمنظور اطمینان از وجود تمامی احتیاجات امنیتی لازم در یک سیستم بانکی، یک سیستم رمزنگاری سبک وزن را پیشنهاد می کنیم که در آن از یک مکانیزم تصدیق هویت چند عامله و یک استراتژی مناسب جهت ورود به سیستم برای انجام تراکنش های بانکی استفاده می شود. پیش از این نیز چندین معماری برای سیستم های پرداخت ارائه شده است [1] اما سیستم مورد نظر ما در مقایسه با معماری های پیشین جهت استفاده در سیستم های پرداخت سیار دوسویه مانند دستگاه های تلفن همراه که دارای منابع محدود می باشند ،بسیار ساده تر و مناسب تر می باشد.

۲.تحقیقات انجام شده

مطالعه در مورد پیشینه سیسم های پرداخت الکترونیک می تواند در درک معماری پیشنهاد شده مفید باشد. سیستم های پرداخت الکترونیکی متنوع اند و هر کدام با ویژگی های خاص و با هدف استفاده در شرایط خاص طراحی شده اند. میزان رواج و استقبال از این سیستم ها به ضریب امنیتی، دقت و میزان اعتماد، سرعت آن ها در انجام امورمالی و سهولت استفاده از آن ها بستگی دارد.

ما در این تحقیق دستگاه های تلفن همراه را بعنوان دستگاه های جیبی که بطور کلی دارای قابلیت های محاسباتی و مشاهده سایت های اینترنتی هستند، فرض می کنیم.یک دستگاه موبایل می تواند بعنوان یک شناسه هویت فردی در نظر گرفته شود،که در ان هر فرد بطور کلی صاحب یک دستگاه موبایل بوده و معمولا آن را برای استفاده در اختیار دیگران قرار نمی دهد. در این صورت هر گونه تراکنش مالی که در آن از یک دستگاه سیار مانند موبایل بجای پایانه فروش برای انجام عملیات پرداخت استفاده شود را می توان بعنوان یک سیستم پرداخت سیار در نظر گرفت.[۴] سیستم های پرداخت سیار موجود را می توان به دو دسته تقسیم کرد:یکی دستگاه های پایانه فروش سیار یا همان کارت خوان ها ،که از طریق ارتباط تلفنی یا شبکه‌ای به سیستم بانکی امکان انتقال خودکار مبلغ خرید از حساب فروشنده را فراهم می‌سازد. دستگاه‌های پایانه فروش علاوه بر امکان پرداخت دارای عملکردهای مختلفی از جمله پرداخت قبوض، شارژ سیم‌کارت، اعلام موجودی، دریافت صورتحساب، امکان انصراف از خرید و گزارش روزانه از طریق تلفن همراه است که صاحبان آن را از مزایای شعبه کوچک بانکی برخوردار می‌کند.و دیگری سیستم های مبتنی بر حساب می باشند و کلیه کارت های اعتباری،بدهی و هوشمند در این دسته قرار دارند [۳] . سیستم پیشنهادی مورد نظر ماهم در این دسته قرار دارد. مدل پرداخت دو سویه(طرفه) یکی از ساده ترین مدل های پرداخت سیار می باشد.که در این مدل دوطرف ارتباط مشتری و ارائه دهنده خدمات مالی هستند. عموما شبکه های(کانال های) انتقال بیسیم را بصورت شبکه های محلی بیسیم و شبکه های تلفن همراه می شناسیم.شبکه تلفن همراه یک شبکه رادیویی است که از تعدادی سلول تشکیل شده و هر سلول توسط یک تا تعدادی بیشتری فرستنده که بصورت ثابت

و معمولا در مرکز سلول نصب می گردند،سرویس دهی می شود.سیستم پیشنهادی ما نیر بمنظور استفاده در این نوع شبکه های بیسیم ارائه گردیده است. معمولا اکثر معماری هایی که برای ایجاد امنیت در تبادلات دوسویه ارائه می گردد در یکی از دو لایه انتقال یا کاربردی پیاده سازی می شود. [۷] .معماری مورد نظر ما نیزجهت پیاده سازی بر روی لایه کاربرد پیشنهاد شده است. معماری امنیتی لایه کاربردی، مستقل از پروتکل‌های امنیتی لایه‌های پایین‌تر است و طوری طراحی شده که همه توابع مربوط به امنیت را استفاده می کند. علاوه براین، برای پیاده سازی یک معماری امنیتی لایه کاربردی نیازی به اصلاح پروتکل‌ها و زیرساخت‌های شبکه‌ی بی‌سیم جاری نیست.

- برخی از مشکلات مشتریان در مورد امنیت سیستم های پرداخت سیاردر [۱۱] آورده شده است.جدول شماره۱ بطور خلاصه برخی از نیازمندی های امنیتی و تکنولوژی هایی که قبلا برای آن پیشنهاد شده ،را نشان می دهـد.همچنین ،ستون سوم این جدول راه حل‌هایی ویژه ای است که ما در این مقاله برای حل مشـکلات امنیتـی موجـود پیشـنهاد کرده ایم.

راه حل	تکنولوژی	احتیاجات امنیتی
پین کد دستگاه همراه نام کاربری /رمزعبور	PKP	تصدیق هویت
الگوریتم امضای دیجیتال منحنی بیضوی	امضای دیجیتال	
	امضای دیجیتال	صحت
	امضای دیجیتال	عدم انکار
اتصال تراکنش تجاری	اتصال/ورود	
AES	رمزنگاری/رمزگشایی	محرمانگی

جدول ۱:احتیاجات امنیتی و تکنولوژی های قابل استفاده در سیستم های پرداخت سیار

۳-معماری امنیتی سبک وزن برای تراکنش‌های تجاری سیار

پیش از این مکانیزم های امنیتی سبک وزن برای تراکنش‌های الکترونیکی ایمن با دستگاه‌های دستی پیشنهاد شده است که در آن از مفهوم دروازه پروتوکل بی‌سیم، استفاده شده است.دروازه پروتوکل بی سیم به عنوان یک عامل ثابت برای دستگاه های دستی بکار می‌رود. دستگاه‌های دستی توسط شبکه تلفن همراه به دروازه متصل می‌شوند و دروازه توسط یک شبکه خط ثابت به برنامه کاربردی سرور وصل می‌شود.

- تراکنش‌ها در این روش توسط ترکیبی از دروازه پروتکل بی‌سیم و یک مکانیزم امنیتی انتها به انتها به اجرا در می‌آیند. در این مکانیزم فرض بر این است که دستگاه دستی، قابلیت اتصال در محیط مرورگر اینترنتی را دارا می باشند. در ارتباط بین دستگاه دستی و دروازه پروتوکل بی‌سیم توسط یک کلید محرمانه که بین طرفین به اشتراک گذاشته می شود،عمل تصدیق هویت انجام می گردد.شبکه خط ثابت ، ارتباط بین دروازه پروتوکل بی‌سیم و برنامه کاربردی سرور که ترکیبی از رمزنگاری کلید عمومی و تصدیق هویت پسورد ساد می باشد،را انجام می‌دهد. برای جلوگیری از مشکل عدم انکار نیز یک دستگاه سخت افزاری مقاوم پیشنهاد شد.علی رغم اینکه سیستم ارائه شده پیش نیازهای امنیتی را در تجارت سیار از قبیل تصدیق هویت،

محرمانگی، یکپارچگی و عدم انکار را فراهم می‌کند ولی معایبی نیز در این طرح وجود دارد. یکی از معایب آن این است که یک شکاف امنیتی در دروازه پروتکل بیسیم وجود دارد. دروازه بی‌سیم،داده ها را از دستگاههای ارتباطی دریافت کرده، آنها را توسط یک کلید متقارن رمزگشایی می کند و مجددا آنها را با استفاده از یک کلید رمزنگاری عمومی رمزگذاری می کند، و سپس داده‌ها را به سرور مربوطه می فرستد که این می‌تواند باعث افشای اطلاعات شود.

یکی دیگر از معایب این روش این است که تراکنش سیار در شبکه تلفن همراه انجام می شود. شبکه تلفن همراه توسط اپراتورهای شبکه موبایل ایجاد می شوند؛ در حالی که سرویس های مربوط به برنامه های کاربردی موبایل توسط تولید کنندگان برنامه کاربردی مانند بانک ها و سازمان های تجاری عرضه می شود. ممکن است تولیدکنندگان برنامه های کاربردی تمایل نداشته باشند اپراتورهای شبکه موبایل در برنامه امنیتی‌شان دخالتی داشته باشند. درحالی که در این سیستم هم برای مشتری و هم برای سرور این ضروری است که کلید رمزنگاری مشترکشان توسط یک طرف سومی قابل اعتمادی نگهداری شود،بنابراین لازم است همکاری های مشترکی بین اپراتور تلفن و بانک ها انجام شود.

۱-۳ پروتکل های پرداخت اینترنتی[۱] و تراکنش الکترونیکی امن

پروتکل‌های پرداخت اینترنتی ، گروهی از پروتوکل‌های پرداخت ایمن است که توسط بخش تحقیقاتی شرکت آی.بی.ام توسعه یافته است.[۱]

همه پروتوکل‌های ikp [۱۶]بر پایه رمزنگاری کلید عمومی هستند. به هر حال تعداد کلیدهای عمومی (که گاهی توسط i در ikp نشان داده می شود) بر طبق نیازهای تجاری خاص متفاوت است. این پروتکل ها بسته به تعداد کلیدی که دارند به نام های :.1KP,2KP,3KP شناخته می شوند. ساده‌ترین پروتکل یعنی 1KP، فقط از یکی از سه طرف ارتبا می خواهد که کلید عمومی را نگه دارد . خصوصیات تراکنش الکترونیکی امن[۲] [۲] ، یک رمزگذاری باز و یک طراحی خاص امنیتی است که برای محافظت تراکنش‌های کارت‌های اعتباری در اینترنت طراحی شده است. شرکت های مشهور مختلفی در توسعه set همکاری کرده‌اند و set هم اکنون توسط شرکت‌های مهمی همچون MasterCard و Visa inc پشتیبانی می شود. همانگونه که پروتکل استاندارد set برای تضمین امنیت در پرداخت‌های اینترنتی کارت‌های اعتباری ارائه شد، می‌توان آنرا در شبکه‌های بی‌سیم هم بکار برد. [۱۷]

هم set وهم پروتوکل‌های پرداخت اینترنت جزء پروتکل های پرداخت کارت اعتباری می باشند. اگرچه اجرای آنها برای تجارت الکترونیک روی شبکه‌های بی‌سیم موفق بوده است ولی بارگذاری آنها روی دستگاه‌های با منابع محدود مانند دستگاه-

---

[۱] Internet Keyed Payment Protocols

[۲] Secure Electronic Transaction (set)

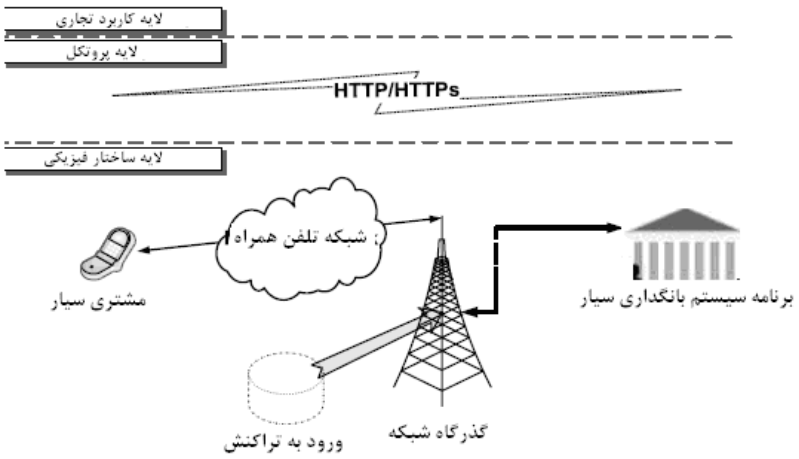
های موبایل و شبکه‌های بی‌سیم بسیار سنگین می باشد.این مسئه باعث شده است تا پیاده سازی موثر و کارای این پروتکل ها در تراکنش های دوسویه کمی با مشکل روبرو شود.

۴- طرح پیشنهادی

ما یک طرح امن جدید برای پرداخت دو طرفه سیار پیشنهاد می‌کنیم. این سیستم با بکارگیری مکانیزم امضای دیجیتال و یک استراتژی قوی برای ثبت تراکنش مشکل عدم انکار در سیستم های پرداخت الکترونیکی را حل می کند. طرح پیشنهادی ، شکاف امنیتی موجود درپروتوکل های بی‌سیم را از بین می برد.

۴-۱ ساختار شبکه

معماری ارائه شده در این مقاله برای تراکنش‌های بانکی که با دستگاه‌های سیار مانند تلفن همراه انجام می‌شود، پیشنهادشده است. در یک تراکنش بانکی دوطرف درگیر هستند: مشتری و بانک .که در این سیستم ارتباطی مشتری همان صاحب دستگاه تلفن همراه می باشد.دستگاه موبایل مشتری با سرور موبایلی بانک، از طریق پروتکل های اینترنتی مانند http یا https ارتباط برقرار می‌کند. همانطور که در شکل۱ نشان داده شده است، دستگاه موبایل از طریق یک سرویس اتصال به شبکه که توسط یک اپراتور ارائه دهنده خدماتی ارتباطی بیسیم ارائه می شود،به شبکه وصل می‌شود.



شکل ۱:ساختار کلی شبکه ارتباطی طرح پیشنهادی

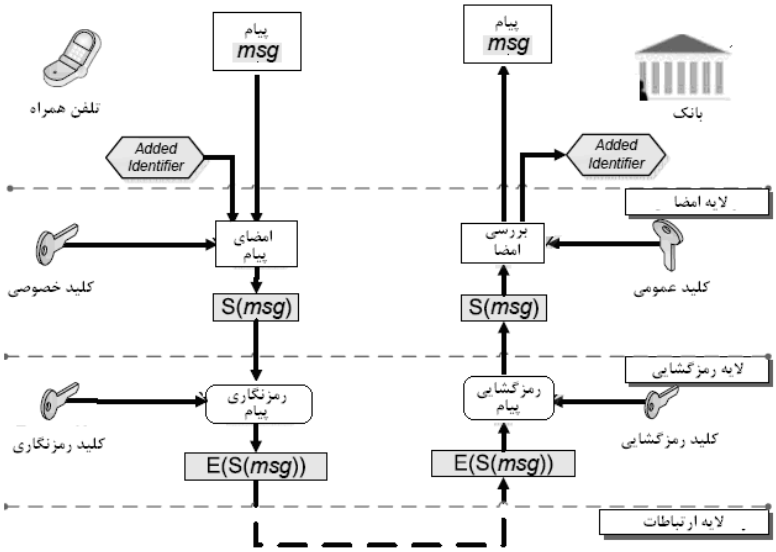
۴-۲- مکانیزم امنیتی استفاده شده در طرح پیشنهادی

همانطور که در شکل ۲ نشان داده شده است، داده‌ها دریک شبکه بی‌سیم عمومی و محافظت نشده منتقل می شودند،درنتیجه این شبکه یک شبکه امن بحساب نمی آید.بهمین منظور لازم است که یکسری مکانیزم های امنیتی برای ارتباط امن تعریف گردد.در طی ارتباط، سیستم پیام ارتباطی وکلید عمومی امضای دیجیتالی را با هم ترکیب کرده و هر دو را از طریق یک اتصال شبکه نامان انتقال می دهد.لازم نیست تا کلید عمومی استفاده شده در سیستم امضای دیجیتال استفاده

رمز شود و بنابراین می‌توانیم کلید عمومی را در یک شبکه‌ی بی‌سیم باز، انتقال دهیم. پیام تراکنش باید از استراق سمع طرف سوم محفوظ بماند و بنابراین ما از لایه امضا ی دیجیتال و لایه رمزنگاری برای پردازش پیام استفاده می کنیم .البته در طرح پیشنهادی لایه امضای دیجیتال و لایه رمزنگاری مستقل و جدا از هم نیستند. دلیل دیگر در استفاده از لایه امضا و لایه رمزنگاری این است که مطمئن شویم پیام از یک مشتری خاص به یک سرور خاص فرستاده شده است. به این دلایل ما شماره شناسایی مشتری[1] ، و شماره سریال گوشی موبایل یا همان شناسه گوشی و شماره حساب بانکی کاربر را با هم ترکیب کرده و آن را به بعنوان شماره شناسه مشتری درنظر می گیریم،و سپس آن را به همراه پیام،امضا می کنیم.

$$Client \rightarrow Bank : E(S(msg, ID_C)) \qquad (1)$$

که در آن E، نشان دهنده رمز نگاری و S امضای دیجیتال می باشد.



شکل۲:معماری امنیتی سیستم پرداخت سیار دوسویه

۴-۲-۱ رمزنگاری

الگوریتم امضای دیجیتال بیضوی یکی از روشهای پیاده سازی الگوریتم امضای دیجیتال است. این الگوریتم بدلیل هزینه محاسباتی پایین و اندازه کوچک کلید ، زمان پردازش را در شبکه و محیطهای با منابع محدود کاهش می دهد،از اینرو برای استفاده در شبکه‌های بی‌سیم بسیار مناسب می باشد.. جزئیات مربوط به الگوریتم امضای دیجیتال منحنی بیضوی در[۹] آمده است.بر اساس تحقیقات صورت گرفته در شبکه های بیسیم سایز کلید، ۱۹۲ بیت در نظر گرفته شده است. این الگوریتم برای خلاصه کردن پیام از SHA-1 استفاده می کند.همچنین از الگوریتم AES [۷و ۱۴]برای رمزنگاری و رمزگشایی استفاده می-شود.

[1] SIM

۴-۲-۲ استراتژی تصدیق هویت چند فاکتوره

مکانیزم تصدیق هویت برای اطمینان از اینکه طرفین ارتباط همان کسانی هستند که انتضار داریم لازم و ضروری می باشد .ما نیز در طرح پیشنهادی برای ایجاد یک فرایند تصویق هویت امن و مطمئن فاکتورها ی زیر را درنظر گرفته ایم:

- دستگاه تلفن همراه است که یک شی فیزیکی است، و خود کاربر مالک این شیء فیزیکی است ،که این می تواند یک فاکتور در تضمین هویت باشد.
- اساس بانکداری سیار یک سیستم بانکداری یکپارچه است. از این رو آن بخشی از زیرساخت بانکی است و هر شخص در این سیستم، منام کاریری و رمز عبور مخصوص خودش را دارد.
- دستگاه های سیار به سرویس های ارتباطی بیسیم که توسط اپراتورهای شبکه تلفن همراه ارائه می شود،نیاز دارند.همچنین هر دستگاه موبایل یک شماره تلفن همراه مخصوص به خود را دارد که توسط سرویس‌های شبکه بی-سیم ارائه می شود. این شماره، نقش شماره هویت شخص را بازی می کند.
- امضای دیجیتال یک تکنولوژی مهم می باشد که در تصدیق هویت یک پیام، ازآن استفاده می شود.

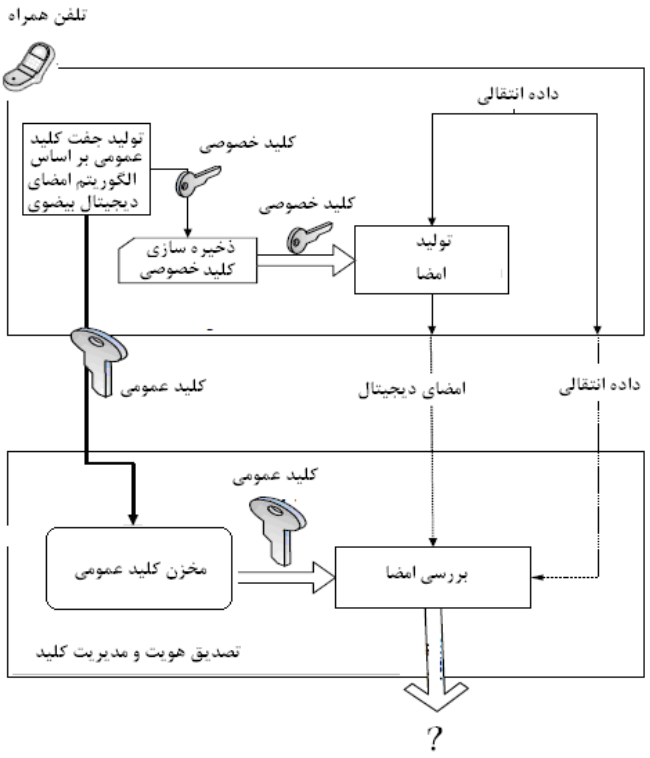
۴-۲-۳ استراتژی ورود به تراکنش

ما یک طرح جدید برای ارتباط بین ارائه دهنده خدمات مالی و اپراتور شبکه بی‌سیم پیشنهاد می کنیم. همزمان با امضای دیجیتال بمنظور تضمین عدم انکار یک استراتژی جدید برای ورود به سیستم تراکنش مالی مورد استفاده قرار خواهد گرفت. سرور ثبت تراکنش یک مکانیزم امنیتی است که بانک را از مشکل عدم انکار بین کاربر و بانک محافظت می کند. اگر یک کاربر منکر انجام یک تراکنش سیار شود، سرور ثبت تراکنش می تواند زمان و جزئیات تراکنش ثبت شده را به عنوان یک مدرک معتبر ارائه دهد.. همانطور که درشکل ۱ نشان داده شد، گذرگاه شبکه توسط اپراتور شبکه سیار فراهم می شود. اپراتور شبکه موبایل دقیقا نقش یک طرف سوم قابل اعتماد را بازی می‌کند که درآن سرور ثبت تراکنش، از لحاظ منطقی قسمتی از پلتفرم بانکداری سیار است، ولی در طرح پیشنهادی بصورت فیزیکی و روی گذرگاه شبکه قرار می گیرد.

۴-۳- مدیریت کلید

نگرانی اصلی در مدیریت کلید تولید، توزیع و ذخیره کلیدهاست.استفاده از روشهای امن مدیریت کلید، برای یک سیستم پرداخت سیار امن، امری مهم و حیاتی است. زمانی که کلید به طور تصادفی انتخاب می‌شود، سیستم باید از جعل هویت آن جلوگیری کند. در عمل، بیشتر حملات روی سیستم‌های کلید عمومی، مربوط به مدیریت کلید است تا الگوریتم‌های رمزنگاری [۱۳] .

در طرح پیشنهادی ما دو جفت کلید نیاز است که هر دو برای رمزنگاری و امضای دیجیتال استفاده می شوند. شکل۳ استراتژی مدیریت کلید پیشنهادی را برای امضای دیجیتال نشان می دهد.



شکل ۳:مدیریت کلید امضای دیجیتال

۱-۳-۴ مدیریت کلید امضای دیجیتال

ما برای جلوگیری از عدم انکار در طول تراکنش‌ها استفاده از امضای دیجیتال را پیشنهاد کردیم. رمزنگاری کلید عمومی هیچ اطلاعات سری را بین دو طرف درگیر، به اشتراک نمی‌گذارد. کلید خصوصی در یک طرف به تولید امضای دیجیتال کمک می کند و در طرف دیگر کلید عمومی برای تایید امضای عمومی بکار می رود. برای اینکه کلید خصوصی محرمانه بماند، ما پیشنهاد کردیم یک زوج کید در دستگاه تلفن همراه تولید شود. زمانی که یک کاربر شروع به استفاده از برنامه کاربردی پرداخت سیار در سیستم می‌کند، هنوز هیچ کلیدی وجود ندارد و قبل از فرآیند تراکنش یک عمل تولید کلید برای تولید زوج کلید صورت می‌گیرد. سپس کیلدها ذخیره و توزیع می شوند.

کلید عمومی به سرور تصدیق هویت که در سرور بانکداری است منتقل می شود و سپس کلید عمومی در یک مخزن کلید ذخیره می شود. امنیت طرف سرور در حوزه طرح پیشنهادی ما نمی باشد از اینرو به جزئیات مربوط آن نمی پردازیم .

این کارامر فقط یک بار اتفاق خواهد افتاد مگر اینکه یک جفت کلید جدید درخواست شده باشد. این فرایند می تواند به صورت آف-لاین وبدون نیاز به هیچ گونه ارتباطی انجام شود. یک جفت کلید سرانجام منقضی شده و سرور بانکداری باید یک

جفت کلید جدید را تولید کند. زمانی که سرور تشخیص داد که نیاز به تجدید کلید است، یک هشدار(مانند یک پیام کوتاه) باید به دستگاه تلفن همراه فرستاده شود تا یک جفت کلید جدید ایجاد شود.

۲-۳-۴ مدیریت کلید رمزنگاری

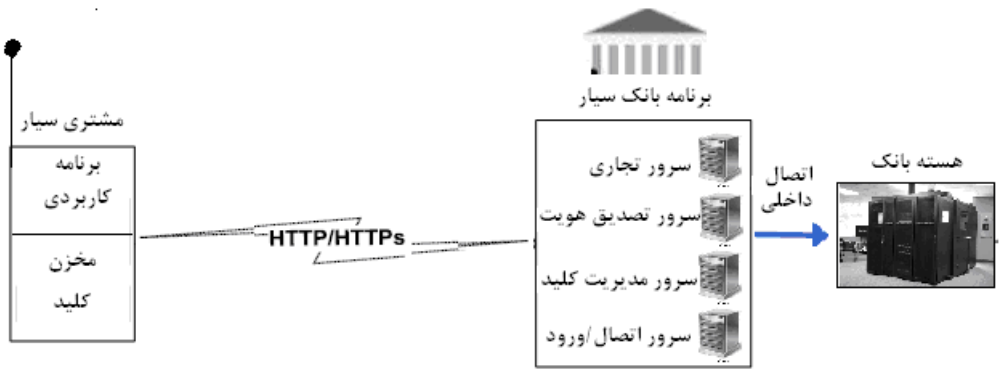
تولید کلید رمزنگاری توسط سرور اتفاق می‌افتد.در رمزنگاری و رمزگشایی، کلید محرمانه یکسانی به اشتراک گذاشته می شود و نباید در شبکه بی‌سیم محافظت نشده به خاطر خطر استراق سمع انتقال یابند. ما پیشنهاد می‌کنیم که این کلید در بسته نرم افزاری jar ذخیره شود و سپس کاربران، زمانی که برای خدمات بانکی سیار در بانک مورد نظرشان ثبت نام می‌کنند، از این کلید در بسته نرم‌افزاری استفاده خواهند کرد. در طرف سرور هم ما فرض می‌کنیم که اقدامات امنیتی به اندازه کافی لحاظ شده است .

۵- پیاده سازی

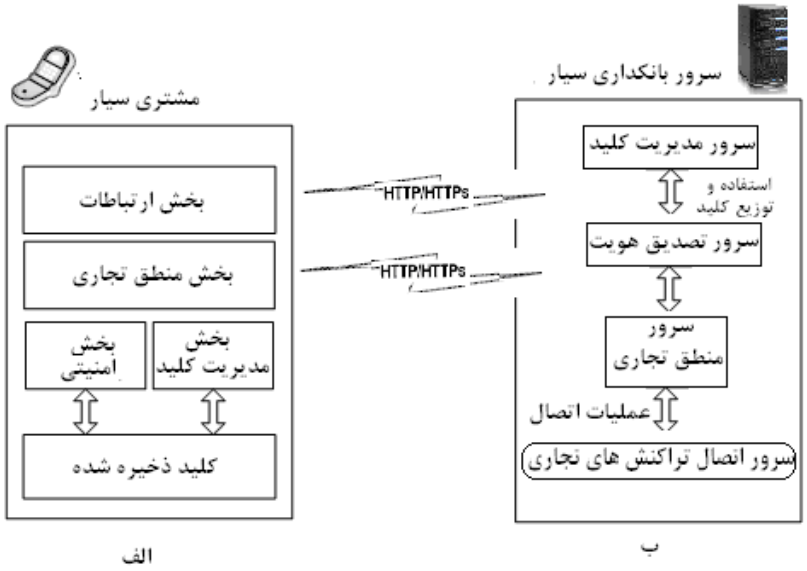
در ادامه معماری پیشنهادی برای بانک، و مشتری توضیح داده شده است.

۱-۵- معماری سمت مشتری در سیستم سیار پیشنهادی

تلفن همراه مشتری در این طرح باید قابلیت اجرای برنامه های جاوا را داشته باشد.شکل ۵(قسمت الف) معماری کلاینت سیار را نشان می دهد.سیستم کلاینت یا مشتری سیار از چهار بخش تشکیل شده است که در زیر آمده است :



شکل :۴بخش های مختلف سیستم بانکداری پیشنهادی در سمت کاربر



شکل۵:الف:بخش های مختلف سیستم پیشنهادی در طرف مشتری ب: بخش های مختلف سیستم پیشنهادی در طرف سرور

۵-۱-۱ بخش منطق تجاری

این بخش مسئول تمام عملکردهای تجاری خاص بین بانک و کاربر است.

۵-۱-۲ بخش امنیتی

این بخش پاسخگوی مباحث امنیتی می باشد. پس از اینکه درخواست کاربر توسط بخش تجاری پردازش شد، یک پیام تولید می شود. این پیغام با امضای دیجیتال و رمزگذاری، در بخش امنیتی پردازش خواهد شد. با توجه به الگوریتم الگوریتم امضای دیجیتال منحنی بیضوی ، ما کلید خصوصی را از سرور مدیریت کلید میخوانیم و سپس امضای دیجیتال را برای رمزنگاری برروی پیام اصلی اعمال می کنیم .پیام رمزنگاری شده، توسط بخش ارتباطی به سرور بانک ارسال می شود .

۵-۱-۳ بخش ارتباطی

این بخش مسئول اتصال به شبکه است. ما استفاده ازپروتکل HTTP را پیشنهاد می کنیم. بخش ارتباطی وظیفه کنترل تبادل اطلاعات بین برنامه مشتری و سرور بانکی را برعهده دارد.

۵-۱-۴ بخش مدیریت کلید

این بخش مسئول مدیریت کلید هایی که قبلا گفته شده می باشد.

۵-۲ معماری سرور

سرور بانکداری سیار شامل اجزایی است که درادامه توضیح داده می شوند. شکل ۵(قسمت ب) معماری پیشنهادی در سروررا نشان می دهد.

۵-۲-۱ سرور مدیریت کلید

این بخش وظیفه دریافت و ذخیره کلید عمومی را برعهده دارد ،همچنین ارسال پیام هشدار به مشتری برای تازه سازی جفت کلید هایی که استفاده می کند برعهده این بخش می باشد.

۵-۲-۲ سرور تصدیق هویت

این بخش وظیفه تصدیق هویت سیستم بانکداری سیار رابرعهده دارد. موارد امنیتی که در سرور تصدیق هویت باید انجام شود به صورت زیر است :

۱- بررسی اعتبار نام کاربردی و رمز عبور در طی فرایند اتصال

۲ - بررسی و تایید امضای دیجیتال

۳- رمزنگاری پیام‌ها

۵-۲-۳ سرور منطق تجاری

این بخش همه احتیاجات تجاری قانونی را کنترل می کند .زمانی که این بخش فرآیند پردازش یک کار تجاری را تمام می-کند با فرستادن یک پیام ،نتیجه را به دستگاه تلفن همراه کاربر،اعلام می کند.

۵-۲-۴ سرور ثبت تراکنش

این بخش فایل‌های ثبت تراکنش‌های انجام شده را در پایگاه داده بانک تولید و نگه می‌دارد. این بخش در واقع یک مکانیزم امنیتی برای حفاظت بانک از انکار بین کاربران و بانک است . زمانی که کاربران انجام فعالیت‌های انجام شده در سیستم بانکی سیار را انکار کنند، این بخش با ارائه رکوردهای تراکنشی ثبت شده ، از این کار جلوگیری می‌کند.

۶- نتیجه گیری

ما یک معماری امن را برای پرداخت‌های دوطرفه در سیستم بانکداری و تجارت الکترونیک سیار پیشنهاد کردیم. اگر چه قبلا طرح‌ها و پروتکل های دیگری پیشنهاد شده‌اند ولی برای دستگاه ی سیار مانند تلفن همراه بدلیل منابع محدود زیاد مناسب

نیستند در آنها نگرانی‌های امنیتی مربوط به تراکنش‌های مالی سیار برطرف نشده است.این طرح با زبان برنامه نویسی جاوا بر روی دستگاه تلفن همراه مشتری قابل پیاده سازی است، وتوسط یک سرور سیار قابل پشتیبانی می باشد.همچنین در این طرح ازامضای دیجیتال و یک استراتژی ثبت تراکنش امن برای افزایش امنیت و حل مشکل عدم انکار استفاده شده است و برای پیاده سازی بر روی دستگاه‌های سیار بسیار مناسب باشداین سیستم می تواند بخوبی در سیستم های تجارت الکترونیک و سیستم های مالی سیار بکار گرفته شودو بعنوان سکوی پرتابی در سیستم های پرداخت سیار تبدیل گردد..

.منابع:

[۱]ارزیابی ویژگی‌های انواع سیستم‌های پرداخت الکترونیک از دیدگاه کاربران ایرانی -مهرداد مدهوشی،محمد رضا زالی،محمد رئوف امانی

[2]] http://www.zurich.ibm.com/security/pasterojects/ecommerce/iKP_overv.htmliew
[3]] http://www.investopedia.com/terms/s/secur_electronicransaction set.asp.
[4]] http://www.hasintech.com/?page=mobile_payment&lang=fa.
[5] Rolf Oppliger, Ralf Ha,David Basin,SSL/TLS Session-Aware User Authentication: A Lightweight Alternative to Client-Side Certificates, eethovenstrasse 10, CH-3073 Gümligen,2008.
[6] Yaniv Shaked, Avishai Wool, Cracking the Bluetooth PIN, 3rd International Conference on Mobile Systems, Applications, and Services (MobiSys 2005), June 2005 .
[7] RSA Security Inc. (2001), RSA SecurID Authentication: a better value for a better ROI. RSA *Whitepaper*.
Available at: <http://www.rsasecurity. com/ products/securid/>.
[8] Harkins, D. and Carrel, D. (1998), RFC 2409. The Internet Key Exchange (IKE). *IETF Network Working Group*
Request for Comments.
[9] L. A. Martucci, T. C. M. B. Carvalho and W. V. Ruggiero, A Lightweight Distributed Group Authentication Mechanism, Department of Computer Engineering and Digital System - University of Sao Paulo – Brazil
[10] Niina Mallat and Matti Rossi, Virpikristina Tuunainen, “Mobile banking services,” Communications of the ACM, Volume, 47, Issue 5,pp. 42-46, 2004.
[11] Soriano M, Ponce D. “A security and usability proposal for mobile electronic commerce,” IEEE Commun 2002; August.
[12] Amir Herzberg, “Payments and Banking with Mobile Personal Devices,” Communications of the ACM,Volume 46, Issue 5, pp. 53-58, 2003.
[13] Y. Chou, C.-W. Lee, and J. Chung, “Understanding m-commerce payment systems through the analytic hierarchy process,” Journal of Business Research,57:1423– 1430, 2004.
[14] Mohammad Musa, Edward Schaefer, and StephenWedig, A simplified AES algorithm and its linear and differential cryptanalyses, Cryptologia 27 (April 2003), no. 2, 148–177.
[15] NIST (National Institute of Standards and Technology) Special Publication 800-57 (May 2006) http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part1.pdf
[16] (D.SPA.21ECRYPT Yearly Report on Algorithms and Keysizes) by the European Network of Excellence in Cryptology (January 2007) http://www.ecrypt.eu.org/documents/D.SPA.21-1.1.pdf
[17] Tan Soo Fun, Leau Yu Beng, Rozaini Roslan, and Habeeb Saleh Habeeb,Privacy in New Mobile Payment Protocol, World Academy of Science, Engineering and Technology 47 2008.
[18] Tiwari, A., Sanyal, S., Abraham, A., Knapskog, J. S. & Sanyal, S., “A Multi-factor Security Protocol for Wireless Payment-Secure Web Authentication Using Mobile Devices”, IADIS International Conference Applied Computing, pp.160-167, 2007.