بسم الله الرحمن الرحیم

راه‌کارهای امن‌سازی بانکداری الکترونیک

شرکت مهندسی پیام‌پرداز

خرداد ماه ۸۹

این پیشنهاد توسط شرکت پیام‌پرداز تهیه شده است و هرگونه استفاده از تمام یا بخشی از آن منوط به اجازه کتبی از این شرکت می‌باشد.

فهرست

عنوان **صفحه**

۱- مقدمه ۱
۲- *Core Banking* ۳
۲-۱- نیازمندی‌های امنیتی ۳
۲-۲- راه حل‌های امن‌سازی ۵
۲-۲-۱- امن‌سازی ارتباطات *LAN* ۵
۲-۲-۲- امن‌سازی ارتباطات *WAN* ٦
۳- بانکداری اینترنتی ۸
۳-۱- تهدیدات بانکداری اینترنتی ۹
۳-۲- روش‌های امن‌سازی ۱۰
۳-۳- پیشنهاد سطح‌بندی امنیتی خدمات اینترنتی ۱۲
۳-۳-۱- سرویس اطلاع‌رسانی ۱۲
۳-۳-۲- سرویس تراکنش‌های مالی پایین ۱۳
۳-۳-۳- سرویس تراکنش‌های مالی بالا ۱۳
۴- تجهیزات خودپرداز و کیوسک ۱۵
۵- بانکداری با تلفن همراه ۱٦
۵-۱- خدمات *m-banking* ۱۷
۵-۲- نیازمندی‌های امنیتی ۱۸
۵-۳- راه حل امن‌سازی ۱۹
۶- بانکداری تلفنی ۲۰
۶-۱- نیازمندی‌های امنیتی ۲۱
۶-۲- راه حل‌های امن‌سازی ۲۲

۱- مقدمه

رشد و گسترش روزافزون فناوری اطلاعات، انقلابی را در ابعاد مختلف زندگی انسانها و عملکرد سازمانها ایجاد کرده است. این فناوری روشهای کارکرد و نگرش افراد، سازمانها و دولتها را دگرگون ساخته و باعث ایجاد صنایع نوین، مشاغل جدید و خلاقیت در انجام امور شده است. ظهور پدیده‌هایی چون کسب و کار الکترونیک، تجارت الکترونیک و بانکداری الکترونیک از نتایج عمده نفوذ و گسترش فناوری اطلاعات در بعد اقتصادی است.

بانکداری الکترونیکی به معنای ارایه خدمات بانکی مبتنی بر فناوری اطلاعات است. فناوری اطلاعات باعث شده علاوه بر اینکه خدمات سنتی بانکداری به نحو مطلوب‌تر و با کیفیت بیشتری به مشتریان ارایه گردد بلکه یکسری خدمات نوین نیز که قبلا امکان ارایه آنها وجود نداشت ایجاد شود. در سرویس‌های جدید، مشتری در هر زمان و هر مکان بدون نیاز به حضور فیزیکی در شعبه بانک، خدمات خود را دریافت می‌نماید. این ملاحظات در مجموع باعث می‌شود میزان رضایت‌مندی مشتریان بیشتر شده، حجم تراکنش‌ها توام با بهره‌وری مناسب به طور چشم‌گیری بالا رود و نهایتا درآمد بانک افزایش پیدا کند.

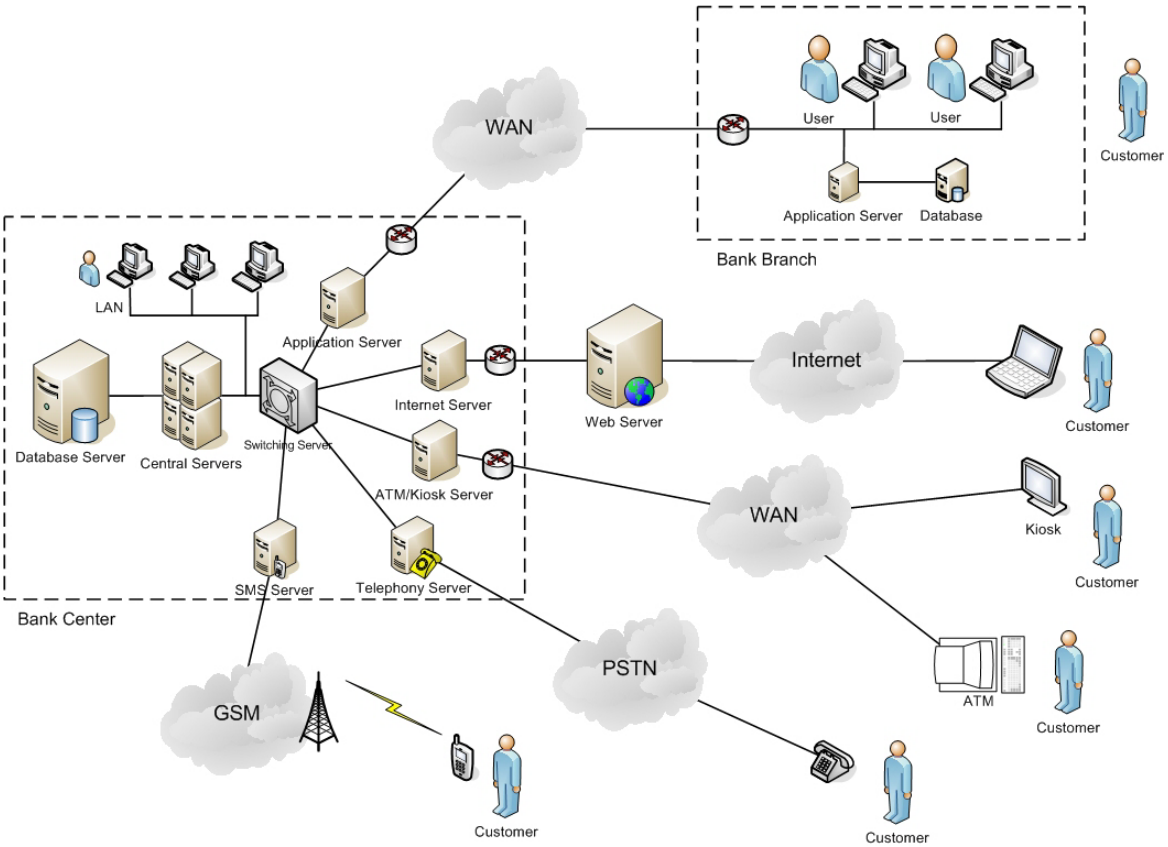
سرویس‌های مطرح شده در زیر عمده‌ترین سرویس‌های بانکداری الکترونیکی هستند:

- *Core Banking*
- بانکداری اینترنتی[1]
- تجهیزات خودپرداز[2] (*ATM*) و کیوسک
- بانکداری با تلفن همراه[3]
- بانکداری تلفنی[1]

[1] *Internet Banking*
[2] *Automatic Teller Machine*
[3] *Mobile Banking*

شکل ۱ به طور نوعی سیستم اطلاعاتی یک سیستم بانکداری الکترونیکی را نشان می‌دهد. در این شکل به دلیل اختصار، ارتباطات بین بانکی (از قبیل شبکه شتاب) نشان داده نشده است.

با توجه به رشد سریع حملات الکترونیکی همگام با رشد تکنولوژی و حرفه‌ای شدن مجرمین فضای *Cyber*، امن‌سازی بانکداری الکترونیکی یکی از مسائل مهم پیش رو و از دغدغه‌های عمده مدیران *IT* بانکهاست.



شکل ۱: سیستم بانکداری الکترونیکی نوعی

هدف از این نوشتار مروری سریع بر تهدیدات امنیتی پیش رو در سیستم بانکداری الکترونیک و ارایه راه‌کارهایی برای امن‌سازی آن می‌باشد. راه‌کارهای ارایه شده جنبه عمومی داشته و در آنها شرایط ویژه فنی و مسایل خاص موجود در بانک‌های مختلف لحاظ نشده است. لذا در صورت لزوم باید با توجه به شرایط شبکه بانک مورد نظر، طراحی‌های خاص منظوره و یا بومی‌سازی‌هایی در محصولات ارایه شده انجام گیرد.

شرکت مهندسی پیام‌پرداز بر این باور است که براساس توان، تجربه و سوابق کارهای انجام شده، قابلیتهای لازم را برای طراحی معماری امنیت سیستم اطلاعاتی بانک‌ها و اجرای امن‌سازی آن داراست.

---

[1] *Telephone Banking*

این قابلیتها منبعث از دانش و تجربه عملی کارشناسان شرکت در زمینه ارایه خدمات مشاوره و اجرای امنیت فضای تبادل اطلاعات و به ویژه برخورداری از یک سبد متنوع از محصولات امنیت فناوری اطلاعات در این شرکت می‌باشد.

در ادامه به معرفی راه‌کارهای امن‌سازی سرویس‌های مختلف بانکداری الکترونیک می‌پردازیم.

۲- *Core Banking*

منظور از *Core Banking*، برنامه‌های کاربردی بانکی است که در داخل بخش‌های مختلف بانک مثل مرکز و شعب به وسیله کارکنان بانک (کاربران) مورد استفاده قرار می‌گیرد و خدمات بانکی را به طور متمرکز در اختیار مشتریان قرار می‌دهد. اکثر این برنامه‌ها (از قبیل نرم‌افزار تحویل‌داری) ساختار *Client/Server* دارند.

۲-۱- نیازمندی‌های امنیتی

از آنجا که عملیات انجام گرفته با سیستم *Core Banking* معمولا حساس و حیاتی هستند این سیستم به سرویس‌های مختلف امنیتی از قبیل موارد زیر نیاز دارد:

- احراز اصالت[1] کاربر: لازم است هویت کاربر در هنگام درخواست سرویس به صورت کاملا مطمئن برای سرور احراز گردد. روش معمول در این حالت استفاده از نام و کلمه عبور است که دارای ضعف‌های زیادی است. به عنوان مثال انتخاب کلمات عبور ضعیف توسط کاربران، شنود کلمه عبور از روی شبکه، سرقت کلمه عبور با استفاده از برنامه‌های *Key Logger* از روی کامپیوتر کاربر و حمله دیکشنری نمونه‌ای از تهدیدات روش احراز اصالت یک عاملی است. برای رفع این مشکلات روش‌های احراز اصالت دوعاملی[2] پیشنهاد می‌شود که در آن علاوه بر کلمه عبور (یا اصطلاحا *PIN*[3]) از یک توکن امنیتی[4] نیز برای بررسی هویت کاربر استفاده می‌شود.
- کنترل دسترسی: پس از احراز اصالت کاربر لازم است سطح دسترسی وی به منابع بررسی و کنترل گردد. در واقع کارمندان بانک بسته به شغل و سمت خود، وظایف و مسئولیت‌های متفاوتی دارند و بنابراین هر کاربر ممکن است اجازه دسترسی به برخی برنامه‌های کاربردی یا سرورها را داشته باشد.

---

[1] *Authentication*
[2] *Two-Factor*
[3] *Personal Identity Number*
[4] *Secure Token*

- ردگیری[1] فعالیت‌های کاربر: به منظور پیش‌گیری از وقوع اقدامات خلاف توسط کاربران یا مشتریان و نیز تشخیص و ردگیری این‌گونه فعالیت‌ها در صورت وقوع، سیستم‌های اطلاعاتی کلیه فعالیت‌های انجام گرفته را رویدادنگاری کرده و آنها را در اختیار مدیر سیستم قرار می‌دهند. بسته به سطح رویدادنگاری و جزییات مورد نظر، ممکن است عملیات ردگیری توسط برنامه‌های کاربردی و یا تجهیزات شبکه انجام بگیرد. به عنوان نمونه اگر یک نفوذگر وجهی را به طور غیر مجاز از حساب یک مشتری به حساب خود یا یکی از هم‌دستان خود منتقل نماید در صورت شکایت مشتری، می‌توان نفوذگر را ردگیری نمود.
- محرمانگی[2] داده‌های مبادله شده: محرمانگی اطلاعات حساس مبادله شده بین کامپیوتر کاربر و سرور باید با روش‌های مدرن رمزنگاری تامین گردد تا هیچ‌کس امکان شنود اطلاعات را از روی شبکه نداشته باشد. به عنوان مثال ممکن است فرد نفوذی کلمه عبور یک کاربر را بر روی شبکه شنود کرده و با ایفای نقش به منابع و اختیارات وی دسترسی پیدا کند. همچنین شنود اطلاعات مالی حساب مشتریان از روی شبکه، علاوه بر نقض حریم خصوصی شهروندان می‌تواند مقدمه‌ای برای انجام برخی حملات دیگر گردد.
- صحت[3] داده‌های مبادله شده: از آنجا که اعتبار داده‌های بانکی از حساسیت زیادی برخوردار است لذا باید با بکارگیری روش‌های مناسب، صحت اطلاعات مبادله شده بین کامپیوتر کاربر و سرور را بر روی شبکه تضمین کرد. به عنوان نمونه در سرویس انتقال وجه از یک حساب به حساب دیگر، نفوذگر با تغییر شماره حساب مقصد به شماره حساب خود می‌تواند یک سرقت الکترونیکی انجام دهد.
- جلوگیری از نفوذ افراد غیرمجاز به *LAN* مرکز یا شعبه: از آنجا که معمولا شبکه‌های محلی مرکز و شعب به شبکه‌های عمومی نظیر اینترانت ملی یا اینترنت متصل هستند امکان نفوذ هکرها به شبکه بانک و انجام فعالیت‌های خراب‌کارانه وجود دارد. بنابراین لازم است با استفاده از دیواره‌های آتش[4] مناسب از نفوذ بیگانگان به شبکه داخلی جلوگیری کرد.
- جلوگیری از نفوذ کدهای مخرب به *LAN* مرکز یا شعبه: با توجه به اتصال شبکه‌های محلی به شبکه‌های عمومی لازم است از ورود کدهای مخرب اعم از ویروس‌ها، کرم‌ها، اسب‌های تروا و ... به شبکه محلی جلوگیری شود.

---
[1] *Auditing*
[2] *Confidentiality*
[3] *Integrity*
[4] *Firewall*

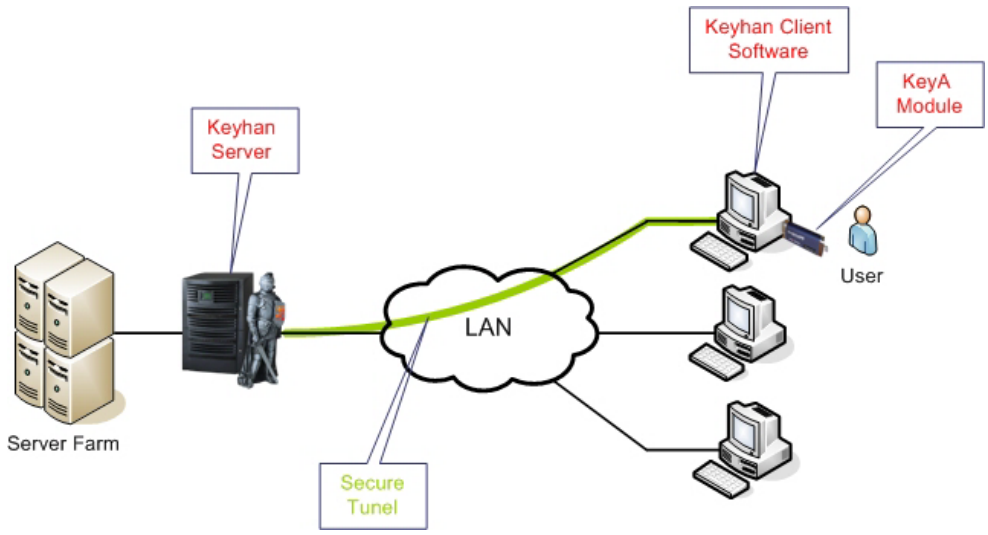
۲-۲- راه حل‌های امن‌سازی

راه حل‌های امن‌سازی برای سیستم *Core Banking* را در دو بخش ارتباطات *LAN* و ارتباطات *WAN* بیان می‌کنیم.

۲-۲-۱- امن‌سازی ارتباطات *LAN*

در صورتی که مرکز یا هر یک از شعب دارای سرورهایی در داخل شبکه محلی باشند که به طور محلی به کاربران سرویس می‌دهند پیشنهاد ما برای امن‌سازی شبکه محلی، استفاده از محصول کیهان است. این محصول توسط شرکت پیام‌پرداز طراحی و پیاده‌سازی شده است.

شکل ۲ طرح امن‌سازی *LAN* با سیستم کیهان را نشان می‌دهد. در این طرح یک سرویس‌دهنده[1] کیهان در جلوی سرورها قرار گرفته و بر روی هر یک از کامپیوترهای کاربران نرم‌افزار *Client* کیهان نصب می‌شود. هر کاربر برای ارتباط با سرورهای اصلی ابتدا لازم است از طریق سرور کیهان احراز اصالت شده و اجازه دسترسی وی صادر گردد. فرایند احراز اصالت کاربر با استفاده از یک پروتکل احراز اصالت اختصاصی و به صورت دوعاملی (با بکارگیری ماژول کیای کاربر و *PIN* وی) انجام می‌گیرد. پس از احراز اصالت موفقیت‌آمیز کاربر، یک تونل امن بین کامپیوتر کاربر و سرور کیهان برقرار می‌شود که کلیه داده‌های مبادله شده درون آن رمز می‌شود و بدین ترتیب سرویس‌های محرمانگی و صحت تامین می‌گردد.



شکل ۲: امن‌سازی ارتباطات *LAN* با کیهان

[1] *Server*

سیستم کیهان در لایه شبکه عمل کرده و از دید لایه کاربرد کاملا شفاف است. بنابراین نیازی به تغییر در برنامه‌های کاربردی فعلی وجود نخواهد داشت. از طرف دیگر یک سرویس خاصی که کیهان می‌تواند ارایه کند سرویس اختصاص آدرس *IP* مجازی به کاربر است که با استفاده از آن می‌توان با تغییرات جزیی در برنامه‌های کاربردی فعلی، سرویس *SSO*[1] را در شبکه ارایه نمود. بدین ترتیب کاربر با یک بار *Login* به سیستم کیهان احراز اصالت می‌شود و برنامه‌های کاربردی جهت احراز اصالت، نیازی به گرفتن نام و کلمه عبور کاربر ندارند. از این خاصیت می‌توان برای ثبت اطلاعات مربوط به ارتباطات هر یک از کاربران نظیر سرورها و پورتهای متصل شده و حجم اطلاعات مبادله شده استفاده نمود.

سرور کیهان به عنوان یک دیواره آتش قوی عمل کرده و از نفوذ افراد غیرمجاز به *LAN* مرکزی (*Server Farm*) جلوگیری می‌کند.

قابلیت خاص دیگری از سیستم کیهان که در اینجا به خوبی می‌تواند به کار برده شود این است که می‌توان *Client* را محدود به یک کامپیوتر خاص کرد. در این حالت کاربر تنها از روی یک کامپیوتر مشخص که به وسیله مدیر تعیین شده قادر است به سیستم کیهان متصل شود.

سرویس‌های امنیتی ارایه شده در این طرح عبارتند از: احراز اصالت کاربر، کنترل دسترسی کاربر، محرمانگی و صحت داده‌های مبادله شده، جلوگیری از نفوذ به سرورها، ردگیری فعالیت‌های کاربر در سطح شبکه (شامل زمان‌های ورود و خروج و ...) و امکان ارایه سرویس *SSO*.

۲-۲-۲- امن‌سازی ارتباطات *WAN*

در سیستم *Core Banking*، هر شعبه شبکه محلی مستقلی داشته و ارتباط بین شعب با مرکز از طریق *WAN* انجام می‌گیرد. شبکه‌های محلی شعب را می‌توان از یک دیدگاه به دو گروه زیر تقسیم‌بندی نمود:

- **شبکه‌های محلی بدون نیاز به حفاظت:** در این شبکه‌ها، تعداد کامپیوترهای میزبان کم بوده و شبکه فاقد سرور محلی می‌باشد. برنامه‌های کاربردی بانکی مورد استفاده در این شعب تحت ویندوز بوده و بصورت *Client/Server* با سرویس‌دهنده‌های واقع در *LAN* مرکزی شبکه ارتباط دارند. در سطح کامپیوترهای میزبان این شعب، هیچگونه اطلاعات حساسی ذخیره نشده و اطلاعات در سطح سرویس‌دهنده‌های مرکزی ذخیره و بازیابی می‌گردد.
- **شبکه‌های محلی نیازمند به حفاظت:** این شبکه‌های محلی ترکیب ناهمگنی از انواع کامپیوترهای *PC*، *Mini* یا *Mainframe* با سیستم‌عامل‌های مختلف *DOS*، ویندوز، *Unix*، *OS/2* و ... و انواع برنامه‌های کاربردی بانکی می‌باشند. برنامه‌های کاربردی مورد استفاده در

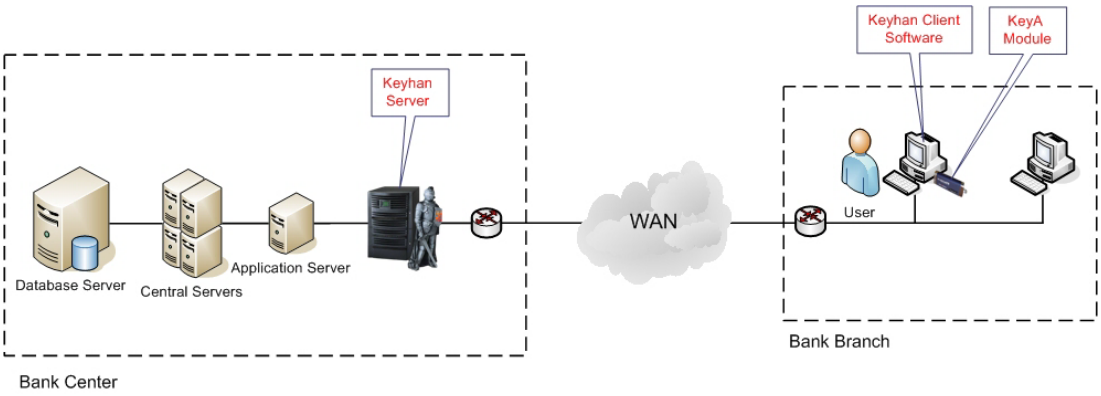
[1] *Single Sign On*

این شعب با سرویس‌دهنده‌های محلی همان شعب یا با سرویس‌دهنده‌های واقع در مرکز ارتباط دارند. در این نوع شبکه‌ها در سطح کامپیوترهای میزبان یا سرویس‌دهنده‌های محلی، اطلاعات حساسی نظیر حساب‌های مشتریان وجود دارد.

در ادامه راه‌حل‌های امن‌سازی برای هر یک از دو گروه بیان می‌گردد.

الف- امن‌سازی شعب بدون نیاز به حفاظت

به منظور امن‌سازی برنامه‌های کاربردی در این حالت، مشابه روش امن‌سازی ارتباطات *LAN*، از محصول امن‌سازی شبکه کیهان استفاده خواهد شد. شکل ۳ این طرح امن‌سازی را نشان می‌دهد. در این طرح یک سرویس‌دهنده کیهان در جلوی مجموعه سرورهای مرکزی بانک قرار می‌گیرد که عملیات احراز اصالت دوعاملی کاربران و کنترل دسترسی آنان را بر عهده دارد. همچنین این سرور سر انتهایی تونل امنیتی است که با کامپیوتر کاربر برقرار شده و سرویس‌های محرمانگی و صحت داده‌ها از طریق آن ارایه می‌گردد. سرویس‌های امنیتی ارایه شده در این طرح مشابه بخش قبل خواهند بود.



شکل ۳: امن‌سازی شعب بدون نیاز به حفاظت با استفاده از سیستم کیهان

ب- امن‌سازی شعب نیازمند به حفاظت

جهت امن‌سازی این شعب استفاده از سیستم مدیریت یکپارچه تهدیدات[1] (*UTM*) طریق پیشنهاد می‌گردد. سیستم طریق به وسیله شرکت پیام‌پرداز طراحی و توسعه یافته است.

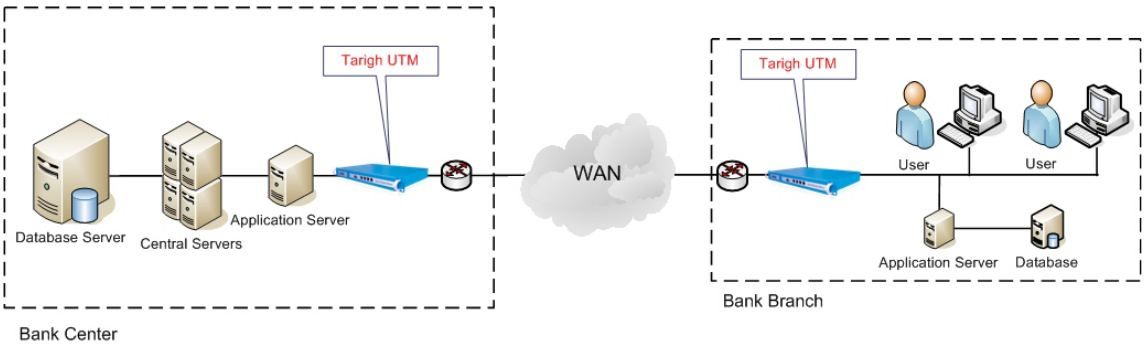
طریق در محل ارتباط شبکه محلی با شبکه بیرونی قرار گرفته و سرویس‌های امنیتی مختلف را بصورت کاملا شفاف و مستقل از کاربردهای شبکه محلی بصورت متمرکز و یک‌جا ارایه می‌کند. شکل ۴ استفاده از سیستم طریق را در شبکه بانکی نشان می‌دهد. همانگونه که در این شکل مشخص است طریق به عنوان یک دروازه امنیتی[2] ضمن ارایه سرویس‌های امنیتی مختلف برای ترافیک ارتباطی، از نفوذ

[1] *Unified Threat Management*
[2] *Security Gateway*

هکرها و افراد غیرمجاز به شبکه محلی شعب و مرکز جلوگیری می‌کند. سرویس‌های امنیتی ارایه شده توسط سیستم *UTM* طریق عبارتند از:

- محرمانگی و صحت ترافیک مبادله شده با استفاده از مکانیزم *IPsec VPN*
- دیواره آتش
- سیستم تشخیص نفوذ[1]
- سیستم ضد هرزنامه[2]
- سیستم ضد ویروس[3] و کدهای مخرب

از آنجایی که طریق به عنوان دروازه امنیتی در شبکه قرار می‌گیرد از دید کاربران مخفی بوده و احتیاج به نصب برنامه اضافی یا تغییری در سطح کامپیوترهای شعب یا مرکز نخواهد داشت. لازم به ذکر است که طرح شکل ۴ قادر است ارتباطات بین شعب را نیز در صورت وجود امن نماید.



شکل ۴: امن‌سازی شعب نیازمند به حفاظت با استفاده از سیستم طریق

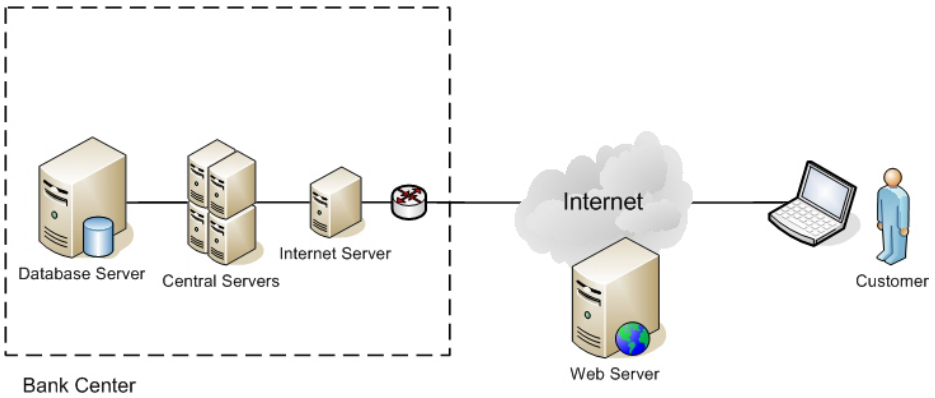
۳- بانکداری اینترنتی

بانکداری اینترنتی یکی از شاخه‌های اصلی بانکداری الکترونیکی است که هدف از آن ارایه خدمات بانکی از طریق شبکه جهانی اینترنت می‌باشد. اهمیت بانکداری اینترنتی از آنجا ناشی می‌شود که هم اینک شبکه جهانی اینترنت به شدت گسترده شده و مشتریان می‌توانند در هر مکان و هر زمان به راحتی به این شبکه دسترسی پیدا نمایند. بنابراین ارایه خدمات بانکی از طریق اینترنت می‌تواند در جلب نظر و رضایت مشتریان تاثیر عمده‌ای داشته باشد.

معماری یک سیستم بانکداری اینترنتی در شکل ۵ نشان داده شده است. همانگونه که این شکل نشان می‌دهد برنامه کاربردی تحت وب بانک بر روی یک سرویس‌دهنده وب در اینترنت قرار دارد و به عموم سرویس می‌دهد. سرویس‌دهنده وب می‌تواند یک سرور اختصاصی در شبکه محلی بانک باشد که

[1] *Intrusion Detection System*
[2] *Anti-Spam*
[3] *Anti-Virus*

به اینترنت متصل شده است و یا اینکه یک سرور عمومی یا اختصاصی در یک مرکز داده اینترنتی[1] (*IDC*) باشد. سرور وب برای ارایه خدمات بانکی لازم است به برنامه‌های اصلی بانکداری و از آنجا به پایگاه داده در *LAN* مرکزی بانک متصل باشد.



شکل ۵: معماری سیستم بانکداری اینترنتی

۳-۱- تهدیدات بانکداری اینترنتی

در سیستم بانکداری اینترنتی از پروتکل *http* در بستر *TCP/IP* برای تبادل اطلاعات بین *Client* و سرور وب بر روی شبکه اینترنت استفاده می‌شود. این پروتکل داده‌ها را در قالب یک استاندارد مشخص به صورت فاش مبادله می‌کند و فاقد هر گونه مکانیزم امنیتی است. تهدیدات مطرح در این زمینه عبارتند از:

- تهدید علیه اصالت مشتری یا سرور: ممکن است یک طرف ارتباط دارای نقش‌جعلی باشد. به عنوان مثال مشتری، با یک سرویس‌دهنده جعلی ارتباط برقرار کند و اطلاعات خود را برای سرویس‌دهنده جعلی فاش نماید. یا ممکن است مشتری خود را در نقش مشتری دیگری به سرور معرفی نموده تا به اطلاعات او دسترسی پیدا کند و یا از جانب او تراکنشهای مورد نظر خود را انجام دهد.
- تهدید علیه محرمانگی پیام‌ها: این تهدید مربوط به ایمنی کانال انتقال بین *Client* و سرور است. در این مسیر ممکن است امکان شنود وجود داشته باشد و دشمن اطلاعات حساس مثل کلمه عبور مشتری را از روی شبکه شنود نماید.
- تهدید علیه صحت پیام‌ها: در این تهدید نیز که به ایمنی کانال انتقال برمی‌گردد حمله کننده می‌تواند پیامهای ارسالی را تعویض نموده و یا آنها را مخدوش کند.

[1] *Internet Data Center*

۳-۲- روش‌های امن‌سازی

برای برطرف کردن تهدیدات موجود، نیاز به استفاده از مکانیزم‌های امنیتی برای امن‌سازی ارتباط بین *Client* و سرور است. راه حل مرسوم در این زمینه استفاده از پروتکل استاندارد *SSL*[1] در برقراری ارتباط بین *Client* و سرور می‌باشد. این پروتکل در اکثر سرویس‌دهنده‌های وب و مرورگرهای مختلف پشتیبانی شده و براحتی می‌توان از آن استفاده نمود. در این پروتکل پس از طی مرحله احراز اصالت طرفین، با استفاده از گواهی دیجیتال[2]، یک کلید مشترک توافق شده تا پس از آن اطلاعات بصورت امن مبادله گردد.

با توجه به سطح امنیت مورد نیاز، *SSL* را می‌توان به دو صورت به کار گرفت. در ادامه به نحوه بکارگیری این دو روش و محاسن و معایب هر یک می‌پردازیم.

الف- استفاده از *SSL* با احراز اصالت یک‌طرفه

در *SSL* احراز اصالت *Client* اختیاری است و می‌توان در پروتکل *SSL* از آن صرف نظر نمود. در این حالت فقط نیاز به گواهی سرویس‌دهنده است و کاربران نیازی به داشتن گواهی برای برقراری ارتباط نمی‌باشند. واضح است که در این وضعیت سرویس‌دهنده برای کاربران احراز اصالت می‌شود اما کاربر برای سرویس‌دهنده احراز اصالت نمی‌گردد. گواهی سرویس‌دهنده در این حالت حاوی کلید خصوصی، کلید عمومی و امضای مرکز صدور گواهی[3] (*CA*) بر روی پارامترهای عمومی گواهی است.

این روش به خاطر سادگی استفاده، بیشتر مرسوم بوده و در بسیاری از سرویس‌دهنده‌های وب بکارگیری می‌شود. در صورتی که در این روش به احراز اصالت کاربر نیاز باشد، احراز اصالت باید در برنامه کاربردی تحت وب انجام گیرد. به همین منظور پس از برقراری کانال امن *SSL*، نام و کلمه عبور کاربر در صفحه وب پرسیده شده و برای سرویس‌دهنده ارسال می‌شود.

ب- استفاده از *SLL* با احراز اصالت دوطرفه

در این روش *Client* و سرور هر دو دارای گواهی دیجیتال هستند و با استفاده از آن اصالت خود را به طرف مقابل اثبات می‌کنند. اگر چه در این روش احراز اصالت طرفین به طور کامل انجام

---

[1] *Secure Socket Layer*
[2] *Certificate*
[3] *Certificate Authority*

می‌گیرد اما از آنجا که پروتکل *SSL* در لایه انتقال انجام می‌شود امکان استفاده از نتایج احراز اصالت در لایه کاربرد براحتی میسر نبوده و بنابراین در این حالت هم احراز اصالت باید در برنامه کاربردی تحت وب (با پرسیدن نام و کلمه عبور کاربر) به طور جداگانه انجام گیرد (البته امکان گرفتن اطلاعات گواهی کاربر در محیط *ASP.NET* بر روی وب سرور *IIS* و ارایه سرویس *SSO* وجود دارد).

یکی از چالش‌های اصلی روش *SSL* دوطرفه، نحوه نگهداری امن گواهی کاربران است. از آنجا که این گواهی حاوی کلید خصوصی کاربر است در صورتی که به دست افراد سودجو بیافتد این افراد می‌توانند از آن سوء استفاده کرده و خود را به جای کاربر به سرور معرفی کنند. برای رفع این مشکل به جای نصب گواهی در کامپیوتر کاربر از توکن‌های امنیتی برای ذخیره امن گواهی استفاده می‌شود. در این صورت کلید خصوصی کاربر در مکان امنی قرار گرفته و امکان دسترسی غیر مجاز به آن وجود نخواهد داشت. توکن‌های امنیتی معمولا به دو صورت کارت هوشمند و ماژول *USB* هستند که انواع مختلفی از آنها در بازار وجود دارد.

اگرچه با ایجاد شدن کانال *SSL* (در هر یک از دو روش فوق) سرویس‌های محرمانگی و صحت داده‌ها محقق می‌شود و بخش مهمی از حملات مرتفع می‌گردد اما هنوز استفاده نادرست و بدون آگاهی از *SSL* می‌تواند زمینه حملات مهم دیگری از جمله *Man in the Middle* را فراهم نماید. این حمله زمانی می‌تواند بروز نماید که سرویس‌دهنده از گواهی معتبری استفاده نکند و یا اینکه گواهی *CA* مربوط به سرویس‌دهنده بر روی کامپیوتر مشتری وجود نداشته باشد. در هر دو حالت اخطاری مبنی بر نامعتبر بودن گواهی سرویس‌دهنده به مشتری گزارش داده می‌شود که چون معمولا مشتریان با مسائل امنیتی آشنایی کافی ندارند هشدار سیستم را نادیده گرفته و ارتباط *SSL* با سرویس‌دهنده مزبور را (بدون اطمینان از واقعی یا جعلی بودن آن) قبول می‌نمایند. افراد سوء استفاده کننده می‌توانند از این سهل‌انگاری مشتری استفاده کرده و سرور جعلی خود را به جای سرور اصلی معرفی نموده و کانال *SSL* را با مشتری برقرار کنند. بدین ترتیب مشتری اطلاعات محرمانه خود (از قبیل نام و کلمه عبور) را در اختیار سرور جعلی قرار داده و سرور جعلی به جای مشتری با سرور اصلی ارتباط برقرار می‌کند و پاسخ‌های سرور را برای مشتری برمی‌گرداند (حمله *Man in the Middle*). بنابراین مشتری از وقوع حمله مطلع نخواهد شد. در این حمله کافی است حمله کننده یکبار این عملیات را انجام داده و با بدست آوردن نام و کلمه عبور، سوء استفاده‌های بعدی را به راحتی انجام دهد.

برای رفع مشکل فوق به دو صورت می‌توان عمل کرد:

- تهیه گواهی از CAهای بین‌المللی که کامپیوتر مشتری به طور خودکار اعتبار آن را تشخیص می‌دهد:

در موقع نصب سیستم عامل ویندوز مجموعه‌ای از گواهی *CA*های مهم بین‌المللی از جمله *VeriSign*، *Thawte* و.... به طور خودکار بر روی کامپیوتر مشتری نصب می‌شود. بنابراین اگر گواهی سرور وب توسط این مراجع امضا شده باشد کامپیوتر مشتری به طور خودکار گواهی سرور را معتبر و قابل قبول تلقی می‌کند.

- تهیه گواهی از CAای که نیاز به نصب گواهی دارد:

در این روش برای تشخیص صحت گواهی سرور وب، نیاز به نصب گواهی *CA* صادر کننده در کامپیوتر می‌باشد. در این حالت مشتری باید با مراجعه به صادر کننده گواهی و تشخیص معتبر بودن آن، گواهی مربوطه را در لیست گواهی‌های معتبر[1] نصب کند. پس از نصب گواهی *CA*، در ارتباطات بعدی گواهی ارسالی از طرف سرویس‌دهنده معتبر تلقی می‌شود. روشن است که در این حالت آگاهی دادن به مشتریان مساله بسیار مهمی است.

۳-۳- پیشنهاد سطح‌بندی امنیتی خدمات اینترنتی

همانطور که در بخش قبل بدان اشاره شد *SSL* به عنوان راهکار استاندارد می‌تواند امنیت ارتباطات اینترنتی مشتریان را تحقق بخشد. این پروتکل در مرورگرهای مختلف پشتیبانی شده و بدون دغدغه می‌توان از آن استفاده نمود. البته با توجه به تنوع مشتریان بانک باید راهکار مناسبی برای استفاده از این پروتکل در سیستم بانکداری اینترنتی ارایه شود تا علاوه بر ارایه سطح امنیت مناسب، به سادگی نیز قابل استفاده باشد.

به منظور امن‌سازی ارتباط اینترنتی مشتریان و چگونگی استفاده از *SSL*، سرویس‌های اینترنتی بانک را به سه دسته زیر تقسیم‌بندی می‌کنیم و برای هر دسته راه حل متناسب را ارایه می‌نماییم. لازم به ذکر است که به منظور امن‌سازی ارتباط بین سرور وب و برنامه مرکزی بانکداری، بسته به جزییات معماری و شرایط فنی شبکه، می‌توان از راه حل‌های ارایه شده در امن‌سازی *Core Banking* (مثلا بکارگیری سیستم‌های کیهان و طریق) و یا راه حل‌های استاندارد مثل *SSL* استفاده نمود. در اینجا به دلیل مشابهت بحث با *Core Banking*، از معرفی این راه حل‌ها صرف نظر می‌کنیم.

۳-۳-۱- سرویس اطلاع‌رسانی

این سرویس به منظور اطلاع از موجودی و گردش حساب بوده و هیچ تراکنش مالی یا انتقال وجه

[1] *Trusted Root Certificate Authority*

را به همراه ندارد. با توجه به گستردگی کاربران این نوع سرویس، امنیت برای آن باید به ساده‌ترین شکل ممکن ارایه شود. از این رو روش *SSL* یک‌طرفه که در آن نیازی به گواهی کاربر نیست، می‌تواند راه کار مناسبی برای این سرویس باشد. در این راه حل با اتصال کاربر به سرور از زمانی که نیاز به امنیت در ارتباط باشد، کانال *SSL* بین کاربر و سرویس‌دهنده برقرار می‌گردد. لازم به ذکر است که اصالت سرویس‌دهنده باید توسط گواهی معتبر برای کاربر محرز شود. احراز اصالت کاربر در این شرایط می‌تواند توسط کلمه عبور انجام شود. تهدیدی که در این روش وجود دارد دزدیده شدن کلمه عبور توسط برنامه‌های جاسوسی مستقر بر روی کامپیوتر مشتری است که برای رفع این تهدید نیز می‌توان از برنامه‌های آنتی‌ویروس قوی یا مولفه‌های نرم‌افزاری که دارای ضریب امنیت بالایی هستند استفاده نمود.

۳-۳-۲- سرویس تراکنش‌های مالی پایین

این سرویس به منظور تبادلات مالی پایین مثل انتقال وجه به حساب‌های دیگر در یک سقف محدود یا پرداخت قبوض یا اقساط مورد استفاده قرار می‌گیرد. با توجه به انجام تراکنش‌های مالی، این سرویس به امنیت بیشتری نسبت به سرویس قبلی نیاز دارد و باید در مقابل حملاتی نظیر دزدیده شدن کلمه عبور مقاوم باشد.

برای امن‌سازی این سرویس، راهکار *SSL* دوطرفه پیشنهاد می‌شود. بدین منظور هر یک از مشتریان متقاضی این سرویس باید یک گواهی دیجیتال در اختیار داشته باشند که از طریق آن خود را به سرویس‌دهنده احراز اصالت کنند. گواهی کاربر بر روی کامپیوترش نصب شده و از آن در فرایند احراز اصالت پروتکل *SSL* استفاده می‌گردد. در این روش بعد از برقراری کانال *SSL* و احراز اصالت کاربر توسط گواهی، کلمه عبور را همانند قبل از مشتری دریافت می‌نماییم تا اصالت مشتری برای برنامه تحت وب نیز احراز شود.

برای صدور گواهی مشتریان، بانک می‌تواند یک مرکز *CA* با گواهی خودامضا راه‌اندازی کرده و برای مشتریان متقاضی، گواهی صادر نموده و به آنان تحویل دهد. روش دیگر این است که بانک برای مشتریان از یک *CA*، گواهی خریداری نموده وبه آنان تحویل دهد و یا از مشتریان بخواهد از یک *CA* مورد اعتماد بانک، گواهی خریداری نمایند.

۳-۳-۳- سرویس تراکنش‌های مالی بالا

از آنجا که مشتریان متقاضی این سرویس می‌توانند تبادلات مالی بالایی از طریق اینترنت داشته باشند، سطح بالایی از امنیت برای این سرویس مهم و ضروری است. از این رو در این روش همانند دسته دوم از *SSL* دوطرفه استفاده می‌شود با این تفاوت که گواهی مشتری به جای کامپیوتر در توکن او

قرار می‌گیرد. در ابتدا توکن، مشتری را با استفاده از شناسه شخصی (*PIN*) احراز اصالت می‌کند و سپس گواهی درون توکن برای سرویس‌دهنده احراز اصالت می‌شود.

در اینجا نیز عملیات صدور گواهی می‌تواند توسط *CA* خود بانک انجام بگیرد و یا اینکه بانک از طرف مشتریان از یک مرکز *CA* گواهی‌ها را خریداری نماید. در این حالت بانک باید توکن امنیتی تهیه کرده و گواهی هر مشتری را در درون توکن وی تزریق نماید. یک انتخاب مناسب برای توکن امنیتی ماژول سخت‌افزاری کیاست. این توکن امنیتی که از نوع *USB* است و از ویژگی‌های ممتاز امنیتی برخوردار می‌باشد برای اولین بار در کشور در سال ۱۳۸۳ به وسیله شرکت پیام‌پرداز ارایه گردید. مراحل طراحی، توسعه و تولید این محصول به صورت کامل در داخل شرکت پیام‌پرداز و زیر نظر تیم‌هایی متشکل از متخصصین امنیت، سخت‌افزار و نرم‌افزار انجام گرفته است. این محصول از لحاظ نفوذ به بازار وضعیت رضایت‌بخشی داشته و تاکنون دو گونه از این محصول ارایه شده است.

نکات دیگری که در مورد استفاده از ماژول امنیتی کیا قابل ذکر هستند عبارتند از:

- یک‌سری نرم‌افزارهای امنیتی همراه با کیا ارایه می‌گردد که می‌تواند به خوبی در سیستم بانکداری الکترونیک بکارگیری شود. به عنوان مثال یکی از نرم‌افزارهای قابل استفاده، نرم‌افزار کیان برای ورود امن به ویندوز است که *Login* به کامپیوتر را به صورت دوعاملی تبدیل می‌کند. این محصول را می‌توان بر روی کامپیوترهای کلیه کاربران در مرکز و شعب بانک نصب کرده و از ورود افراد غیر مجاز به کامپیوترها جلوگیری نمود.
- ماژول کیا دارای مجموعه کاملی از کیتها و ابزارهای نرم‌افزاری در محیط‌های مختلف برنامه‌نویسی است که از آنها می‌توان برای توسعه نرم‌افزارهای کاربردی جهت پیاده‌سازی سرویس‌های امنیتی استفاده نمود. در واقع تدوین‌کنندگان نرم‌افزارهای *Core Banking* می‌توانند برنامه‌های کاربردی خود را با استفاده از ماژول کیا به سرویس‌های امنیتی بیشتر مجهز کنند.

شایان ذکر است در صورتی که سطح بالاتری از امنیت *SSL* دوطرفه برای ارتباط اینترنتی مشتریان با سرور وب مد نظر باشد می‌توان از سیستم کیهان بدین منظور استفاده کرد. در این حالت سیستم کیهان به صورت قوی (دوسویه و دوعاملی) کاربر را احراز اصالت کرده و یک تونل امن با کامپیوتر کاربر برقرار می‌کند. اگرچه این روش امنیت بالاتری نسبت به روش استاندارد *SSL* ارایه می‌کند ولیکن محدودیت‌های زیر را به همراه دارد:

- در صورتی که میزبان سرور وب در خارج کشور قرار داشته باشد گذاشتن سرور کیهان در مقابل آن ممکن است خیلی راحت نباشد.

- از آنجا که باید بر روی کامپیوتر مشتری، نرم‌افزار *Client* کیهان نصب شود از این روش نمی‌توان به راحتی در محیط‌های عمومی مثل کافی‌نت‌ها استفاده نمود.

۴- تجهیزات خودپرداز و کیوسک

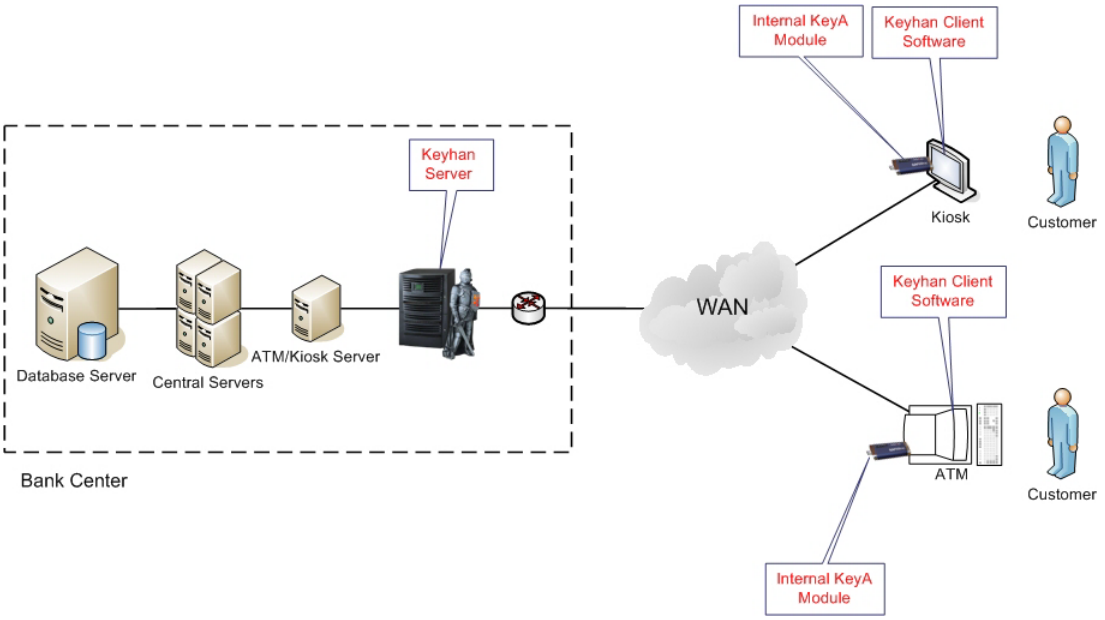
خودپردازها دستگاههایی هستند که انواع خدمات بانکی مانند پرداخت پول و یا پرداخت قبوض را می‌توان به کمک آنها انجام داد. کیوسک‌ها اکثرا سرویس‌هایی شبیه به بانکداری اینترنتی را ارایه می‌کنند با این تفاوت که تا حدی محدودتر از بانکداری اینترنتی هستند. به عنوان مثال مشتری امکان اتصال یک توکن *USB* را به آنها ندارد. دستگاه‌های خودپرداز و کیوسکها به صورت برخط[1] به شبکه مرکزی بانک متصل هستند و سرویس‌های لازم را به مشتریان ارایه می‌کنند.

با توجه به اینکه این تجهیزات در حال حاضر از یکسری مکانیزم‌های امنیتی مثل کارت‌های مغناطیسی یا هوشمند (برای احراز اصالت مشتری) و ... استفاده می‌کنند به نظر می‌رسد سرویس‌های امنیتی زیر نیز مورد نیاز باشد:

- محرمانگی داده‌های مبادله شده بین تجهیزات (خودپرداز یا کیوسک) و سرور
- صحت داده‌های مبادله شده بین تجهیزات (خودپرداز یا کیوسک) و سرور
- احراز اصالت تجهیزات (خودپرداز یا کیوسک) برای سرور

از آنجا که تجهیزات خودپرداز و کیوسک به صورت داخلی دارای یک کامپیوتر (معمولا با سیستم عامل ویندوز) هستند برای امن‌سازی ارتباط این تجهیزات با مرکز می‌توان از سیستم کیهان استفاده نمود (شکل ۶). در این حالت نیز یک سرور کیهان در مقابل سرور مربوطه در *LAN* مرکزی بانک قرار گرفته و بر روی کامپیوتر داخلی تجهیزات، نرم‌افزار *Client* کیهان قرار می‌گیرد. این نرم‌افزار از ماژول کیایی که قبلا توسط مدیر سیستم برنامه‌ریزی شده و بر روی این کامپیوتر قرار دارد برای اتصال امن به سرور کیهان استفاده می‌کند. با توجه به اینکه این تجهیزات همیشه روشن بوده و کاربر خاصی ندارند نرم‌افزار *Client* کیهان در این راه حل برای *Login* به سرور کیهان، *PIN* دریافت نمی‌کند. همچنین می‌توان در اینجا نیز از امکان محدود کردن *Client* برای برقراری ارتباط از روی کامپیوتر خاص مربوط به تجهیزات خودپرداز یا کیوسک استفاده نمود.

[1] *On-Line*



شکل ۶: امن‌سازی ارتباط تجهیزات خودپرداز و کیوسک با سیستم کیهان

شایان ذکر است در صورتی که تجهیزات خودپرداز یا کیوسک دارای سیستم عامل ویندوز نباشند (و یا در شرایط خاص دیگر) یک انتخاب جایگزین به جای سیستم کیهان، محصول رمزکننده شبکه سدید است که در شرکت پیام‌پرداز طراحی و ساخته شده است. این سیستم یک رمزکننده لایه پیوند داده است که به دو فرم پل[1] (سخت‌افزاری) و میزبان[2] (نرم‌افزاری) قابل ارایه است.

۵- بانکداری با تلفن همراه

بانکداری با تلفن همراه (*m-banking*) به مجموعه‌ای از ابزارها و تکنیکهایی اطلاق می‌گردد که با استفاده از آنها مشتریان بانک امکان دسترسی به برخی از خدمات بانکی را از طریق تلفن همراهشان به دست می‌آورند. در بین رسانه‌های ارتباطی پشتیبانی شده به وسیله تلفن همراه، *SMS* به علت همه‌گیر بودن، ارزان بودن، در دسترس بودن، پشتیبانی همه گوشی‌ها و ... اکثر اوقات به عنوان ابزار ارتباطی *m-banking* به کار می‌رود. البته رسانه‌های جدید ارتباطی روی موبایل مثل *GPRS* نیز می‌تواند بدین منظور به کار رود ولیکن به دلیل محدودیت‌های موجود از قبیل عدم پشتیبانی همه گوشی‌ها، این سرویس در حال حاضر کمتر در کشور ما مورد استفاده قرار گرفته است. سرویس‌های بانکداری مبتنی بر *GPRS* عموما مشابه با سرویس‌های بانکداری اینترنتی هستند و بنابراین راه حل‌های امن‌سازی مطرح شده در بانکداری اینترنتی مثل *SSL* در اینجا نیز قابل استفاده‌اند. هرچند سرویس‌های خاص بانکداری

[1] *Bridge*
[2] *Host*

مبتنی بر *GPRS* نیز قابل ارایه است. در ادامه توجه خود را بر روی رسانه *SMS* به عنوان ابزار ارتباطی *m-banking* معطوف می‌کنیم.

در سیستم *m-banking* یک سرور *SMS* در سمت بانک و معمولا یک برنامه کاربردی در سمت گوشی مشتری، عملیات تبادل پیامک را انجام می‌دهند. البته ممکن است برنامه کاربردی خاصی در سمت مشتری وجود نداشته باشد و مشتری از امکانات معمول *SMS* گوشی، برای ارسال پیام‌های خود (با فرمت مشخص) و یا دریافت پاسخ‌های بانک استفاده نماید. برنامه کاربردی سمت گوشی (در صورت وجود) به دلیل اینکه لازم است بر روی گوشی‌های مختلف اجرا گردد معمولا به زبان جاوا تهیه می‌شود.

۵-۱- خدمات *m-banking*

خدمات *m-banking* زیرمجموعه‌ای از خدمات مرسوم بانکی است. در حقیقت کلیه خدمات بانکی که نیاز به تبادل اطلاعات حجیم ندارند در سیستم *m-banking* قابل ارایه هستند. همچنین خدمات *m-payment* و *m-commerce* نیز که اکثرا با مشارکت بانکها انجام می‌شوند، از جمله امکانات محبوب در تلفن همراه به شمار می‌روند.

برخی از خدماتی که در سیستمهای *m-banking* ارایه می‌گردند عبارتند از:

- پرداخت قبوض
- پرداخت اقساط
- دریافت موجودی‌ها و اطلاعات حساب
- اطلاع‌رسانی گردشهای مالی حساب
- مسدود کردن برخی از امکانات توسط کاربر در مواقع خطر
- انتقال وجه
- انجام تنظیمات حسابهای مختلف به منظور خودکار شدن دریافتها و پرداختها
- خرید کالا از فروشگاه‌ها
- خرید شارژ سیم‌کارتهای اعتباری

روشن است که هر چه قدر برنامه سمت گوشی مشتری، قابلیتهای بیشتری را ارایه نماید، متناسب با آن و یا شاید بیش از آن نیاز به پشتیبانی در سمت سرور خواهد بود. می‌توان قابلیتها را دسته‌بندی نمود و هر دسته را در اختیار مشتریان با سطح موجودی، توانایی و یا آموزش کافی قرار داد. می‌توان برنامه را به نحوی خودکار و قابل تنظیم طراحی کرد تا بانک در زمان دلخواه، توان تعیین خدمات قابل دسترس

برای هر مشتری را داشته باشد. همچنین می‌توان گوشی را به یک کنترل پانل قوی برای مشتریان تبدیل کرد ولی برای اطمینان از استفاده صحیح ممکن است نیاز به گذر زمان و آموزش یا افزودن و عرضه تدریجی امکانات پیچیده‌تر باشد.

۵-۲- نیازمندی‌های امنیتی

یکی از نکات مهم و قابل ملاحظه در سرویس پیام کوتاه، بحث امنیت این ابزار سودمند می‌باشد. اگرچه در شبکه *GSM* امکان رمز پیام‌های کوتاه در هنگام انتقال بر روی کانال هوایی وجود داشته و این سرویس اکثرا (توسط اپراتورهای مخابراتی) فعال می‌باشد ولیکن پیام‌های کوتاه در مرکز *SMS*[1] اپراتور مخابراتی و همچنین گوشی تلفن همراه کاربر به صورت فاش ذخیره می‌شوند و لذا امکان دسترسی افراد غیرمجاز و حملاتی از قبیل مشاهده، جعل، دستکاری و سوء استفاده از پیام‌ها وجود دارد. بنابراین در رابطه با سرویس بانکداری با تلفن همراه، نیازمندیهای امنیتی زیر مورد نظر است:

- محرمانگی پیامهای مبادله شده: به این دلیل که اطلاعات ارزشمند و حساسی همچون کلمات عبور و همچنین اطلاعات مالی مشتریان بر روی شبکه *GSM* مبادله (و در مرکز *SMS* اپراتور مخابراتی ذخیره) می‌شوند نیاز به محرمانگی وجود خواهد داشت.
- محرمانگی پیامهای ذخیره شده در گوشی: روشن است که دسترسی یک فرد غیرمجاز به گوشی یک مشتری نباید باعث افشای اطلاعات حساس شده یا زمینه سوء استفاده برای وی فراهم گردد.
- صحت پیامهای مبادله شده: به دلیل اهمیت اطلاعات مبادله شده در سیستم‌های مالی، یکی از نیازمندیهای مهم سیستمهای بانکداری با تلفن همراه صحت پیامک‌های مبادله شده است.
- احراز اصالت مشتری: چون لازم است هیچ کس به جز صاحب حساب یا کارت اجازه دسترسی به حساب را نداشته باشد احراز اصالت مشتری ضروری است.
- مشکلات امنیتی محیط جاوا: محدودیتهایی که به دلیل همه‌گیر و عمومی بودن تکنولوژی جاوا به وجود آمده است، بعضا در زمینه امنیتی گریبان‌گیر جاوا می‌شود. عمده محدودیت موجود عدم وجود محلی امن برای ذخیره داده‌های حساس در تلفن همراه است. محدودیت دیگر به خود زبان جاوا و وجود امکان دیکامپایل کردن برنامه‌های آن برمی‌گردد.

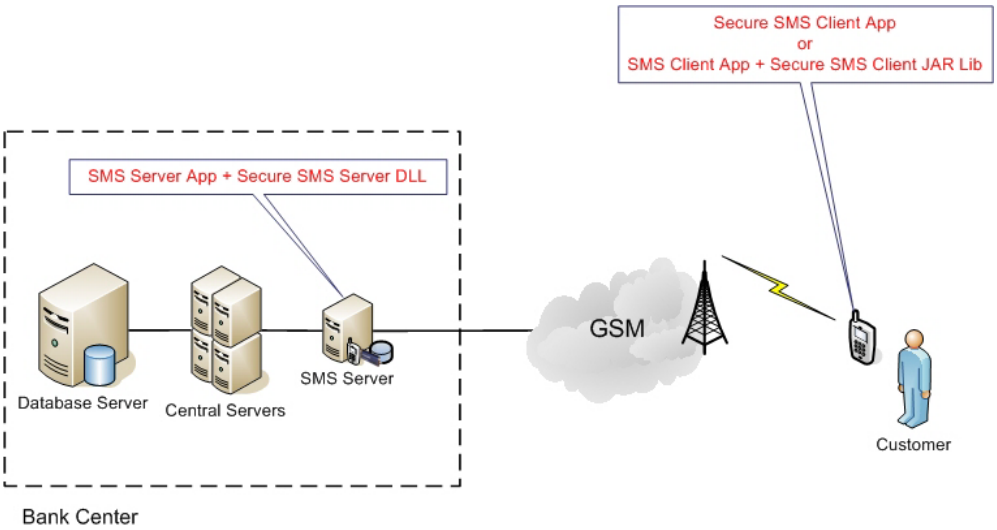
[1] *SMS Center*

۵-۳- راه حل امن‌سازی

به منظور امن‌سازی سیستم *m-banking* و ارایه سرویس‌های امنیتی محرمانگی و صحت پیام‌ها می‌توان از مکانیزم رمزنگاری استفاده نمود. بدین منظور لازم است امکانات رمزنگاری در هر دو سمت سرویس‌دهنده و مشتری پیاده‌سازی گردد. شرکت پیام‌پرداز تجربه طراحی و پیاده‌سازی نرم‌افزار رمزکننده *SMS* بر روی گوشی‌های مبتنی بر جاوا و همچنین گوشی‌های مبتنی بر سیستم‌عامل‌های *Windows Mobile* و *Symbian* را داشته است. راه حل مورد استفاده برای امن‌سازی در ادامه آمده است.

در سمت مشتری یک برنامه کاربردی رمزکننده برای اجرا بر روی تلفن همراه ارایه می‌شود. البته در صورتی که مشتریان از برنامه کاربردی خاصی بر روی گوشی خود برای انتقال *SMS* استفاده نمایند، یک کتابخانه رمز جهت اتصال به برنامه کاربردی گوشی ارایه خواهد گردید. در سمت سرور، از آنجا که سیستم *m-banking* و سرور توزیع *SMS* مربوطه معمولا در بانک وجود دارد یک کتابخانه رمزکننده *SMS* ارایه خواهد شد که باید به برنامه سرویس‌دهنده *SMS* بانک افزوده شود.

شکل ۷ معماری امن‌سازی سرویس *m-banking* را نشان می‌دهد. روش رمزنگاری در این طرح به صورت متقارن بوده و بر اساس کلید مشترک بین هر مشتری و سرور انجام می‌پذیرد. با استفاده از این طرح *SMS*ها به صورت کاملاً محرمانه و معتبر رد و بدل شده و امکان مشاهده، دستکاری و سوء استفاده از آن، در هنگام انتقال و در مدت ذخیره‌سازی بر روی گوشی مشتری یا مرکز *SMS* اپراتور مخابراتی وجود نخواهد داشت. در این طرح از مکانیزم‌هایی برای ذخیره اطلاعات حساس برنامه جاوا بر روی گوشی استفاده خواهد شد.



شکل ۷: معماری امن‌سازی سرویس *m-banking*

سیستم امن‌سازی ارایه شده به طور دقیق‌تر شامل اجزای اصلی زیر می‌باشد:

- **نرم‌افزار رمزکننده *SMS* برای استفاده در گوشی‌های تلفن همراه:**

این نرم‌افزار وظیفه امن‌سازی سرویس پیام کوتاه در گوشی‌های تلفن همراه را بر عهده دارد. نرم‌افزار، پیام کوتاه را در هنگام ارسال رمزگذاری کرده و در هنگام دریافت، رمزگشایی می‌کند. این نرم‌افزار در محیطهای دارای پشتیبانی جاوا (قابل نصب بر روی گوشی‌های دارای *package*های *MIDP2.0* و *WMA1.0* به بالا)، سیستم عامل *Symbian* (قابل نصب بر روی گوشی‌های دارای این سیستم عامل) و سیستم عامل‌های *Windows Mobile* (قابل نصب بر روی رایانه‌های جیبی[1] و تلفن‌های هوشمند[2]) ارایه می‌شود. لازم به ذکر است که گوشی‌های پشتیبانی کننده از جاوا وسعت بیشتری داشته و گوشی‌های *Symbian* و *Windows Mobile* نیز معمولا از برنامه‌های جاوا حمایت می‌کنند. بنابراین می‌توان نرم‌افزار را تنها در محیط جاوا ارایه کرد.

- **کتابخانه رمزنگاری برای استفاده در برنامه کاربردی گوشی‌های تلفن همراه (در صورت لزوم):**

این کتابخانه که به زبان جاوا پیاده‌سازی شده باید به برنامه کاربردی ارسال و دریافت پیام کوتاه در سمت مشتری اضافه گردیده و توابع آن در موقع نیاز فراخوانی شوند. توابع اصلی این کتابخانه توابع رمزگذاری و رمزگشایی هستند که از آنها باید به ترتیب قبل از ارسال پیام کوتاه و بعد از دریافت پیام کوتاه استفاده نمود.

- **کتابخانه رمزنگاری برای سرویس‌دهنده *SMS*:**

این کتابخانه بصورت *DLL* در کنار برنامه سرویس‌دهنده مرکزی قرار گرفته و عملیات رمزنگاری را بر روی پیام‌های رد و بدل شده انجام می‌دهد. در کنار این کتابخانه رمز، یک پایگاه داده داخلی برای نگهداری کلیدهای مشتریان قرار خواهد گرفت. کلید مربوط به هر مشتری از طریق جستجو در پایگاه داده بر حسب شماره تلفن یا شناسه وی به دست می‌آید. کتابخانه از یک ماژول امنیت کیا برای امن‌سازی پایگاه داده داخلی استفاده می‌کند.

۶- بانکداری تلفنی

بانکداری تلفنی به دسته‌ای از خدمات بانکی اطلاق می‌شود که مشتری می‌تواند از طریق تلفن به آنها دسترسی داشته باشد. معمولا در این سیستم یک ماشین تلفن گویا در سمت مرکز به مشتریان

[1] *Pocket PC*
[2] *Smartphone*

سرویس می‌دهد. فرمان‌های صادر شده به وسیله مشتریان در این سیستم، سیگنال‌های صوتی *DTMF*[1] تولید شده به وسیله شماره‌گیر دستگاه تلفن است.

خدمات مرسوم بانکداری تلفنی عبارتند از:

- دریافت موجودی حساب
- دریافت اطلاعات گردش حساب
- مسدود کردن کارتها، چکها و حسابها در موقع نیاز
- آگاهی از وضعیت حسابها، چکها و ...
- تعیین سقف تراکنش برای چکها و حسابها و ...
- دریافت اطلاعات حساب از طریق فاکس
- انتقال وجه (این سرویس معمولا به دلیل وجود تهدیدات امنیتی ارایه نمی‌شود)

۶-۱- نیازمندی‌های امنیتی

در سیستم‌های بانکداری تلفنی ارتباط مشتری با سرور از طریق شبکه *PSTN* برقرار می‌شود. در نقاط مختلف این شبکه (شامل سیم‌های مسی ارتباط مشتری یا سرور با مراکز تلفن مربوطه، *MDF* مراکز تلفن، مراکز سوییچ و خطوط انتقال) امکان شنود سیگنال‌های صوتی به راحتی وجود دارد. البته با توجه به برخط و زمان واقعی[2] بودن ارتباط تلفنی، امکان دستکاری در پاسخ‌های سرور وجود ندارد. اما می‌توان با ساخت یک دستگاه سخت‌افزاری (نسبتا پیچیده) که روی خط تلفن سرور قرار می‌گیرد فرمان‌های *DTMF* صادر شده به وسیله مشتری را دستکاری کرد (حمله *Man in the Middle*). بنابراین مهمترین نیازمندی‌های امنیتی در سیستم بانکداری تلفنی را می‌توان به صورت زیر در نظر گرفت:

- احراز اصالت مشتری: از آنجا که لازم است تنها صاحب حساب امکان دسترسی به حساب خود را داشته باشد لذا احراز اصالت مشتری در این سیستم بسیار مهم است. در سیستم‌های موجود از *PIN* برای احراز هویت مشتری استفاده می‌شود.
- محرمانگی اطلاعات صوتی: این اطلاعات شامل پاسخ‌های صوتی (یا فاکس) پخش شده از طرف سرور و نیز فرمان‌های حساس وارد شده توسط مشتری مثل *PIN* می‌باشد. به عنوان مثال یک نفر با سرقت *PIN* یک مشتری می‌تواند نقش وی را بازی کرده و به طور غیر مجاز به سیستم وارد شود.
- صحت فرمان‌های *DTMF* مشتری: همانگونه که بیان شد اگرچه مکانیزم تغییر فرمان‌های

[1] *Dual Tone Multi-Frequency*
[2] *Real Time*

مشتری در شبکه *PSTN* نسبتا پیچیده است ولیکن امکان آن وجود دارد. بنابراین در صورت امکان باید جلوی این حمله گرفته شود.

۶-۲- راه حل‌های امن‌سازی

یک روش مناسب برای احراز اصالت قوی مشتری و حل مشکل شنود *PIN* استفاده از کلمات عبور یک بار مصرف[1] (*OTP*) است. این کلمات عبور در هر بار استفاده تغییر می‌نمایند و بدین ترتیب امکان سوء استفاده از کلمات عبور لو رفته به حداقل می‌رسد. روشن است که در سمت مرکز باید یک سرور *OTP* سرویس‌دهی لازم را انجام دهد.

سیستم *OTP* در سمت مشتری می‌تواند به دو روش سخت‌افزاری یا نرم‌افزاری پیاده‌سازی گردد. در روش سخت‌افزاری از یک ماژول سخت‌افزاری استفاده می‌شود که کلمه عبور را به روشی امن و همخوان با سرور *OTP* تولید می‌کند. در روش نرم‌افزاری برنامه‌ای در سمت مشتری، عملیات تولید کلمه عبور را انجام می‌دهد.

شرکت پیام‌پرداز امکان ساخت و تولید سیستم‌های *OTP* نرم‌افزاری و سخت‌افزاری را دارد. این سیستم شامل اجزای زیر خواهد بود:

- نرم‌افزار سرویس‌دهنده *OTP* برای سمت مرکز
- نرم‌افزار *OTP Client* برای سمت مشتری که می‌تواند بر روی موبایل (محیط‌های جاوا، *Symbian* یا *Windows Mobile*) اجرا شود. از آنجا که امروزه اکثر افراد دارای تلفن همراه هستند با ارایه نرم‌افزار *OTP* بر روی موبایل می‌توان این سرویس را به گروه عمده‌ای از مشتریان ارایه نمود.
- ماژول سخت‌افزاری *OTP Client* برای مشتری

ارایه سرویس‌های محرمانگی وصحت اطلاعات در سیستم بانکداری تلفنی مستلزم استفاده از رمزکننده‌های تلفنی است. اگرچه شرکت پیام‌پرداز تکنولوژی ساخت انواع سخت‌افزاری و نرم‌افزاری این رمزکننده‌ها را در اختیار دارد اما از آنجا که اولا هزینه این رمزکننده‌ها بالا بوده و ثانیا کاربری آنها پیچیده است لذا در کاربردهای بانکی که عموم مردم با آن سروکار دارند چندان قابل توصیه نیست. بنابراین در مجموع به نظر می‌رسد باید در بانکداری تلفنی از ارایه خدمات با حساسیت زیاد که نیاز به سطح امنیت بالایی دارند صرف نظر کرد.

[1] *One Time Password*