فن آوری اطلاعات

بخش چهارم

تجارت الکترونیک

"امنیت و تجارت بی سیم"

INFORMATION TECHNOLOGY

PART 4

e-COMMERCE

"SECURITY AND WIRELESS COMMERCE"

بخش تحقیق و توسعه

تابستان ۱۳۸۲

۶۴

RAH SHAHR

گروه مهندسین مشاور معمار و شهرساز، عمران آب و انرژی Architects, Urban Design, Hydraulics & Energy Consultants

فن‌آوری اطلاعات- بخش چهارم : **تجارت الکترونیک** 'امنیت و تجارت بی سیم'

INFORMATION TECHNOLOGY -PART 4: **e - COMMERCE**

"SECURITY AND WIRELESS COMMERCE"

به کوشش: مهندس روزبه علی‌بیک، مهندس لیلا ملاصالحی، خانم مهناز کیائی، ساناز سیدموسوی ، علی پور ناصح ، ،محمد مهدی شعار، مهندس شیوا نیکزاد، (بخش IT ره‌شهر)

حروفچینی کامپیوتری: بخش حروفچینی ره‌شهر

چاپ و صحافی: چاپ شهر

فهرست مطالب

عنوان **صفحه**

پیشگفتار

سیاستمداران و مدیران در کشورهای در حـــال توسعه با چالشـــهای زیادی در حـوزه‌هـای مـدیریت، نیـروی کـــار، امور بین المللی روابط تجاری و مقررات محلی مواجه هستند،فرآیند تصمیم گیری در بیشتر ایـن مـوارد فقط از طریق مذاکرات می‌تواند انجام شود.

سنت استعمار کهن بر این فرض متکی بود که فقـط نوابـغ و نماینـدگان کشـورهای ثروتمنـد و دارای سـطح آموزشی بالا نیاز به مذاکره و تعامل با هم دارند، این سنت براین فرض غلط و کوته بینانه استوار بود که افـراد تحصیل کرده در دانشگاه‌های غرب شایستگی‌های بیشتری برای تصمیم گیری دارند. تعمیم ایـن فرضـیه بـه این تفکر منتهی می‌شد که غرب در تمام حوزه‌های مربوط به حکومت برتر است و نتایج این تفکر در مسـئله مذاکرات و رفتارهای متناظر با آن رخ نموده است و کشورهای پیشرفته اینطور فرض می‌کردند که نیـازی بـه مذاکره با دیگران ندارند با جهانی شدن تجـارت و ایجـاد تجـارت الکترونیـک، مـذاکرات و تجـاری بصـورت الکترونیکی جهان را درهم نوردید و تحولی عظیم در عرصه روابط بین المللی ایجاد کرد. به‌این ترتیب تجارت الکترونیک نه تنها تجارت جهانی را متحول نمود، بلکه زمینهٔ مذاکره و گفتگـو بـین تمـدنها و فرهنـگ‌هـا، را فراهم آورد.

در ماه‌های اخیر شاهد تحولات زیادی در زمینهٔ تجارت الکترونیک در کشورمان بوده‌ایم، بسیاری از شرکتها در تلاش هستند تا زمینه ورود خود به تجارت الکترونیک را فراهم آورند. که این امـر نیازمنـد داشـتن اطلاعـات کافی در زمینه مذاکرات الکترونیکی، در سطح جهان و زیرساخت‌های کافی جهت ارایه خدمات می‌باشد.
در این راستا گروه مهندسین مشاور ره‌شهر برای ایجاد بستر فرهنگی و فضـای توسـعه فـن‌آوری اطلاعـات و ارتباطات اقدام به تاسیس بخش IT نموده و دستاوردهای مطالعات خود را به‌صـورت نشـریات جهـت اطـلاع مدیران، کارشناسان و مسؤلین محترم ارایه می‌نمایـد. ایـن نشـریه در ادامـه سـه نشـریه قبـل و بـا موضـوع *تجارت الکترونیک* منتشر می‌گردد.

امید است این مجموعه بتواند، اندکی از آگاهی‌های لازم، جهت افزایش کـارآیی و اثـر بخشـی سیسـتم‌هـای اطلاعات نوین برای حصول به اهداف بزرگ را درکشور پهناور اسلامی ما داشته باشد.

سعید شهیدی
مدیر بخش تحقیق و توسعه

مقدمه

پیوستن اکثر کشورهای جهان به سازمان تجارت جهانی، و تقاضای عضویت کشور جمهوری اسلامی ایران، سازمانهای مختلف را بر آن داشته که آمادگی لازم را در این رابطه کسب نمایند. با روند جهانی شدن تجارت از جمله ایجاد مبادله الکترونیکی داده‌ها و ایجاد سازمان تجارت جهانی توسط مراجع بین‌المللی، بنظر می‌رسد که تجارت الکترونیک و زیرساخت‌های نرم‌افزاری و سخت‌افزاری جهت پیاده‌سازی آن مهمترین برنامه کاری تجاری در دهه نخست هزاره سوم باشد ضمن آنکه مبادلات الکترونیک، منحصر به تجارت نیست و رشته‌ها و زمنیه‌های متنوعی را در بر می‌گیرد ولی ما در اینجا تنها به جنبه تجاری آن خواهیم پرداخت.

هدف از تجارت الکترونیک گسترش روشهای تجاری قدیمی نیست، بلکه ارائه روشهای جدید در امور تجاری است به نحوی که تمامی خریداران از سراسر جهان بتوانند از محصولات عرضه شده بهره‌مند گردند. با فرا رسیدن موج جدید تجارت الکترونیک که همان تجارت بی‌سیم و بانک‌های الکترونیکی است، عمومیت تجارت الکترونیک در کشورهای پیشرفته جهان بیش از پیش گردیده است.

بدین ترتیب تجارت الکترونیکی یک نیاز آتی خواهد بود چون با حداقل دخالت انسان و شاید هم بدون دخالت انسان شکل خواهد گرفت.

توجه به این رشد سریع و روزافزون تجارت الکترونیک و مزیت‌های رقابتی حاصل از آن باعث گردیده تا روش‌های تجاری با قابلیت ها و توانایی‌های مناسب و قابل اطمینان ایجاد گردد بنابراین سیستم‌های کارآ و با امنیت بسیار بالا مورد توجه قرار خواهد گرفت.

سرعت در ارائه خدمات تجارت الکترونیک، سهولت در بکارگیری و امنیت بالای سیستم‌ها مواردی است که باعث افزایش مقبولیت تجارت بی‌سیم شده است. در این نشریه به بررسی وضعیت تجارت بی‌سیم، مذاکرات تجاری در زمینه تجارت الکترونیک و همچنین امنیت در تجارت الکترونیک می‌پردازیم.

پیشرفت تکنولوژی کامپیوتر و رواج آن از یک‌سو و توسعه کمی و کیفی مخابرات داده‌ها از سوی دیگر باعث شده است که سرعت فزاینده و تصاعدی در تولید اطلاعات ایجاد شود. امروزه، در موارد بسیاری چرخش امور روزمره افراد و سازمان‌ها تولید اطلاعات می‌کند. این فرآیند، با رشد تکنولوژی ذخیره‌سازی و انتقال اطلاعات همراه بوده است به‌گونه‌ای که ماهیت اطلاعات امروز با ماهیت اطلاعات دهه‌های گذشته متفاوت بوده و می‌توان گفت که اطلاعات امروزی الکترونیکی و اطلاعات قبلی غیر الکترونیکی هستند.

بر خلاف سیستم مدیریت و حفظ اطلاعات غیر الکترونیکی که عمدتاً از حفاظت فیزیکی برای امنیت اطلاعات استفاده می‌کند، اطلاعات الکترونیکی در معرض تهدیدات متنوع‌تر و پیچیده‌تری هستند. انتقال اطلاعات در رسانه‌های بعضاً عمومی (حتی در سطح جهانی)، امکان اتصال به انباره‌های اطلاعاتی، هزینه بسیار کم در انتقال حجم قابل توجهی از اطلاعات از جمله مواردی هستند که زمینه‌ساز این تهدیدات هستند. در عصر اطلاعات غیر الکترونیکی، سرقت اطلاعات عمدتاً معطوف انتقال فیزیکی رسانه‌های ذخیره‌سازی اطلاعات بود که به راحتی توسط نگهبانان قابل مشاهده و کنترل بود. اکنون سرقت اطلاعات نه تنها از چشم نگهبانان به دور است بلکه بعضاً با هزینه دارنده اطلاعات نیز دزدی صورت می‌گیرد. کپی‌برداری از اطلاعات در حال مبادله، تغییر اطلاعات در حال مبادله، و جعل اطلاعات سه تهدید اصلی در مورد اطلاعات الکترونیکی هستند.

اصول امنیت شبکه

هدف از امنیت اطلاعات، استفاده از مجموعه‌ای از سیاست‌ها، راهکارها، ابزار، سخت‌افزارها و نرم‌افزارها، برای فراهم آوردن محیطی عاری از تهدید در تولید، پالایش انتقال و توزیع اطلاعات است. فراهم آوردن چنین محیطی مستلزم انجام مواردی است که می‌توان از آنها به نیازهای امنیتی اطلاعات نام برد. برخی از این موارد به شرح زیر هستند:

۱. ارزش هر واحد اطلاعاتی برای مالک آن باید مشخص شود. بر اساس ارزش واحدهای اطلاعاتی بایستی آنها را رده‌بندی کرده و یک سقف هزینه را برای امنیت آنها تعیین نموده و برچسب رده امنیتی را بر روی آنها نصب کرد.

۲. تمهیدات لازم اعم از ابزار سخت‌افزاری و نرم‌افزاری برای حفاظت از اطلاعات با اولویت بالاتر فراهم گردد.

۳. سیاست‌گذاری یکپارچه و سازگار در خصوص امنیت اطلاعات در بخش‌های مختلف مدیریتی یک سازمان اعمال گردد.

۴. ساز و کار و تشکیلات مناسب برای انطباق امنیتی اطلاعات با پیشرفت‌های تکنولوژی تولید، توزیع و انتقال اطلاعات از یک طرف و تهدیدات جدید از طرف دیگر فراهم گردد.

۵. امنیت اطلاعات مانع و محدودیتی برای دسترسی کاربران مجاز آن فراهم نکند.

۶. امکان تعقیب عملکردهای مشکوک روی اطلاعات فراهم شده باشد.

امنیت اطلاعات

امنیت عموماً به صورت عاری بودن از خطرات و شرط اصلی برای سلامت تعریف می‌شود. امنیت کامپیوتر به شکل حفاظت از داده‌های یک سیستم در مقابل افشاسازی، تغییر یا تخریب غیرمجاز و حفاظت از خود سیستم کامپیوتر در مقابل استفاده غیرمجاز تعریف می‌شود. از سوی دیگر مفهوم امنیت زمانی که در مورد اطلاعات مطرح می‌شود، به شکل حفاظت از اطلاعات در مقابل آسیب یا حمله و پایداری، قابل اعتماد بودن و بی‌خطا بودن اطلاعات تعریف می‌شود. از آنجا که کنترل‌هایی که برای تأمین امنیت کامپیوتر و اطلاعات انجام می‌شود باعث ایجاد محدودیت‌هایی در استفاده از آن می‌شوند، معمولاً نیاز به برقراری مصالحه یا تعادل بین این دو وجود دارد.

کنترل امنیت کامل اطلاعات در سه لایه انجام می‌شود:

۱. **فیزیکی:** امنیت فیزیکی عبارت است از استفاده از قفل‌ها، نگهبان‌ها، علایم، وسایل اعلام خطر و ابزارهای مشابه برای حفاظت از کامپیوترها و محتویات آنها در مقابل جاسوسی، سرقت و تخریب یا آسیب دیدن که در اثر اتفاقاتی نظیر آتش‌سوزی یا بمب‌گذاری لازم است.

۲. **فنی:** امنیت فنی مربوط است به استفاده از خود نگهبان‌ها در سخت‌افزار، عملیات یا برنامه‌های کاربردی، سخت‌افزار یا نرم‌افزار ارتباط شبکه‌ای و سایر تجهیزات. این نوع کنترل‌ها، به نام کنترل‌های منطقی نیز شناخته می‌شوند.

۳. **مدیریتی:** امنیت مدیریتی یا امنیت پرسنلی شامل محدودیت‌های مدیریتی، روش‌های عملیاتی، روش‌های ثبت رویدادها، و دیگر کنترل‌های مدیریتی است که برای تأمین سطح قابل قبولی از حفاظت و امنیت به کار می‌روند. علاوه بر این، کنترل‌های امنیتی شامل روش‌هایی می‌شوند که برای اطمینان از اینکه تمامی پرسنلی که به منابع کامپیوتری دسترسی دارند، مجاز به این کار هستند، برقرار می‌شوند.

این سه دسته را می‌توان از جنبه دیگری به صورت کنترل‌های پیشگیرانه و اکتشافی تقسیم‌بندی کرد. کنترل‌های پیشگیرانه سعی دارند که ا ز وقوع رویدادهای غیرقابل پیش‌بینی جلوگیری کنند، در حالیکه در کنترل‌های اکتشافی سعی بر این است که رویدادهای پیش‌بینی نشده بعد از اینکه رخ دادند، شناسایی شوند و اثرات آنها از روی سیستم رفع شود.

مدیریت برنامه‌های امنیت کامپیوتر و شبکه به مرور زمان پیچیده‌تر می‌شود. پیشرفت‌های بسیار سریع در زمینه کامپیوترها و شبکه‌های کامپیوتری در سالهای اخیر، تمرکز صنعت پردازش داده‌ها را از صورت متمرکز در یک ساختمان به پایانه‌هایی که در ادارات و خانه‌های شخصی قرار دارند، منتقل کرده است در نتیجه مدیران اکنون باید امنیت را در یک مقیاس بسیار وسیعتر تأمین و مدیریت کنند. این تغییرات و پیشرفت‌ها با شتابی روزافزون در حال زیاد شدن هستند و به این ترتیب مدیریت امنیت نیز پیچیده‌تر می‌شود. وظیفه مدیر امنیت اطلاعات، برقراری یک برنامه امنیت است که سه نیاز را مورد توجه قرار می‌دهد: محرمانه بودن، جامعیت و دسترس‌پذیری منابع اطلاعاتی سازمان.

محرمانه بودن (confidentiality)

محرمانه بودن، حفاظت از داده‌های یک سیستم است بطوری که افراد غیرمجاز نتوانند به این اطلاعات دسترسی داشته باشند. به اعتقاد بسیاری از متخصصان امنیت اطلاعات، این نوع حفاظت، مهم‌ترین جنبه امنیتی برای سازمان‌های نظامی و دولتی است که نیاز به حفظ برنامه‌ها و اطلاعات خود در مقابل دشمنان بالقوه دارند. البته این نوع حفاظت برای محیطهای تجاری که در آنها اسرار تجاری باید از دسترس رقیبان دور نگهداشته شوند نیز کاربرد زیادی دارد.

برای حفظ محرمانه بودن اطلاعات، می‌توان از روش‌های متعددی استفاده کرد. یکی از پرکاربردترین و مناسب‌ترین روش‌ها، رمزگذاری اطلاعات است. الگوریتم‌های بسیاری برای رمزگذاری اطلاعات وجود دارند که هر یک دارای نقاط ضعف و قوتی هستند. انتخاب یک الگوریتم کارآمد و امن برای رمزگذاری اطلاعات می‌تواند تا حد بسیار زیادی محرمانه بودن اطلاعات را تضمین کند.

روش دیگری که برای حفظ محرمانه بودن اطلاعات مورد استفاده قرار می‌گیرد، روش کنترل دسترسی است. کنترل دسترسی به معنای اعمال روش‌هائی برای هویت‌شناسی و مجازشناسی کاربران یک سیستم است.

یکپارچگی (integrity)

حفظ یکپارچگی به معنای حفاظت داده‌های سیستم در مقابل تغییرات غیرمجاز سهوی یا عمدی است. برای حفظ جامعیت، برنامه امنیتی باید همواره اطلاعات را در حالتی که مورد انتظار کاربران سیستم است، نگهدارد. اگر چه برنامه امنیتی نمی‌تواند دقت داده‌هایی را که توسط کاربران در سیستم قرار داده می‌شوند ارزیابی کند ولی می‌تواند تضمین کند که همه تغییراتی را که توسط کاربران درخواست می‌شوند، به شکل صحیح روی سیستم اعمال می‌شوند. جنبه دیگری از یکپارچگی، نیاز به حفاظت از برنامه‌هایی است که داده‌های سیستم را تغییر می‌دهند تا این برنامه‌ها توسط افراد غیرمجاز تغییر داده نشوند.

به منظور جلوگیری از بروز خطا در سیستم‌های کامپیوتری و بروز جرایم از این طریق، اطمینان از یکپارچگی داده‌ها یک نیاز اساسی در سیستم‌های نظامی، دولتی و تجاری محسوب می‌شود. به این منظور لازم است که هیچ کاربری نتواند داده‌ها را به نحوی تغییر دهد که داده‌های با ارزش از بین بروند یا تغییر یابند. به عنوان مثال‌هایی از سیستم‌هایی که یکپارچگی داده‌ها در آنها از اهمیت بسیار زیادی برخوردار است، می‌توان سیستم کنترل ترافیک هوایی و سیستم‌هایی کنترل پرتاب نظامی (که پرتاب جنگ‌افزارهای اتوماتیک را کنترل می‌کنند) را نام برد. مشابه با محرمانه بودن، استفاده از روش‌های مناسب کنترل دسترسی، روشی کلیدی در حفظ جامعیت داده‌ها محسوب می‌شود.

در دسترس بودن (availability)

در دسترس بودن عبارت است از اطمینان از اینکه یک سیستم کامپیوتر هر زمان که لازم باشد توسط کاربران مجاز قابل دسترسی باشد. دو جنبه‌ای که معمولا توسط در دسترس بودن مورد توجه قرار می‌گیرد، عبارتند از:

- مختل شدن سرویس‌ها
- از دست دادن توانایی پردازش داده‌ها در نتیجه بروز وقایع طبیعی مانند آتش‌سوزی و زلزله، یا انجام عملیات تخریبی توسط انسان‌ها نظیر بمب‌گذاری

مختل شدن سرویس‌ها معمولاً به اعمالی اطلاق می‌شود که خدمات کامپیوتری را به نحوی مورد حمله قرار می‌دهند که باعث می‌شود سیستم برای کاربران مجاز، غیر قابل استفاده شود. به عنوان مثال می‌توان از قطع کردن سیم ارتباط شبکه‌ای میان دو کامپیوتر، استفاده از ویروس‌ها برای از کار انداختن سیستم‌های کامپیوتر و استفاده از حملات الکترونیکی نام برد.

برای مقابله با این نوع تهدیدات می‌توان از روش‌های کنترل دسترسی استفاده کرد. به این ترتیب تنها کاربران مجاز اجازه دسترسی به سیستم‌ها و تجهیزات کامپیوتری (چه دسترسی فیزیکی و چه دسترسی الکترونیکی) خواهند داشت و در دسترس بودن سیستم مورد تهدید قرار نمی‌گیرد.

از دست دادن توانایی پردازش اطلاعات در نتیجه وقایع طبیعی یا عملیات انسانی، مورد دیگری است که می‌تواند دسترسی کاربران مجاز به سیستم را مختل کند. برای حفاظت از داده‌ها درمقابل چنین اتفاقاتی می‌توان روش‌هایی نظیر نگهداری نسخه‌های متعدد از داده‌ها یا بکار بردن روش‌های مناسب فیزیکی را مورد استفاده قرارداد.

شکل‌های امنیت اطلاعات

امنیت اطلاعات می‌تواند به صورت‌های زیر تقسیم‌بندی شود:

- **امنیت فیزیکی:** این دسته شامل امنیت دسترسی فیزیکی و امنیت نیروی انسانی خواهد بود.
- **امنیت محلی:** امنیت سیستم عامل، داده‌ها و برنامه‌های کاربردی در این دسته قرار می‌گیرند.
- **امنیت ارتباطات:** امنیت شبکه را شامل خواهد شد.

امنیت دسترسی فیزیکی

تأمین امنیت هر شبکه کامپیوتری مستلزم تأمین امنیت در محیط فیزیکی سخت‌افزارها است. عواملی مانند حوادث غیر مترقبه (سیل، زلزله، طوفان و مانند اینها)، دستبردهای جاسوسی و یا دستبردهای معمولی می‌توانند امنیت فیزیکی را مورد تهدید قرار دهند.

تأمین امنیت فیزیکی شامل بخش‌های زیر است:

- ارتباط فیزیکی خطوط ارتباطی (مانند فیبر نوری، کابل، ماهواره (امواج رادیویی)، مایکروویو و نظایر آن) از نظر قطع شدن خطوط و استفاده غیر مجاز
- دستگاه‌های رابط شامل تکرارکننده‌ها، مسیریاب‌ها، پل‌ها، دروازه‌ها و نظایر آن
- مکان‌های نگهداری تجهیزات کامپیوتری
- محل استقرار و نحوه استقرار تجهیزات

روش‌های مقابله با نقاط ضعف دسترسی فیزیکی عبارتند از:

- **کنترل دسترسی:** این روش، کارآمدترین روش برای تأمین امنیت دسترسی فیزیکی است بدین ترتیب که می‌توان نوع دسترسی و افراد مجاز را تعریف نمود. برای مثال، افراد خاصی اجازه ورود به مکان‌هایی که تجهیزات شبکه در آن قرار می‌گیرند را داشته باشند.

- **ایجاد پوشش:** یکی دیگر از روش‌های تأمین امنیت دسترسی فیزیکی، قرار دادن پوشش است. برای مثال می‌توان خط مسی انتقال را در داخل لوله‌های محافظ قرار داد تا به این صورت هکر نتواند از آن انشعاب بگیرد یا اینکه کامپیوترها و سخت‌افزارها را داخل اتاق مناسب مستقر نمود تا امنیت دسترسی فیزیکی توسط حفاظ ساختمانی ایجاد گردد. بعلاوه می‌توان دستگاه‌هایی که وظایف مهم در شبکه انجام می‌دهند را به UPS مجهز نمود تا در موقع قطع برق دچار وقفه نشوند.
- **کشف خطا و رفع آن:** با توجه به اینکه پیش‌بینی همهٔ خطاها و خسارات امکان‌پذیر نیست، باید راه‌هایی برای کشف خطا و رفع آن، مثلاً روشی برای کشف قطع خطوط ارتباطی یا خرابی مسیریاب‌ها، وجود داشته باشد.
- **انتخاب نوع رسانه‌ها و دستگاه‌های فیزیکی:** سطح امنیت در رسانه‌ها و دستگاه ها بسیار متفاوت است. مثلاً فیبر نوری از سیم مسی امن‌تر است، زیرا بسادگی نمی‌توان از آن انشعاب گرفت و همچنین نرخ خطای بسیار پایینی دارد.
- **تهیه دستورالعمل‌های بهره‌برداری:** از دیگر راه‌های تامین امنیت فیزیکی، آگاه سازی نیروی انسانی در مورد نحوهٔ استفادهٔ امن از سیستم‌ها و تجهیزات از طریق صدور بخشنامه‌ها و دستورالعمل‌های بهره‌برداری می‌باشد.

تامین امنیت دسترسی فیزیکی علاوه بر تأمین امنیت در برابر خطاهای عمدی به تأمین امنیت در مقابل خطاهای غیرعمدی (خرابی و از کار افتادن دستگاه‌ها و رسانه‌ها) نیز وابسته است.

امنیت نیروی انسانی

منظور از نیروی انسانی، تمام افرادی هستند که بنحوی با شبکه کامپیوتری در ارتباط هستند. این افراد شامل کاربران و گردانندگان، سیاست‌گذاران شبکه، طراحان، مجریان و اپراتورهای شبکه می‌باشند. مشکلات ناشی از عدم رعایت اصول امنیت توسط نیروی انسانی، معمولاً جبران‌ناپذیر است و با آموزش نیروی انسانی، می‌توان از بروز چنین مشکلاتی جلوگیری کرد. افرادی که با شبکه سر و کار دارند، به سه دستهٔ زیر تقسیم می‌شوند:

- **کاربران خارجی:** افرادی خارج از سازمان با نفوذ به سازمان، می‌توانند سبب انتقال اطلاعات به صورت فیزیکی یا منطقی شوند. هکرها می‌توانند با کارگزارهای داخلی ارتباط برقرار کنند و شبکه را مورد حمله قرار دهند و امنیت سیستم را به مخاطره بیندازند.
- **کاربران داخلی:** در بیشتر موارد، کاربران داخلی اجازهٔ دسترسی به کلیهٔ منابع اطلاعاتی را دارند و در صورت استفاده نادرست از این امکانات، خسارات جبران‌ناپذیری وارد خواهد شد.
- **دست‌اندرکاران شبکه:** این گروه مسئول تأمین و حفظ امنیت شبکه‌های کامپیوتری هستند. طراحی، اجرا، پیاده‌سازی و حفظ و نگهداری پارامترهای امنیتی از وظایف این گروه است. با توجه به اینکه این گروه اطلاعات بیشتر در اختیار دارند، احتمال ایجاد آسیب‌های امنیتی عمیق‌تر بوده و معمولاً این آسیب‌ها بسیار گران تمام می‌شوند.

روش‌های مقابله با خطرات ناشی از عدم رعایت امنیت در بعد نیروی انسانی، عبارتند از:

- **تعریف دقیق سیاست‌های امنیتی شبکه:** سیاستگذاران امنیتی باید بطور شفاف اهداف امنیتی سیاست‌های امنیتی را مشخص کنند. هر فرد به اندازه مسئولیت و شغل سازمانی خود و به اندازه اطلاعات و منابع مهمی که در دست دارد باید از اهداف امنیتی سازمان اطلاع داشته باشد تا بر طبق آن، امنیت قابل قبولی را در محیط کار خود ایجاد نماید.
- **تعریف دقیق پست‌ها و جداسازی مسئولیت‌ها:** مسئولیت‌ها باید جدا شوند تا هر کس بطور شفاف وظایف مشخصی داشته باشد. همچنین میزان مسئولیت هر پست نسبت به حفظ امنیت باید مشخص گردد تا فرد مسئول از سطح امنیتی پست خود مطلع گردد.
- **آموزش نیروی انسانی:** مهمترین عاملی که می‌تواند نیروی انسانی را در مقابل حملات امنیتی حفظ نماید دانایی و آگاهی آنها از روش‌های از دست رفتن اطلاعات و روش‌های مقابله است.
- **مدیریت و کنترل کاربران:** بمنظور حفظ امنیت و پیگیری وقایع ضدامنیتی، مدیریت و کنترل مداوم کاربران ضروری است.

در صورت جابجایی فرد در سازمان نباید فرد بتواند از امکانات قبلی خود در دسترسی به اطلاعات استفاده نماید. فعالیت‌های غیرقانونی کاربران با ثبت وقایع و آمارگیری از تعداد دسترسی به انواع اطلاعات مشخص خواهد شد. در مجموع، حفظ امنیت توسط نیروی انسانی سازمان الزامی است. استخدام دقیق و آموزش متناوب نیروی انسانی، تعیین مرزها و پست‌ها و مسئولیت‌ها برای تأمین امنیت ضروری است.

امنیت سیستم عامل

تامین امنیت در سیستم عامل، یکی از ابعاد مهم حفظ و تأمین امنیت در هر شبکهٔ کامپیوتری به شمار می‌رود. سیستم عامل به عنوان پایه‌ای ترین نرم‌افزار در هر کامپیوتر، مسئولیت مدیریت منابع و برقراری ارتباط میان کاربر و سخت‌افزار را برعهده دارد. بنابراین، می‌توان گفت که هرگونه ناامنی در سیستم عامل موجب بروز ناامنی در کل یک سیستم کامپیوتری و در زیر سیستم ارتباطی آن می‌شود.

سیستم‌هـای عامل دارای سطوح مختلفـی از امنیت هستند که تحت رده‌بندی استاندارد TESEC (Trusted Computer Systems Evaluation Criteria) توصیف می‌شوند. یک سیستم عامل حداقل باید پیاده‌سازی امنی از پروتکل‌های شبکه و از جمله TCP/IP را دارا باشد. سایر ویژگی‌های یک سیستم عامل امن عبارتند از:

- وجود سطوح مختلف امنیتی، حداقل در دو سطح کاربر و سیستم به منظور تأثیرناپذیری سیستم عامل از خطاهای سهوی و عمدی کاربران مجاز
- بکارگیری روش‌های مناسب برای ذخیره اطلاعات هویت‌شناسی کاربران، جلوگیری از انتخاب کلمه عبورهای ضعیف و جلوگیری از عدم تغییر کلمه عبور برای مدت طولانی
- ثبت واقع سیستم برای پیگیری‌های اداری و قانونی و رفع خطا
- وجود و پشتیبانی از یک سطح حداقل امنیت به گونه‌ای که این حداقل سطح، قابل از کارانداختن نباشد. به عنوان مثال، بدون دسترسی فیزیکی به کنسول (واقع در سایت نگهداری کامپیوتر) امکان راه اندازی دوباره، فرمت کردن دیسک و یا خاموش کردن، سیستم وجود نداشته باشد.

امنیت داده‌ها

رشد فزایندهٔ حجم و نوع داده‌های ذخیره شده از یک سو و کلیدی‌تر شدن نقش آنها در تصمیم‌گیری‌ها از سوی دیگر، سبب شده تا ضرورت حفاظت داده‌ها برای همهٔ مدیران روشن شود. از طرف دیگر، گسترش شبکه‌های کامپیوتری و افزایش تعداد کاربران شبکه، سبب شده است تا علاوه بر آنکه احتمال نفوذ غیرمجاز هکرها افزایش یابد، داده‌ها نیز بطور پراکنده و توزیع شده در سراسر شبکه ذخیره شوند. بدیهی است که تأمین و حفظ امنیت برای داده‌های توزیع شده دشوارتر است.

در حالت کلی می‌توان داده‌ها را به دو دسته کاربردی و کنترلی تقسیم‌بندی نمود. داده‌های کاربردی همان داده‌ها یا اطلاعاتی هستند که مورد استفاده کاربران قرار می‌گیرند و در کاربردهای متفاوتی مطرح می‌شوند. داده‌های کنترلی شامل اطلاعاتی پیکربندی سیستم، مشخصات کاربران و رویدادهای ثبت شده در سیستم هستند. این داده‌ها نقش اساسی در چگونگی عملکرد سیستم دارند و ناامنی در آنها منجر به توقف خدمات و مانع از کارکرد سیستم می‌شود. وظیفه مدیریت این داده‌ها، برعهدهٔ سیستم است.

وظیفه مدیریت داده‌های کاربردی در سیستم‌های کامپیوتری معمولاً بر عهدهٔ نرم‌افزارهای مدیریت پایگاه داده (DBMS) است. این نرم‌افزار امکان ذخیره‌سازی و بازیابی داده‌ها را فراهم می‌کند. برای حفظ و تأمین امنیت داده‌ها، باید امنیت در مدیریت پایگاه داده تأمین شود. ممکن است امنیت سیستم عامل بر روی امنیت مدیریت پایگاه داده‌ها تأثیر گذارد. روش‌های تامین امنیت داده‌ها عبارتند از:

- **ایجاد حصار در اطراف داده:** حصاربندی منطقی یا فیزیکی داده‌ها یکی دیگر از روش‌های مقابله با خطاهای احتمالی در داده‌ها محسوب می‌شود. منظور از حصار فیزیکی، حصار کشیدن در اطراف رسانه‌های ذخیره‌سازی یا در اطراف خطوط انتقال داده یا در اطراف مکان‌های استفاده و تولید داده است و حصار منطقی به معنای قراردادن قواعد و ضوابط مربوط به نحوه کار با داده برای کاربران یا ضوابط مربوط به نحوه ارسال و ذخیره داده‌ها است.
- **رمزنگاری Cryptography:** این روش قدرتمندترین و مطمئن‌ترین روش برای ایجاد امنیت است زیرا حتی اگر خطوط ارسال داده و رسانه‌های ذخیره‌سازی داده در مکان‌های ناامن باشند، باز هم داده‌های رمز شده از حملات هکرها مصون خواهند ماند.
- **بکارگیری روش‌های هویت شناسی Authentication :** در این روش پیش از ارسال داده، طرفین یکدیگر را شناسایی کرده و از هویت طرف مقابل مطمئن می‌شوند.
- **ثبت رویداد Log :** دو هدف آن عبارتند از پیگیری و بررسی تراکنش‌های کاربران و یافتن فرد هکر و ترمیم داده‌ها به حالت درست و سازگار در صورت بروز خطا یا خرابی.

بعلاوه، معمولاً برای ایجاد امنیت داده‌ای، از نوعی طبقه‌بندی امنیتی نیز استفاده می‌گردد. بدین ترتیب که داده‌ها از نظر امنیتی براساس اهمیت و نقش داده‌ها و یا براساس میزان خسارتی که با فاش شدن داده ایجاد می‌شود طبقه‌بندی می‌شوند و خدمات امنیتی موردنیاز هر طبقه تعیین و طراحی می‌شود.

امنیت برنامه‌های کاربردی

برنامه‌های کاربردی نقطهٔ ارتباط سیستم‌های کامپیوتری با کاربران آنها را تشکیل می‌دهند. وجود ضعف‌های امنیتی در این برنامه‌ها و یا در مبادلات میان آنها می‌تواند امنیت کلی سیستم را به خطر بیندازد. برای مثال وجود یک برنامه کاربردی غیرامن در سیستم حتی در صورتی که سیستم عامل آن امن شده باشد، می‌تواند باعث آسیب رساندن به منابع و اطلاعات محلی سیستم شود. همچنین یک برنامهٔ کاربردی غیرامن می‌تواند اطلاعات حساس و سری سیستم را از طریق شبکه به بیرون از سازمان انتقال دهد که این کار نیز با امن کردن شبکه قابل پیشگیری نمی‌باشد. درجهٔ خطرناک بودن چنین اتفاقاتی را زمانی می‌توان به درستی درک کرد که این برنامهٔ ناامن در کاربردهای حساسی نظیر کاربردهای نظامی مورد استفاده قرار گیرد.

با توجه به مطالبی که گفته شد، برای اطمینان از امنیت برنامه‌های کاربردی و استفاده از آنها در کاربردهایی که نیاز به امنیت دارند، اقدامات زیر می‌توانند صورت گیرند.

- **تهیه نرم‌افزارهای کاربردی از ایجادکنندگان مطمئن:** یکی از راه‌های اطمینان از امنیت برنامه‌های کاربردی، تهیه آنها از منابعی است که می‌توان از نظر امنیتی به آنها اطمینان کرد. بعنوان مثال بهتر است که این نوع برنامه‌ها از منابعی که امکان همکاری آنها با سرویس‌های جاسوسی وجود دارد، تهیه نشود.
- **ارزیابی برنامه قبل از عملیاتی کردن آن:** پس از تهیه یک برنامه کاربردی و قبل از استفاده از آن در سیستم‌های حساس اطلاعاتی، بهتر است این برنامه مدتی در محلی غیر از محل نصب نهایی مورد استفاده قرار گیرد و عملکرد آن به دقت مورد بررسی قرار گیرد.

امنیت شبکه

رشد روز افزون شبکه‌های کامپیوتری از یک سو و ماهیت توزیع شده و عدم امکان کنترل مرکزی در شبکه‌ها از سوی دیگر سبب شده تا تأمین امنیت شبکه‌های کامپیوتری از اهمیت ویژه‌ای برخوردار شود. همچنین وجود مشکلات امنیتی در پروتکل‌های شبکه و در دسترس بودن مشخصات این پروتکل‌ها و بعضاً کد پیاده‌سازی شدهٔ آنها باعث بروز ناامنی‌های بسیاری در شبکه‌های عمومی شده است.

کنجکاوان در مراکز آموزشی و دانشگاه‌ها، رقبای تجاری و دشمنان سیاسی می‌توانند سبب بروز مشکلاتی در شبکه‌های مبتنی بر TCP/IP شوند. همچنین، از آنجا که شبکه‌های کامپیوتری بستر ایجاد

سایر سیستم‌های توزیع شده مانند سیستم‌های عامل توزیع شده و سیستم‌های مدیریت پایگاه داده‌های توزیع شده نیز هستند. تأمین و حفظ امنیت در شبکه‌های کامپیوتری مبنایی برای تأمین امنیت در سیستم‌ها و کاربری‌های توزیع شده نیز خواهد بود. قبل از بررسی راه‌های تامین امنیت شبکه، ابتدا انواع تهدیدات شبکه را بررسی کرده و سپس به بحث برقراری امنیت شبکه خواهیم پرداخت.

تهدیدات امنیتی شبکه‌های کامپیوتری

در این بخش به موضوع امنیت و تهدیدات امنیتی در شبکه‌های کامپیوتری می‌پردازیم بدین صورت که ابتدا به موضوع تهدیدات امنیتی پرداخته و منشأ آنها را مورد بررسی قرار می‌دهیم و در ادامه فصل به بررسی و توصیف انواع تهدیدات خواهیم پرداخت.

منشأ تهدیدات امنیتی

تهدیدها و خطرات زیادی نیز وجود دارند که از راه‌های دیگری چون خود کاربران به شبکه تحمیل می‌شوند، وجود یک فرد غیرمتعهد در داخل می‌تواند خطرات هکری بوجود آورد. دقت نکردن افراد در انتقال اطلاعات توسط منابع قابل حمل مانند دیسک می‌تواند شبکه را آلوده کند و سایر مسائلی که برای رفع آنها، باید راه حل‌های مناسبی پیدا کرد. در اینجا ما با دو عامل عمده تهدیدات که از طریق ارتباط شبکه با محیط خارج ناامنی ایجاد می‌کنند، آشنا می‌شویم که عبارتند از افراد و نرم‌افزار. در دو بخش زیر به تشریح این تهدیدات می‌پردازیم:

تهدید افراد

یک فرد می‌تواند با انگیزه‌های مختلف عامل مزاحمت در شبکه باشد. کنجکاوی، سرگرمی، رقابت اقتصادی و یا سیاسی از عمده‌ترین انگیزه‌های نفوذ افراد به شبکه‌های کامپیوتری می‌باشند.

تهدید نرم‌افزار

امنیت شبکه توسط نرم‌افزارهای مورد استفاده نیز تهدید می‌شود. یک نرم‌افزار به دو صورت می‌تواند خطرساز باشد. حالت اول اینکه بطور عمدی برای ایجاد تهدید ساخته می‌شود و حالت دوم اشکالات غیرعمدی در برنامه می‌باشد. هر چه برنامه بزرگتر باشد، تعداد اشکال در برنامه زیادتر خواهد بود. همچنین هر چه تعداد برنامه‌های مورد استفاده بیشتر باشد، باز تعداد اشکال و در نتیجه تهدیدات زیادتر خواهند بود.

گروهی از برنامه‌ها هستند که صرفاً به منظور صدمه‌زدن به امنیت طراحی می‌شوند. برنامه‌ها یا مستقل عمل می‌کنند و یا برای پنهان‌کردن خود در کنار برنامه های کابردی قرار می‌گیرند. ویروس‌ها

مشهورترین این نوع برنامه‌ها هستند. از معروفترین انواع ویروس که در شبکه بیشتر فعال هستند کرم‌ها (worm) و اسب‌های تروا (Horse Trojan) هستند. هدف یک ویروس در مرحله اول انتشار و چسباندن خود به برنامه‌های کاربردی و دستکاری آنها هستند. کرم‌ها نیز به این صورت عمل می‌کنند، در شبکه می‌خزند و با تکثیر در آن عملیات شبکه را مختل می‌کنند. اسب تروا معمولاً به صورت برنامهٔ کارفرما ظاهر می‌شود. از اطمینان کاربر سوء استفاده کرده و اطلاعات مورد لزوم را به مکان‌های از پیش تعیین شده ارسال می‌دارد.

در ادامه، انواع تهدیدات که توسط افراد و نرم‌افزار صورت می‌گیرد به طور خلاصه بیان می‌شود:

کشف کلمه عبور

ساده‌ترین راه نفوذ به شبکه این است که خود را بجای یکی از کاربران داخل شبکه جا بزنیم. برای این کار کافی است کلمهٔ عبور یکی از کاربران داخلی را داشته باشیم. یکی از تلاش‌های عمدی هکرها کشف کلمهٔ عبور است. برای این کار راه‌های گوناگونی وجود دارد که می‌توان آنها را به صورت زیر تقسیم‌بندی کرد:

- حدس کلمه عبور
- حدس الگوریتمی با استفاده از فایل کلمهٔ عبور
- تحلیل پروتکل و فیلتر کردن کلمهٔ عبور از داخل بسته‌های انتقالی
- بررسی تصدیق کاربر توسط برنامه‌های مقیم در حافظه (TSR) یا اسب تروا.

ابتدایی‌ترین راه بدست آوردن کلمهٔ عبور دیگران حدس آن است. معمولاً کاربران کم تجربه از کلمات ساده‌ای بعنوان کلمه عبور خود استفاده می‌کنند و بطور کلی احتیاط لازم را در انتخاب و تعویض کلمه عبور نمی‌کنند. به این دلیل با حدس و امتحان کلماتی که رایج هستند، می‌توان کلمهٔ عبور را بدست آورد.

روش دیگر که بسیار سریعتر به نتیجه می‌رسد، استفاده از فایل کلمهٔ عبور است. معمولاً اطلاعات کلمهٔ عبور در هر سیستمی با استراتژی خاصی حفظ می‌شود. در سیستم عامل لینوکس Linux این اطلاعات به صورت رمز شده در فایل عمومی (که برای همه قابل خواندن است) حفظ می‌شود. هکر با استفاده از الگوریتم‌هایی که برای شکستن رمز بکار می‌رود، می‌تواند در مدت نه چندان طولانی کلید رمز را پیدا کرده و به همه کلمات عبور کاربران یک شبکه دسترسی پیدا کند.

روش سوم در اینترنت براحتی قابل انجام است. برنامه بوکننده، در دروازه‌های (Gateway) سر راه بسته قرار می‌گیرند و بسته‌های انتقالی از دروازه را فیلتر کرده و اطلاعات سری دیگران را (از قبیل کلمهٔ عبور) بدست می‌آورد. بعنوان مثال سرویس‌های انتقال فایل و ترمینال مجازی در ابتدای اتصال نام کاربر و کلمهٔ عبور را به کارگزار ارسال می‌دارند. انتقال این اطلاعات بدون هیچگونه رمزگذاری صورت می‌گیرد.

روش چهارم به دو صورت انجام می‌شود: یک روش این است که دربرنامه کاربردی تغییراتی ایجاد می‌شود و در داخل آن تروا قرار می‌گیرد تا در هنگام استفاده از آن اطلاعاتی چون کلمهٔ عبور را به هکر ارسال کند و در جای مناسبی برای استفاده‌های بعدی ذخیره نماید.

سوء استفاده از اشکال برنامه‌ها

وجود یک اشکال در برنامهٔ ارتباط شبکه‌ای، به معنی باز بودن یک راه برای نفوذ هکرها است. در چند سال اخیر هکرها موجب پیشرفت و رفع نقایص و ضعف‌های امنیتی برنامه‌ها شده‌اند زیرا با کشف آن اشکالات و سوء استفاده از آنها موجب رفع آن نقیصه‌ها توسط برنامه‌نویس‌ها شده‌اند. چنین جریانی در دو برنامه کارگزار پست الکترونیک (Unix Sendmail) و برنامه شناسایی افراد (Finger) رخ داده است. راه اصولی رفع نقیصه‌های این برنامه‌ها، استفاده از روش‌های مهندسی نرم‌افزار در تعیین مشخصات سیستم، طراحی و پیاده‌سازی برنامه‌های ارتباطی است.

ضعف در تصدیق

مراحل بررسی مجاز بودن کاربر در هنگام ورود به سیستم را تصدیق می‌گویند. ضعف تصدیق موجب نفوذ افراد غیرمجاز به داخل سیستم می‌شود. در کل، وظیفه مراحل تصدیق این است که نام کاربر و کلمه عبور آن را دریافت کرده و مجاز بودن آن را بررسی نماید و در صورت مجاز بودن، اجازه استفاده از سرویس به کاربر داده می‌شود. برای ارسال کلمه عبور، از مکانیزم‌های رمزنگاری استفاده می‌شود تا برنامه‌های بو کننده نتوانند به راحتی به اصل اطلاعات دست یابند.

ضعف پروتکل

یکی از روش‌های نفوذ در شبکه‌ها، استفاده از ضعف‌های امنیتی موجود در پروتکل‌های ارتباطی است. امنیت یک پروتکل بستگی به این دارد که آیا در طراحی آن اهداف امنیتی مدنظر بوده است یا نه؟ پروتکل‌های موجود از نظر برقراری امنیت شبکه با هم تفاوت‌های زیادی دارند. هر چه درجه امنیتی یک پروتکل زیاد باشد، از کارآیی و انعطاف کمتری برخوردار خواهد بود. به این دلیل پروتکل‌ها حد پایینی از امنیت را خود انجام می‌دهند و عمدهٔ کار را به عهدهٔ برنامه‌های کاربردی می‌گذارند و در حال حاضر عمدهٔ دلیل رشد هکرها در اینترنت، وجود ضعف‌های امنیتی در پروتکل TCP/IP است. این پروتکل از انعطاف‌پذیری خوبی در ارتباط بین شبکه‌ای برخودار است اما در عوض دارای ضعف‌های امنیتی عمده‌ای است.

فاش شدن اطلاعات

وقتی دو نقطه انتهایی در شبکه با هم ارتباط برقرار کرده و اطلاعاتی را به هم منتقل می‌کنند، فرض بر این است که جز دو فرد فوق، فرد سومی اطلاعات را نمی‌بیند. اگر یک هکر اطلاعات دیگران را بررسی کند، می‌تواند موجب تهدید باشد. در یک ارتباط اطلاعات سری، کلمه عبور و سایر اطلاعات رد و بدل می‌شود. در شبکه اینترنت این ضعف با قوت زیادی وجود دارد. بخاطر عمومی بودن شبکه، دروازه‌های بین راه لزوماً امن نیستند. یک هکر می‌تواند بااستفاده از به یک دروازه حساس تمام اطلاعات عبوری را شنود کند. در پروتکل‌هایی که از رمزنگاری استفاده نمی‌کنند این مساله نمود بیشتری پیدا می‌کند. یک هکر بدون هیچ مشکلی تمام اطلاعات را بررسی کرده و اطلاعات مور دنیاز برای یک حمله نرم‌افزاری را استخراج می‌کند.

انکار سرویس

یک نوع دیگر تهدید در شبکه‌ها، مختل کردن سرویس‌ها است. یک هکر می‌تواند با ارسال اطلاعات بسیار حجیم توسط پست الکترونیک یا سرویس انتقال فایل به یک کارگزار، حافظه آن را پر کرده و آن را از کار بیندازد.

روش‌های برقراری امنیت شبکه

امنیت شبکه‌های کامپیوتری از یک طرف به امنیت معماری پروتکل مورد استفاده در نقاط انتهایی و میانی یک اتصال و از طرف دیگر به امنیت کانال‌های ارتباط متعددی که اتصال بین مبدأ و مقصد را فراهم می‌آورند؛ مربوط می‌شود. معماری پروتکل مورد استفاده در نقاط واسط بین کاربر مبدأ و کارگزار مقصد، معمولاً یکسان بوده و با معماری لایه‌بندی منطبق است. TCP/IP به عنوان رایج‌ترین معماری پروتکل‌های ارتباطی شبکه‌های کامپیوتری دارای پنج لایه است که دو لایه زیرین (یعنی لایه‌های فیزیکی و پیوند داده) دارای یک استقلال ماهوی از لایه‌های بالاتر بوده و تنها لازم است واسط ارتباطی درستی را با لایهٔ بالاتر فراهم آورند.

وظیفه دو لایه زیرین فراهم آوردن یک ارتباط مطمئن در سطح کامپیوترهای همسایه‌ای است که به یک کانال ارتباطی یکسان متصل هستند. واحد تبادل در سطح لایه پیوند داده قاب (Frame) است و گسترهٔ جغرافیایی مدیریت آن از یک شبکه تجاوز نمی‌کند و مسائل امنیتی قابل توجهی درخصوص آن مطرح نیست. بر این اساس، امنیت پروتکل ارتباطی شبکه‌های گسترده مبتنی بر TCP/IP در سطح بسته (Packet) و واحدهای بزرگتر تبادل داده یعنی اتصال (Connection) و فایل از یک طرف و در محدودهٔ لایه‌های شبکه، انتقال و کاربرد از طرف دیگر مطرح می‌شود. کاربر از طریق لایهٔ کاربرد، اتصال خود را با یک کارگزار (در سطح لایهٔ کاربرد ماشین مقصد) برقرار می‌کند. کلیهٔ مبادلات داده‌ای و کنترلی لازم برای انجام یک کار از

طریق لایه‌های روی هم قرار گرفته به سطح لایه فیزیکی منتقل شده، جریان داده‌ای معکوس آن نیز از طریق لایه فیزیکی به لایه‌های بالاتر منتقل می شود لذا امنیت پروتکل مورد استفاده به دو مورد زیر مربوط می شود :

- **امنیت کاربردها:** کاربردها را می‌توان به دو دسته کاربردهای خاص و عام تقسیم کرد. امنیت کاربردهای خاص – کارفرما / کارگزار – بستگی کامل به ماهیت آن کاربرد داشته، نمی‌توان تمهید عمومی قابل استفاده در آنها را از پیش طراحی کرد. البته در این خصوص امکان تهیه یک کتابخانه ارتباطی امن وجود دارد. کاربردهای عام ارتباط محیطهای اینترانت و اینترنت در کاربردهای جدید شبکه و ایده‌هایی نظیر ادارات بدون کاغذ شامل پست الکترونیکی، تور جهان‌گستر، سرویس انتقال فایل و ورود از راه دور می‌باشند. درخصوص این کاربردها، بایستی نرم‌افزارهای مناسبی برای طرف کارفرما و طرف کارگزار تهیه شود که با استفاده از روش‌های رمزگذاری و هویت شناسی درخصوص امنیت کانال‌های ارتباطی، امنیت انتها به انتها را فراهم می‌آورد.
- **امنیت پیاده‌سازی:** منظور اطمینان از صحت کد از نظر انجام وظایف تعیین شده هر لایه و عدم امکان نفوذ، تهاجم و احتمالاً هکری است. این کار تنها با بازبینی، اصلاح، و ارتقاء منبع پیاده‌سازی از پروتکل انجام می‌شود.

امنیت در لایه‌های مختلف شبکه

با توجه به تاکید TCP/IP بر سه لایهٔ بالاتر شبکه، انتقال و کاربرد، پروتکل‌هایی برای فراهم آوردن امنیت در این سه لایه فراهم آمده است. در لایهٔ شبکه، IPSec (Internet Protocol Security) به عنوان یک امکان در کنار IPV6 (نسخه ۶ از پروتکل IP) طرح شده است که رمزنگاری و هویت‌شناسی را در سطح بسته‌هایIP فراهم می‌آورد.

در لایه انتقال، دو پروتکل SSH (Secure Shell) و SSL (Secure Socket Layer) مطرح هستند و یک تونل امن برای ارتباط کاربردها فراهم می‌کنند. نسخه‌هایی از نرم‌افزارهای Ftp و Telnet مبتنی بر SSH و SSL در دنیا بوجود آمده است. به منظور رفع اشکالاتSSL و یکپارچه‌سازی روش‌های امنیتی در سطح لایهٔ انتقال، پروتکلTIS (Transport Layer Security) در حال تدوین و پیاده‌سازی است که کلاً یک لایهٔ امنیتی واحد در سطح لایه انتقال فراهم آید. در عین حال کار روی SSH به عنوان رقیبی برای TIS همچنان ادامه دارد.

در سطح لایهٔ کاربرد نیز بسته به مورد اقداماتی انجام شده است که از آن جمله می‌توان به ETS (Electronic Transaction Secure) برای کاربردهای مالی اشاره کرد.

امنیت کانال‌های ارتباطی

کانال‌های ارتباطی در معرض دید و شنود مهاجمین قرار دارند بنابراین استفاده از مکانیزم‌هایی در جلوگیری از فاش شدن اطلاعات ضروری به نظر می‌رسد. روش‌های مختلفی برای برقراری امنیت شبکه وجود دارد که در ادامه بطور مختصر، به چند روش اشاره خواهد شد:

- **رمزنگاری:** مهمترین روش جلوگیری از نشت اطلاعات، رمزنگاری است. از این روش، برای محرمانه‌کردن داده‌های در حال عبور استفاده می‌شود. رمزنگاری می‌تواند در سطوح مختلف لایهٔ شبکه، لایهٔ انتقال و لایهٔ کاربرد انجام شود. هر چه سطح رمزنگاری پایین‌تر باشد عمومی‌تر ولی محدودتر است. لازم به ذکر است که رمزنگاری در هر سطح از شبکه که انجام شود موجب افزایش بار کاری کانال ارتباطی خواهد بود در لایه‌های نرم‌افزاری کاربرد رمزنگاری توسط برنامه‌های کاربردی که اطلاعات خود را از طریق شبکه منتقل می‌کنند انجام می‌شود. در لایه‌های پایین‌تر شبکه نیز استفاده از پروتکل‌هایی نظیر SSL و IPSEC می‌تواند ارتباطات شبکه‌ای را امن کند. پیغام محافظت نشده، متن ساده نامیده می‌شود. فرایندی که طی آن متن ساده به متن رمز شده تبدیل می‌شود، رمزگذاری خوانده می‌شود. الگوریتمی که برای گشودن رمز بکار می‌رود، رمز گشایی نامیده می‌شود. رمزگذاری و رمزگشایی به وسیله کلیدهای رمزنگاری انجام می‌شوند. بسته به نوع سیستم رمزنگاری ممکن است کلیدهای رمزگذاری و رمزگشایی با هم مساوی و یا متمایز از یکدیگر باشند. اگر این دو کلید یکسان باشند، سیستم رمزنگاری متقارن یا کلید سری (Secret Key) است، در غیر اینصورت سیستم رمزنگاری، نامتقارن یا کلید عمومی (Public Key) نامیده می‌شود.
- **هویت‌شناسی:** برای شناسایی افراد و تعیین اعتبار ارتباطات از هویت‌شناسی استفاده می‌شود. غالباً در این روش از رمزنگاری استفاده می‌شود و با الگوریتم خاصی در ابتدای اتصال با رد و بدل کردن چند پیغام مشخص، طرفین یکدیگر را شناسایی می‌کنند.
- **ثبت رویداد:** در بسیاری از موارد، حملات قابل پیش‌بینی و پیشگیری نیستند و رویدادنگاری می‌تواند مدیران را در ترمیم خرابی یا پیگیری و ردیابی حملات کمک نماید.
- **مهاجم‌یاب شبکه:** این سیستم وظیفه دارد که با نظارت بر مبادلات اطلاعات روی شبکه، در صورت بروز حمله، آن را تشخیص داده و اقدامات لازم را در مورد آن انجام دهد. اقدامات مهاجم‌یاب شبکه می‌تواند از خنثی‌سازی حمله تا اطلاع آن به مدیر شبکه، متنوع باشد.

- **دیوار آتش (Firewall):** با وجود همه روش‌های ذکر شده در بالا، تضمینی به برقراری کامل امنیت وجود ندارد و نیاز به روشی جامع برای کنترل امنیت ترافیک عبوری، اعمال سیاست‌های امنیتی سازمان و کنترل کاربران داخلی نیز وجود دارد. حفاظ، یک نرم‌افزار یا ترکیبی از نرم‌افزار و سخت‌افزار است که با قرار گرفتن در محل اتصال یک شبکهٔ محلی به شبکهٔ سراسری، ارتباطات و تبادلات داده‌ای میان دو سوی خود را کنترل می‌کند و روش بسیار مناسبی برای تامین امنیت شبکه‌های محلی به شمار می‌رود.

تحول در ساختار تصمیم‌های تجاری

بانگاهی اجمالی به وضعیت گسترش فن‌آوری اطلاعات در می‌یابیم این فن‌آوری مسائل اقتصادی و اجتماعی جهان را تحت تاثیر خود قرارداده و ساختارهای تجاری را دستخوش تغییر و تحول نموده است . این تغییر و تحول را می‌توان در موارد زیر جست‌وجو نمود :

مقرون به صرفه تر شدن پهنای باند در مقایسه با فن‌آوری کامپیوتر

ظرفیت شبکه در مقایسه با ظرفیت حافظه و انبار ذخیره سازی با سرعت بیشتری افزایش خواهد یافت که بر اثر آن، تغییر نسبتاً چشمگیری در محاسبه هزینه نسبی پردازش راه دور در مقابل پردازش محلی به وجود خواهد آمد. دسترسی به پهنای باند ارزان و فراوان حرکت در جهت خدمات شبکه‌ای متمرکزتر را با استفاده از مدلهای پردازش شبکه‌ای و دستگاه‌های مشتری کوچک هموار خواهد کرد.

بین شرکتی شدن اغلب برنامه‌های کاربردی

تکامل تدریجی برنامه‌های کاربردی و میان افزارها، در جهت معماری نرم افزارهای تطبیقی پیش می‌رود که بلافاصله و با حداقل دردسر پیکربندی باشند. این فرایافت در راستای تکامل مدل نرم‌افزاری است که مجموعه نرم‌افزارهای برنامه‌ریزی منابع شرکت‌ها و زنجیره برنامه‌های کاربردی اقتصادی شامل بخشهای مختلف فعال در یک سیستم را تولید کرده است.

چنین تحولاتی در دنیای نرم‌افزارها، به عهده خدمات وب است و چنانچه به واقعیت تبدیل شود قابلیت اتصال و اجرا برای پیکربندی برنامه‌های کاربردی افزایش خواهدیافت.

شکوفایی اقتصاد کلان بر اثر ظهور سیستم‌های بین شرکتی

چنانچه یکپارچگی برنامه‌های کاربردی در بین شرکت‌ها محقق گردد، کارایی آن در کل نظام اقتصادی منعکس خواهد شد. بر اساس این استدلال، شرکتهایی که از طریق بخش صنعت یا یک زنجیره ارزشی دیگر با یکدیگر ارتباط تنگاتنگ دارند باید در واقع شاهد افزایش کارایی و تاثیر آن بر

اقتصاد کلان باشند. اگر دولت از این فرآیند تجاری پیروی کند و معماری فناوری را بپذیرد، آیا می‌توانید مجسم کنید که میزان صرفه جویی و کارایی تا چه حد افزایش خواهد یافت؟

بازخرید میلیون‌ها کارمند توسط شرکتهای موفق حتی در شرایط خوب اقتصادی

پیش‌بینی می‌شود در صورت افزایش کارایی ناشی از انجام اصلاحات IT و به مرحله سودآوری رسیدن شرکتها در حد متعادل، طبیعی است که نیروی کار باید کاهش یابد. به عبارت دیگر، فن‌آوری نیز مانند صنعت کشاورزی به نقطه‌ای خواهد رسید که در آن خودکار سازی سیستم IT، نیازمندیهای نیروی کار را به میزان چشمگیری کاهش خواهد داد.

این پیش‌بینی حاکی از این است که کارمندان این فن آوری باید در حیطه‌های دیگر به دنبال کار باشند. با توجه به تعداد زیاد کارمندانی که در بحران اقتصادی سالهای گذشته بازخرید شدند، انتظار می‌رود که یک تکان یا واکنش، بازار محصولات و مهارتهای IT را گسترش دهد و مؤسسات بعضی از این افراد را دوباره بعنوان نیروی کار فراخوانند. به نظر می‌رسد که این دو نیروی مخالف ظرف چند سال آینده با یکدیگر به تقابل خواهند پرداخت و اکثر مؤسسات احتمالاً قادر نخواهند بود قبل از به پایان رسیدن نیمه دوم این دهه، اختلاف نظرها را از فرآیندهای خود دور سازند.

اتحاد بیشتر تولید کنندگان در بسیاری از بخشهای اقتصادی

تا سال ۲۰۰۴ در اکثر بخشها دست کم یک تولید کننده مهم بر اثر ورشکستگی یا ادغام با یک شرکت دیگر، ناپدید خواهد شد. این پیش‌بینی مخاطره آمیز نیست. در این مدت تعداد بیشتری از شرکتهای مهم منحل خواهد شد و شرکتهای بزرگ، شرکتهای کوچک را از صحنه خارج خواهند کرد. همچنین صنعت در یک دوره به دست عده معدودی از بازاریان خواهد افتاد که در آن تعداد انگشت‌شماری از تولید کنندگان در بازار به برتری خواهند رسید و به احتمال زیاد تا سال ۲۰۰۷ چرخه ابداع و رشد دوباره آغاز خواهد شد.

تبدیل بانکها تا سال ۲۰۰۷ به مهمترین تامین‌کنندگان خدمات حضوری

خدمات حضوری می‌توانند اولویت‌ها، اطلاعات و تجربه‌های شخصی شما را در اینترنت سازماندهی کنند. از نظر گارتنر، " اینترنت یک کلیکی" در راحت‌تر کردن و افزودن بر قابلیت همراهی اینترنت نقش مهمی ایفا خواهد کرد. سایتهای مایکروسافت AOL، Liberty Alliance ،(Passport)، Yahooو

سایرین برای به دست آوردن حضور شما با یکدیگر رقابت می‌کنند. اما گارتنر پیش‌بینی می‌کند که آینده به شرکتهای مستقل یاتامین کنندگان خدمات مالی (از قبیل بانکها) تعلق خواهد داشت.

سالهاست که بانکها به ناگزیر مدیریت مسائل امنیتی، شخصی و مسائل مربوط به جلب اعتماد را بر عهده گرفته‌اند و این میراث به ویژه در عصر دیجیتال از اهمیت خاصی برخوردار است. بنابر پیش‌بینی گارتنر بانکها تا سال ۲۰۰۷ از ۷۰ درصد شانس موفقیت برای تجارت حضوری برخوردار خواهند بود. گارتنر پیش‌بینی کرده است که بانکها در پذیرش چیزی مثل آزادی یا گذرنامه (Liberty or Passport) به عنوان چارچوب زیربنایی برای بخش واسطه سپرده‌ها نقش مهمی ایفا خواهند کرد.

تغییر گرایش از ساختارهای متمرکز به ساختارهای غیر متمرکز در صنعت کامپیوتر

تمرکز بیشتر بخشهای IT از سال ۲۰۰۴ تغییر کرده و این بخشها از یک مدل غیر متمرکز تر پیروی خواهند کرد. اهداف تجاری به جز کنترل هزینه‌ها، مسئولیت تصمیم‌گیری را به واحدهای تجاری واگذار خواهد کرد زیرا در این واحدها، سرعت عمل یک عامل با ارزش محسوب می‌شود و رشد اقتصادی در آن نهفته است.

چک الکترونیکی (e-Cheque)

بکارگیری اینترنت و شبکه‌های کامپیوتری گسترده باعث تحولات چشمگیری در عرصه تجارت شده است. ساده‌ترین تعریف برای تجارت الکترونیکی " انجام مبادلات تجاری در یک قالب الکترونیکی به صورت online روی اینترنت" است. سرعت کارآیی، کاهش هزینه‌ها و بهره‌برداری از فرصتهای زودگذر مزایایی است که استفاده از تجارت الکترونیکی را گریزناپذیر می‌سازد. یک فرآیند کامل در تجارت الکترونیکی شامل بازاریابی، مذاکره، قرارداد و تنظیم توافق‌نامه، پرداخت و تحویل کالا و پشتیبانی است. در بین این مراحل، پرداخت الکترونیکی نقش بسیار حساس و کلیدی را ایفا می‌کند و این امکان را بوجود می‌آورد که عمل پرداخت به سهولت، ارزان، سریع و با امنیت قابل قبولی در محیط اینترنت انجام شود.

سیستم‌های پرداخت الکترونیکی

امروزه در دنیای کسب و کار، روش‌های متفاوتی برای پرداخت به کار گرفته می‌شود. این روشها شامل پول نقد، کارت اعتباری، کارت پیش پرداخت، چک و انتقال وجوه بدهکار، بستانکار می‌گردد. برای مشابه سازی الکترونیکی هر کدام از این روشها، پروتکل‌هایی توسط مؤسسات و مراکز تحقیقاتی ارائه شده

است که در مراحل تحقیقاتی و استفاده آزمایشی قرار دارند. یک سیستم پرداخت الکترونیکی باید امکان استفاده از تمام روش‌های پرداخت را در اختیار کاربران قرار دهد و علاوه بر ویژگیهای پرداخت سنتی، دارای امکاناتی باشد که در محیط الکترونیکی و اینترنت مورد استفاده قرار گیرد. مهمترین ویژگیهای سیستم پرداخت الکترونیکی به شرح زیر است:

– اختفا: مشخصات افراد در سیستم آشکار نباشد.

– سادگی کار: روند کار پیچیده نباشد و مشتری بطور مؤثر، کارآمد و با رضایت بتواند به سادگی خرید کرده و پرداخت خود را انجام دهد.

– کارآیی: سرعت و کارآیی سیستم باید در حد مطلوب باشد. همچنین ترافیک حاصل از تعداد زیاد معاملات خرد، کارآیی را پایین نیاورد و پیچیدگی پروتکل در حد مطلوب باشد تا هزینه پردازش تعامل‌ها هم برای معاملات خرد و هم برای معاملات کلان منطقی باشد.

– قابل اطمینان بودن: سیستم هموار در دسترس باشد.

– امنیت: از حملات مصون بوده و امکان جعل وجود نداشته باشد.

– اعتماد: درجه امنیت پول و اطلاعات افراد در سیستم، بالا باشد.

– قابلیت ردگیری: یعنی سادگی ردگیری جریان پول و مسیرهایی که توسط مشتری طی می‌شود. اختفاء ارتباط مستقیمی با قابلیت ردگیری دارد.

– مقیاس پذیری: زیر ساختار سیستم باید مقیاس پذیر باشد و ازدیاد مشتریان یا فروشندگان، کارآیی سیستم را پایین نیاورد و مستلزم نصب سخت افزار اضافی نباشد.

– نوع مجوز: انجام پرداخت بدون نیاز به اتصال به مرجع مرکزی، مربوط به این بخش است.

– قابلیت انتقال: یعنی کاربر قابلیت پرداخت، بدون دخالت شخص ثالث (بانک) را داشته باشد.

از آنجا که افراد می‌توانند به سادگی نسخه مجددی از داده‌ها را در کامپیوتر خود تولید کنند، بدون دخالت شخص ثالث برای تصدیق فرآیند پرداخت، پرداخت وجوه جعلی امکان‌پذیر می‌شود. لذا تاکنون امکان پیاده سازی قابلیت انتقال در سیستم‌های پرداخت الکترونیکی محقق نشده است.

سیستم‌های پرداخت الکترونیکی از نظر نحوه انتقال پول به دو نوع تقسیم می‌شوند:

– پرداخت از طریق حساب بانکی و پرداخت به صورت مستقیم در سیستم‌های پرداخت از طریق حساب بانکی هویت پرداخت کننده مخفی نیست. این روش به دو صورت اعتباری و یا پیش پرداخت انجام می‌شود. در مدل پیش پرداخت، مشتری باید در حساب خود اعتبار کافی داشته باشد و موقع انجام معامله، مبلغ مورد نظر از

حساب او کسر می‌شود. در مدل اعتباری، صورت حساب‌ها توسط بانک به آدرس مشتری ارسال می‌شود و او بعداً صورت حساب را می پردازد. در سیستم‌های پرداخت به صورت مستقیم (یا پول نقد الکترونیکی) مشتری، اعتبارات از شرکت مربوطه خریداری کرده و با ذخیره در کارت هوشمند یا دیسک کامپیوتر، از آنها برای پرداخت استفاده می‌کند.

– پول نقد الکترونیکی به دلیل مکانیزم‌های امنیتی ساده برای پرداختهای کلان بازرگانی مناسب نیست. پرداخت با کارت اعتباری نیز مستلزم آن است که فروشگاه یا فروشنده، حساب بانکی ویژه تجارت الکترونیکی، در یکی از معدود بانکهایی که این گونه حسابها را می‌پذیرند، داشته باشد، علاوه بر آن، هنوز مجوز صدور و استفاده از کارتهای اعتباری در نظام بانکداری اسلامی کشور فراهم نیامده است. لذا، با توجه به وسعت استفاده از چک کاغذی در کشور، پیاده سازی چک الکترونیکی، ضمن میسر ساختن پرداخت الکترونیکی در کشور، می‌تواند مقدمه‌ای برای پیوستن به بازارهای جهانی باشد.

مدل چک الکترونیکی

پرداخت چک به روش سنتی، بصورت ارائه چک کاغذی در تاریخ ذکر شده بر روی چک که با توافق طرفین معامله درج شده، با برداشت از حساب مشتری و واریز به حساب فروشنده صورت می گیرد. در هیچ یک از دو نوع چک کاغذی و الکترونیکی، قابلیت انتقال وجود ندارد و شخص نمی‌تواند بدون دخالت شخص ثالث (بانک)، پرداخت کند. در میان ابزارهای پرداخت، چک، بار اضافی نسبتاً زیادی از نظر هزینه پردازش دارد. در چک الکترونیکی نیز همانند چک کاغذی هویت افراد مرتبط در فرآیند واگذاری و دریافت، مخفی نمی‌ماند اما پایین بودن هزینه پردازش و تسویه چک الکترونیکی به دلیل سود جستن از ارتباطات الکترونیکی به جای ارتباطات سنتی، استفاده از آن را توجیه پذیر می‌سازد. دیگر آنکه، در صورت کسب گواهی دیجیتالی از سازمانهای بین‌المللی، علاوه بر گواهی‌های بین بانکی، می‌توان بر خلاف چکهای کاغذی، از چک الکترونیکی برای پرداختهای خارجی استفاده کرد. مفهوم سیستم‌های چک الکترونیکی بر اساس روش چک سنتی است و پردازش الکترونیکی آنها به دو گونه زیر امکان پذیر است:

۱- جابجایی الکترونیکی چک

در این حالت، بانک پس از وصول چک کاغذی، اطلاعات روی آن را به صورت الکترونیکی به مرکز مبادلات بانکی می‌فرستد و چک‌های کاغذی را بایگانی می‌کند بدین طریق انتقال چکها بین بانک‌ها

حذف می‌شود و هزینه پردازش چک کاهش و امنیت تسویه بین بانکی افزایش می‌یابد. اطلاعات روی چکها توسط حروف خوان مغناطیسی یا بصورت دستی به سیستم وارد می‌شود.

سیستم‌های e-cheque, Net-Cheque از این گونه هستند.

همچنین روش دیگری وجود دارد که تصویر هر دو طرف بین بانک‌ها مبادله می‌شود. در این خصوص، الگوریتم‌های مورد استفاده برای فشرده سازی تصویر، علاوه بر امنیت مبادله حائز اهمیت هستند. امکان پیاده سازی چنین سیستمی در پروژه PACES در دست بررسی است.

۱- تولید و پردازش چک الکترونیکی

مفهوم چک الکترونیکی توسط FSTC (کنسرسیوم فن آوری سرویس‌های مالی) پایه گذاری شد و رمزنگاری گواهی دیجیتالی و کارتهای هوشمند را برای تامین امنیت به خدمت گرفت. برای اینکه سیستم مورد اعتماد باشد هر کدام از مشتریها، فروشندگان و بانکها، دارای گواهی دیجیتالی و دو کلید عمومی و خصوصی هستند. بانکها به عنوان مرجع صدور گواهی عمل کرده و برای مشتریان گواهی صادر می‌کنند.

امنیت پولهای الکترونیکی

امروزه پرداخت به صورت online یکی از مهمترین ارکان تجارتهای مبتنی بر وب یا به عبارت بهتر e-commerce را تشکیل می‌دهد. از جمله بحث‌های مطرح در این راه، بحث ایمن سازی عملیات پرداخت است. در زیر روشهای ایمن سازی پول الکترونیکی معرفی شده‌اند:

- عملیات پرداخت غیر قابل ردیابی

معمولاً در دنیای واقعی پس از دریافت پول از بانک یا هر ارگان دیگری، شماره سریال‌های اسکناسهای دریافتی را یادداشت نمی‌کنیم. اما در دنیای دیجیتال، وضع به گونه‌ای دیگری است. هر پول الکترونیکی دارای یک شماره سریال منحصر بفرد است و در هر عملیات پرداخت، ناگزیر به ثبت آنها در فرمهای ویژه‌ای خواهیم بود. اما اشکال عمده این سیستم بدین صورت است که افراد سودجو و متقلب قادر خواهند بود علاوه بر رویت و دزدیدن شماره‌های سریال واقعی پول‌های الکترونیکی، هویت شما را نیز شناسایی کرده و در اهداف سودجویانه خود بکار گیرند. برای جلوگیری از این امر، راه حلهای متعددی طراحی و ایجاد شده است.

۱- امضای مخفی (Blind Signature)

این مکانیزم برای اولین بار توسط دکتر چام ایجاد شد. مبنای این سیستم بر مخفی و مبهم کردن هویت پرداخت کننده و نیز کدگذاری شماره سریال‌های واقعی است. مراحل کار به این صورت است که ابتدا شماره‌های سریال به کد تبدیل می‌شوند، سپس امضای پرداخت کننده مخفی می‌شود (تمام مراحل توسط نرم‌افزار صورت می‌گیرد) و در نهایت، فروشگاه شماره‌ها را از حالت کد خارج کرده و پس از اطمینان از صحت پرداخت، خدمات درخواستی را ارایه می‌دهد. اشکال عمده این سیستم، لزوم ارتباط همزمان مشتری با بانک ناشر است.

۲- اعتبارات تبادلی

در این روش عنصر سومی به نام سرور مالی به سیستم افزوده می‌شود که وظیفه آن معاوضه اعتبارات مجازی با اعتبارات اصلی است و به پرداخت کننده امکان می‌دهد از اعتبارات مجازی در معاملات استفاده کند. این سرویس دهنده باید مورد اعتماد دو طرف (فروشنده و خریدار) باشد. این روش به دلایل زیر از روش امضای مخفی ضعیفتر است:

- لزوم یافتن یک سرویس دهنده قابل اعتماد
- بالا نبودن ایمنی از لحاظ فاش شدن هویت پرداخت کننده
- حفاظت از مصرف دوباره اعتبارات
- چون این اعتبارات فقط در عالم دیجیتال معنی پیدا می‌کنند، ممکن است اشخاصی به مصرف مجدد آنها مبادرت ورزند. برای جلوگیری از این امر، روش‌های زیر ابداع شده است:

۳- روش برداشت و انتخاب

در این روش از هر شماره سریال، چند شماره کد که دارای اندیس است تولید می‌شود. خریدار بطور اتفاقی یکی را انتخاب و از آن استفاده می‌کند. در مرحله بعد در صورتی که کسی مجدداً از آن شماره استفاده کند. به منزله بزرگتر شدن ظرفیت حافظه سیستم بوده و خطا محسوب می‌شود.

۴- قیم (Guardian)

در این روش، خریدار، کیف الکترونیکی را انتخاب می‌نماید که مورد اعتماد وی و فروشنده است. این کیف شامل یک محل ذخیره پول و یک قیم (یک ریز پردازنده ویژه) که وظیفه جلوگیری از مصرف اعتبارات را به عهده دارد است که البته تمام این موارد بصورت دیجیتالی هستند.

۵- امضای قیم

در این سیستم اعتبارات به دو بخش مکمل تقسیم می‌شوند. یک بخش، محل ذخیره کیف پول الکترونیکی و بخش دیگر در اختیار قیم قرار می‌گیرد. در هنگام پرداخت، وجود هر دو بخش در کنار هم الزامی است. (هیچکدام به تنهایی ارزش ندارد) و باید تأییدیه قیم را نیز به دنبال داشته باشد.

۶- امضای بانک منتشر کننده پول

در این روش چون عملیات کد گذاری اعتبارات توسط خود بانک ناشر پول انجام می‌گیرد، بنابراین نظارت بر عدم استفاده مجدد از اعتبارات و غیره به عهده خود بانک است.

۳- محافظت در برابر جعل اعتبارات

در دنیای واقعی، جعل اعتبارات امری دشوار و پر هزینه است اما در دنیای دیجیتال به علت خصوصیات منحصر به فرد محیط، این امر بسیار آسان است و تنها دغدغه خاطر متقلبین، ایجاد و ساخت شماره سریال‌های تقلبی است. اما همانطور که در گذشته نیز گفته شد با در اختیار داشتن شماره سریال های اصلی منتشر شده توسط بانک مربوطه، می‌توان صحت آنها را بررسی کرد.

۴- محافظت در برابر سرقت اعتبارات

مرسوم‌ترین روش برای جلوگیری از این امر، رمزگذاری اعتبارات است. اما در پاره‌ای از موارد به علت بالاتر بودن هزینه کدگذاری نسبت به ارزش خود اعتبارات، این کار مقرون به صرفه نیست که روشهای زیر برای جوابگویی این مساله ابداع شده است:

۱- حقوقی کردن اعتبارات

در این روش، اطلاعات شناسایی و حقوقی پرداخت کننده نیز به اعتبارات افزوده می‌شود اگرچه مشتریان ترجیح می‌دهند هویت آنها در مرحله پرداخت، ناشناس باقی بماند.

در این سیستم تا زمانی که مشتری خاصی از اعتبارات استفاده می‌کند، آن اعتبارات قانونی و قابل مصرف هستند. این سیستم با روش ذکر شده از مصرف دوباره اعتبارات ممانعت به عمل آورده و رسیدی را که حاوی جزئیات عملیات پرداخت است، به پرداخت کننده ارایه می‌دهد.

۲- اعتبارات خاص برای مشتری

در این روش، اعتبارات در گروه‌های مختلفی دسته‌بندی می‌شوند و هر دسته دارای تعدادی عضو است. بزرگی بیش از حد گروهها، بالارفتن امکان سرقت اعتبارات و کوچکی بیش از حد آنها، موجب عدم امکان پاسخگوئی به تمام خواسته‌های اعضا می‌شود. مکانیزم کار به این صورت است که ابتدا

ناشر پول برای پرداخت کننده یک حساب باز می‌کند و اعتبارات دیجیتالی که در این روش Pay word نامیده می‌شود، مخصوص وی ضرب می‌شود. مشتری در هنگام خرید، علاوه بر ارسال رمز اصلی، باید گواهی نامه Pay word را نیز ارسال دارد تا صحت تعلق اعتبارات به وی تایید شود.

۳- اعتبارات خاص مشتری و فروشنده

Millicent خانواده پروتکل‌های Online Micro payment در دنیای دیجیتال است. این پروتکل‌ها برای خریدهای کمتر از ۵۰ سنت مانند تولیدات الکترونیکی (مجلات، موسیقی و غیره) طراحی شده است. در این مدل، واسطه‌ها مورد اعتمادترین افرادی هستند که می‌توانید به بانک معرفی کنید. در این طرح، اعتبارات دیجیتالی، Scrip نامیده می‌شوند که شامل اطلاعات زیر هستند:

- مشخصات فروشنده، مشخصات خریدار، ارزش، تاریخ انقضا
- Scrip ID
- ID مشتری

این سیستم مشخصات، از سرقت یا مصرف مجدد آنها جلوگیری می‌کند. Scrip ها دارای گواهینامه و شماره سریال هستند که در هر نوبت خرید، باید اطلاعات با فرم های موجود تطبیق داده شوند.

امنیت در سیستم‌های پرداخت الکترونیکی

پروتکل Kerberos:

پروتکل Kerberos که یکی از ابزارهای امنیت در اینترنت است در سال ۱۹۸۶ در دانشگاه MIT پیشنهاد شد. هدف از این کار فراهم آوردن تائید اعتبار پرداخت و نیز صحت و درستی هویت کاربران می‌باشد. طراحی سیستم Kerberos به شرح زیر است:

- از تائیدیه‌های اعتباری از پرداخت یک طرفه (مشتری به فروشنده) و دو طرفه، پشتیبانی می‌کنند.
- تائیدیه اعتبار پرداخت، باید بدون انتقال کلمه عبورهای رمز گشایی شده یا متنهای واضح در اینترنت، قابل اجرا باشد.
- کلمه عبورهایی که رمزگشایی نشده‌اند، باید در میزبان قابل اعتماد ذخیره شوند.
- کلمه عبورها و متن‌های واضحی که توسط کاربران وارد می‌شوند باید مدت کوتاهی در حافظه نگاه داشته شوند و سپس از بین بروند.

- هر گونه تائیدیه اعتبار پرداخت از طریق اینترنت، باید عمر محدودی داشته باشد و در خلال این مدت، ممکن است تائیدیه اعتبار چندین بار مورد نیاز واقع شود.

یک کاربر و مشتری که قصد خرید در اینترنت دارد، خواهان استفاده از یک شبکه خدماتی امن می‌باشد. Kerberos به میزان زیادی توانسته است این امنیت را بر اساس اصولی که در بالا ذکر شد، ایجاد کند. Kereros برای هر سرویس گیرنده (Client) از طریق سرویس دهنده، یک بلیط اعتباری اختصاص می‌دهد.

این بلیط اعتباری شامل چهار بخش است:

۱- نام کاربران که توسط سرویس برای او ارسال شده است.

۲- آدرس ایستگاه کاری که شخص هنگام دریافت بلیط از آن استفاده می‌کند.

۳- کلید رمز مورد استفاده (Session key)

۴- تاریخ آغاز و پایان دوره اعتبار و ارزش بلیط

بطور خلاصه فرآیند تائید اعتبار در Keberos بدین گونه است که وقتی سرویس گیرنده، خواهان استفاده از یک سرویس ویژه باشد، باید یک بلیط دارای اعتبار خدماتی از سرویس اهدا کننده بلیط (TGS: Ticket Granting Service) دریافت کند اما سرویس گیرنده باید قبل از دریافت بلیط و قبل از تقاضای آن، اعتبار خود را در سرویس تصدیق کننده تایید کند. اگر تائید اعتبار با موفقیت انجام شود، سرویس گیرنده یک بلیط TGS و همچنین یک Session Key دریافت می‌کند.

در Kerberos، تصدیق اعتبار پرداخت در چهار سطح انجام می پذیرد.

- اولین آزمایشی که سرویس انجام می‌دهد، بررسی « قابل رمزگشایی بودن بلیط» دارای اعتبار است. اگر سرویس نتواند رمز بلیط را بگشاید، معلوم می‌شود که رمز وارد شده مربوط به یک کاربر حقیقی نیست ولی اگر رمزگشایی بلیط موفقیت آمیز باشد، سرویس درمی‌یابد که بلیط از جانب یک کاربر واقعی آمده است. این آزمایش به منظور ممانعت از دستیابی به شبکه خدماتی، از طریق بلیط جعلی است.
- دومین آزمایش Time stampو Lifespan مربوط به برگه دارای اعتبار است، که اگر مدت زمان ارزش آنها گذشته باشد سرویس خدماتی بلیط را باطل می‌کند. این آزمایش، کاربرانی را که قصد استفاده از بلیط‌های قدیمی یا بلیط‌های مسروقه را دارند، متوقف می‌کند.

- آزمایش سوم و چهارم شامل بررسی نام کاربر، اعتبار بلیط و همچنین آدرس ایستگاه کاری است. اگر آزمایش مردود شود، معلوم خواهد شد که کاربر بلیط شخص دیگری را در اختیار گرفته است و در این هنگام، سرویس، کاربر را متوقف می‌سازد. اگر تمامی موارد بالا درست باشند و صحت آنها بدرستی انجام پذیرد، سیستم تعیین می‌کند که فرستنده بلیط دارای اعتبار، به راستی صاحب واقعی آن است.

متاسفانه یکی از مشکلات عمده موجود این است که لزوماً حساب خریدار و فروشنده، در یک بانک مشابه نیستند و پرداخت پول و همچنین دریافت آن، از طریق چند سرویس دهنده حساب صورت می‌پذیرد.

از دیگر مشکلات Kerberos می‌توان به آسیب‌پذیری کلمه عبور و کلیدهای رمزگذاری (مادامی که توسط ایستگاه کاری ارایه و یا نگهداری می‌شوند) و همچنین نیاز به مطابقت ساعتها (مدت زمان اعتبار و ارزش بلیط)، اشاره کرد.

در مجموع و بطور خلاصه، سیستم Kerberos با تکیه بر فرض دو طرفه بودن تائید از طریق یک بلیط رمزگذاری شده که در سرویس دهنده حساب کاربر و مشتری باید مورد تایید قرار گیرد، عمل می‌کند.

مدیریت ارتباط با مشتریان (Customer Relationship Management)

امروزه تجارت الکترونیک تنها به فرآیند خرید و فروش محصولات محدود نمی‌گردد، بلکه ارایه خدمات و سرویس به مشتریان از جمله فعالیت‌های عمده در این حوزه محسوب می‌شود و نظر به اهمیت مدیریت ارتباط با مشتریان نرم‌افزارهای تحت نام CRM مورد بهره‌برداری قرار می‌گیرند.

با افزایش بکارگیری اینترنت و فاکس، موج دیگری از امکانات ارتباطی، سازمان‌هایی را که نیازمند برقراری ارتباط با مشتریان خود می‌باشند فرا گرفته است و مراکز Call centre تبدیل به مراکز چند رسانه‌ای موسوم به Contact centre و نهایتاً به Interactive Contact Centre گردیده‌اند.

Voice mail, Fax ،Voice over net Web callbacks, Web chat, web و Phone Calls از جمله کانال‌های ارتباطی موجود در حال حاضر می‌باشند.

بدین ترتیب با تبدیل مراکز تماس Call Centres، به Contact centres، مشتریان می‌توانند بجای استفاده از تلفن، فاکس و یا پست الکترونیکی از روش‌های دیگری نیز به دلخواه خود جهت برقراری ارتباط با فروشندگان و یا ارایه دهندگان خدمات، استفاده نمایند. از سوی دیگر نیز سازمانها و شرکت‌ها در تلاش بکارگیری راه حل‌های جامع در زمینه کسب و کار الکترونیکی می‌باشند تا بتوانند ضمن حفظ مشتریان خود،

خدمات بهتری را به آنها ارایه نمایند. آمارهای منتشر شده در رابطه با حجم مبادلات تجاری و یا ارایه خدمات، مبین اهمیت بکارگیری تکنولوژی تجارت الکترونیکی است.

چشم‌اندازها در این رابطه متحیر کننده است، پیش‌بینی می‌گردد طی کمتر از سه سال آینده۵۶ درصد تماس‌های مشتریان از طریق شبکه‌های وب صورت پذیرد و در مقابل تماس‌های تلفنی به کمتر از ۵ درصد کاهش یابد.

چه این آمار را باور داشته باشیم یا نداشته باشیم، بکارگیری مراکز تماس چند رسانه‌ای (Multimedia Contact centres) بسرعت جایگزین "Call Centre" ها خواهند شد و برای این انتقال، بکارگیری تکنولوژی کلیدی از جمله Unified Messaging و Web Integration اجتناب‌ناپذیر می‌باشد.

۲- پیام‌های یکسان (Unified Messaging)

انتظاری که مشتریان از شرکت‌ها دارند، پاسخگویی سریع به پست‌های الکترونیکی، فاکس‌ها و Voice mail می‌باشد، به همان فرمی که در تماس‌های فوری تلفنی بصورت هم زمان این پاسخگویی صورت می‌پذیرد.

مفهوم Unified Messaging خیلی ساده است، مراکز خدمات مبتنی بر Contact Centre تنها می‌توانند از طریق یک واسط کاربر فعالیت‌های ارسال و دریافت نامه‌های مبتنی بر پست الکترونیکی، Voice mail و پیام‌های فاکس خود را انجام دهد.

دریافت پیام‌های مذکور، ردیف کردن، توزیع، ردیابی و گزارش‌گیری آنها توسط Unified Messaging به همان شیوه‌ای که در مکالمات تلفنی انجام می‌گیرد، صورت می‌پذیرد.

بدین ترتیب با جمع‌آوری تمامی پیام‌ها در یک مکان، ارسال، ذخیره سازی و اولویت بندی آنها و همچنین مدیریت بر روی پیام‌های مشتریان بسیار ساده‌تر خواهد شد.

در سیستم‌های سنتی سرنوشت پست‌های الکترونیکی و فاکس مشخص است، تا زمانی که شخصی به آنها پاسخ ندهد، در سیستم انباشته می‌شوند، سرنوشت آنها زمانی وخیم‌تر می‌شود که به فراموشی سپرده شوند، در حالی که مراکز تماس می‌توانند با این درخواست‌ها بر اساس اولویت‌ها و درجه اهمیت واقعی هر پیام برخورد نمایند، درست همانند زمانی که پیام‌ها از طریق تلفن ارسال می‌گردند.

توانا سازی مرکز تماس (Call Centre) با استفاده از شبکه‌های اینترنت

امروزه مشخص گردیده است که خرید مشتریان و حجم و میزان آنها به نوع خدماتی که در فرآیند فروش ارایه می‌گردد بستگی داشته و از آن تأثیر می‌پذیرد. بطوریکه خرید انجام شده صرفاً و تنها به علت کیفیت یا ویژگی خود محصول نمی‌باشد. همچنین آمار نشان می‌دهد که در سال ۱۹۹۸ به علت عدم ارایه خدمات مؤثر بصورت online، تجارت ایالات متحده با ۱/۶ میلیارد دلار زیان مواجه گشته است. به همین دلیل فروشندگان الکترونیکی (e-retailers) اکنون دریافته‌اند که فروش on line به خودی خود بخش کوچکی از تجارت الکترونیکی را تشکیل می‌دهد در حالی که ارایه سرویس خوب به مشتریان است که تا مدت طولانی در ذهن و خاطر مشتریان باقی می‌ماند، از این رو عامل مهمی تلقی می‌گردد.

انتظار می‌رود Call centreها حداقل بطور مؤثر پیام‌های وارده را مدیریت نمایند تا از سرعت و صحت پاسخگویی به‌آنها اطمینان حاصل نمایند. یکی از عوامل عمده در فرآیند Call centre ها مسیریابی هوشمندانه پست‌های الکترونیکی است که به محض دریافت e-mail باید انجام شود.

در نتیجه، پاسخگویی به این نوع تماس‌ها در مقایسه با تماس‌های تلفنی مهارت‌های خاص خود را نیاز دارد. بعلاوه ، گفتگو از طریق web (web chat) که از قابلیت‌های افزوده شده در مراکز Contact Centre نسبت به مرکز Call Centre می‌باشد امکان تماس‌های Real time را برای مشتریان فراهم نموده است.

بدین ترتیب مشتریان مستقیماً با مراکز تماس (Contact Centre) تماس داشته و سؤالات خود را بصورت متن تایپ و ارسال نموده و پاسخ لازم را نیز بصورت متن از طریق همان مراکز دریافت می‌نمایند.

امکان ارایه راهنمایی‌های لازم به مشتریان از وظایف این مراکز بوده و این راهنمایی‌ها عمدتاً با در اختیار قرار دادن اتوماتیک آدرس‌های مناسب (URL) به مشتری و برحسب نیاز او انجام می‌پذیرد. این قابلیت به مدد نرم‌افزارهای خاص و در سایت Contact Centre صورت می‌پذیرد.

چنانچه مشتری انتظار دریافت کمک‌های شنیداری (voice) را داشته باشد قابلیت VON (voice over net) این امکان را به او می‌دهد تا با استفاده از کامپیوتر بتواند گفتگو انجام دهد.

محصولاتی مانند MSN messenger و Yahoo messenger بسادگی قابلیت chat ، voice chat و ایجاد کنفرانس بین چندین نفر را فراهم می‌سازد. این توانایی به مدد تکنولوژی voice over IP فراهم آمده است.

معمولاً مشتریان به منظور دستیابی به مراکز تماس (Contact centre) مناسب ترین و ساده ترین شیوه را انتخاب می‌نماید. اگر سابقاً استفاده از تلفن و فاکس شیوه‌های مناسبی برای مشتریان به حساب می‌آمد ، امروزه اکثر مشتریان با استفاده از امکانات تکنولوژی شیوه‌های جدیدتری را که مناسبتر و راحت‌تر می‌باشد انتخاب می‌نماید.

لذا بخاطر ارایه خدمات مناسب بکارگیری فن آوری unified message ، و " وب" بصورت یک الزام برای سازمانها درآمده است که در نهایت تکنولوژی را به سمت ارایه مراکز تماس چند رسانه‌ای واقعی و بصورت تعاملی تبدیل خواهد نمود.

مذاکرات تجاری در تجارت الکترونیکی

پشتیبانی از مذاکرات در سطح بین المللی نیازمند ترکیب روشهای تئوری تصمیم گیری با ابزارهای تکنولوژی ارتباطات باشد.

برای این کارسیستمهای پشتیبانی کننده مذاکرات باید انعطاف لازم را، برای کاربران با فرهنگ‌ها و زمینه‌های آموزشی گوناگون داشته باشند در ضمن رشد سریع و گسترده اینترنت و تجارت الکترونیکی بستر لازم را برای مذاکرات در سطح بین المللی بالاخص در جهت مبادلات تجاری ایجاد کرده است .

تجارت الکترونیکی بستر مناسبی را برای رشد و تکامل پدیده مذاکره و گفتگوی بین تمدن‌ها و فرهنگ‌ها و درنتیجه حرکت بسوی ایجاد سیستم‌های خودکار مذاکره فراهم می‌آورد . از این‌رو اهمیت آموزش مدیران و دانشگاهیان برای مذاکرات اینترنتی در زمینه مشارکت هرچه موثرتر در فرآیند جهانی شدن انکار ناپذیر می‌باشد. با توجه به اینکه شروع به یادگیری و کسب مهارت‌های اولیه در این سیستم‌ها بطوری طراحی شده‌اند که کاربران را متعلق به خود احساس میکند و یا به عبارتی دیگر کاربر احساس میکند که یک نسخه از سیستم در اختیار اوست، انرژی و زمان زیادی صرف آموزش کاربر نمی‌شود .

نهایتاً این سیستمها امکانات عدیده‌ای را برای افزایش قابلیت‌های مدیران در عرصه تصمیم گیری فراهم می‌کنند ، خصوصاً کاربردهای آن در بحث انتقال تکنولوژی برای کشورهای در حال توسعه می‌تواند از اهمیت ویژه برخوردار باشد.

محققان موضوع مذاکره،سیستمی بنام (Internet Intimation Negotiation) را طراحی و پیاده سازی کرده‌اند که می‌تواند پروژه‌های بین المللی مذاکره را پشتیبانی نماید . چکیده کارها در دو سیستم INSPRIRE (Internet Support for International Research Experiment) INSS (International Negotiation Support System) تجلی یافته است که اولی بیشتر برای مقاصد آموزشی و تحقیقاتی و دومی به عنوان نسخه تجاری در حال توسعه است.

کسب کار در تجارت الکترونیکی

تجارت الکترونیکی نامی عمومی برای گستره‌ای از نرم‌افزارها و سیستم‌ها است که خدماتی نظیر جستجوی اطلاعات، مدیریت تبادلات، بررسی وضعیت اعتبار، اعطای اعتبار، پرداخت به‌صورت بر خط، عملیات گزارش‌گیری و مدیریت حسابها و غیره را در اینترنت به عهده گیرند. این سیستم‌ها زیربنای اساسی فعالیتهای اقتصادی مبتنی بر اینترنت را فراهم آورند.

دسترسی به ابزارهای تجارت الکترونیکی برای مشتریان، خواه به‌صورت یک سازمان، این امکان را می‌دهد که آنها تأمین‌کنندگان و فروشندگان را در هرجایی که هستند یافته و با آنها به صورت الکترونیکی معامله کنند. در این حالت دو مسأله عمده و کاملاً مرتبط با هم که وضعیت فروشگاه‌های اینترنتی را پیچیده میکنند عبارتند از:

الف- افزایش قابل ملاحظه دسترسی به شرکتها

دسترسی به شرکتهایی که بتوانند نیاز مشتری را برآورده سازند، بطور قابل ملاحظه‌ای افزایش یافته است به همراه سعی وافر شرکتها در جذب مشتریان، آنها را با سردرگمی مواجه می‌کند.

ب- پیچیده‌تر شدن تصمیم‌گیری و مذاکره

با امکان دسترسی به بازارها از طریق اینترنت و سریع‌تر و وسیع‌تر شدن آنها فرآیندهای تصمیم‌گیری و مذاکره به دلایل مختلفی نظیر به میان آمدن فرهنگها، زبان‌ها و قوانین متفاوت پیچیده‌تر می‌گردد و در این میان نیاز به سیستمهایی احساس میگردد که نه تنها بتوانند معاملات ممکن را جستجو کنند بلکه بتوانند در مذاکرات تجاری بصورت مستقل درگیرشده و تصمیمات تجاری اتخاذ کنند . همچنین عدم تغییر مدلهای اقتصادی و تطبیق نیافتن آنها با شرایط متغیر امروزی پیچیدگی تصمیم‌گیری‌ها را چه برای افراد و چه برای طراحان سیستم‌های ذکر شده مشکل‌تر می‌کند.

جایگاه مذاکرات در تجارت

۱- مذاکرات در مدل زنجیره ارزش

مذاکره بین خریداران و فروشندگان با فعالیت‌های متعدد دیگری که در مدل زنجیره‌ای ارزش آنها وجود دارد، در ارتباط است. این فعالیتها موازی هم بوده و هم خریدار و هم فروشنده را درگیر می‌کند.

۲- اگر تأثیر تجارت را از دیدگاه خریدار بررسی کنیم و توجه خود را به سمت سه فعالیت اول یعنی کشف محصول، ارزشیابی و مذاکراه معطوف کنیم، در می یابیم که تجارت الکترونیکی تغیراتی کیفی در این فعالیت‌ها ایجاد میکند.

در مرحله کشف محصول، خریدار نیاز خود را مشخص می‌کند و به دنبال محصولاتی است که این نیاز را برآورده سازد. تجارت الکترونیکی این امکان را ایجاد می‌کند که او با بازارهای زیادی که قبلاً ناشناخته و غیر قابل دسترس بودند آشنایی پیدا کند. علاوه بر افزایش قابل ملاحظه فروشندگان ، او با مسایل دیگری نیز نظیر برخورد با فرهنگ‌ها و قوانین گوناگون مواجه است.

در مرحله ارزشیابی محصول، خواص محصول کشف شده مورد ارزیابی قرار می‌گیرد. در این مرحله محصول کشف شده بر اساس معیار مقایسه‌ای در این مرحله محصول کشف شده بر اساس ارتباط دیداری مستقیم مشتری با جنس صورت می‌گیرد. در تجارت الکترونیکی ارزشیابی مستقیم ممکن نیست و از این رو خریداران یا باید به دیگـران اعتماد کننـد و یا کالاها را با توجه به انواع مشـابه موجود بازارهای محلـی ارزیابی نماید.

در خلال فرآیندهای مذاکره، خریدار و فروشنده با هم به تبادل اطلاعات می پردازند. اگر مذاکره آنها فقط در مورد قیمت باشد، فرآیندی مانند مناقصه یا مزایده است و اگر روی دامنه وسیعتری از موضوعات نظیر وضعیت تضمین، زمان تحویل، زمان بندی پرداخت، چگونگی خدمات رسانی و غیره باشند آنگاه بطور خاص در حال دنبال کردن فرآیند مذاکره می باشند. نتیجه مذاکره اگر با توافق، یعنی رسیدن به نقطه نظرات مشترک همراه باشد می‌تواند منجر به دادن سفارش از جانب مشتری گردد. از این جنبه مرحله مذاکره دارای اهمیت زیادی است و می‌تواند پل ارتباطی برقرار شده بین مشتری و فروشنده را برای ادامه دادو ستد مستحکم کرده و به عبارت دیگر تکمیل بقیه مراحل زنجیره ارزش را تا حدود زیادی تضمین می‌کند. آژانس‌های نرم‌فزاری می‌توانند به استفاده‌کنندگان کمک کنند تا خیلی از پیچیدگی‌های مذاکره بصورت خودکار، مدل شده و از مشکلات روشهای سنتی بکاهند در ادامه بعضی از مفاهیم تئوری مذاکره که می‌تواند ما را در درک بهتر این پیچیدگی‌ها یاری کند، آورده شده است:

تعریف و مفاهیم

چند نمونه از از لغات و تعاریف آنها عبارتند از:

۱. **موضوع مذاکره** : یکی از مواد مورد علاقه طرفین برای مذاکره مثل قیمت، زمان تحویل و..... می باشد.

۲. گزینه (option) : یکی از مقادیری که یک موضوع در مذاکره مجاز است به آن نسبت داده شود و توسط کاربر تعیین می‌شود.

۳. بسته (package) : اگر به تمام موضوعات مذاکره مقداری از گزینه‌های مجاز را نسبت دهیم ، به مجموعه این مقادیر یک بسته می‌گویند.

۴. پیشنهاد (offer) : بسته‌ای است که توسط یک طرف مذاکره برای طرف دیگر ارسال می شود و پیشنهاد او برای مقادیر موضوعات به طرف مقابل نشان می‌دهد.

۵. **پیشنهاد متقابل (counteroffer) :** پیشنهادی که در جواب پیشنهاد طرف مقابل ارسال گردد.

۶. هدف (objective) : برداری است که هر مولفه آن تابعی از موضوعات مورد مذاکره بوده و مذاکره کننده علاقه‌مند است که این توابع بیشترین مقدار را داشته باشند .

۷. **ترجیحات** (preferences) : مشخص کننده اهمیت یک تابع هدف در برابر اهداف دیگر است . قسمتی از یک موضوع را به بهای از دست دادن قسمتی از موضوع دیگر بدست آورد .

۸ . داد و ستد (Trade off) : فرآیند مبادله‌ای که در آن مذاکره کننده قسمتی از یک موضوع را به بهای از دست دادن قسمتی از موضوع دیگر بدست آورد .

۹- **مطلوبیت** : معیاری است که به کمک آن پیشنهادات مختلف از نظر سطح دسترسی به مجموعه اهداف مورد ارزیابی قرار میگیرند. مطلوبیت بصورت زیر می‌باشد:

۱۰- **مخالفت** (Opposition) : معیاری است که مشخص کننده تفاوتهای طرفین مذاکره کننده در ارزشیابی‌هایشان از یک پیشنهاد می‌باشد.

تجارت بی‌سیم

در تاریخ فن آوری، هیچ پدیده علمی یا فنی امکانات و هیجانات فن آوری بی‌سیم را نداشته است. این پدیده نه تنها در برگیرنده بازگشت داده، تجارت الکترونیکی، پیغام رسانی و دسترسی به وب می‌باشد بلکه بوجود آورنده قدرتی خواهد بود که توسط آن بتوان با ارسال و دریافت امواج ماشینها وسایل دیگر را کنترل

کرد. لذا برای حداکثر بهره برداری از آیندهٔ بی‌سیم، آگاهی هر چه بیشتر از تولید این فن آوری و سرعت هجوم آن اهمیت زیادی دارد. فن آوری بی‌سیم، شیوهٔ فعالیتهای روزانه مردم را در تمامی وجوه تحت تأثیر قرار خواهد داد. با توجه به هدف شرکتهای سرمایهٔ گذاری در ارتباطات بی سیم و نرم افزارهای مبتنی بر داد و ستد، نام فن آوری جدید را تجارت الکترونیکی همراه Mobile Electronic Commerce یا m -Commerce نامیده‌اند.

بر اساس آمار تحلیل‌گران ، حدود ۲۵٪ از کاربران بی‌سیم با دستگاههای سیار خود، به نوعی با تجارت همراه درگیر خواهند بود که با توجه به گستردگی و نبوغ نرم‌افزارهای تجاری، تخمین ۲۵٪ بسیار کم می‌باشد چرا که فرض ما بر این است که در آینده هر اتفاقی که در تولید سخت‌افزار، نرم افزارهای کاربری رخ دهد، این است که وسیله باید بی‌سیم و قابل حمل باشد. مشکلات سر راه تولیدات و مسایل بی‌سیم که به آسانی در دستان جا بگیرند بسیار زیاد هستند. در مقام مقایسه با پروژه‌های مهندسی بزرگ، کل هزینه‌ها، مجموع ساعات کاری که در فن آوریهای بی‌سیم سرمایه گذاری شده است بسیار فراتر از مجموع همه سرمایه گذاریها در برنامه‌های فضایی ۴۰ سال گذشته است. بر اساس مطالعات انجام شده، تا سال ۲۰۰۰ ، تعداد کسانیکه برای ارتباط با اینترنت از تلفنهای همراه استفاده خواهند نمود بیشتر از کسانی است که از کامپیوتر استفاده می‌نمایند. علاوه بر تلفنهای بی‌سیم، PDA یا وسایل دیجیتال شخصی و کامپیوترهای اندازه کف دست، از کاربرد گسترده‌ای در تجارت و سایر زمینه‌ها برخوردار هستند.

- موارد دسترسی کنونی در تجارت الکترونیک:
- فهرست خدمات قابل دسترس مربوط به تلفنهای همراه محدود می‌باشد، ولی هر روز از گستردگی بیشتری برخوردار می‌گردد. در حال حاضر می‌توانید اخبار موثقی راجع به مسابقات ورزشی، اخبار سیاسی و گزارش آب و هوا کسب نمایید. POD ها در وسایل مشابه نیز پیشرفتهای قابل ملاحظه‌ای داشته‌اند و از آنها می‌توان برای ویرایش و ارسال داده‌ها، اسناد Wordو صفحه گسترده‌ها به سایر سایتها استفاده نمود بعلاوه تجارت بصورت محدود شروع گردیده است. البته وسایل ارتباط بی‌سیم بدون شک از پیشرفتهای فوق‌العاده زیادی برخوردار خواهند گردید و انتظار همگان بر این است که سایر توانائی‌ها و قابلیت‌های کامپیوتر شخصی را در تلفنهای همراه بیابند. در حال حاضر، کیفیت نمایش و عرض باند، اجازه انتقال راحت و آسان در یک وسیله بی‌سیم، بین آنچه که شما ایجاد، ذخیره، بازیابی و مشاهده می‌کنید را ، نمی‌دهد.

بر اساس تعریف، محل و مبدأ ورود بی‌سیم یک نقطه ورود سفارشی شده می‌باشد که از طریق این نقطه، مشترک بی‌سیم به سایتها و اطلاعات موجود در اینترنت دسترسی پیدا می‌کند. از نمونه‌هایی که در حال حاضر می‌توان برای میزبانان با سیم نام برد Yahoo، AOL هستند. این شرکتها مدل بازار مستحکمی را بر مبنای ورود از یک درب بنا نهاده‌اند. به نظر می‌رسد که مشتریان سهولت ورود از یک سایت (یک مبدأ) را برای رسیدن به اطلاعات مورد نیاز خود ترجیح می‌دهند. در واقع خواهان یک مدخل ساده بی‌سیم هستند که از لحاظ پرداخت صورت حسابهای خرید بدون مشکل باشد و بخوبی بتوانند آنرا کنترل کنند. بهرحال صورت حساب هزینه مدخلهای ورود بی‌سیم برای شما از طرق مختلف می‌تواند ارسال گردد، از طریق عضویت در خدمات، از طریق کاربر ارتباط بی‌سیم یا، از طریق کمیسیونی که به مرکز ارائه خدمات بی‌سیم خود پرداخت می‌نمایید. علیرغم انتظاری که از شرکتهای خطوط تلفن در دنیای ارتباطات و کامپیوتر و اینترنت می‌رفت، شرکت AOL با رشد فوق‌العاده خود سیطرهٔ خود را در دنیای کامپیوتر و تجاری مستولی نمود. اما قدرت ISP را در دست گرفتن تجاری مدخلهای بی سیم نباید دست کم گرفت که مهمترین خدمت در عرصهٔ مدخلهای بی‌سیم e-Mail است، با توجه به تغییر دادن آدرس e-Mail که چه قدر دشوار است AOL متجاوز از ۲۳ میلیون نفر مشتری که دارای e-Mail در تلفنهای همراه خود می‌باشند، موفق بوده است. با توجه به تمامی این موارد، بیشتر کارشناسان انتظار دارند که نه کاربرها و نه ISPها و یا شخص یا سازمان ثالث دیگری بر مدخلهای وب سیطره و کنترل تعیین‌کننده پیدا کنند . به احتمال زیاد ، ترکیبی از شرکتهای مختلف که بتوانند بهترین خدمات و شیوه کار را عرضه کننده در عرصه حضور خواهند داشت . از لحاظ دیدگاه جهانی، بازار تلفن همراه تا سال ۲۰۰۵ به تعداد دو میلیارد مصرف کننده خواهد رسید و با توجه به اینکه بیشتر کاربران از تلفن همراه خارج از ایالات متحده هستند ، انتظار می‌رود تأثیرات بیشتری روی مدخلهای بی‌سیم و تجارت همراه از ناحیهٔ اروپا و آسیا سر خواهد گرفت. اگر نقش مراکز ارائه خدمات اینترنت ISP ها را که در زندگی کامپیوتری اروپائیان نقشی محوری است نادیده بگیریم، همکاری ارتباط بین کاربردها، کارخانجات سازنده وسایل، فراهم کنندگان اطلاعات و بازرگانان می‌توانسته است بیشتر از این باشد. کارخانجاتی نظیر اریکسون و نوکیا در اسکاندیناوی با شرکتهای مشتری‌محور کار می‌کنند تا وسایل و تجهیزاتی را تولید کنند که پاسخگوی خواسته‌ها و نظریات مشتریان باشد. از طرفی توزیع جمعیت در اروپا و آسیا از تمرکز بیشتری برخوردار است و در نتیجه مردم شهر نشین بیشتری وجود دارند و همین نکته دو دلیل مهم را برای تأثیر و نفوذ بیشتر این بازارها در تولید مدخلهای وب و وسایل بی سیم، به بار

می‌آورد. در محیط بی سیم و سیار، مشتری در حرکت است و اگر شرایط مطابق میل وی نباشد، به راحتی حرکت خود را به جهت دیگری سوق می‌دهد. در تاریخ تجارت هرگز حق و حقوق مشتری، هرگز به اندازهٔ حق و حقوقش در تجارت به همراه نبوده و نخواهد بود. ایده موفقیت در Download کردن اطلاعات، می‌تواند به مشتریان نیز سرایت کند. مشتریانی که مشاهدات اطلاعات دریافتی را مطابق خواسته‌های خود نیابند به جای دیگری مراجعه خواهند کرد .

همانطور که قبلا گفته شد ، در حال حاضر، کیفیت نمایش و عرض باند اجازه انتقال راحت و آسان را در یک وسیله بی‌سیم، بین آنچه که شما ایجاد، ذخیره، بازیابی و مشاهده می‌کنید، نمی‌دهد. لذا بعنوان کاربر ، ما مجبور هستیم که فهم و درک و خواسته‌های خودمان را به هنگام استفاده از این وسایل، تغییر دهیم. معهذا، طراحان و مهندسین این وسایل ، تمامی تلاش خود را انجام می‌دهند تا رضایت مصرف کنندگان را فراهم نمایند.

وسایل بی‌سیم و قابل حمل نقش محوری در ارتباطات دنیای امروز ایفا می‌کنند و ارتباط آنها با اینترنت، ارتباطی منطقی به نظر می‌رسد. نسل جدیدی از وسایل بی‌سیم، اطلاعات موجود در اینترنت را در اختیار ما خواهند گذارد ، نه فقط به صورت اطلاعات خالص بلکه به صورت موسیقی، ویدیو و همچنین ارتباطی دو طرفه را نیز فراهم خواهند کرد. عنصر کلیدی در ارتباطات بی‌سیم ، پروتکل برنامه‌های بی‌سیم یعنی (Wireless Application Protocol) WAP است. خدمات خبری نظیر CCN Mobile اخبار و اطلاعات مستقیم به تلفنهای سلولی و وسایل بی‌سیم ارسال می‌کند.

مدخلهای ارتباط با اینترنت امکان ارتباط با خدمات مختلف در وب را امکان‌پذیر خواهند ساخت. برای مثال (Http://Mobile.msn.com) MSN Mobile به کاربران امکان می‌دهد e-Mail خود را از طریق Hotmail.com بخوانند و MSNBC.com را برای دریافت اخبار سیاسی، ورزشی یا گزارش آب و هوا مرور کنند. MSN به کاربران اجازه می‌دهد تا از برنامه‌های مسافرتها و پروازها از طریق expedia.com باخبر شوند و همچنین از دفتر راهنمای تلفن- بخش آگهی‌ها (yellow page) استفاده کنند. (http:/mobile.yahoo.com/wireless/home) امکان دسترسی به خدمات گسترده‌ای نظیر Yahoo! Actions، ارسال پست و پیام‌گذاری و خدمات فهرستی WAB ارائه اخبار ورزشی، بازار بورس، آب و هوا و طالع‌شناسی در تلفنهای همراه و یا سایر وسایل بی‌سیم را امکان‌پذیر می‌سازد.

GPS- و وسایل نقشه نگار وسایل و ابزار تعیین کنید. موقعیت جهانی (Global Positioning Devices) از طریق ماهواره‌ها، این امکان را به شما می‌دهند که موقعیت یک وسیله نقلیه را هر لحظه تعیین کنید. علاوه بر این، در دسترس بودن نقشه‌ها و نمودارهای بی‌سیم به راننده و یا کاربر اجازه می‌دهند که مسیریابی صحیح را انجام دهند.

– سیستمهای وسایل نقلیه شخصی سیستمهای نظیر سیستمهای فوق‌العاده پیشرفته On stare ساخته شده در کارخانه جنرال موتور (General Motors) ، ارتباطات بی‌سیم و پیگیری GPS را با امکان ارتباط زنده در هم آمیخته تا به رانندگان وسایط نقلیه شخصی امکان بهره‌گیری از خدمات مختلف و متنوعی را بدهند.

– سیستمهای سفارش و فهرست: سالها است که مشاغلی نظیر سوپر مارکتها و فروشگاههای کوچکتر و همچنین فروشندگان قطعات، از سیستمهای بی‌سیم مستقیم برای دریافت فهرست‌ها و سفارشات مشتریان استفاده می‌نمایند. علاوه بر این، فن آوریهای جدید در پیگیری ثبت و ضبط نقدی، فروش و برگشت، ارتباط بی‌سیم فوری را بین خرده‌فروشان و عرضه‌کنندگان کالا برقرار می‌سازد.

– عملیات بانکی و مالی: بانکها و سایر مؤسسات مالی از پیشگامان عرضه خدمات از طریق وسایل بی‌سیم و ارسال منابع مالی از طریق شبکه بی‌سیم هستند.

– خدمات عامل المنفعه : از سالها پیش، شرکتهای برق، تلفن و کابل کشی از وسایل بی سیم برای تشخیص مشکلات دستگاه‌ها و همچنین برقراری ارتباط با ستادهای اطلاعاتی استفاده می‌کنند.

– عوارض جاده‌ها : گذشتن از باجه‌های اخذ عوارض به شما این امکان را می‌دهد که در وقت خود برای پرداخت عوارض جاده‌ها و اتوبانها از طریق سیستم پرداخت بی‌سیم، صرفه جویی کنید.

– تحقیقات علمی : برای کارهای میدانی و آزمایشگاهی می‌توان یادداشتها، داده‌های GPS و محاسبات و داده‌های مختلف را با هم از طریق شبکه‌های بی‌سیم ترکیب نمود.

– وسایل و ابزار Palmtop، PDA : این وسایل و ابزار موجود در بازار، عملکردهای مختلف را با هم ترکیب می‌کنند از جمله آنها می‌توان به تقویم، ساعت، کتابچه آدرس، ارتباط دهنده‌های پست الکترونیکی جستجوگرهای وب، ارتباطات بانکهای اطلاعاتی، جستجوهای محدود و تولید محصولاتی نظیر کتابهای الکترونیکی اشاره کرد.

- وسایل نظامی : در ارتش وسایل بی‌سیم برای هر مقوله‌ای ساخته می‌شود. از وسایل بی‌سیم برای برقراری ارتباطات تیمی تا راهنمای پزشکی برای صحنه درگیری و از تعقیب‌های هدف تا اشتراک اطلاعات و مدیریت گروه استفاده می‌گردد.

نرم‌افزارهای پیشرفته در تجارت همراه

- کارخانه سازنده تلفن همراه، اریکسون (Ericsson) و غول صنایع غذایی انگلستان Safeway « وسایل کنترل در نقطه- خرید » (Point of Purchase Check out) را می‌سازند. مشتریان قادر خواهند بود که کالای مورد نظر خود را در قفسه اسکن نمایند سپس آن را در چرخ خرید بگـذارند و بطور اتوماتیـک همه چیز کنتـرل گردد و پول اجناس هم از حساب بانکی وی کسر گردد.

- Download کردن کوپن: بسیاری از مراکز خدماتی کوپنهای تخفیف را برای خرید کالا عرضه می‌کنند. شما می‌توانید کالای مورد نظر خود را تعیین و کوپن‌های تخفیف را Download نموده و از طریق ارتباط بی‌سیم برای صندوقدار فروشگاه ارسال کنید.

- بازاریابی و جستجو: آیا می‌دانید که برای پیدا کردن مواد مورد نیاز کجا را جستجو کنید. یک جستجوی بی سیم در وب، این امکان را به شما می‌دهد که محل مورد نظر را یافته و از طرحها و تخفیف‌های آنها نیز استفاده کنید.

- پرداخت بی سیم: والت‌های الکترونیکی نوکیا و سایر تولید کنندگان وسایل الکترونیکی مشغول کار با شرکتهایی هستند که بتوانند با ارسال سیگنالهای بی‌سیم پول خریدهای مشتری را از کیف پول الکترونیکی یا حساب بانکی وی برداشت کنند. تصور کنید که از یک دستگاه فروشنده بدون استفاده از هیچگونه پول خردی، خرید نمایید. وسیله بی‌سیم شما، پیغامی را به ماشین می‌فرستد و ماشین جنس مورد نظر را به شما تحویل می‌دهد و در همان حال پول جنس نیز از حساب بانکی شما کسر می‌گردد.

سایت تجاری ebay

سایت ebay با تنها هدف ساده حراج‌های اینترنتی و سرمایه ۱۱۶ میلیارد دلار، بخش عظیمی از درآمد اینترنت را با بیش از دو میلیون کاربر ثبت شده به خود اختصاص داده است. آیا فکر می‌کنید دست از تلاش برای پیشرفت و گسترش بیشتر برداشته است؟ خیر! ebay به طور دائم در جستجوی راههای جدید

برای گشودن بازارهای جدید و فراهم کردن سایت بین‌المللی است. در سال ۲۰۰۰ این شرکت با شرکت aipreality.com شریک شد تا یک طبقه بندی جدیدی از محصولات و خدمات را با نام ebay Real Estate به مشتریان عرضه کند. شرکت zipreality.com خدمات ملکی را به صورت حرفه‌ای و به عنوان بخشی از طبقه‌بندی جدید فراهم خواهد آورد. مطمئناً با بکارگیری zipreality.com و قدرت فن آوری و زیر ساختار ebay، هر دو شرکت از این اتحاد سود کلانی به دست خواهند آورد. اگر چه ebay نامی کاملاً شناخته شده در حراج‌های online می‌باشد ولی مرتباً در تفکر و جستجوی راههای جدیدتری برای باقی ماندن در نوک هرم موفق‌ترین سایت‌ها است.

سایت آمازون (Amazon)

آمازون یکی دیگر از سایت‌های کاملاً شناخته شده و معروف در زمینه عرضه کتاب می‌باشد اگر چه این سایت محصولات دیگری چون وسایل باغبانی و آشپزخانه را نیز به فروش می‌رساند و از نظر ارسال و تحویل سفارشات بسیار قابل اعتماد و سرعت کار آن فوق‌العاده بالا است. یکی از ابداعات کلیدی آمازون مساله « سفارش تک کلیکی » است (1-Click ordering)

زمانی که مشتری انتخاب online خود را انجام و سفارش را ثبت نمود، آنگاه می‌تواند « سفارش تک کلیکی» را انتخاب کند. این کار بطور خودکار همه اطلاعات قبلی وارد شده از نظر صورت حساب و ارسال را انتخاب می‌کند. سایت آمازون دریافته است که بازار وی بر اساس راحتی و خرید ناگهانی (بدون تفکر قبلی) صورت می‌گیرد لذا از این ابداع فوق‌العاده بهره گرفته است، ابتکاری که موجب می‌شود خریدار بدون آنکه دخالتی در مسائل صورت حساب و ارسال و پرکردن فرمهای آنها داشته باشد و فقط با یک کلیک خرید خودرا انجام دهد.

سایت JC Penney

سایت Penney.com در خلال ماه ژوئن سال ۲۰۰۰ رقمی بالغ بر ۷۹ میلیون دلار فروش online داشته اشت. جای تعجب و شگفتی بسیار می‌باشد که این سایت با داشتن فقط چند کاتالوگ online توانست به یکی از مراکز پر ترافیک در اینترنت تبدیل گردد.

برای پیشرفت کار، این سایت شرکت جداگانه دیگری را به نام راه حل‌های تجاری اینترنتی JCP بوجود آورده که هدف عمده آن حضور تجاری و کاتالوگ است. راز موفقیت JC Penney در عملکرد آن برای هر چه بهتر عرضه کردن خدمات به مشتریان، انجام تعهدات و نیز شخصی سازی دادو ستدها بوده است.

سایت Bid

سایت Bid.com که برپایه حراج تاسیس شده است ،تلاش خود را روی حراجهای تجاری مصرف کنندگان (B2C) متمرکز نموده است. این سایت مایل بود که دارای موقعیتی مانند ebay باشد ولی به علت عدم توان رقابت این شرکت در طول یکسال با از دست دادن بخش عمده‌ای از سرمایه مواجه گشت.

تجارت همراه چیست ؟

تعریف خاصی برای تجارت همراه وجود ندارد هر تحلیل‌گر، فروشنده و مجله تجاری تفاسیر متفاوتی از این واژه دارد . در حقیقت یک توافق عمومی بر روی معنی مترادف آن وجود ندارد. نمونه‌هایی از تعاریف تجارت همراه در ذیل وجود دارد:

- تجارت همراه به معنای استفاده از وسایل همراه به منظور ارتباط برقرار کردن، تبادل اطلاعات و ارائه متن و اطلاعات از طریق ارتباط با شبکه‌های خصوصی و عمومی می‌باشد
- قسمت اصلی تجارت همراه استفاده از یک ترمینال مانند تجهیزات PDA (وسایل شخصی همراه)، PC یا ترمینال عمومی و همچنین خطوط ارتباطی می‌باشد، که البته برای انجام مبادلات که منجر به انتقال مقادیر از طریق تبادل اطلاعات، خدمات و کالاها می‌باشد، کافی نیست.
- انجام تجارت و معاملات مشتری از طریق یک وسیله همراه
- تجارت همراه اشاره دارد به هر نوع معامله‌ای که با مقادیر پولی سروکار دارد و از طریق شبکه ارتباط تلفنی همراه انجام می‌گیرد.

- استفاده از وسایل همراه و دستی به منظور ارتباط برقرار کردن و ایجاد ارتباط با اینترنت از طریق یک راه ارتباطی سریع و همیشه در دسترس
- استفاده از تکنولوژی‌های بی‌سیم به منظور ارائه خدمات محلی و شخصی برای مشتریان، کارمندان و شرکا
- همچنین تجارت همراه را می‌توان چنین تعریف نمود، " هر نوع معاملات یا تبادل اطلاعات الکترونیکی از طریق وسیله همراه و شبکه‌های همراه که منجر به انتقال مقادیر واقعی یا پولی شود تجارت همراه نامیده می‌شود.

تجارت همراه در مقایسه با تجارت الکترونیکی

غالبا تجارت همراه ، بعنوان زیر مجموعه‌ی تجارت الکترونیک معرفی می‌شود و اشاره بر این داردکه هر تجارت الکترونیک می‌تواند از طریق وسایل بی‌سیم همواره در دسترس باشد ولی با گذشت زمان تجارت همراه به‌عنوان یک تجارت مجزا با ویژگیها و عملکردهای مستقل به خود شکل گرفته است، هر چند شباهت‌هایی بین تجارت همراه و تجارت الکترونیکی از جهت خرید کالا و خدمات، وجود دارد.

مقایسه ویژگیهای خطوط بی‌سیم و باسیم

حضور در هر لحظه و در هر مکان: استفاده از وسایل بی‌سیم این امکان را به کاربر می‌دهد تا در هر زمان و هر مکان قادر به دریافت اطلاعات و انجام معاملات باشد .

- دسترسی : وسایلی که در تجارت همواره مورد استفاده قرار می گیرند در تمام زمانها می‌توانند کاربر را به هر مکان بصورت مجازی مرتبط سازند. بنابراین کاربر این قابلیت را دارد که دسترسی خود را به هر شخص که بخواهد در هر زمانی قطع نماید.

- راحتی در بکار بردن : راحتی از جنبه قابلیت حمل و عملکرد آن، که شامل ذخیره کردن اطلاعات و دسترسی به افراد و اطلاعات می‌باشد.

- محلی کردن: تعیین موقعیت ویژه بر اساس عملکردها، کاربرها را قادر می‌سازد که به اطلاعات مربوطه، به منظور انجام کارها دسترسی داشته باشند.

- ارتباط دائم: همیشه در دسترس بودن، از ضرورت شبکه‌ها می‌باشد و کاربران از راحت‌ترین و سریعترین دسترسی به اینترنت استفاده خواهند نمود.

– خصوصی سازی: ترکیب خصوصی سازی و تعیین موقعیت، فرصت جدیدی را برای انجام تجارت به منظور جذب مشتریان مهیا می‌سازد. خصوصی‌سازی شامل، اطلاعات ویژه، اولویتهای کاربران که توسط مکانیزمهای پرداخت دنبال می‌شود، می‌باشد و این امکان را بوجود می‌آورد که اطلاعات خصوصی ذخیره گردد و همچنین نیاز به اطلاعات مربوط به کارت اعتباری را برای انجام هر معامله بر طرف سازد.

سرویسهای پیام کوتاه (SMS) چیست ؟

SMS پروتکلی است که به شما اجازه می‌دهد پیام‌های کوتاهی به صورت متن از طریق تلفنهای موبایل خود ارسال نمایید. این پیام‌ها در واقع بسیار کوتاه هستند: ۱۶۰ حرف برای پیامهایی با زبان لاتین و حداکثر ۷۰ حرف برای زبانهای غیرلاتین مثل فارسی و عربی و چینی .

به رغم این محدودیت، SMS در آوریل ۱۹۹۹ بسیار فراگیر شده بود تا آنجا که بیش از یک میلیارد پیام در آن ماه با استفاده از این سیستم ارسال شد که در حال‌حاضر تعداد این پیامها هر شش ماه دو برابر می‌شود.

استفاده اولیه SMS برای اطلاع به کاربران در خصوص دریافت یک نامه از طریق پست الکترونیک یا اطلاع به وی در مورد دریافت یک پیغام صوتی بود . بدون استفاده از این سرویس، کاربران ناچارهستند بطور مرتب صندوق پستی یا صوتی خود را بررسی کنند که آیا پیغام جدیدی رسیده است یا خیر که در مورد پیامهای فوری این سرویس بسیار مفید خواهد بود .

قالب SMS به نحوی است که نمی‌تواند متن کامل یک نامه را برایتان نمایش دهد، زیرا محدودیت ۱۶۰ حرفی تنها برای نمایش تاریخ، ساعت، فرستنده و عنوان نامه کفایت می‌کند . البته برخی خدمات در حال گسترش ارایه خدمات پیامهای چندگانه هستند که به مرور در حال گسترش می‌باشند.

از آنجا که بشر شیفته برقراری ارتباط با دیگران است، توانایی SMS در ارسال پیامهای کوتاه میان تلفنهای موبایل و همچنین بین موبایل و کامپیوترهای شخصی توانسته آن را به محبوب‌ترین و پر استفاده ترین ابزار تبدیل کند. در بسیاری از کشورها که استفاده از کامپیوترهای شخصی و تلفن موبایل و حتی پیجر رواج دارد، به خصوص جوانها و نوجوانها، برای غلبه بر محدودیت تعداد حروف، زبان خاص خود را ابداع کرده‌اند که روزبه‌روز توسعه بیشتری می‌یابد.

GSM و SMS

GSM (Global System for Mobile Technology) ، شایع‌ترین سرویس در اروپا و آسیا است. بر خلاف ایالات متحده که از نوع دیگری از سیستمهای بی‌سیم در آن استفاده می‌شود، از GSM تقریباً در تمام کشورهای دنیا استفاده می‌شود. GSM پروتوکلی است که نه تنها در اروپا استفاده می‌شود بلکه به علت باز بودن پروتوکل و قابلیت اضافه شدن کارکردهای جدید، به یکی از فراگیرترین استانداردها تبدیل شده است.

SMS یکی از نرم‌افزارهای نسل اولیه GSM بود که نخستین بار در سال ۱۹۹۲ از یک کامپیوتر شخصی به یک موبایل ارسال شد. این نوع نرم‌افزارهای نسل اول (G1) برای ابزارهای بی‌سیم با پهنای باند کم طراحی شده بود اما اتحادیه GSM برای نرم‌افزارهای نسل دوم (G2) نسل سوم (G3) برنامه‌ریزی می‌کنند و امیدوار هستند بتوانند امکان ارسال جریان داده‌ها بصورت کاملاً رنگی از طریق گیرنده‌های بی‌سیم را فراهم کنند.

اتحادیه GSM که در دوبلین(ایرلند جنوبی) و لندن مستقر است مالک بیش از پانصد ماهواره، عملگرهای G3 کارخانجات و تهیه کنندگان خدمات دیگر است که در بیش از دویست کشور جهان فعال می‌باشند. GSM گرچه در شمال قاره امریکا زیاد شایع نیست اما شرکت‌هایی چون نوکیا و لوسنت (Lucent) که در زمینه توسعه کامپیوترهای شخصی و تکنولوژی‌های ارتباطی فعالیت می‌کنند عضو اتحادیه آن هستند. این گروه که در سال ۱۹۹۵ تشکیل شد تلاش می‌کند تا استاندارد GSM را در شمال قاره امریکا نیز رواج دهد.

در حال حاضر بیش از شش میلیون نفر در آمریکای شمالی و ۲۹۰ میلیون نفر در سایر کشورها از این استاندارد استفاده می‌کنند. در کشورما نیز همین استاندارد به کارگرفته شده است اما سرویس پیام کوتاه در آن فعال نیست.

از دیگر تکنولوژی‌ها شبکه همراه TDMAوCDMA می‌باشند که با SMS تاحدودی متفاوت می‌باشند. نکته مهم این است که دستگاههای همراه از نوع TDMA گرچه پیامها را دریافت می‌کند، اما فاقد کارایی ضبط پیغام روی Handset ها می‌باشد.

تلفنهای WAP به جای استفاده از IP، اساس پروتوکل‌های WAP بطور کامل از SMS به عنوان یک رسانه فیزیکی که کلیه اطلاعات را دریافت و ارسال می‌کند، استفاده می‌نماید.

اولین مرحله SMS، EMS (Enhanced Message Service) گسترش خدمات پیام رسانی می‌باشد. جدیدترین امکانات SMS، MMS (Multi Media Messaging Service)است.

تاریخچه کارت‌های اعتباری

در فرآیند کسب و کار که قدمت آن به هزاران سال پیش می‌رسد ، کالا در مقابل کالا مبادله می‌شد. پس از آن استفاده از سکه‌های فلزی جایگزین سیستم کالا با کالا شد و از حدود صدها سال پیش پول کاغذی (اسکناس) نیز متداول و جاری گردید تا آنکه در آوریل سال ۱۹۵۰ در کشور ایالات متحده ، پول پلاستیکی به جای پرداخت مستقیم هزینه‌های خرید کالا یا خدمات متداول گردید. ابتداء این کارتها به صورت خاص و برحسب مورد بکار گرفته می‌شد تا آنکه به تدریج مبنای کارتهای متداول امروزی را بنیان نهاد. هم اکنون نیز با روند تکنولوژی الکترونیکی و مخابراتی در چند سال اخیر پول دیجیتالی مورد استفاده بسیاری از فعالیت‌های بنگاه با بنگاه و بنگاه با خریدار قرار گرفته است به نحوی که اکنون در اغلب کشورها شرکت‌های بسیاری، تولیدکننده انواع کارتهای اعتباری می‌باشند.

طبیعی است استفاده از انواع کارتهای اعتباری بدون پشتوانه موسسات اعتباری معتبر بین‌المللی و منطقه‌ای ممکن نمی‌باشد و لذا در گردش عملیات تجاری نقش بانکها و مؤسسات مالی و اعتباری و تبدیل بانکهای سنتی به بانک‌های الکترونیکی و در نهایت شیوه‌های نوین عرضه خدمات بانکی نظیر بانکهای اینترنتی، بانک‌های مبتنی بر موبایل و بانکداری مجازی (cyber banking) اجتناب ناپذیر می‌نماید، از اینرو در ادامه به موضوع بانکداری الکترونیکی نیز پرداخته شده است.

از سوی دیگر با بکارگیری ترمینال‌های کامپیوتری خاص به صورت online یا offline در نقاط فروش که به POS (point of sale) موسوم می‌باشند. اجرای عملیات بانکی در هر لحظه و در محل استقرار POS محقق گردیده است. در هر حال وظیفه تشخیص هویت و اعتبار دارنده کارت توسط ایستگاه‌های POS صورت می‌پذیرد. اطلاعات هویتی و اعتباری و رمز مشتری بعضاً روی نوار مغناطیسی یا chip الکترونیکی و نظایر آن ذخیره و بازیابی می‌گردد و صورتحسابهای مربوط نیز معمولاً در فواصل زمانی مشخص توسط موسسه مالی برای مشتری ارسال می‌گردد.

برخلاف كارتهاي اعتباري كه مصرف كننده قبل از انجام هزينه وجهي را به بانك يا موسسه پرداخت نمي‌كند، كارتهاي غير اعتباري (Debit card) نيز وجود دارند كه مصرف كنندگان مي‌بايست قبلاً وجوه خود را به بانك يا مؤسسه پرداخت نمايند. كارتهاي تلفن، كارتهاي عابر بانك (ATM) نيز وجود دارند كه

مصرف کنندگان می بایست قبلاً وجوه خود را به بانک یا مؤسسه پرداخت نمایند. کارتهای تلفن، کارتهای عابر بانک (Automatic Teller Machine) (ATM) از جمله کارتهای غیر اعتباری می‌باشند.

کارتهای هوشمند که در مقایسه با کارتهای مغناطیسی از قابلیت ذخیره‌سازی اطلاعات بیشتر و ذخیره الگوریتم‌های رمزنگاری پیچیده برخوردار می‌باشند عموماً با نام ICC (Integrated Circuit Card) خوانده می‌شوند که در سال ۱۹۷۴ اولین نوع آن توسط Roland Moreno به بازار عرضه گردید. این کارتهای هوشمند امروزه توسط موسسات مالی طراز اول نظیر Master cardو Visa به عنوان اساس سیستم‌های تجاری شناخته شده‌اند. بر اساس نوع کاربرد، این کارتها می‌توانند شامل تنها یک مدار مجتمع شامل یک حافظه یا مداری پیچیده‌تر شامل برنامه‌های کاربردی اجرایی نیز باشند.

واضح است زمانی که کارت دارای پردازنده باشد، عملیات حذف و اضافه و سایر عملیات روی داده‌های کارت به سرعت انجام می‌پذیرد در حالیکه کارتهائی که تنها مجهز به حافظه می‌باشند مانند کارتهای تلفن، تنها مسئولیت انجام عملیات محدود و از پیش‌تعیین شده را بعهده دارند.

کارتهای هوشمند برخلاف کارتهای مغناطیسی، تمام توابع محاسباتی لازم را جهت اعمال روی اطلاعات کارت بهمراه دارند. لذا زمانی که در pos مورد استفاده قرار می‌گیرند دستیابی راه دور به پایگاه داده را نیاز ندارند.

امروزه بطور کلی کارتهای هوشمند را به سه گروه زیر تقسیم می‌نمایند:

- کارتهایی که دارای پردازنده هستند (Inegrated Circuit Microprocessor Cards)

این نوع کارتها که در صنایع معروف به کارتهای تراشه‌ای Chip Card می‌باشند، در مقایسه با کارت‌های مغناطیسی دارای حجم حافظه بالاتر و امنیت داده‌های بهتر می باشند این کارت‌ها معمولاً دارای پردازنده‌های ۸ بیتی، همراه با ۱۶ حافظه فقط خواندنی و ۵۱۲ بایت حافظه از نوع RAM می‌باشند.

از جمله کاربردهای کارت‌های فوق که رمزنگاری بصورت built-in روی کارت تعبیه شده است عبارتند از: کارت پول‌ها، کارتهای دسترسی به شبکه‌های امن، کارتهای محافظ تلفن همراه برای جلوگیری از دسترسی‌های غیر مجاز و کارتهایی که در گیرنده‌های تلویزیون جهت کنترل دسترسی به کانالها مورد استفاده قرار می‌گیرند.

- کارتهای با حافظه نوری (Optical Memory Cards)

این کارتها می‌توانند تا ۴ مگابایت داده را روی خود ذخیره نمایند با این محدودیت که پس از نوشتن اطلاعات به هیچ وجه نمی‌توان آنها را روی کارت تغییر داده و یا حذف نمود لذا آرشیو اطلاعات پزشکی و اطلاعات گواهینامه رانندگی از جمله موارد کاربرد این کارت‌ها می‌باشند. این کارتها در حال حاضر فاقد پردازنده مستقیم روی کارت بوده و قرار است در آینده نزدیک مجهز به پردازنده نیز گردند.

کارتهای هوشمند می‌توانند به صورت کارتهای چند منظوره مورد استفاده قرار گیرند و بطور همزمان چندین برنامه کاربردی را پشتیبانی نمایند. بعنوان مثال یک کارت می‌تواند بعنوان کارت شناسایی، گواهینامه رانندگی، کارت مالکیت خودرو، کارت بیمه درمانی و نظایر آن بکار رود.

برای مصارف محدودتر مانند پرداخت هزینه پارکینگ، عوارض بزرگراه‌ها و کارت تلفن، تکنولوژی کارت‌ها ساده‌تر و حجم حافظه کمتری مورد نیاز است.

بزرگترین دغدغه بکارگیری این کارتها امنیت و عدم بکارگیری غیر مجاز آنها می‌باشد. خوشبختانه هم اکنون الگوریتم‌هایی پیشنهاد گردیده است که عملاً رمزگشایی کارتهای هوشمند را غیر ممکن می‌سازد. امروزه نتیجه تحقیقات نشان می‌دهد که حدود یک میلیارد کارت اعتباری در گردش بوده و استفاده از آنها موجب بهبود خدمات مالی، افزایش ضریب امنیت و قابلیت انعطاف تلفن‌های همراه و امنیت ماهواره‌ها و تلویزیونهای کابلی گردیده است.

یکی از عمده‌ترین کاربردهای کارتهای هوشمند کارتهایی است موسوم به کارت درمان که علاوه بر مشخصات فردی صاحب کارت، مشخصات بیمه‌گر، سوابق بیماری‌ها، واکسیناسیون، بیماریهای خاص و داروی مصرف شده، آزمایشات و حتی تصویر رادیولوژی و ... را نیز در خود ذخیره و بازیابی می‌نماید.

Java Card

یکی از متداولترین تکنولوژی‌های نرم افزاری جهت ایجاد و توسعه سیستم‌های کاربردی مبتنی بر کارت‌های هوشمند توسط شرکت سان مایکروسیستم ارائه گردیده است. این تکنولوژی در بسته نرم‌افزاری این شرکت، موسوم به Java Card Development Kit عرضه شده و شامل زیر مجموعه‌ای از زبان برنامه نویسی همه‌منظوره و شی‌گرای جاوا می‌باشد که برای کارت‌های هوشمند آورده شده‌است. با استفاده از این ابزار اپلت‌های جاوا (برنامه‌های کوچک جاوا که تحت مرورگرها اجرا می‌شوند) برای کارت‌های هوشمند مبتنی بر جاوا نوشته شده و به اجرا در می‌آیند. اپلت‌های ایجاد شده می‌توانند از توانایی‌های زبان برنامه

نویسی جاوا و ویژگیهای آن استفاده نمایند. مؤلفه‌های موجود در کارت‌های هوشمند مبتنی بر جاوا طراحی مؤثر و امنی را فراهم کنند.

کارت‌های مبتنی بر جاوا با استانداردهای بین‌المللی از جمله ISO 7816 و استانداردهای صنعتی Europay، Master Card، Visa (emv) مطابقت دارند.

بانکداری الکترونیکی در ایران- از تئوری تا عمل

با توجه به ورود تکنولوژی جدید در پردازش و تبادل داده‌ها، نیاز جدیدی برای نحوه ارائه خدمات بانکی مطرح شده است و با نگاهی به تجارب کشورهای پیشرفته و رشد خدمات بانکداری الکترونیکی می‌توان نیازهای در حال شکل‌گیری و روند رو به رشد آن را در زمینه خدمات بانکی در ایران تا حد مناسبی پیش‌بینی نمود. نظر به روشهای سنتی موجود در بانکهای کشور و نارسایی این روشها در ارائه خدمات جدید و تهیه زیر ساخت مناسب به صورت اتوماسیون جامع بانکها در برنامه تحولات بانکی کشور قرار گرفته است.

بر پایه این بستر است که ارائه خدمات جدید، تهیه زیر ساخت مناسب به صورت اتوماسیون جامع بانکها در برنامه تحولات بانکی کشور قرار گرفته است. بر پایه این بستر که ارائه بانکداری الکترونیکی و دیگر خدمات پیشرفته بانکی به تحقق می‌پیوندد. هم اکنون بانکهای کشور در ایجاد این زیر ساخت و ورود به بانکداری نوین، رقابت خوبی را آغاز نموده و خدمات بانکی الکترونیکی را، هر چند هنوز بسیار محدود، در کشور پایه‌گذاری نموده‌اند.

بانکداری نوین در آغاز قرن ۲۱، چهره بانکداری سنتی که بیش از دو سده حیات دارد را به نحوی دگرگون نموده است که آموزشها و تئوریهای بظاهر خدشه ناپذیر موجود در این صنعت نه تنها پاسخگوی نیاز آن نیست بلکه با تغییرات شتابزده و ظاهری نیز قادر به پرکردن جایگاه سابق نمی‌باشد. فن آوری اطلاعات و ارتباطات به این صنعت شکل منعطف و متحول بخشیده و آن را مجبور به ترک قیدها و مقررات کهنه نموده است.

ارائه خدمات مختلف در بازار الکترونیکی و سهولت دستیابی به اطلاعات مورد نیاز تجار و تولید کنندگان در این بازار، زمینه ساز اصلی بانکداری الکترونیکی بوده است و با گسترش فراگیر اینترنت و اینترانت، شهروندان عادی نیز مشتاق ورود به این بازار و به تبع آن نیازمند دریافت خدمات بانکی، از جمله دسترسی به حسابهای شخصی خود هستند.

فن آوری، قابلیت ها را به نمایش می‌گذارد. قابلیتها نیازها را شکل داده و مسیر فعالیتها را معین می‌کنند. بازاریاب ها محصولاتشان را با توجه به این روند ارائه می‌دهند و انتهای این کاروان قانونگذار وارد صحنه شده و مقررات وضع می‌شود. دنیای تجارت در آستانه هزاره سوم روشهای کاری خود را با بکارگیری فن آوری رایانه‌ای و ارتباطات سریع مخابراتی سازماندهی می نماید و علیرغم نبود قوانین مدون، بخش عمده‌ای از داد و ستدهایش را با کمک این فن آوری انجام می‌دهد. هم اکنون در اکثر کشورهای دنیا، اعم از پیشرفته، در حال پیشرفت و در حال توسعه، رشد چشمگیر و غیر منتظره‌ای از روی آوری مشتریان به دریافت خدمات الکترونیکی بانک‌ها، صنعت بانکداری را به تکاپو وادار کرده است. علاوه بر بانکهای جدیدی که خدمات خود را صرفاً از طریق ارتباط الکترونیکی به مشتریانشان ارائه می‌کنند، بانک‌های پر سابقه نیز در کنار فعالیت فعلی خود و یا با تاسیس بانکی مستقل با شیوه الکترونیکی به عملیات خود وسعت می‌بخشند.

در ایران گسترش تدریجی دسترسی به اینترنت و در اختیار داشتن کامپیوترهای خانگی توسط اقشار مختلف مردم و شرکتها، نیازهای بالقوه‌ای را در زمینه دریافت خدمات بانکداری الکترونیکی آشکار نموده است. از این رو بانکهای تجاری و تخصصی کشور هم سو با برنامه‌های متحول ساختن روشهای خود و حرکت به سمت بانکداری نوین، بانکداری الکترونیکی را از اهم فعالیتهای برنامه ریزی آتی خود در نظر گرفته‌اند. در ادامه با عنایت به شرایط خاص روند تحول، به فعالیتهای آماده‌سازی زمینه ارائه بانکداری الکترونیکی در ایران پرداخته می‌شود و کوششهای انجام یافته در این مسیر از تئوری تا عمل تشریح می‌گردد.

در ابتدا نگاهی اجمالی به تاریخچه و رشد بانکداری الکترونیکی در جهان شده و سپس بخشهای بعدی، ورود این پدیده به صنعت بانکداری ایران از تئوری تا عمل بررسی گردید و سپس طرح جامع اتوماسیون بانکی بعنوان گام های بلند و استواری در مسیر حرکت بسوی بانکداری الکترونیکی در بانکهای تجاری و تخصصی کشور تشریح شد و مروری بر ارائه بانکداری از طریق اینترانت و اینترنت در قالب این طرح انجام گرفت.

نفوذ بانکداری الکترونیکی در مبادلات پولی

مدت زیادی از پا گرفتن پرداختهای الکترونیکی و انتقال وجه الکترونیکی نمی‌گذرد که رشد دور از انتظار آن کارشناسان بانکی را به تحلیل جدی این پدیده و نگارش مقاله‌های آگاه کننده و هشدار دهنده به صاحبان موسسات مالی واداشته است. شروع این پدیده را می‌توان بکارگیری پیامهای SWIFT برای انتقال وجوه تجاری و مالی و سپس پرداخت دانست. SWIFT ابزاری اختصاصی در دست مؤسسات معتبر مالی

محسوب می‌شود. مؤسسات ارائه دهنده کارت اعتباری، بازاریابی وسیعی را در ارائه خدمات پرداخت از طریق شماره کارت اعتباری در میان مشتریان خود انجام داده و برای مدتی کارت اعتباری وسیله پرداخت بی رقیبی در بازار الکترونیکی محسوب می‌شد. مؤسسات مالی و از جمله بانکهای معتبر دنیا تا مدتها بازار الکترونیکی و بکارگیری فن آوری مربوط به آنرا با شک و احتیاط می‌نگریستند و حتی در بحران‌های مالی آنرا یک کالای لوکس در کنار فعالیتهای تبلیغی تلقی کردند که به آسانی می‌توان از آن چشم پوشید. مؤسسات نوپای فعال و جوان از این شرایط بهره گرفتند چون آنها نگران مقررات جا افتاده و گردش سنتی اسناد نبودند. خدمات انتقال وجوه را با صرف کمترین انرژی از مشتری برای او انجام می‌دادند و پیامهای متقاعد کننده را بر روی آدرس الکترونیکی او را ارسال می‌کردند.

به این ترتیب با انجام پرداختهای مشتریان توسط e-mail، شرکت Paypal ظرف کمتر از هشت ماه مشتریان خود را از صفر به ۲/۵ میلیون نفر رساند. شرکت دیگری به نام paymobills که خدمات پرداخت قبوض را از طریق حساب جاری اشخاص انجام می‌دهد، ادعای افزایش مشتریانش را با نرخ ۵۰٪ در ماه دارد و ظرف چهار ماه ۱/۵ میلیون مشتری را جذب نموده است.

در این شرایط است که بانکها و مؤسسات جا افتاده مالی دیگر نمی‌توانند نظاره گر باشند و شاهد از دست دادن مشتریان و فعالیتهای اقتصادی خود شوند. در حال حاضر مشتریانی که به این ترتیب به ارائه دهندگان خدمات الکترونیکی بانکی متوسل می‌شوند کمتر از ۱٪ تخمین زده می‌شوند ولی به دو دلیل این انتقال مشتریان برای بانکها نگران کننده است، اولاً این دسته از مشتریان آنهایی هستند که بانک به صلاح خود نمی‌داند که آنها را از دست بدهد. ثانیاً بدون هیچ شبهه‌ای روند فعالیت‌های بانکی، شتاب گرفتن خدمات بانکی الکترونیکی را اثبات می‌کند.

لذا دیگر این فن‌آوری نوین را نمی‌توان لوکس و کم استفاده دانست. بانکهای بزرگ دنیا هم اکنون بدنبال وارد شدن هر چه سریعتر و جدی تر در بازار تراکنشهای الکترونیکی و ارائه خدمات بانکداری الکترونیکی به مشتریان خود هستند.

آشنایی بانکهای ایران با بانکداری الکترونیکی

اگر بتوان SWIFT را طلیعه بانکداری الکترونیکی دانست، در بانکهای داخل ایران این پیشقراول با کندی مورد استقبال قرار گرفت ولی مفاهیم ارتباط الکترونیکی و ارسال و دریافت پیامهای مالی از طریق بکارگیری فن آوری رایانه‌ای و شبکه مخابراتی مطمئن، با رواج SWIFT جای خود را در فعالیتهای بانکی ایران باز نمود، با این وجود راه درازی در مقابل بانکهای کشور برای وارد شدن به این بازار جدید وجود دارد. زیر ساخت قدیمی بانکها، عدم تغییر اساسی در روشهای بانکداری و مقررات محدود کننده از جمله موانع بزرگ در مسیر حرکت بانکها در جهت تحول و همگام شدن با بانکداری نوین جهانی به شمار می‌روند که باید توسط موج جدید بانکداران تحول گرا به کنار زده شوند.

موج همه‌گیر شبکه‌های اطلاع رسانی رایانه‌ای منتظر نمی‌ماند که جامعه بانکداری در گوشه‌ای از دنیا، آمادگی لازم را پیدا نماید و هجوم نیاز مشتریان و فعالیتهای تجاری الکترونیکی با روند فزاینده خود در پشت در بانکها فشار لازم را وارد می‌نمایند.

پاسخگویی به این نیازها با بافت سنتی بانکهای کشور آسان نیست. ایجاد زمینه و در اختیار گرفتن فن آوری مناسب الزامی است. کندی و نادیده گرفتن این بازار، فضای مناسبی را برای شرکت‌ها و مؤسسات غیر بانکی ایجاد می‌کند تا با ارائه خدمات خود، در حد توان، سهم بزرگی از فعالیتهای مالی را از آن خود نمایند.

چنانکه اکنون کاربران شبکه اینترنت آغاز خدمات خرید مایحتاج را مستقیماً از طریق حساب بانکی خود شاهد هستند ، بزودی پرداخت قبوض برخی از سازمانهای خدماتی مستقیماً از طریق سایت آن سازمانها و با موسسات هم پیمانشان امکان پذیر می‌شود. همانطور که در کشورهای غربی تجربه شده است، پس از دوره کوتاهی که صرف کسب اعتماد مشتریان می‌گردد، سرعت رشد استفاده از این خدمات، ارائه دهندگان آنرا دچار بهت و حیران خواهد نمود و قابل پیش‌بینی است که خدمات دیگر و موسسات بیشتری در فاصله کوتاهی سهم خود را از بازار جدید جویا شوند.

کارت اعتباری گرچه در کشورهای پیشرفته از اولین ابزار همگانی فعالیت مالی الکترونیکی محسوب می‌شود ولی در ایران که با توجه به بافت محتاط و سنتی جامعه بانکداران، راهکارهای مناسبی برای بکارگیری آن اندیشیده نشده است، کماکان ابزار ناشناسی در فعالیتهای اقتصادی اشخاص محسوب می‌گردد. خوشبختانه با وارد شدن موج تحول در بانکداری می‌توان امیدوار بود که در آینده‌ای نه چندان دور، کارت

اعتباری جایگاه خود را در بکار انداختن موتور تولید و اقتصاد داخلی بدست آورد. از طرفی با وسعت گرفتن این ابزار، می‌توان پیش‌بینی نمود که سرعت ورود تجارت الکترونیکی شتاب بیشتری نیز پیدا نماید.

آشنائی بانکهای ایران با اتوماسیون بانکی

از ورود کامپیوتر به صنعت بانکداری در ایران سالهای زیادی می‌گذرد. در آن سالها کامپیوتر شخصی برای همگان ناشناس بود . کامپیوترهای بزرگ، نصب شده در مراکز بانکها، آشنایی با پردازش و ذخیره سازی داده‌های الکترونیکی را برای بانکها به ارمغان آوردند. این کامپیوترها امکانات تهیه انواع گزارشهای آماری و مدیریتی را بر اساس داده‌های ذخیره شده در آن به مدیریت و ادارات مرکزی بانک می‌داد.

در اواخر دهه ۶۰ بانکها با توجه به ورود کامپیوترهای شخصی و احساس نیاز به اتوماسیون عملیات بانکی در جهت رایانه‌ای کردن وضعیت موجود برآمدند ولی بکارگیری یک سیستم جامع نرم افزاری و طرح همه گیر اتوماسیون در هیچیک از بانکها راهی پیدا نکرد.

تحول و پیشرفت فعالیتهای بانکی و ارتقاء خدمات قابل ارائه در بانکها منوط به بکارگیری فن آوری رایانه‌ها و شبکه‌های وسیع تبادل داده‌ها در چارچوب یک طرح یکپارچه اتوماسیون می‌باشد. حرکت به سوی بانکداری الکترونیکی برای بانکهای کشور بدون ایجاد زیربنای آن تصویری مبهم و نا استوار است. بانکداری الکترونیکی در یک سیستم یکپارچه نرم‌افزاری و سخت افزاری توان حرکت می‌یابد و جایگاه واقعی خود را پیدا می‌کند.

فعالیتها و اقداماتی که در زمینه تهیه یک طرح جامع اتوماسیون در بانکها دیده می‌شود مؤید این نظر است که بانکها نیز لزوم زیربناسازی را شناخته و بدون تجهیز خود به یک سیستم اتوماسیون یکپارچه، قدم در عرصه‌های جدید بانکداری را امکان پذیر نمی‌دانند. اکنون طرح جامع اتوماسیون در صدر برنامه‌های بانکی برای تحول به سوی بانکداری نوین می‌باشد. با پیاده شدن این طرحها آمادگی لازم برای ارائه بانکداری الکترونیکی نیز در بانکها پدیدار خواهد شد.

چشم انداز تغییرات و استفاده از تجارب

بانکداری الکترونیکی، فرهنگ جدیدی از دریافت خدمات را در جامعه عرضه می‌کند. هم اکنون درکشورهای پیشرفته خدمات گسترده این شیوه جدید بانکداری جای خود را بین میلیونها مشتری باز کرده

است. البته بنا به اظهارات متخصصین و آمارهای جمع‌آوری شده، این تکنولوژی توسط متقاضیان جوان بیشتر پذیرفته شده است.

در کشورهای پیشرفته استقبال بیشتری از بانکداری الکترونیکی شده‌است. شعب بانکهای این کشورها از نمونه شعبی هستند که روابط بانکداری مدرن، داخل آنها را از مشتری خالی نموده است و متناسب با آن لزوم کاهش تعداد شعب در دستور کار اغلب بانکها قرار دارد.

طرح جامع اتوماسیون

در بالا به طرح جامع اتوماسیون بعنوان زیر بنا و زمینه‌ساز ارائه خدمات نوین بانکداری و از جمله بانکداری الکترونیکی اشاره شد. در اینجا مختصری درباره این طرح و تجربه پیاده سازی و چشم انداز تغییرات ناشی از آن در عملکرد، ساختار سازمانی و ارائه خدمات در بانکها تشریح می‌گردد.

تاریخچه شکل گیری

طرح جامع اتوماسیون سیستم بانکی در سال ۱۳۷۲ بطور رسمی مطرح شد. پس از بررسی فعالیتهای مکانیزاسیون انجام شده تا آن زمان، عدم حصول به اهداف کلان این سرمایه گذاری ها در بانکها مشخص گردید.

نتیجه مطالعات فوق در قالب پیشنهادی، برای حرکت در جهت جامع نگری در برنامه ریزی فعالیتهای انفورماتیکی بانکها به مسئولین سیستم بانکی کشور ارائه گردید.

با پذیرش دلایل و بر اساس مصوبه مجمع عمومی بانکها در سال ۱۳۷۲، طرح جامع اتوماسیون سیستم بانکی شکل گرفت. مسئولیت و پیشبرد طرح بر اساس همین مصوبه به عهده مشاور اجرایی ریاست کل بانک مرکزی گذاشته شد.

اهداف طرح

اهداف کلان طرح جامع با بررسیهای همه جانبه به شرح زیر تعیین گردید:

- کاهش مشکلات اجرایی در شعب و ادارات مرکزی بانکها و افزایش توان اجرایی سیستم
- تسریع در اجرای عملیات نظام بانکی و ارتقای کیفیت آن
- ایجاد زمینه لازم برای کاهش مبادلات نقدی و نقل و انتقال پول

- ایجاد امکان دسترسی به اطلاعات به هنگام برای اتخاذ تصمیم در مورد سیاستهای پولی و بانکی
- صرفه جویی در وقت کارکنان و مشریان بانکها، کاهش نقل و انتقال فیزیکی مدارک در شعب، کاهش سفرهای شهری و ...
- ایجاد هماهنگی لازم برای ارتباط به بانکهای خارج از کشور

جامع نگری طرح به این معنی مطرح گردید که کلیه فعالیتها حول محور مدل اطلاعاتی لازم برای رسیدن به کلیه اهداف طرح صورت می‌گیرد و به این ترتیب فعالیتها ضمن پوشش دادن بخشی از مدل اطلاعاتی، نقش مکمل سایر فعالیتها را نیز دارند.

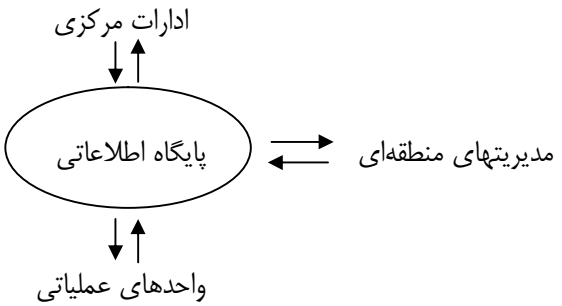
معیارهای عمده طرح جامع

معیارهایی که این طرح در روند تعیین ساختار اطلاعاتی مد نظر داشته است بصورت کلی به شرح زیر می‌باشند:

- قطع وابستگی جغرافیایی مشتریان به شعب خاص
- گسترش ارائه خدمات بانکی به خارج از واحدهای بانک
- گسترش ارائه خدمات بانکی به خارج از ساعات کار رسمی بانک
- محور قراردادن مشتری در مبادلاتش با بانک (و نه حسابهای مشتری)
- حفظ یکپارچگی اطلاعات بانک و اجتناب از ذخیره چند باره و زائد اطلاعات
- استفاده از تکنولوژی های اثبات شده

الگوی انفورماتیکی طرح جامع

طرح جامع با در نظر داشتن نیازهای اطلاعاتی بانک و ساختار گردش اطلاعات، مدل متمرکز اطلاعات را در بانکها شناسایی نموده است. بکارگیری این الگو با توجه به معیارهای عمده طرح تأثیر به سزایی بر کارآیی بانک و رضایت مشتری از ارائه خدمات بانکی گسترده و توین و نحوه برخورداری از آن خواهد داشت.



ساختار اطلاعاتی بانک در طرح جامع اتوماسیون

امنیت اطلاعات در تجارت الکترونیک:

بدین منظور برای برقراری امنیت اطلاعات در تجارت الکترونیک، استانداردها و تکنولوژی خاصی مورد استفاده قرار می‌گیرد. روشهای امنیت اطلاعات در واقع حاصل ترکیب مفاهیم منطقی و ریاضی است که در قالب الگوریتم‌هائی ارائه گردیده‌اند.

در حال حاضر مردم به طور فزآینده‌ای از اطلاعات مالی، اعتباری و شخصی از شبکه‌های مبتنی بر اینترنت در سرتاسر جهان استفاده می‌نمایند. از سوی دیگر از آنجایی که مسیر گردش اطلاعات و منابع روی شبکه بسیاراست، لذا مشخص نمی‌باشد که اطلاعات مذکور کجا می‌روند و چه اشخاصی از آنها بهره‌برداری می‌نمایند. بدین ترتیب حفظ امنیت اطلاعات از مباحث مهم در تجارت الکترونیک بشمار می‌آید. هر چند امنیت مطلق وجود ندارد اما حـداقل برای برخورداری از یک وضعیت غیر شـکننده می‌باید هزینه‌هایی را صرف نمود.

در ادبیات تجارت الکترونیک و در ارتباط با امنیت اطلاعات در شبکه‌های اینترنت سه موضوع مهم مطرح می باشند:

۱) **شناسایی**(Authentication) : که عبارت است از احراز هویت طرفین فرآیند تجاری.

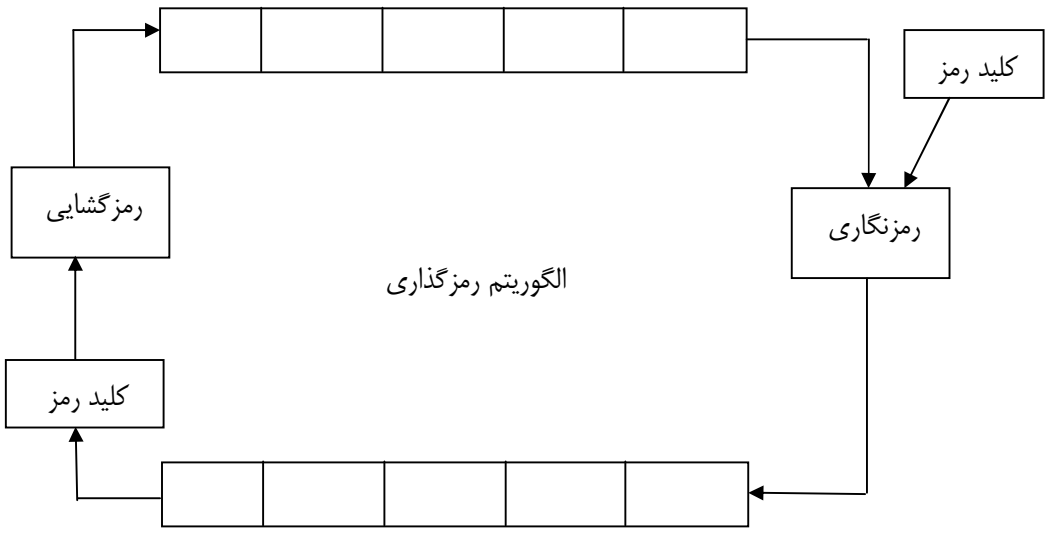
۲) **رمزنگاری**(Encryption) : هر رکورد اطلاعاتی می‌باید به گونه‌ای رمزنگاری شود تا سایر افراد نتوانند آنرا خوانده یا در آن تغییراتی را اعمال نمایند .

۳) **مجوز دستیابی(Authorization) :** پس از احراز هویت و رمزگشایی و رکورد دریافتی متقاضی موضوع بعدی، محدوده دستیابی به رکوردهای بانک‌های اطلاعاتی و مجموعه عملیاتی که از قبل تعیین گردیده است تحت عنوان مجوز دستیابی می‌باشد که آنهم از اهمیت ویژه‌ای برخوردار است .

الگوریتم رمزگذاری (Cryptoghraphic algorithms): فرآیند رمزگذاری و رمزگشائی داده‌ها مطابق شکل زیر توسط یک کلید و مجموعه‌ای از الگوریتم‌های رمزنگاری صورت می‌پذیرد. در فرآیند مذکور پیامی که می‌باید رمز گردد و به آن Plain Text Massage گفته می‌شود ابتدا به ردیفی از بلوک‌های چند بیتی(N-Bit Blocks) تقسیم می‌گردد.

سپس فرآیند الگوریتم رمزنگاری(Encipher Algorithm) با استفاده از یک کلید و بلوکهای فوق بعنوان داده‌های ورودی پس از اجرای فرآیندهای تعریف شده در الگوریتم رمزگذاری، بلوکهای رمز شده نظیر را با همان طول به عنوان خروجی جهت انتقال روی شبکه اینترنت در اختیار قرار می‌دهد و متعاقبا در سمت گیرنده، الگوریتم های رمز گشا (Cipher algorithm) را تبدیل به پیام اولیه می‌نماید.

در الگوریتم‌های پیشرفته، رمزگذاری زنجیره رمزگذاری (Cipher chaining) یعنی عملیات رمزگذاری و رمزگشایی روی هر بلوک، بستگی به محتویات قبلی دارد.



باید توجه داشت که در این روش، الگوریتم های مذکور در اختیار همگان قرار دارد و سالهااست که از آنها استفاده می‌گردد. آنچه که مهم است دانستن کلید توسط طرفین فرآیند تجاری می‌باشد. قابل ذکر است علاوه بر بکار گیری شیوه فوق در انتقال داده‌ها نیز از این الگوریتم‌ها استفاده می‌گردد. نکته قابل تعمق در این روش توزیع کلید روی اینترنت است.

الگوریتم‌های متداول در رمزنگاری (Crypto Algorithms)

در فرآیند رمز نگاری، سه دسته از الگوریتم‌های رمز نگاری اصلی به شرح زیر مورد استفاده قرار می‌گیرند:

الگوریتم های Message-Digest

این الگوریتم‌ها پیامهای رمز نشده با طول‌های متفاوت را به پیامهای رمز شده کوتاه‌تر و با طول‌های ثابت تبدیل می‌نمایند.

الگوریتم‌های Secret-key

این الگوریتم‌ها یک کلید را هم به منظور رمزگذاری و رمزگشایی به طور مشترک مورد استفاده قرار می‌دهند و به آن کلید مشترک یا Shared Key اتلاق می‌گردد.

این کلید مشترک معروف بهSymmetric Key نیز می‌باشد.

الگوریتم های Public Key

در این الگوریتم یک زوج کلید موسوم به کلید عمومی (Public key) و یک کلید خصوصی (Private key) به کار گرفته می‌شود.

این کلیدها اعداد اول هستند و نامتناهی بودن آنها در ریاضیات به اثبات رسیده است.

در الگوریتم‌های Public key پیام رمز شده به وسیله کلید عمومی با استفاده از کلید خصوصی متناظر با آن رمز گشایی میگردد و بالعکس، این الگوریتم‌ها Asymmetric key نامیده می‌شوند.

یادآوری می‌شود که از آنجاییکه احتمال یافتن کلید توسط افراد غیر مجاز همواره وجود دارد، برای پیدا نمودن کلید تنها نیاز به منابع محاسباتی نظیر CPU، فضای دیسک و پهنای باند زیاد می‌باشد تا با ایجاد یک شمارنده حالتهای مختلف آشکارسازی را آزمایش نمایند. بدیهی است هرچه طول کلید بیشتر باشد زمان پیدا نمودن کلید نیز افزایش می‌یابد زیرا برای کلید با طول n می‌باید حداکثر 2^n بار آزمایش انجام گیرد.

سوال اصلی این است، آیا می‌توان کلیدی ساخت که هرگز افراد غیر مجاز نتوانند آنرا بیابند؟ برای پاسخ به این سوال چنانچه فرض نماییم سخت افزاری یک میلیون دلاری در اختیار داریم و می‌توان در هر ثانیه در حدود $۲^{۴۰}$ کلید را ایجاد نمائیم، زمان تقریبی یافتن کلید مورد نظر جهت رمزگشایی داده‌ها طبق جدول زیر محاسبه گردیده است.

زمان	طول کلید symmetric برحسب بیت	طول کلیدAsymmetric برحسب بیت
میلی ثانیه	۴۰	۲۷۴
ساعت	۵۶	۳۸۴
روز	۶۴	۵۱۲
قرن	۸۰	۷۶۸
هزاره	۱۲۸	۲۳۰۴

بر اساس جدول بالا چنانچه از کلیدی با طول ۱۲۸ بیت استفاده نمائیم قطعا به امنیت بالایی دست خواهیم یافت که در اصطلاح به این سطح امنیت در ارسال و دریافت اسناد مالی تحت اینترنت، لایه امن یا Secure Socket Layer (SSL) گفته می‌شود.

الگوریتم های خلاصه کردن پیام‌ها (Message Digest) :

این اگوریتم در فرآیندهای ارسال و دریافت امضاء دیجیتال در تجارت الکترونیک مورد استفاده قرار می‌گیرد این الگوریتم با دریافت پیامی با طول متغیر آنرا به یک پیام خلاصه با طول ثابت نگاشت می‌نماید. نقطه قوت این الگوریتم در آن است که امکان نگاشت خلاصه پیام به پیام اولیه میسر نمی‌باشد. متداول‌ترین توابع این الگوریتم عبارتند از:

- MD4/MD5 برایRSA های با طول خلاصه شده(Digest) ۱۲۸ بیت
- SHA1 که توسط دولت ایالات متحده برای digest هایی با طول ۱۶۰ بیت مورد استفاده قرار می‌گیرد .

امضای دیجیتال

با استفاده از الگوریتم‌های فوق و تکنولوژی کلید عمومی می‌توان به امضای دیجیتالی دست یافت. یک امضای دیجیتالی در واقع یک کلید خصوصی رمز شده بر اساس پیام خلاصه شده است. در سمت گیرنده نیز با استفاده از کلید عمومی، امضاء دیجیتال را رمز گشائی و صحت آنرا مورد تایید قرار می‌دهند . RAS و DSS دواستاندارد متداول برای امضاهای دیجیتالی می‌باشند.

RAS از سال ۱۹۹۱ بعنوان استاندارد بازار مورد استفاده قرار گرفته است درحالیکه DSS پیشنهاد انستیتوی ملی تکنولوژی و استانداردها (NIST) می‌باشد.

نکاتی در خصوص توزیع کلیدهای Symmetric در شبکه اینترنت

همانگونه که توضیح داده شد در فرآیند رمز نگاری دو طرف فرآیند تجاری در شبکه از کلید مشابهی جهت رمز گذاری و رمز گشایی استفاده می‌نمایند. مشکل اصلی در این روش حصول اطمینان از ارسال این کلید به طرف گیرنده است که می‌باید ضمانت لازم در خصوص عدم دستیابی و رمزگشائی این اطلاعات توسط اشخاص غیر مجاز حاصل گردد که خود عاملی محدود کننده در بکارگیری سیستمهای مبتنی بر Symmetric Key می‌باشد زیرا یک کلید مشترک در دو طرف استفاده می‌شود و این روش از بکار گیریPublic key متداول‌تر است.

برای رفع مشکل مذکور الگوریتم هایی موسوم به Kerberos مورد استفاده قرار می‌گیرند که این نام از نام یک سگ افسانه‌ای یونانی که دارای سه سر بود اقتباس گردیده است!

چگونگی فرآیند بکارگیری الگوریتم Public key و محدودیتهای آن

از این روش به منظور ارسال مطمئن پیامها در اینترنت استفاده میکند. در این روش ابتدا ارسال کننده پیام را با کلید عمومی دریافت کننده رمزگذاری کرده و از سوی دیگر دریافت کننده پیام را با کلید خصوصی خود رمزگشائی می‌نماید. این سیستم پیام را بصورت محرمانه، یکپارچه و همراه با احراز و شناسائی هویت گیرنده تهیه می‌نماید لیکن دو مشکل عمده کارایی و توزیع کلیدها بشرح ذیل در مورد الگوریتم Public key وجود دارد:

کارایی : الگوریتم های Public key حدودا سه برابر کندتر از الگوریتم‌هایی Symmetric key می‌باشند و برای رفع این نقصان تغییراتی در رمزنگاری به صورت زیر انجام پذیرفته است.

- فرستنده پیام را با یک Symmetric key که بصورت تصادفی ایجاد می‌گردد، رمزگذاری می‌نماید.
- این کلید سپس بر اساس Public key گیرنده رمزگذاری می‌شود.
- هنگام دریافت، دریافت کننده با استفاده از Private key اقدام به رمزگشایی Symmetric key می‌نماید.

- گیرنده سپس با استفاده از Symmetric key اقدام به رمزگشایی پیام می‌نماید.

توزیع کلید : شبکه‌های اینترنت متولی حقوقی خاصی ندارند و بعضا بلاصاحب هستند و ارسال داده‌ها می‌تواند توسط افراد غیرمجاز مورد دستبرد قرار گیرد لذا مسئله توزیع کلیدها از جمله دغدغه‌های ارسال و دریافت در شبکه‌های اینترنت می‌باشد. بنابراین نیاز به مکانیزمی برای ایجاد Public key می‌باشد به نحوی که ضمانت گردد هر کلید عمومی متعلق به یک نام، معرف یک شخص یا موجودیت حقیقی یا حقوقی می‌باشد.

گواهینامه : گواهینامه (Certificate) یک سند تائیدیه رسمی است که مشخص می‌نماید Public key متعلق به یک نام بعنوان موجودیتی حقیقی یا حقوقی و مستقل می‌باشد.

Certificate یک سند رسمی است زیرا به صورت دیجیتالی به امضای یک مؤسسه شناخته شده موسوم به Certificate authority رسیده است. این گواهی پس از صدور بصورت الکترونیکی برای متقاضی ارسال میگردد.

در حال حاضر مؤسسات بسیاری به عنوان مراکز CA به ثبت رسیده و فعالیت می‌نمایند از جمله مؤسسه Revising که تعداد بسیاری سند احراز هویت برای سایتهای وب، مؤسسات ارائه کنندگان خدمات تجارت الکترونیکی و اشخاص حقیقی و حقوقی ثبت و صادر نموده است.

واضح است از آنجایی که امضای اشخاص محرمانه نیست لذا ارسال گواهی صادره از یک مرکز CA به ثبت رسیده است لـذا هرکس می‌تواند Public key خود را در شبکه توزیع نماید و جهت خواندن سندی که بصورت دیجیـتالی امضاء شده است نیاز به یک Public key صـادر شده توسط CA می‌باشد.

یک سند Certificate مانند کارتهای اعتباری دارای یک مدت اعتبار مشخص و معین می‌باشد و می‌توان قبل از انقضای تاریخ اعتبار دارای یک مدت اعتبار مشخص و معین باشد و می‌تواند قبل از انقضای تاریخ اعتبار در لیست اسناد یا غیر معتبر قرار گیرد.

هر مؤسسه CA فهرستی از گواهی‌های غیر معتبر خود که مرسوم به Certificate Revocation Lists (CRL) می‌باشد را به صورت متناوب تهیه نماید. این فهرست حاوی شماره سریال گواهی‌هایی است که علیرغم عدم انقضای تاریخ، به‌دلایل مختلف غیر معتبر گردیده‌اند.

اسناد و گواهی‌ها (Certificates) در تجارت الکترونیک از استانداردهای مصوبه ایزو تحت عنوانX509V3 پیروی می‌نمایند.

توصیه‌هایی جهت انتخاب کلمات عبور

بر اساس یک تحقیق انجام شده توسط شرکت High light اکثر کلمات عبور انتخاب شده کاربران توسط برنامه‌های قفل‌شکن موجود قابل تشخیص است و بر اساس یک تحقیق دیگر که توسط شرکت Centeralnic که در حوزه ثبت Domain فعالیت دارد انجام گردیده است ۵۰ درصد افراد، نام و یا نام مستعار خود را به عنوان کلمه عبور انتخاب می‌نماید، لذا کارشناسان معتقدند اکثر کاربران به اهمیت انتخاب کلمه عبور واقف نیستند و تعداد زیادی از افراد نیز نام تیم ورزشی مورد علاقه خود را به عنوان کلمه عبور انتخاب می‌نمایند، از این رو بعضاً مورد تهاجم افراد غیر مجاز قرار می‌گیرند. به همین منظور راه حل پیشنهادی، طراحی و ساخت عبارتی متشکل از حروف و اعداد است که این نیز بدلیل مشکل بخاطر سپردن آن، کمتر مورد استفاده قرار می‌گیرد. اما برخی از کاربران برای رفع این مشکل نیز حرف عبور خود را توسط پست الکترونیکی برای خودشان ارسال می‌کنند یا در جای خاصی روی سیستم نگه می‌دارند. این مسئله نیز کمک چندانی به فاش نشدن حرف عبور نمی‌کند، بهر حال ابزارهای ایجاد شده به منظور قفل شکنی و کشف کلمات عبور توانایی‌های بسیاری دارند که با بهره گیری از یک فرهنگ لغات به جستجوی کلمه مورد نظر می‌پردازند و حتی برخی از آنها با الگوریتم‌های خاص شناخته شده‌ای اقدام به یافتن کلمات ترکیبی از اعداد و حروف نیز می‌نمایند.

یکی از ابزارهای قفل شکن معروف به نام Loft crack می‌باشد که در عرض چهل و هشت ساعت می‌تواند تمامی فایلهای کلمات عبور یک شرکت را جستجو نماید. بنابراین توصیه می‌گردد کاربران در انتخاب کلمات عبور خود دقت بیشتری داشته باشند تا از آسیب‌های احتمالی ناشی از فاش شدن آن مصون بمانند.

نتیجه‌گیری

با سرعت نفوذ کامپیوترهای شخصی در منازل و محلهای کار و گسترش استفاده کنندگان اینترنت در ایران، تجارت الکترونیکی و خدمات بانکی الکترونیکی دیگر مفاهیم ناآشنایی برای مردم ایران نیستند. از طرفی، شناسایی لزوم ایجاد بستر حرکتی بانکهای داخلی ایران به سوی بانکداری نوین از طرف جامعه بانکی کشور نیز درحال انجام است. با حمایت و سرمایه گذاری بانک مرکزی جمهوری اسلامی ایران این حرکت با قدمهای سنجیده و کارشناسانه آغاز گشته و تحول نظام بانکی کشور را در آینده نزدیک در جهت اعتلای خدمات بانکی نوید می‌دهد. بانکداری الکترونیکی نیز که یکی از طلایه داران بانکداری پیشرفته محسوب می‌گردد، جایگاه متناسب خود را در برنامه ریزی متحولانه بانکها کسب نموده است.

منابع و مآخذ :

۱ -دکتر محمدجعفر تارخ _ مهندس امیرعلی رامی، "تکنولوژی اطلاعات و صادرات نرم‌افزار"، 1381 انتشارات پیام‌آوران کلک آزاد

۲ -دکتر مهدی ثاقب تهرانی _ مهندس شبنم تدین، "مدیریت فن‌آوری اطلاعات"1380 مرکز آموزش مدیریت دولتی

۳ -بتول ذاکری، "روشهای ساخت‌یافته تجزیه و تحلیل و طراحی سیستمهای اطلاعاتی 1372 سازمان مدیریت صنعتی

۴ -ماهنامه کامپیوتر شماره 113، 114، 115، 116 و 117

۵ -ماهنامه web شماره‌های 24، 25، 26، 27، 28، 29، 30 و 31

۶ -ماهنامه شبکه شماره‌های 25، 26، 27 و 28

۷ -مهندس انوشیروان اخوان نیاکی، "مقایسه متدولوژی‌های ایجاد و توسعه سیستم‌های اطلاعاتی"، 1380 انستیتو ایزایران

۸ -تجارت الکترونیک و رایانه شماره‌های 1 و 2

۹ - صنایع الکترونیک شماره‌های 1، 2 و 3

10- خبرنامه انفورماتیک

11- آشنایی با تجارت الکترونیک و زیرساخت‌های آن _ مهندس حسن نیکبخش تهرانی، مهندس مهدی آذرصابر- انستیتو ایزایران

12- تجارت الکترونیکی _ Steffane Kopper ،Juanita Ellis، مترجم: خسرو مهدی پور- عطایی- موسسه فرهنگی هنری دیباگران تهران

13- راه‌حل ERP مبتنی بر فن‌آوری اطلاعات_ افشین کازرونی، مهرداد کازرونی، محسن شکوری‌مقدم

14- "What is Technology park?" www.American.Edu/Carmel

15- "Technology park Mason Lakes" www.techpark.sa

16- www.Raech.jo

17- www.ecomity.com

18- www.Itech.com

19- www.News.com

20- www.eurasia-ict.org

21- Stanford Research park www.Stanford.edu

22- James A. Obrien – "Management Information System"-1990

مهندسین مشاور ره‌شهر تاکنون منتشر کرده است:

۱- کاربرد جدید شیشه در نمای ساختمان (تابستان ۱۳۷۱)

۲- پارکینگ مراکز تجاری (پائیز ۱۳۷۱)

۳- محافظت در مقابل زلزله (زمستان ۱۳۷۱)

۴- جمع‌آوری و دفع زباله و مسائل ناشی از آن (زمستان ۱۳۷۱)

۵- طرح اسکان سریع (زمستان ۱۳۷۱)

۶- مجموعه مقالات راجع به ژئوسنتز (بهار ۱۳۷۲)

۷- مهار آب با آب (بهار ۱۳۷۲)

۸- تحول سبز در معماری (بهار ۱۳۷۲)

۹- روندیابی و مدیریت سیلاب (بهار ۱۳۷۲)

۱۰- مطالعات اقتصادی جهت احداث مراکز خرید (تابستان ۱۳۷۲)

۱۱- نگاهی کوتاه بر طراحی فضای سبز - «تجربیات کشورهای مختلف» (تابستان ۱۳۷۲)

۱۲- بازیافت آب در صنایع شن و ماسه‌شوئی (پائیز ۱۳۷۲)

۱۳- بناهای چوبی (کنده‌ای) در ایران و تجربیات کشورهای دیگر (پائیز ۱۳۷۲)

۱۴- نکاتی در مورد طراحی ساختمانهای بتنی پیش ساخته پیش‌تنیده در مناطق زلزله‌خیز (پائیز ۱۳۷۲)

۱۵- اتوماسیون و بهینه‌سازی در سیستم‌های توزیع الکتریکی (زمستان ۱۳۷۲)

۱۶- انرژی دریاها (زمستان ۱۳۷۲)

۱۷- پارکینگهای مکانیکی اتوماتیک و نیمه اتوماتیک (بهار ۱۳۷۳)

۱۸- انرژی باد (بهار ۱۳۷۳)

۱۹- اصول طراحی ساختمانهای اداری و بانک‌ها (بهار ۱۳۷۳)

۲۰- انرژی خورشیدی (بهار ۱۳۷۳)

۲۱- طراحی مرکز خرید - جلد اول: مطالعات مقدماتی جهت طراحی مراکز خرید (تابستان ۱۳۷۳)

۲۲- شهر سالم با آمورتون (تابستان ۱۳۷۳)

۲۳- شهر سالم- کاربرد سیستم‌های فتوولتائیک از میلی‌وات تا مگاوات (تابستان ۱۳۷۳)

۲۴- شهر سالم - اصول طراحی برای افراد دارای کهولت، ناتوانی، اختلال و معلولیت (تابستان ۱۳۷۳)

۲۵- نسل چهارم نیروگاهها (پائیز ۱۳۷۳)

۲۶- بازیافت آب در صنایع نساجی (پائیز ۱۳۷۳)

۲۷- مراکز درمانی و بیمارستانهای آینده (پائیز ۱۳۷۳)

۲۸- شهر سالم - انبوه سازی (انبوه سازان اسکان) (زمستان ۱۳۷۳)

۲۹- سیستم‌های مدیریت بار و مدیریت انرژی در شبکه‌های انرژی الکتریکی (زمستان ۱۳۷۳)

۳۰- بازیافت آب - «تصفیه پساب صنایع لبنی» (بهار ۱۳۷۴)

۳۱- شهر سالم - صنعت چوب و کاغذ و نقش آن در فرهنگ، اقتصاد و سیاست (در ایران و جهان) (بهار ۱۳۷۴)

۳۲- صرفه‌جوئی انرژی در ساختمانهای مسکونی (بهار ۱۳۷۴)

۳۳- شهر سالم - معماری و پرورش فکری کودکان و نوجوانان (تابستان ۱۳۷۴)

۳۴- شهر سالم - بازیافت زباله و مصالح ساختمانی و نقش آن در حفظ خاک و پاکسازی محیط (پائیز ۱۳۷۴)

۳۵- شهر ما کجاست (زمستان ۱۳۷۴)

۳۶- حفاظت سواحل دریا و رودخانه‌ها - معرفی روشهای سنتی و پیشرفته (زمستان ۱۳۷۵)

۳۷- بهینه‌سازی آموزش عالی - نگاهی کوتاه بر کارکرد نظام آموزشی ایران و جهان (زمستان ۱۳۷۵)

۳۸- استفاده از ژئوگرید در راهها و باند فرودگاهها (بهار ۱۳۷۶)

۳۹- اقتصاد گردشگری (جلد اول) (زمستان ۱۳۷۶)

۴۰- نگرش‌هائی نوین به طراحی فضای باز اداری (تابستان ۱۳۷۷)

۴۱- اقتصاد گردشگری جلد دوم (فصول سوم و چهارم) (زمستان ۱۳۷۷)

۴۲- فهرست مطابقه‌ای عملیات اجرایی جهت تسهیل در امر نظارت (پائیز ۱۳۷۸)

۴۳- دانسته‌هایی در مورد مناطق آزاد و ویژه اقتصادی در جهان (پائیز ۱۳۷۸)

۴۴- هدایت منابع مالی و فنی غیردولتی جهت اجرای طرح‌های عمرانی (زمستان ۱۳۷۸)

۴۵- پژوهش در تاریخچه، مفهوم و سیر تحول شهرسازی و شهر سالم در فرهنگ ایران و اسلام (زمستان ۱۳۷۸)

۴۶- پارک انرژی‌های نو (تابستان ۱۳۷۹)

۴۷- فضای باز اداری- مدیریت تجهیزات و طراحی داخلی (پائیز ۱۳۷۹)

۴۸- شهرک ترافیکی کودکان (زمستان ۱۳۷۹)

۴۹- فضای باز اداری- استانداردهای طراحی فضاهای اداری جداکننده‌ها، قطعات و اتصالات (زمستان ۱۳۷۹)

۵۰- فضای سبز - مناطق صنعتی - پارک‌های صنعتی (تابستان ۱۳۸۰)

۵۱- تنظیم شرایط محیطی - بخش اول: استانداردهای عملکرد حسی- جلد اول: محیط روشنایی (پاییز ۱۳۸۰)

۵۲- تنظیم شرایط محیطی - بخش اول: استانداردهای عملکرد حسی- محیط‌های صوتی و حرارتی (پاییز ۱۳۸۰)

۵۳- منظرسازی- جلد اول: طراحی کاشت (زمستان ۱۳۸۰)

۵۴- منظرسازی- جلد دوم: آبیاری و نگهداری منظر (زمستان ۱۳۸۰)

۵۵- تنظیم شرایط محیطی - بخش دوم: سیستمهای کنترل محیط - جلد اول: تولید و کنترل نور و صدا (زمستان ۱۳۸۰)

۵۶- تنظیم شرایط محیطی- بخش دوم: سیستمهای‌کنترل محیط - جلد دوم: تولید و کنترل‌حرارت (زمستان ۱۳۸۰)

۵۷- منظرسازی- جلد سوم: راهبردهای تکمیلی آراستن مناظر (بهار ۱۳۸۱)

۵۸- تنظیم شرایط محیطی- بخش دوم: سیستم های کنترل محیط- جلد سوم: سیستم جامع محیطی (تابستان ۱۳۸۱)

۵۹- شهرسالم- توسعه (کلان شهر تهران) (تابستان ۱۳۸۱)

۶۰- فن آوری اطلاعات- بخش اول : مفاهیم کلی (پاییز ۱۳۸۱)

۶۱- منظر سازی - جلد چهارم : چمن (روش های تکثیر و کاشت ونگهداری) (زمستان ۱۳۸۱)

۶۲ - فن آوری اطلاعات - بخش دوم : مدیریت فن آوری اطلاعات (بهار ۱۳۸۲)

۶۳ – فن آوری اطلاعات – بخش سوم : تجارت الکترونیک (بهار ۱۳۸۲)

همچنین نشریات تخصصی ذیل نیز منتشر گردیده‌اند:

- حقایقی در مورد شرکتهای بزرگ (بخش تحقیق و توسعه) (زمستان ۱۳۷۲)
- انتخاب محل و نوع سد براساس شرایط ژئومورفولوژی و ژئولوژی (بخش عمران آب) (زمستان ۱۳۷۲)
- تحلیل منطقه‌ای سیلاب در حوضه‌های شمالی تهران (بخش عمران آب) (بهار ۱۳۷۳)
- اصول طراحی مراکز دیسپاچینگ (بخش انرژی) (زمستان ۱۳۷۲)
- پارک‌پویش: اندیشه‌سالم/ بدن‌سالم در شهرک فاطمیه منطقهٔ ۲۰شهرداری‌تهران (بخش شهر سالم)- (پائیز ۱۳۷۲)
- شهرک ترافیکی کودکان (بخش شهر سالم) (پائیز ۱۳۷۲)
- سازماندهی کارکردهای بهینهٔ نمایشگرهای دیجیتالی (بخش شهر سالم) (زمستان ۱۳۷۲)
- استفاده از مولتی ویژن در مراکز پرتردد شهری (بخش شهر سالم) (بهار ۱۳۷۳)
- پارک انرژی‌های نو (بخش شهر سالم) (تابستان ۱۳۷۳)
- بهینه‌سازی خدمات پرواز (بخش شهر سالم) (زمستان ۱۳۷۳)
- بازارچه صنایع دستی در کوهپایه‌های شمال تهران (بخش شهر سالم) (تابستان ۱۳۷۴)

ضمناً کتب زیر منتشر گردیده‌اند:

۱- سازهٔ پارکینگهای طبقاتی (PARKING STRUCTURES) (۱۳۷۲)

۲- سازه‌های آبی (HYDRAULIC STRUCTURES) (۱۳۷۳)

۳- خودآموز اتوکد ۱۲ (AUTO CAD. V.12 USER'S GUIDE) (۱۳۷۳)

۴- برنامه‌ریزی و طراحی هتل (دفتر تحقیقات و معیارهای فنی سازمان برنامه و بودجه - ۱۳۷۵)

۵- بیست و پنج جلد استانداردهای‌صنعت آب کشور (دفتر امور فنی و تدوین معیارهای‌سازمان برنامه و بودجه - ۱۳۷۵)

کتب زیر بزودی منتشر می‌شوند:

۱- منظرسازی (طراحی، اجراء) LANDSCAPING PRINCIPLES & PRACTICES (مترجم: ره شهر)

۲- اصول زمین کردن الکتریکی (اتصال به زمین) ELECTRICAL GROUNDING (مترجم: ره شهر)