بسترهای نرم افزاری تجارت و بانکداری الکترونیک در ایران

دکتر بیژن بیدآباد[1] محمود الهیاری فرد[2]

چکیده

اجرای تجارت و بانکداری الکترونیک نیازمند وجود بسترهای مختلفی است که از جمله آنها مسائل مهم در این بخش نرم‌افزار است که در زمینه‌های مختلف مسائل تجارت و بانکداری الکترونیک مطرح می‌باشد. وابسته نبودن برنامه‌های تحت وب به Platform و قابل اجرا بودن آن در اینترنت در تمام نقاط موجب رونق گرفتن مجازی سازی جهت کاهش هزینه‌ها شده است. رونق گرفتن برنامه‌های سرویس‌دهنده و سرویس گیرنده و همچنین گسترش بانکهای اطلاعاتی قدرتمند نصب شده در سرویس‌دهنده‌ها با توانائی ایجاد دومیلیون جدول و امن بودن اطلاعات با توجه به قابلیتهای تهیه پشتیبان خودکار از اطلاعات موجب آسودگی مشتریان و بانکداران شده است. شرکتهای بزرگ نرم‌افزاری بیش از پیش به مقوله امنیت در تولید سیستم‌های عامل و برنامه‌های تولید کننده Web Applications اندیشیدند، و در قرن ۲۱ به جای افزایش کمی نرم‌افزارها در جهت ارتقاء کیفی کوشیدند زیرا بخوبی می‌دانستند که تجارت و بانکداری الکترونیک به سرعت در حال رشد و توسعه است بنابراین می‌بایست بسترهای آنرا فراهم نمایند. بسترهای نرم‌افزاری بطور خلاصه می‌توان در ابعاد فنی ، فرهنگی، آموزش و حقوقی مورد توجه قرار داد. بعد فنی بسترهای نرم‌افزاری را می‌توان در فناوریهای ایجاد شده در زمینه‌های سیستم‌های عامل، مرورگرهای وب، زبانهای برنامه‌نویسی تولید کننده‌های برنامه‌های تحت وب، بانکهای اطلاعاتی مبتنی بر سرویس‌دهنده مورد بررسی قرارداد. علاوه بر بعد فنی در بسترهای نرم‌افزاری ابعاد آموزشی، فرهنگی و حقوقی نیز در پذیرش تجارت و بانکداری از اهمیت فراوانی برخوردار است. عدم توجه به وضعیت آموزشی، فرهنگی و عدم بسترهای حقوقی مناسب در یک کشور موجب شکست تجارت و بانکداری الکترونیک خواهد شد.

تجارت الکترونیک

تجارت الکترونیک فرآیندی است که بوسیله آن کلیه محصولات اعم از محسوس یا نامحسوس از طریق یک شبکه‌های ارتباطی رایانه‌ای، مخابراتی و یا هر دو خرید و فروش می شود. تجارت الکترونیک مفهوم گسترده‌ای دارد و تنها محدود به مبادلات و تراکنشهای انجام شده بر روی اینترنت نمی شود، بلکه کلیه تراکنشهای مالی که از طریق شبکه‌های مخابراتی و ارتباطی رایانه‌ای انجام می‌گیرد را شامل می‌شود.

مبادله الکترونیکی داده‌ها(*EDI*)

از مبادله الکترونیکی داده‌ها می‌توان برای مخابره الکترونیکی مدارک و اسناد مانند سفارشات خرید، فاکتور، اعلامیه حمل، تاییدیه وصول کالا و سایر مکاتبات استاندارد و بازرگانی بین طرفین تجاری استفاده نمود. موضوع مبادله الکترونیکی داده‌ها (EDI) از دهه ۱۹۶۰مطرح شد و به بیان چگونگی مبادله اطلاعات بین شرکتها و ادارات پرداخت.

---

[1] عضو هیئت علمی پژوهشی و مدیرگروه ارزی پژوهشکده پولی و بانکی www.bidabad.com bidabad@yahoo.com

[2] کارشناس ۲ اقتصادی اداره تحقیقات و برنامه‌ریزی بانک ملی ایران allahyarifard@gmail.com

در ارتباطات تجاری سنتی بر پایه کاغذ، وارد نمودن مکرر یک رشته اطلاعات یکسان و واحد می‌تواند موجب بروز مشکلاتی گردد، ولی با استفاده از مبادله الکترونیکی داده‌ها این مشکلات بطور قابل ملاحظه‌ای کاهش می یابد، این مشکلات بطور کلی عبارتند از:

صرف زمان بیشتر

دقت کمتر

هزینه بالای نیروی کار

در فن آوری مبادله الکترونیکی داده‌ها برای اسناد تجاری عادی مانند استعلام قیمت، سفارش خرید، اصلاحیه سفارش خرید، بارنامه، اعلامیه وصول، فاکتور و مدارک نظیر آنها قالبهای استاندارد پیام الکترونیکی تهیه شده است. این مجموعه‌های الکترونیکی، رایانه واقع در یک سازمان را قادر می‌سازد که بدون تهیه و تولید مدارک کاغذی با رایانه واقع در یک سازمان دیگر ارتباط برقرار نماید. به این ترتیب، تلاشی که بوسیله انسان برای خواندن، طبقه بندی و حمل فیزیکی این گونه اسناد صرف می‌گردد، حذف می‌شود.

اسنادی که برای آنها قالب استاندارد الکترونیکی تهیه شده یا در دست تهیه می‌باشد. ۸۵درصد از مکاتبات رسمی تجاری بین شرکتها، مؤسسات دولتی، نهادهای آموزشی و سازمانهای غیرانتفاعی درکشورهای صنعتی را تشکیل می‌دهد. [۱]

سه جزء اصلی در ارسال ودریافت پیامهای مبادله الکترونیکی داده‌ها عبارتندار:

استانداردهای مبادله الکترونیکی داده‌ها

نرم‌افزار مبادله الکترونیکی داده‌ها

شبکه‌های طرف ثالث جهت برقراری ارتباط

مبادله اسناد تجاری به شکل پیش ساخته و مورد توافق طرفین مورد معامله ایجاد می‌شود که استانداردهایی برای این منظور تدوین شده است. استانداردهای مبادلات الکترونیکی اساسا استانداردهای مبتنی بر داده‌های دیجیتال می‌باشد، زیرا ترکیب و مفهوم داده‌های مورد مبادله را تعیین می‌نمایند. بعضی ازاین استانداردها عبارتنداز:

استاندارد مربوط به قسمت حمل ونقل درایالات متحده آمریکا

استاندارد ارتباطات یکنواخت (UCS)[۲]

استاندارد مبادله داده‌های تجاری (TDI)[۳]

مدل فرایند تجاری در تجارت الکترونیک

تجارت الکترونیک بطور عام و مبادله الکترونیکی داده‌ها بطور خاص، به عنوان ابزاری برای ایجاد تغییر در شیوه‌های عملیاتی سازمانها طراحی و پیش‌بینی شده‌اند. در این فرایند تنها حذف معاملات کاغذی مطرح نیست، بلکه همچنین ایجاد تحول در نحوه انجام معاملات سازمانها با طرفهای تجاری و نیز پاسخگویی به معاملات در مبادله الکترونیکی داده‌ها نیز مورد نظر می‌باشد و این خود موجب بازسازی فرایندهای درون سازمانی می‌شود.

در حقیقت بالاترین سطح بهره‌وری و کارایی زمانی حاصل می‌شود که این فن‌آوری پس از بررسی‌های

[۱] به "از مبادله الکترونیکی داده‌ها تا تجارت الکترونیک" انتشارات مؤسسه مطالعات و پژوهشهای بازرگانی (۱۳۷۸) مراجعه شود.

[۲] Uniform Communication Standard

[۳] Trade Data Interchange

کامل و تجزیه و تحلیل فرایندهای درون سازمانی پیاده شود و پس از برقراری آن نیز فرایندها بطور مداوم مورد بازنگری و بازسازی قرار گیرند.

بازسازی فرایندهای عملیاتی به عنوان ضابطه‌ای جهت ترویج صحیح تجارت الکترونیک در فرایندهای جدید ظهور کرده است. برای ایجاد یک مدل فرایند تجارت الکترونیک راههای مختلفی وجود دارد. طبق نظریه «راجر کلارک» یکی از این مدل‌ها، مدلی است که بر پایه پنج مرحله متداول در معاملات عادی قرار دارد. این مراحل پنجگانه به شرح زیر است:

۱- مرحله پیش از قرارداد: این مرحله مربوط به جمع‌آوری اطلاعات در مورد کالاها یا خدماتی است که خرید یا فروش آنها مورد نظر می‌باشد.

۲- مرحله قرارداد: در این مرحله یک رابطه رسمی بین خریدار و فروشنده بوجود می‌آید و شرایط حاکم بر قرارداد مشخص می‌شود.

۳- مرحله سفارش و پشتیبانی: در این مرحله سفارش خرید داده و پردازش می‌شود، کالاها یا خدمات حمل یا ارائه می‌شوند و امور پس از تحویل مانند بازرسی و قبول موضوع قرارداد انجام می‌شود.

۴- مرحله تسویه حساب: در این مرحله تهیه فاکتور، صدور دستور پرداخت، پرداخت و اعلامیه حواله صورت می‌پذیرد.

۵- مرحله پس از پردازش: این مرحله شامل جمع‌آوری و گزارش اطلاعات مدیریتی، انبارداری و تجزیه و تحلیل آمار تجاری است.

تجارت الکترونیک را در پایین‌ترین سطح آن می‌توان تنها برای خودکار کردن فرایندهای موجود به کار برد ولی با اجرای بازسازی روشهای کاری نحوه انجام کارها را می‌توان منطقی ساخت. این اقدام اثراتی نیز روی ساختار سازمانی دارد و موجب کاهش هزینه‌ها، افزایش سرعت و بهبود کیفیت خدمات می‌شود. از آنجا که خودکار کردن فعالیتهای سازمان الزاماً طرفهای تجاری سازمان را نیز تحت تأثیر قرار می‌دهد، لذا عملیات مربوط به خودکار کردن فعالیتها و منطقی ساختن و تغییر و طراحی مجدد شیوه‌های انجام کار تنها محدود به ساختار و فرایندهای درون سازمانی نمی‌شود. بلکه ممکن است از چارچوب سازمانی فراتر رفته و سراسر یک صنعت یا بخش را فراگیرد.

برای تجارت الکترونیکی چهار مرحله متفاوت و کلی به شرح زیر وجود دارد:

۱) در مرحله ارتباط، اینترنت رابطی است که از طریق آن ارتباط تجاری صورت می‌گیرد.

۲) در مرحله تبادل اطلاعات با مشتریان رابط گرافیکی (GUI)[1] تحت وب تسهیلات تبادل اطلاعات را فراهم می‌نماید.

۳) مرحله در اختیار قراردادن نحوه اجرای معاملات و طبقه بندی آنها.

۴) مرحله‌ایجاد ارتباط دو سویه از طریق پویا کردن صفحات وب در اینترنت بطوریکه امکان تبادل اطلاعات با مشتریان فراهم آید.

هدف از بکارگیری شیوه‌های تجارت الکترونیک، ایجاد سازمانهای الکترونیکی است. گرچه این روش‌ها، مطالعات بدون استفاده از کاغذ را میان بخش‌های تجاری رواج می‌دهد، لیکن غالباً کارهای کاغذی درون یک سازمان یعنی نامه‌ها، درخواست‌های خرید و فرمها، نادیده گرفته می‌شوند. با توجه به این امر، مقصود از خودکار کردن گردش کار، حذف کاغذ در داخل سازمان می‌باشد. بر این اساس فن‌آوری گردش کار باید به نحو مناسبی با تجارت الکترونیک تلفیق شود تا راه حل جامعی برای ایجاد یک محیط تجاری بدون

[1] Graphical user interface

کاغذ فراهم گردد. تمرکز و تأکید این دو فن‌آوری بر روان ساختن فرایندهای تجاری، یعنی طراحی مجدد آنان از طریق بازسازی روشهای کاری قراردارد. این دو فن‌آوری مکمل یکدیگرند. در حقیقت مطالعات نشان داده است که اجرای سیستمهای گردش کار ممکن است پذیرش سیستمهای تجارت الکترونیک را آسان‌تر کند.

نرم‌افزار گردش کار، قواعد پردازش و مدیریت مسیریابی پیامها و اطلاعات را معین می‌کند و به این ترتیب امکان می‌دهد که نقش شرکت‌کنندگان مشخص شود. ممکن است نقش‌هایی به شرکت‌کنندگان واگذار و قواعد مناسبی برای مسیریابی اطلاعات و پیامها بین افراد و پایگاههای اطلاعاتی تعیین شود. معمولاً یک فرم مجازی به کاربران اجازه می‌دهد که فرمهای سنتی و آشنای مبتنی بر کاغذ را روی صفحه رایانه خود ببینند. کاربران باید این فرمها را در ایستگاههای کاری خود با رابطهای گرافیکی که کاربردشان نیز آسان است پر کنند. این کار به آنان کمک خواهد کرد تا وارد محیط الکترونیکی شوند. نرم‌افزارهای گردش کار، معمولاً همراه با رابط‌های کاربردی، برنامه‌نویسی و ابزار توسعه کاربرد، و زبان نوشتاری عرضه می‌شوند تا نقشها و قواعد مسیریابی مشخص شود. مدیران می‌توانند با استفاده از ویژگیهای ردیابی نرم‌افزار، از وضعیت کار باخبر شوند.

زمینه‌هایی که در آنها سیستمهای گردش کار با سیستم تجارت الکترونیک با موفقیت تلفیق شده‌اند عبارتند از: تدارکات، تهیه صورتحساب، امور پشتیبانی، فروش، سفارش و غیره. انتظار می‌رود روند ادغام سیستمهای داخلی گردش کار با سیستم‌های خارجی تجارت الکترونیک به علت کوچکتر شدن شرکتها و افزایش کارایی آنان جنبه عمومی پیدا کند. در بعضی موارد، طرفهای تجاری، استفاده از مبادله الکترونیکی داده‌ها را به سازمان تحمیل می‌کنند. چنین سازمان‌هایی باید لزوماً فرایندهای داخلی خود را بازسازی کنند و در صورت امکان فن‌آوری گردش کار را با تجارت الکترونیک که در حیطه سازمانی آنها اجرا می‌شود، ادغام کنند. گردش کار را می‌توان بطور کامل با تجارت الکترونیک ادغام کرد، چرا که معامله بازرگانی خود نوع خاصی از گردش کار است.

فن‌آوری دیگری که باید بخشی از سیستم اطلاعاتی یکپارچه سازمان را در چارچوب گردش کار تشکیل دهد، خط نماد است. خط نماد به کنترل کار و جریان اطلاعات در سازمان طرف تجاری نیز کمک می‌کند. مزایای واقعی مبادله الکترونیکی داده‌ها در مدیریت کارآمد زنجیره عرضه، از طریق استفاده از خط نماد در تجارت کالاها تحقق می‌یابد. در زمینه استاندارد، «کمیته کد تجاری یکنواخت» ایالات متحده و «موسسه اروپایی شماره‌گذاری کالا » سیستم‌های خود را هماهنگ می‌کنند تا فن‌آوری خط نماد از سازگاری لازم برخوردار شود.

اینترنت

اینترنت عموماً به مجموعه‌ای از شبکه‌ها گفته می‌شود که اولاً بصورت فیزیکی به هم متصل‌اند. ثانیاً می‌توانند با یکدیگر ارتباط برقرار کنند و منابع اطلاعاتی را با هم به اشتراک بگذارند و ثالثاً در کنار یکدیگر بصورت یک شبکه واحد عمل نمایند.

برای اینکه چنین شبکه‌ای بتواند کار کند، شبکه‌ها و رایانه های موجود در اینترنت باید به یکی از دو طریق زیر عمل کنند:

بکارگیری زبان یکسان برای برقراری ارتباط با یکدیگر

بکارگیری مترجم و مفسر مناسب برای درک زبان یکدیگر

اینترنت برای کاربران خود امکان دسترسی به انواع اطلاعات مورد نیاز بصورت متن، صوت، تصویر، نرم‌افزارها

و... را فراهم می‌کند. کاربران با استفاده از اینترنت می‌توانند با یکدیگر ارتباط برقرار سازند. این تسهیلات با استفاده از مجموعه‌ای از سرویس‌ها و ابزارهای متنوع ارتباطی و مبادله کننده اطلاعات صورت می‌گیرد.
پست الکترونیک، انتقال فایل، پایانه راه دور، تور جهان گستر[1] تنها گوشه‌ای از این سرویس‌ها می‌باشد.

گستره اینترنت

امروزه اینترنت تقریباً تمام کره زمین را پوشش می‌دهد و انواع شبکه‌های کوچک و بزرگ محلی و منطقه‌ای را دربر می‌گیرد. تمام خدمات و سرویس‌های موجود، این شبکه‌ها را بصورت یکپارچه به کاربران خود ارائه می‌کنند.
شکی نیست که گسترش اینترنت و افزایش تعداد کاربران موجب گسترش تجارت الکترونیکی گردیده است، اما این بدان معنی نیست که افزایش تعداد کاربران به همان میزان موجب افزایش تجارت الکترونیکی گردد.
بر اساس مطالعه‌ای که بر روی ۱۲ کشور انجام گرفته است بیش از ۵۰ درصد فعالیتهای اینترنتی در هر کدام از این کشورها در شش ماه گذشته در ارتباط با پست الکترونیکی[2] بوده است.
این فرض درست می‌باشد که در کشورهای در حال توسعه کاربران اینترنتی که در فعالیتهای تجارت الکترونیکی دخالت دارند کمتر از سطح میانگین این شاخص قرار دارند. شاید این امر به دلیل بازدهی کم سرمایه و پایین بودن سطح استفاده از کارتهای اعتباری و فقدان محصولات و خدمات و یا پشتیبانی ضعیف باشد.

امنیت در اینترنت

ارتباطات اینترنتی مبتنی بر TCP/IP به عنوان یک پروتکل زیربنایی است ولی TCP/IP و HTTP با در نظر گرفتن مسائل امنیتی طراحی نشده‌اند و بدون استفاده از نرم‌افزارهای خاص تمام ترافیک اینترنت به صورت قابل رویت منتقل می‌شود و هرکسی که ترافیک را مانیتور کند می‌تواند آن را بخواند. مرتکب شدن چنین حمله‌ای با استفاده از نرم‌افزارهای پی برنده به بسته[3] موجود، نسبتاً ساده است. این بدین علت است که اینترنت رسماً یک شبکه باز است[4]. برای مثال شماره کارتهای اعتباری افراد هنگامی که از آنها برای خرید از طریق اینترنت استفاده شود به سادگی می‌تواند در دسترس دیگران قرار گیرد مگر آنکه تدبیری برای محافظت از آنها اتخاذ شود و اطلاعات آنها به صورت امن منتقل شود. برای یک ارسال امن باید نکات زیر رعایت شود:

- اطلاعات تنها و قابل دسترسی برای فرستنده و گیرنده باشد. (محرمانه بودن[5])
- اطلاعات در طول زمان ارسال تغییر نکرده باشد. (صحت[6])
- گیرنده مطمئن شود که اطلاعات از فرستنده مورد نظر رسیده است. (اصلیت[7])
- فرستنده مطمئن شود که گیرنده حقیقی و موثق است. (غیر ساختگی بودن[8])
- فرستنده نتواند منکر ارسال اطلاعاتی که می‌فرستد بشود. (غیرقابل انکار بودن[1])

[1] Word wide web (www)
[2] E-Mail
[3] packet sniffing
[4] Open network
[5] Privacy
[6] Integrity
[7] Authenticity
[8] Non- fabrication

برای رسیدن به اهداف فوق لازم است از روشهای رمزنگاری، گواهینامه‌های دیجیتال و پروتکلهای امنیتی استفاده کرد. در این مقاله روشهای رمزنگاری پایه و گواهینامه‌های دیجیتال بطور خلاصه توضیح داده می‌شوند سپس پروتکلهای امنیتی جدید که برای انجام معاملات بانکی الکترونیکی امن ایجاد شده‌اند، بررسی می‌شوند.

محافظت از داده‌ها با رمزنگاری

رمزنگاری در ساده‌ترین شکل، بطور سیستماتیک ترتیب عناصر یک پیغام (کلمات، حروف) را تغییر می‌دهد تا برای همه به جز گیرنده مورد نظر غیرقابل درک شود. روشهای رمزنگاری و محصولات گوناگونی که ویژه کاربردهای خاصی مانند پست الکترونیک یا معاملات کارت اعتباری هستند، وجود دارند که در اینجا از بین آنها روشهای DES، RSA و PGP به اختصار توضیح داده می‌شوند.

۱- DES (Data Encryption standard)

DES از یک رشته الفبا عددی[۲] به عنوان کلید استفاده می‌کند تا یک پیغام را رمزنگاری و رمزگشایی کند. این روش در سال ۱۹۷۷ ابداع شد و به عنوان یک استاندارد پذیرفته شد. در یک سیستم تک کلیدی (متقارن) مانند DES، فرستنده و گیرنده هر دو از یک کلید برای رمزگذاری و رمزگشایی استفاده می‌کنند. یکی از مشکلات این روش چگونگی رساندن کلید محرمانه به دست طرف مقابل می‌باشد زیرا ممکن است کلید در طول ارسال بدست دیگران بیفتد. بعلاوه سیستمهای تک کلیدی برای اهداف تصدیق فرستنده و مسئله غیرقابل انکار بودن که قبلاً توضیح داده شد، کمکی نمی‌کند. یعنی با رمزنگاری تک کلیدی به تنهایی راهی برای شناسایی کسی که احتمالاً از کلید برای تغییر پیغام استفاده کرده است وجود ندارد. این کمبودها باعث ابداع یک روش دو کلیدی با نام RSA شد.

۲-RSA و رمزنگاری با دو کلید عمومی و خصوصی

Drs ron rivest , adi shamir, Len adelman یک روش نامتقارن به نام RSA را ابداع کردند که به جای استفاده از یک کلید خصوصی برای رمزنگاری و رمزگشایی پیغامها، از یک کلید خصوصی[۳] و یک کلید عمومی[۴] متناظر آن استفاده می‌کند. هر کدام از این دو کلید برای رمزنگاری و رمزگشایی پیغامها به کار می‌روند.

هر شخصی برای رمزنگاری پیغام از کلید عمومی گیرنده پیغام استفاده می‌کند. این کلید عمومی از طریق پست الکترونیک یا سرور کلیدهای عمومی قابل دسترسی است و چون تنها برای رمزنگاری و نه رمزگشایی پیغامهایی که به گیرنده فوق ارسال می‌شوند، استفاده می‌شود، تبادل آن بدین طریق مانعی ندارد. پیغامی که با کلید عمومی گیرنده رمزنگاری شود با کلید خصوصی وی که تنها در دست خود اوست قابل رمزگشایی است. بنابراین از مجموعه این کلیدها می‌توان استفاده کرد تا پیغامهای امن را با هر کسی و بدون مشکل تبادل این کلید رد و بدل کرد. این روش حفاظت از داده‌ها را به خوبی انجام می‌دهد ولی هنوز کاری برای تصدیق هویت انجام نمی‌دهد. برای اطمینان از ارسال درست کلیدهای عمومی می‌توان از گواهینامه‌های

[۱] Non- reputation

[۲] Alpha numeric

[۳] private key

[۴] public key

دیجیتال استفاده کرد که در بخش گواهینامه های دیجیتال توضیح داده می‌شوند. روش رمزنگاری جدیدتری به نام PGP برای رسیدن به هدف صحت اطلاعات از امضاهای دیجیتال نیز استفاده می‌کند.

۳-PGP (Pritty Good Privacy)

این روش توسط Phil Zimmerman ابداع شد و ترکیبی از روشهای IDE, RSA[۱] می‌باشد. PGP همچنین می‌تواند برای ایجاد امضاهای دیجیتال از طریق رمزنگاری کاراکترهایی که در انتهای پیغام اضافه می‌شوند، استفاده کند. این کار اجازه می‌دهد گیرنده پیغام را با امضای آن مطابقت دهد و در صورتیکه حتی یک کاراکتر از پیغام عوض شده باشد این مطابقت وجود نخواهد داشت و مشخص می‌شود که پیغام در مسیر دستکاری شده است.

در حال حاضر PGP هم نام یک استاندارد رمزنگاری و رمزگشایی می‌باشد و هم نام یک محصول نرم‌افزاری خاص برای پست الکترونیکی می‌باشد[۲]. این نرم‌افزار برای سیستم عاملهای متداول تهیه شده است و پس از نصب plugin آن برنامه پست الکترونیکی موجود روی رایانه اضافه می‌شوند. سپس می‌توان بعد از یک بار تولید کدهای عمومی و خصوصی، ارسال ایمن پیغامها را به راحتی آغاز کرد.

آنچه که PGP را منحصر به فرد می‌کند این است که یک پیام می‌تواند دارای چندین امضای دیجیتال باشد یعنی یک نامه می‌تواند توسط بیش از یک شخص امضا شود و هر شخص میزان اطمینان خود را بیان کند.

گواهینامه‌های دیجیتال[۳]

گواهینامه دیجیتال، ضمیمه‌ای است که به یک پیغام الکترونیکی اضافه می‌شود و برای مسائل امنیتی استفاده می‌گردد. برای مثال گواهینامه دیجیتال می‌تواند تصدیق کند که فرستنده پیام همان کسی است که ادعایش را می‌کند یا می‌تواند برای تأمین وسیله‌ای که گیرنده بتواند با آن پاسخش را رمزگذاری[۴]کند، به کار رود. روش کار گواهینامه دیجیتال بدین صورت است که فردی که می‌خواهد یک پیام رمز شده ارسال کند، از یک مرجع گواهینامه[۵](CA) تقاضای یک گواهینامه دیجیتال می‌کند. سپس CA یک گواهینامه دیجیتال رمز شده صادر می‌کند که شامل کلید عمومی متقاضی و برخی اطلاعات شناسایی دیگر است. CA کلید عمومی خودش را از طریق انتشارات کاغذی یا اینترنت در اختیار همگان قرار می‌دهد.

گیرنده پیغام رمز شده از کلید عمومی استفاده می‌کند تا گواهینامه دیجیتالی چسبیده شده به پیغام را رمزگشایی کند و تعیین کند که توسط CA صادر شده است و سپس کلید عمومی فرستنده و اطلاعات شناسایی نگهداری شده در گواهینامه را بدست می‌آورد. با این اطلاعات گیرنده می‌تواند یک پاسخ رمز شده بفرستد.

مسلماً نقش CA در این فرایند اساسی است زیرا به عنوان واسطه‌ای در ارتباطات دو گروه عمل می‌کند. در شبکه بزرگ و پیچیده‌ای مانند اینترنت، این مدل سه گروهه لازم است زیرا دو گروه خاص ممکن

---

[۲] International Data Encryption

[۴] این نرم‌افزار برای استفاده‌های غیر تجاری بطور رایگان در دسترس همگان قرار دارد و می‌توان آخرین نسخه آن را از آدرس http:\\www.pgpi.org\ تهیه کرد.

[۳] digital certificates

[۴] encode

[۵] certificate Authority

است نتوانند به تنهایی در مورد یک روش مورد اعتماد به توافق برسند ولی با این وجود بخواهند یک ارتباط مطمئن داشته باشند. بنابراین هر دو گروه به CA اعتماد می‌کنند و CA هویت و صداقت هر دو گروه را با امضا کردن گواهینامه‌های آنها تصدیق می‌کند و هر گروه بطور ضمنی به گروه دیگر اعتماد می‌کند.

لایه سوکتهای امن (SSL) و HTTP امن (S-HTTP)

بسیاری از تولیدکنندگان بزرگ محصولات اینترنت، توافق کرده‌اند که از یک پروتکل رمزنگاری به نام پروتکل لایه سوکتهای امن[1] (SSL) که توسط Netsacpe برای ارسال اسناد محرمانه از طریق اینترنت ایجاد شده بود، استفاده کنند. SSL از یک کلید خصوصی برای رمزنگاری داده‌هایی که از طریق اتصال SSL ارسال می‌شوند، استفاده می‌کند.

Internet explorer , Netscape Navigator هر دو از SSL پشتیبانی می‌کنند و بسیاری از وب سایتها از این پروتکل برای گرفتن اطلاعات محرمانه از کاربر مانند شماره کارتهای اعتباری استفاده نمایند.

این پروتکل که بین لایه‌های پروتکل سطح Application مانند http و پروتکل لایه Transport یعنی TCP/IP قرار می‌گیرد، برای جلوگیری از استراق سمع، تحریف کردن و جعل پیغام طراحی شده است. چون SSL در زیر پروتکل لایه Application قرار می‌گیرد، می‌تواند برای سایر پروتکلهای لایه Application مانند FTP نیز به کار رود.

پروتکل دیگری برای ارسال ایمن داده‌ها روی وب، HTTP امن[2](S-HTTP) می‌باشد که نسخه تغییر یافته‌ای از پروتکل HTTP استاندارد می‌باشد. S-HTTP توسط شرکت Enterprise integration technologies طراحی شد که در سال ۱۹۹۵ شرکت Verifone آن را خریداری کرد. در حالیکه SSL یک اتصال مطمئن بین یک مشتری (Client) و یک سرور ایجاد می‌کند که در طول آن هر مقدار داده می‌تواند بطور امن منتقل شود، S-HTTP طوری طراحی شده است که پیغامهای جداگانه را بصورت ایمنی ارسال می‌کند. بنابراین SSL و S-HTTP را می‌توان به دید تکنولوژیهای مکمل و نه رقیب یکدیگر نگاه کرد.

این پروتکلها به مشتری و سرور اجازه می‌دهند یکدیگر و اطلاعات امنی را که بطور پیاپی بین آنها جریان دارد، تصدیق کنند. با استفاده از روشهای رمزنگاری و امضاهای دیجیتال این پروتکلها:

- به مشتری و سرور اجازه می‌دهند یکدیگر را تصدیق کنند.
- به دارندگان سایتهای وب اجازه می‌دهد دسترسی به سرورها، دایرکتوریها، فایلها یا سرویسهای خاصی را محدود سازند.
- اجازه می‌دهند اطلاعات حساس (برای مثال شماره کارتهای اعتباری) بین مشتری و سرور مبادله شوند در حالیکه برای افراد دیگر غیرقابل دسترسی میباشند.
- تضمین می‌کنند که داده‌های تبادل شده بین مشتری و سرور قابل اعتماد هستند (یعنی نمی‌توانند بدون اینکه معلوم شود، بطور عمدی یا غیرعمدی تغییر کنند یا خراب شوند)

یک عنصر کلیدی در برقراری ارتباطات امن در اینترنت از طریق پروتکلهای SSL یا S-HTTP، گواهینامه‌های دیجیتال می‌باشد که در واقع بدون گواهینامه‌های دیجیتال پروتکلهایی مانند SSL و S-HTTP نمی‌توانند هیچ امنیتی را تضمین کنند.

پروتکلهای SSL و S-HTTP به منظور تبادل ایمن اطلاعات بین یک مشتری و یک سرور طراحی

---

[1] Secure socket layer

[2] Secure-http

شده‌اند. مثلاً هنگامیکه یک مشتری می‌خواهد از طریق اینترنت یک حساب بانکی جدید نزدبانک افتتاح کند، اطلاعاتی در مورد خود مانند نام، نام خانوادگی، آدرس، تلفن و غیره را به فرم الکترونیکی که سرور بانک در اختیار وی قرار می‌دهد، به بانک ارسال می‌کند. واضح است که این اطلاعات باید محرمانه باقی بمانند و برای این کار از پروتکلهای بالا استفاده می‌شود.

در حالیکه پروتکلهای SSL و S-HTTP به منظور تبادل ایمن اطلاعات از هر نوعی بین یک مشتری و یک سرور طراحی شده‌اند پروتکلهای STT و SET ویژه انجام عملیات بانکی و معاملات با کارت اعتباری طراحی شده‌اند.

مبادلات الکترونیکی امن (SET) و تکنولوژی مبادلات امن (STT):

پروتکل مبادلات الکترونیکی امن[1] (SET) یک استاندارد باز برای پردازش معاملات کارتهای اعتباری روی اینترنت می‌باشد که با همکاری Netscape، Microsoft، Visa، Mastercard، GTE، SAIC،System Tersia و Version ایجاد شده است. هدف SET این است که معاملات با کارت اعتباری روی اینترنت با همان سادگی و ایمنی که در فروشگاهها انجام می‌گیرند، باشد. برای حفظ محرمانه بودن معاملات طوری تقسیم می‌شود که فروشنده به اطلاعات کالای مورد تقاضا، قیمت آن و اینکه آیا پرداخت آن تایید می‌شود، دسترسی دارد، ولی دسترسی به اطلاعات نحوه پرداخت مشتری راندارد، بطورمشابه صادرکننده کارت اعتباری دسترسی به قیمت کالا را دارد ولی دسترسی به اطلاعاتی درباره نوع کالا را ندارد. SET از گواهینامه‌های دیجیتال برای تصدیق کردن صاحب کارت، تصدیق اینکه فروشنده با موسسه اعتباری ارتباط دارد و غیره استفاده می‌کند.

نرم افزارهای مورد نیاز درتجارت و بانکداری الکترونیک

یکی از زیرساختهای مهم و اساسی برای بانکداری الکترونیک ایجاد برنامه‌ای کاربردی است. توانمندی و قابلیتهای برنامه‌های کاربردی مستلزم تجزیه و تحلیل درست نیازها و شناخت وضع موجود در فرآیند عملیاتی و محدودیتها و بهبود روشها می‌باشد. هرچند در طراحی موفق یک برنامه کاربردی، تجزیه و تحلیل درست فرآیند عملیاتی و بهبود روشها لازم می‌باشد، اما موفقیت یک برنامه کاربردی مستلزم قابلیت و توانایی بالای نرم‌افزار در تولید برنامه کاربردی مورد استفاده قرار می‌گیرد، می‌باشد. تواناییها و قابلیتهای نوع سیستم عامل[2] و بانک اطلاعاتی[3] نیز بعنوان ارکان اصلی در تشکیل برنامه‌های کاربردی محسوب می‌شوند. در ارتباط با نرم‌افزارهای مورد نیاز بانکداری الکترونیک نیز می‌توان به نرم‌افزارهای بخش داخلی و بخش خارجی بانک نیز اشاره نمود. نرم‌افزارهای بخش داخلی بانک به در سه گروه زبانهای برنامه نویسی در ایجاد برنامه‌های کاربردی و نمونه‌هایئ از برنامه‌های کاربردی، بانکهای اطلاعاتی و سیستم‌های عامل طبقه‌بندی می‌شوند. نرم‌افزارهای مورد نیاز بخش خارجی بانک (مشتریان) بطور مختصر در این قسمت اشاره خواهیم نمود.

نرم‌افزارهای مورد نیاز بخش خارجی بانک: مشتریان می‌توانند از طریق ایجاد ارنباط با Website بانک به تمامی بخشهای مورد نیاز دسترسی داشته باشند. تنها نرم‌افزار مورد نیاز مشتریان، یک نرم‌افزار مرورگر وب[4] مانند Internet Explorer (محصول شرکت میکروسافت که همرا سیستم عامل Windows ارائه می‌شود)یا Netscape (محصول شرکت میکروسان) است که میبایست از رمزنگاری ۱۲۸بیتی پشتیبانی کند.

---

[1] Secure Electronic Transactions

[2] Operating system

[3] Database

[3] Web browser

زبانهای برنامه‌نویسی مورد استفاده در تولید برنامه‌های کاربردی

بیشتر زبانهای برنامه‌نویسی که اخیراً مورد توجه قرار گرفته‌اند از نوع شی‌گرا[۱] می‌باشند. هر شی دارای ماهیتی است و رفتار هر شی بوسیله عملیاتی که بر روی آن انجام می‌شود تعریف شده و بالعکس. هر شی در واقع نمونه‌ای از کلاس معینی از شی‌ها است. زبان های برنامه‌نویسی که شی‌گرا هستند عبارتند از: delphi, visual c, visual baseic, c^{++}, java و اخیراً $C^{\neq}$[۲], NET.

در طراحی برنامه‌های کاربردی بوسیله زبانهای برنامه‌نویسی شی‌گرا می‌توان قطعات مختلف که تحت عنوان Activex است در کنار یکدیگر قرار داد و برنامه کاربردی را ایجاد نمود. برنامه‌های کاربردی بانکداری الکترونیک با توجه به اینکه باید در سطح اینترنت و یا اینترانت قابل اجرا باشند، می‌بایست به زبانهای HTML[۳] و یا DHTML[۴] و یا ASP[۵] باشند. عدم وابستگی برنامه‌های کاربردی به سخت‌افزار و نوع سیستم عامل (plateform) یکی از خصوصیات برنامه‌های تحت اینترنت و اینترانت محسوب می‌شود.

در طراحی صفحات web بصورت پویا از زبانهای اسکریپت[۶] مانند javascript و یا vbscript استفاده می‌شود. اخیراً زبان برنامه‌نویسی جدیدی تحت عنوان Visual.net توسط شرکت مایکروسافت تولید شده است که امکان طراحی تمامی برنامه‌های کاربردی تحت web با قابلیتهای فراوان از جمله طراحی برنامه‌های کاربردی جهت ردیابی و امکان وصل شدن تلفن‌های همراه به اینترنت از این طریق فراهم شده است. در طراحی برنامه‌های کاربردی بانکداری الکترونیک سعی شده است که از این زبانهای برنامه‌نویسی استفاده شود. در این قسمت نیز به نمونه‌هائی از برنامه‌های کاربردی مورد استفاده در بانکداری الکترونیک اشاره خواهد شد:

- ASP.NET: مایکروسافت با ارائه ASP و زبانهای قدیمی‌تر خود بصورت NET. در قرن بیست و یکم قدم مهمی به سوی برنامه نویسی کاملا حرفه‌ای Online برداشته است. ASP.NET که از VB.NET بهره میبرد، اکنون به برنامه ای کاملا کارآزموده و شی گرا برای تولید نرم افزارهای وب تبدیل شده و بهبودهای زیادی را موجب گردیده است. زبانهائی که از گذشته به ارث رسیده اند، نمی توانند به اندازه NET. ابتکار عملی داشته باشند ، به همین علت مایکروسافت زبان جدیدی تحت عنوان C# برای جارجوب NET. تهیه نمود.(ASP.NET Web Developer's Guide,2002)
- Macromedia Cold Fusion Server: این نرم‌افزار جهت انجام عملیات گزارش‌گیری، محاسبات و دیگر عملیات محاسباتی توسط Cold Fusion Script است. این نرم‌افزار براساس کلید ویژه عملیاتی مورد نیاز در تجارت الکترونیک و برنامه‌های کاربردی تحت Webرا می‌تواند در اختیار قرار دهد و آنگاه با امنیت و سرعت بالا می‌تواند عمل نماید.
- **درایورODBC برای IBM DB2:** این نرم‌افزار بر روی Web Server نصب می‌شود تا ارتباط بین Cold Fusionرا با بانک اطلاعاتی رایانه های بزرگ را فراهم نماید. رایانه های شخصی مشتریان نیز می بایست به نرم‌افزار LivePerson.Com نیز مجهز باشد.

---

[۱] Object oriented programming

[۲] مایکروسافت با ارائه چارچوب کاری NET. زبان جدیدی را نیز برای قرن بیست و یکم تحت عنوان $C^{\neq}$ و NET. عرضه کرد و بر تمامی انتقادهای وارد شده غلبه کرد و روشی کاملا جدید برای بررسی نرم‌افزارها و وب فراهم ساخته است. شاید بتوان گفت که میکروسافت با ایجاد این زبان در مقابل زبان JAVA محصول میکرو سان سیستم اعلان جنگ نمود.

[۳] Hyper text markup language

[۴] Dynamic hypertext markup language

[۵] Active server page

[۶] script

بانکهای اطلاعاتی

یکی از ارکان مهم در تولید موفق برنامه‌های کاربردی بانکداری الکترونیک قابلیتهای بانک اطلاعاتی می‌باشد. نوع بانک اطلاعاتی مورد استفاده در برنامه‌های کاربردی در سطح اینترنت و یا اینترانت بصورت بانک اطلاعاتی مبتنی بر «سرویس دهنده»[۱]می‌باشد، بطوریکه بانک اطلاعاتی در یک «سرویس دهنده» قرار می‌گیرد و تمامی پرس و جوها[۲] از سوی «سرویس گیرنده‌ها» به سمت «سرویس دهنده» هدایت می‌شود. و از طریق مدیریت بانک اطلاعاتی عملیات پردازش شده و آخرین اطلاعات به بانک اطلاعاتی افزوده می‌شود. این نوع از بانکهای اطلاعاتی از نوع رابطه‌ای (RDBMS)[۳]می‌باشند. یکی دیگر از ویژگیهای این نوع از بانکهای اطلاعاتی مربوط است به یکپارچگی داده‌ها[۴]به نحویکه مانع از ذخیره سازی داده‌های تعریف نشده[۵] در آن می‌شود. انواع بانکهای اطلاعاتی مورد استفاده در طراحی سیستمهای سرویس دهنده و سرویس گیرنده[۶]عبارتند از: informix, Db2, Oracle, SQL server

بانک اطلاعاتی *SQL SERVER*:

شیوه کاربرد عملی SQL بانک اطلاعاتی SQL SERVER یکی از قدیمی‌ترین بانکهای اطلاعاتی می‌باشد که امروزه در سطح دنیا بکار می‌رود. این بانک محصول شرکت میکروسافت می‌باشد. بسیاری از پروژه‌هایی که در محیط ویندوز با استفاده از نرم‌افزارهای میکروسافت پیاده سازی می‌شوند و اطلاعات زیادی باید نگهداری و بازیابی شوند معمولاً از این بانک بعنوان محیطی امن و مناسب استفاده می‌کنند. این بانک برای کار در شبکه‌ها طراحی شده است بطوری که برای هر بانک اطلاعاتی موجود در آن و یا هر جدول، view و... موجود در آن بانک و یا هر فیلد و رکورد خاص در جداول آن کاربرد خاصی تعریف و یا به کاربرهای موجود اجازه‌هایی خاصی برای اعمال تغییرات از جمله اضافه، تغییر، حذف می‌دهد. برای این منظور می‌توان هم از کاربرهای تعریف شده در سطح سیستمهای عامل NT و یا ویندوز ۲۰۰۰ استفاده کرد و یا از کاربرهایی که درون خود محیط SQL SERVER ایجاد می‌گردند استفاده کرد.

آخرین نسخه SQL SERVER نسخه ۲۰۰۰ می‌باشد که نسبت به نسخه قبلی آن یعنی SQL SERVER بهینه شده است. نسخه ۶ و ۵ تنها بر روی سیستمهای عامل NT برنامه سرویس دهنده آن قابل نصب بود بطوریکه نسخه ۷ آن بر روی سیستم عاملهای ویندوز ۹۸ به بعد و Windows 2000 قابل نصب و اجرا می‌باشد.

بانک اطلاعاتی SQL SERVER صرفاً یک محیط برای طراحی اجزای مختلف بانک اطلاعاتی و مدیریت آن می‌باشد و برای ایجاد یک برنامه کاربردی با آن باید رابط کاربر را با یک زبان برنامه‌سازی تحت ویندوز مانند ویژوال بیسیک، ویژوال C^{++}، ویژوال J^{++}، Visual interdev، دلفی، NET. و... ایجاد کرد و برای ارتباط با بانک اطلاعاتی از طریق این زبانها از امکاناتی مانند ODBC و ADO استفاده کرد که در ادامه اصطلاحات مورد نیاز شرح داده خواهند شد و سپس اجزای یک بانک اطلاعاتی در SQL SERVER بیان می‌شوند.

---

[۱] data base server

[۲] query

[۳] Relational database management system

[۴] data integrity

[۵] invalid data

[۶] client integrity

نوع ارتباط بین رابط گرافیکی (GUI) و بانک اطلاعاتی به دو صورت امکان پذیر می‌باشند که عبارتند از: رابط ODBC و رابط ADO .

رابط ODBC[1] برقراری ارتباط بانکهای اطلاعاتی راه دور (Back- end) را از طریق یک نرم‌افزار (*front-end*) فراهم می‌کند. یک برنامه کاربردی توابع ODBC را فرا می‌خواند و یک مدیر نیز نرم‌افزار راه‌اندازی ODBC را بارگذاری می‌کند. راه اندازی ODBC پردازش فراخوانی را بر عهده می‌گیرد و درخواست SQL را ارائه می‌دهد و نتایج را از بانک اطلاعاتی برمی‌گرداند.

ODBC توسط محصولاتی چون power builder، فاکس پرو، ویژوال C^{++}، ویژوال بیسیک، دلفی بورلند، Microsoft Access و محصولات دیگر مورد استفاده قرار می‌گیرد.[2]

رابط ADO [3]

روش ADO برای ارتباط با انواع بانکهای اطلاعاتی اعم از بانکهای رابطه‌ای، شبکه‌ای، شی گرا و... بکار می‌رود و نسبت به ODBC سریعتر و بهینه‌تر می‌باشد و یادگیری آن آسانتر است و محدودیت ODBC را که تنها می‌توانست با بانکهای رابطه‌ای ارتباط داشته باشد ندارد. ADO بعنوان استانداردی برای ارتباط با بانکهای اطلاعاتی از طریق web و اینترنت نیز پذیرفته شده است.

سیستمهای عامل [4] (OS)

سیستم عامل (OS) بعنوان رابط بین برنامه‌های کاربردی و سخت‌افزار می‌باشد و بعنوان اساسی‌ترین بخش در اجرای عملیات پردازش اطلاعات در رایانه محسوب می‌شود. انتخاب نوع سیستم عامل (OS) و بررسی امنیت آن جهت اجرای بانکداری الکترونیک بسیار ضروری است. زیرا هسته مرکزی در طراحی یک شبکه «سرویس دهنده» و «سرویس گیرنده» و همچنین نحوه تخصیص و مدیریت منابع در اختیار سیستم عامل (OS) می‌باشد. از مهمترین سیستمهای عامل که می‌توانند در محیط شبکه‌های اینترنت و اینترانت مورد استفاده قرار گیرند عبارتند از:

الف) سیستمهای عامل Windows 2000 family

ب) سیستم عامل Linux

الف- سیستم عامل Windows 2000 family

انواع سیستمهای عامل windows 2000 family که محصول شرکت میکروسافت می‌باشند عبارتند از:

1-windows 2000 professional
2-windows 2000 server
3-windows 2000 advanced server
4-windows 2000 datacenter server

---

[1] Open data base connectivity

[2] بانک اطلاعاتی راه دور بانک اطلاعاتی است که بر روی سرویس دهنده‌ای بغیر از سرویس دهنده‌هایی که به آن متصل هستند قرار گرفته است.

[3] Activex data object

[4] operating system

به استثنای windows 2000 professional که در رایانه‌های «سرویس گیرنده»مـورد اسـتفاده قـرار می‌گیرد سایر محصولات فوق بعنوان سیستمهای عاملی هستند که در «سرویس دهنده» نصب می‌شوند.

تفاوت هرکدام از این سیستمهای عامل در قابلیتها و تواناییهای آنها از نظر تعـداد رایانـه‌هـای تحـت پوشش در شبکه و میزان آدرس دهی فضای دیسـک سـخت و همچنـین تعـداد پردازشـگرهای مرکـزی کـه می‌تواند بطور همزمان عملیات پردازش را انجام دهند، می‌باشند. کـه مـی‌تـوان بـر اسـاس اولویـت در میـزان تواناییهای آن به ترتیب advance server, datacenter server و server یاد کرد.

هر چند که نحوه کار کردن با این سیسـتمهای عامـل بـه دلیـل اسـتفاده کـردن از رابـط گرافیکـی (GUI)[1] برای کاربران راحت (user friendly) ولیکن از نظر امنیت و نفوذ پذیری این نوع از سیستمهای عامل با تردید و شک مورد استفاده قرار می‌گیرند.

ب- سیستم عامل *Linux*

این سیستم عامل نگارش جدید سیستم عامل unix می‌باشد. بدلیل اینکه این سیستم عامـل مبتنـی بر دستورات[2] می‌باشد و هیچگونه رابط گرافیکی (GUI) در آن در نظر گرفته نشده است، لـذا کـاربران رغبـت لازم برای کارکردن با این سیستم عامل را ندارند و از سویی دیگر بدلیل امنیت بالایی که ایـن سیسـتم عامـل داراست از اینرو در اکثر شبکه‌های اینترنت و اینترانت بخصوص زمانیکه امنیت اطلاعات برای صاحبان سازمان مهم می‌باشد از این نوع سیستم عامل استفاده می‌شود. مزیت این نـوع سیسـتم عامـل در ایـن اسـت کـه در انحصار هیچ شرکتی نبوده و بعبارت دیگر تولید کننـده خاصـی نداشـته و ایـن سیسـتم عامـل تکامـل یافتـه متخصصان مختلف می‌باشد و بدلیل دسترسی به source، برنامه قابل تغییر می‌باشد.

بسترهای حقوقی

برقراری یک روش تجارت الکترونیکی کارآمد، مستلزم وجود قوانین متعدد حقوقی (وجزائـی) اسـت. مسائل حقوقی ناشی از رابطه تجاری بوسیله EDI با قراردادهای قبلی تنظـیم مـی‌شـود، یعنـی طرفهـائی کـه مایلند مبادلات اطلاعات تجاری را الکترونیکی کنند طی قراردادی حقوق و تکالیف خـود را معـین مـی‌کننـد بعبارت دیگر موافقت‌نامه تبادل اطلاعات بطور معمول مواردی چـون موضـوع و هـدف قـرارداد، تعـاریف،حوزه فعالیت، استانداردهای تبادل، ایمنی، گواهیها وگواهینامه ها، نحوه دریافت و ارسال پیامها، ذخیره سازی، انجام حسابرسی، تعهدات، بیمه‌نامه‌ها، تبادلات بین بانکی، تبادلات در سطح بانکـداری خـرد، قـوانین حـل اخـتلاف و..... در بر می‌گیرد.

در طی سالهای اخیر سازمانهای متعدد بین‌المللی و محلی سـعی درتعریف،ایجـاد و تبیـین قـوانین و قراردادهای تجارت الکترونیکی نموده‌اند. در همین راستا درسـال ۱۹۸۸ اطـاق بازرگـانی بـین‌المللـی (ICC)[3] قواعد همسان برای تبادل داده‌های الکترونیکی از راه دور را انتشار داد. یک نمونه قرارداد از جمله این موارد را شامل می‌شد:

مراقبت لازم برای ارسال و دریافت پیامها با تشخیص هویت طرفهـای تجـاری،گواهی دریافـت پیـام، بررسی صحت پیام دریافت شده، حمایت از پیامهای مبادله شده، نگهداری رکوردها و سوابق و ذخیـره سـازی

[1] Graphical user interface

[2] command base

[3] International Chamber of Commerce

داده‌ها. ازجمله مسائل حقوقی که در تجارت الکترونیکی برای طرفین تجاری حائز اهمیت است عبارتند از:تعیین رابطه حقوقی و قراردادها، حقوق بین‌المللی در موارد اختلاف بین‌المللی، حریم خصوصی و حمایت از داده‌ها، حمایت از مصرف‌کننده، مسئولیت مدنی و قراردادی، نقش مراجع گواهی الکترونیکی در ابعاد ملی و فراملی، مسائل مربوط به آیین دادرسی مدنی و تجاری و ادله اثبات، پرداختهای الکترونیک شامل پول الکترونیکی و کارتهای اعتباری، سوءاستفاده از کارتهای بانکی، نفوذ بر حسابهای بانکی دیگران، تخریب اطلاعات، بازاریابی و تبلیغات و رقابت مشروع شرکتها، ارتکاب تخلفات عمدی ازجمله جعل و سرقت داده‌ها، مسائل مرتبط با مالیات، گمرکات، حمل و نقل بیمه و.....

در هر معامله(عمل تجاری)چند عنصر ضروری وجود دارد، نخست قصد طرفین از معامله شامل تعهدات و منافعی که هریک در مقابل دیگری دارد که معمولا در تبادل اسناد و اطلاعات دو جانبه مواردی ازجمله موضوع، تعداد، زمان، قیمت و سایر اطلاعات مربوطه مشخص شده است. عنصر دوم، پذیرش و تصدیق طرفین نسبت به محتوا و مندرجات سند است که با امضا (مهر) خود در مراحل مختلف تایید کرده‌اند. و به این طریق مسئولیت تعهدات خود را پذیرفته‌اند. البته صرف وجود این دو عامل برای اثبات انجام معامله کافی نیست زیرا هریک از طرفین می‌توانند در اصالت اسناد تردید کنند. مراجع ثبت اسناد رسمی برای تایید مندرجات اسناد پدید آمده‌اند تا موجب استحکام مبادلات گردند.

مفهومی که از امنیت تبادل داده‌های الکترونیکی و تجارت متبادر در ذهن تداعی می‌شود باید شامل فرآیندی شود که همه عناصر اصلی تشکیل دهنده یک مبادله تجاری را بطور کامل و مطمئن محافظت کند. یعنی دریافت کننده مطمئن باشد که اطلاعات ارسالی توسط فرد مورد نظر ارسال شده است و پس از ارسال از طریق دسترسیهای غیرمجاز دچار تغییر نشده باشد، و ارسال‌کننده نیز از صحت پیام ارسالی مطمئن باشد، در ضمن بتوان اطلاعات را بدون هیچ تغییری نگهداری کرد تا در هر زمان که لازم باشد بتوان اصل آن را به مراجع رسیدگی کننده تحویل نمود. بدیهی است توسعه بانکداری الکترونیک و تجارت الکترونیک منوط به اعتماد و اطمینان مشتریان از عملکرد و قابلیتهای آن است، بطوریکه در صورت برقراری قوانین و حقوق مبتنی بر فعالیتهای الکترونیک لازم‌الاجرا بوده و متخلف از آن، موجب پیگرد قانونی قرارگیرد.

امضای دیجیتال:

امضای دیجیتال به این صورت تعریف شده است. "داده ای که به یک پیام پیوست شده است به نحوی که گیرنده بتواند هویت منبع و صحت و جامعیت پیام را احرازکند". کمیسیون EU در پیشنهادهایی که در مورد امضای دیجیتال داده است، آن را اینگونه تعریف میکند. "یک امضا در شکل دیجیتال یا شکل الصاقی یا منطقی که با داده‌ای ترکیب، متصل یا داخل شده باشد به نحوی که آن داده توسط صاحب امضا برای موافقت با محتویات آن داده‌ها ارائه شده باشد و خواسته های زیر را در برگیرد:

الف) یکتا و منحصر به صاحب امضاء باشد

ب) توانایی تایید هویت صاحب امضا را داشته باشد

ج) ازاطلاعاتی ساخته شده باشد که صاحب امضاء بتواند روی منحصر به فرد بودن آن کنترل داشته باشد.

د)با داده‌هایی پیوند خورده باشد که بتوان با آنها و از طریق یک روش مشخص، هرگونه تغییر در داده‌ها را کشف کرد.

برای اطمینان بیشتر، یک امضای دیجیتال نه تنها باید نشان دهنده فرستنده منحصر به فرد آن

باشد، بلکه باید بتواند نشان دهد پیام مورد دستکاری قرارگرفته است یا خیر. برای اینکه تمامی شرایط امضای دیجیتال محقق شود، لازم است افراد مشخص کنند الزامات قانونی نوشتن یک امضاء چیست و چگونه قانونی می‌شود. امضای الکترونیک باید بر مبنای یک گواهینامه رسمی کنترل شده باشد. یعنی گواهی باید توسط یک مرجع تاییدکننده تهیه شده و به ضمیمه امضاء باشد، تا بتوان هویت شخص را تایید کند، مشخص کند که این گواهی برای چه دوره زمانی معتبر است، منحصر به فرد باشد و محدودیتهای استفاده از گواهی و مسئولیت مراجع تایید کننده را بیان کند. این موضوع امکان اعتماد هر کس را به گواهی تعیین هویت تماس گیرنده فراهم می کند. و در نهایت مشخص می‌شود که فردی که در حال استفاده از اسم مستعار تایید شده‌ای است، قابل شناسایی می‌باشد. این گواهی ممکن است اطلاعاتی را نیز ارائه کند. بعنوان مثال اجازه دیدن تعهدات مالی را بدهد و یا از طرف کارفرما اجازه شرکت در قرارداد را داشته باشد.

در مجموع برای آنکه یک امضای دیجیتال برسمیت شناخته شود لازمست توسط یک مرجع تاییدکننده با مشخصات زیر مورد گواهی قرارگیرد:

الف) قابلیت اطمینان آن اثبات شود

ب) سریع فعالیت کند و امکان لغو آن محفوظ باشد

ج) هویت را گواهی کند و تعداد اشخاص مورد تائید مشخص باشد

د)کارمندان صاحب صلاحیت، کارآزموده و منظم داشته باشد

ه) از سیستمهای امنیت و ضد تقلب و جعل استفاده کند

و) صاحب اعتبار باشد

ز)سوابق تمامی تایید صلاحیت شدگان را برای دوره های زمانی مشخص نگهداری کند

ردیابی الکترونیکی افراد:

ردیابی تروریسم و تبهکاری و کشف آنها قبل از وقوع جرم یکی از اقدامات مهم جهت اطمینان دادن به مشتریان در تبادلات الکترونیکی بخصوص در بانکداری الکترونیک محسوب می‌شود. به گزارش سی. ان. ان "دانشمندان سرگرم دستگاههای الکترونیکی برای ردیابی انسانهای جنایتکارهستند این دستگاه‌ها قادر خواهند بود از طریق پایگاه اطلاعاتی و تکنولوژی ارتباطات جدید که بی نظیر است اعمال افراد را در سراسر جهان نظارت کنند و به مسئولان ذیربط گزارش لازم را ارسال نمایند این دستگاه‌ها قادرند به ارتباطات مخابراتی و الکترونیکی نفوذ و از آنها اطلاع پیدا کنند.

کنوانسیون بین‌المللی مبارزه با جرائم رایانه‌ای و اینترنتی که در اواخرسال ۲۰۰۱ میلادی در شهر بوداپست به امضای اعضای اتحادیه اروپا و چهار کشور صنعتی دیگر جهان رسید شامل اهداف زیر می‌باشد:

۱) هماهنگ کردن ارکان تشکیل دهنده جرم درحقوق جزایی ماهوی داخلی کشورها و وسایل مربوطه در بخش جرایم سایبر اسپیس[۱]

۲) فراهم آوردن اختیارات لازم در آیین دادرسی کیفری داخلی برای جرایمی که با استفاده از سیستم‌های رایانه‌ای ارتکاب می یابند یا مدرک مرتبط با جرم به شکل الکترونیکی است.

۳) تدوین سیستم سریع و موثر همکاری بین‌المللی.

این کنوانسیون شامل چهار فصل می‌باشد:

۱) استفاده از اصلاحات

[۱] منظور از بخش جرایم Cyber space جرایم در بخش رایانه‌ای و اینترنتی است و تمامی جرائم دیجیتالی را شامل می شود.

۲) اقدامات داخلی کشورهای عضو که در این فصل مسائل و موضوعات قانون ماهوی، هم جرم انگاری و هم سایر مسائل مربوطه درحوزه جرائم رایانه‌ای یا مربوط به رایانه را شامل می‌شود. این جرائم شامل دسترسی غیر قانونی، اختلال در داده‌ها، جعل مرتبط با رایانه، جرائم مربوط به حقوق پدیدآورندگان، جرائم ارتکاب یافته با سیستم رایانه‌ای یا ادله رایانه‌ای که به شکل الکترونیک است و.... می‌باشد.

۳) همکاری متقابل بین‌المللی در خصوص جرائم سنتی و رایانه‌ای علاوه بر مقررات مربوط به استرداد می‌باشد. فصل سوم حاوی مبحثی پیرامون نوع خاصی از دستیابی فرامرزی به داده‌های رایانه‌ای ذخیره شده است که نیاز به همکاری متقابل ندارد و راه‌اندازی یک شبکه جهت اطمینان از همکاری فوری مابین کشورهای عضو را فراهم می‌آورد.

۴) موضوعات پایانی که با یک سری استثنائات خاص، موضوعات استاندارد در معاهدات شورای اروپا را تکرار می‌کند.

در بخشی از این مواد آمده است"موارد پی‌جویی جرایم ارتکاب یافته در ارتباط با سیستم رایانه‌ای، داده ترافیک سرنخی برای جمع آوری مدارک بیشتر و ردیابی مبدأء ارتباط و بعنوان بخشی از مدارک جرم محسوب می‌شود"

نرم‌افزار در بانکداری الکترونیک ایران

سیستم‌های عامل مورد استفاده

سیستم‌های عامل مورد استفاده در شبکه‌های محلی شعب، سیستم عامل DOS[1] برای ایستگاههای کاری[2] وNovel برای سرویس‌دهنده میباشد. سیستم عامل در سیستم‌های متمرکز و شبکه‌های WAN نیز از نوع سیستم عامل DB2 است. در حال حاضر هیچکدام از بانکها از سیستم‌های عامل لینوکس و یا گروه ویندوزهای ۲۰۰۰ استفاده نمی‌شود (البته بانک سامان در راه اندازی بانکداری اینترنتی خود از سیستم عامل لینوکس بهره برده است).

بانکهای اطلاعاتی مورد استفاده

بانکهای اطلاعاتی مورد استفاده در برنامه‌های کاربردی شعب بانکها در اکثر مواقع از نوع DBF[3] (در شبکه‌های داخلی) می‌باشد، و در سیستمهای متمرکز از بانکهای اطلاعاتی مورد استفاده در رایانه‌ای بزرگ مانند DB2 استفاده می‌شود، هرچند که اخیرا از بانکهای اطلاعاتی رابطه أی (RDBMS[4])جهت افزایش قابلیتهای مدیریت بانک اطلاعاتی مانند اوراکل نیز که مبتنی برسرویس‌دهنده می‌باشد استفاده شده است. هرچند که در تهیه بعضی از برنامه‌های کاربردی مورد استفاده دربخش ستادی جهت تهیه گزارشهای مدیریتی از بانکهای اطلاعاتی با قابلیت‌های بالا مانند SQLSERVER استفاده می‌شود ولی از این نوع بانکهای اطلاعاتی در سیستم‌های متمرکز و یا در طراحی سیستم‌های مدیریت اطلاعات (MIS[5]) استفاده نشده است.

---

[1] Disk Operating System

[2] Workstations

[3] Database of Foxpro

[4] Relational Database Management System

[5] Management Information System

برنامه‌های کاربردی

برنامه‌های کاربردی مورداستفاده در بانکهای ایرانی رامی‌توان به دو دسته تقسیم نمودکه عبارتنداز:

۱) برنامه‌های کاربردی جهت نصب در شبکه‌های داخلی :

این نوع برنامه‌های کاربردی اکثرا توسط کارشناسان تجزیه وتحلیل سیستم و برنامه نویسان داخلی بانک و یا شرکتهای داخلی طراحی شده است. بیشتر زبانهای برنامه نویسی مورد استفاده جهت ایجاد این نوع برنامه‌ها عبارتند از فاکس پرو، C، پاسکال [۱]، ویژال بیسیک، ASP[۲]. اکثر این گروها از برنامه‌های کاربردی با فاکس‌پرو نوشته و طراحی شده است. وابسته بودن به سکوی رایانه‌ای (وابسته به سخت‌افزار، سیستم عامل، فایلهای اجرای و سایر فایلهای برنامه) از ویژگی این برنامه‌های کاربردی می‌باشد. در ایجاد این نوع از برنامه‌های کاربردی بندرت از برنامه‌های شی گرا[۳]و برنامه های تحت Web استفاده شده است.

۲)برنامه‌های کاربردی مورد استفاده در شبکه‌های (WAN)(سیستم‌های متمرکز)

این نوع از برنامه‌های کاربردی بصورت یک بسته نرم‌افزاری[۴] توسط یک شرکت واسطه داخلی (اکثر مواقع توسط شرکت خدمات انفورماتیک) براساس سفارش بانکها خریداری شده است و بدلیل اینکه کل اسناد و منابع برنامه همراه با برنامه خریداری شده است، لذاپس از بومی نمودن برنامه و اعمال اصلاحات، تغییرات، و افزودن به امکانات برنامه توسط کارشناسان داخلی، در اختیار بانکها قرارمی‌گیرد. بدلیل تحریم تجاری آمریکا و انحصاری بودن شرکتهای آمریکائی در تولیدات نرم‌افزاری و سخت‌افزاری و از طرفی عدم پشتیبانی محصولات نرم‌افزاری تولیدی شرکتهای آمریکائی (مانند میکروسافت) مورد استفاده در ایران موجب نگرانیهای در استفاده از محصولات نوین (مانند NET.) از سوی بانکها شده است. لذا بانکها با قدرت انتخاب کمتری در استفاده ازفن آوریهای روز روبرو می‌باشند، از سوی دیگر نیز محدودیت در برنامه‌های کاربردی خریداری شده بانکهای خارجی موجب چالشهای فراوان فنی در جهت توسعه اتوماسیون بانکها شده است.

بسترهای حقوقی در بانکداری الکترونیک ایران

در ایران نیز مانند بیشتر کشورهای دیگر بسترهای فنی، حقوقی، فرهنگی مورد نیاز اجرای بانکداری الکترونیک و همچنین تجارت الکترونیک فراهم نشده است. ایجاد بسترهای حقوقی مورد نیاز فعالیت بانکداری و ایجاد اطمینان و اعتماد به مشتریان همگام با ایجاد بسترهای فنی، مخابراتی و فرهنگی از جمله ارکان موفقیت اجرای بانکداری الکترونیک محسوب می‌شود. بطور کلی برای تمامی فعالیتهای بانکی در ایران قانون مشخص و معینی وجود ندارد، بخصوص در ارتباط با ارائه خدمات نوین بانکداری از جمله ارائه خدمات کارت و همچنین ارائه خدمات بانکداری اینترنتی بانکها با خلاء قانونی روبرو هستند. هر چند که در راستای دولت الکترونیکی و تجارت الکترونیکی اخیرا در مجلس شورای اسلامی لایحه‌هایی به تصویب رسیده است، ولی منابع و ماخذ حقوقی فعالیتهای الکترونیک در سطح جزئی بخصوص در زمینه بانکداری الکترونیک کافی نمی‌باشد. اجرای احکام تخلفات الکترونیکی منوط است به وجود قانون، ایجاد دادگاههای تخصصی و همچنین قضائی متخصص. در حال حاضر از فقدان هر سه عامل مهم بعنوان محدودیتهای حقوقی بانکداری الکترونیکی

---

[۱] Pascal

[۲] Active Server Page

[۳] Object Oriented Programming

[۴] Package

می‌توان یاد کرد. قانون حمایت از حقوق پدیدآورندگان برنامه‌های کاربردی که در جلسه علنی ۱۳۷۹/۱۰/۱۴ مجلس شورای اسلامی تصویب جهت اجرا به مراجع قانونی ابلاغ شده بود را می‌توان اولین اقدام حقوقی در فعالیتهای الکترونیکی در ایران یاد کرد.

منابع و ماخذ

- "از مبادله الکترونیکی اطلاعات (EDI) تا تجارت الکترونیک"، موسسه مطالعات و پژوهشهای بازرگانی، ۱۳۷۶
- "مجموعه مقالات اولین همایش بانکداری الکترونیکی "، بانک توسعه صادرات، ۱۳۷۹
- الهیاری فرد، محمود، "بررسی مقایسه ای خدمات بانکداری ستنی و بانکداری الکترونیک در ایران"، شهریور ۸۲، پایاننامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد تهران مرکز، دانشکده حسابداری و اقتصاد
- الهیاری فرد، محمود"بانکداری الکترونیک در روسیه"،نشریه بانک ملی ایران ، شماره ۹۲، آبانماه ۱۳۸۲
- الهیاری فرد، محمود"بانکداری الکترونیک در هندوستان"، نشریه بانک ملی ایران، شماره ۹۳، آذرماه ۱۳۸۲
- الهیاری فرد، محمود"بانکداری الکترونیک در استرالیا"،نشریه بانک ملی ایران، شماره ۹۴، دیماه ۱۳۸۲
- "ویژه نامه بانکداری"،شماره ۱۳۸
- "سرویسهای شرکت مخابرات ایران"آدرسهای وب سایت،
- http://www.Irantelecom.org
- http://www.DCI.com
- آمارهای بانک ملی در پایان ۱۳۸۱،۱۳۸۰،۱۳۷۹
- http://www.IranIT.com
- Essinger, James,"The Virtual Banking Revolution", Thomson business press,1999
- "E_commerce and Development Report 2002", http://www.unctad.org/ecommerce/docs/edr01_en/edr01_en.pdf
- "An Exploratory Investigation Of Global Prespective On E_Commerce ,Internet and Digital Economy", http://www.ecommerce.or.the/nceb2002/paper/4200/investigation.pdf
- "Dynamics Of Banking Technology Adoption An Application To Internet Banking , Web Sites at www.warwick.ac.uk/~ecrgt/jobmarket.pdf
- "E_Commerce in Europe Results of the pilot surveys carried out in 2001" Web Sits at www.researchandmarkets.com/reports/479/479.pdf
- "The Emergence of ebanking in russia" Web Sites www.sseru.org/DocFiles/wp01-101R1.doc
- "banking Adaption and Dot.com viability a comparison of Australian and Indian experiences in the banking sector". www.deakin.edu.au/infosys/docs/workingpapers/archive/ _Working_Papers_2001/2001_14_Unnithan.pdf dot .com
- "Networking essentials" ,Microsoft press,1997
- "S.W.I.F.T Annual Report " ,2001,2002
- Garret,Chris,"ASP.NET Web Developer's Guide",Syngress,2002