مشخصات تجارت الکترونیک

آتوسا عباس نژاد

Abnezhad@yahoo.com

مقدمه

با مطرح شدن فناوری اطلاعات در سطح جهانی و گسترش اینترنت، تجارت الکترونیکی جایگاه مهمی یافته است و در این میان ایران نیز ناگزیر به این عرصه خواهد پیوست. در جامعه اطلاعاتی، استفاده بهینه از حجم بالای اطلاعات و فراهم کردن سود بیشتر مورد نظر است. امروزه اکثر کمپانی ها نیروی خود را بیشتر صرف ارائه و فروش اطلاعات از طریق بازار یکپارچه جهانی یا اینترنت متمرکز کرده اند. تجارت الکترونیک در ایران نیز می تواند قابلیتها و مزایای ویژه ای را داشته باشد. در این مقاله تجارت الکترونیکی باتوجه به نیاز در سطوح متفاوتی مطرح شده که به شرح سرویس ها و مزایای استفاده از تجارت الکترونیکی در ایران می پردازد. پروتکل های گوناگونی برای پیاده سازی تجارت الکترونیک از قبیل OFX، SSL، IKP، SET مطرح هستند که زمینه های امنیتی و مالی این سرویس را در شبکه اینترنت پشتیبانی می کنند. پروتکل OTP چهارچوب کلی تجارت الکترونیک را بدون توجه به سیستم پرداختی ایجاد می کند. XML تبادلات داده را در تجارت الکترونیک در بر می گیرد. XML زبان مدل سازی جدیدی است و جایگزین EDI شده است. در این مقاله پروتکلها و استانداردهای تجارت الکترونیکی مطرح می گردد. امنیت در اینترنت در شکلهای متفاوتی مطرح می شود. تجارت الکترونیکی روشهای امنیتی خاص خود را داراست که به آنها اشاره می شود. مسایل مالی، پولهای دیجیتالی از دیگرمباحثی است که در سرویس تجارت الکترونیکی نقش اساسی داشته که به آنها اشاره خواهد شد.

۱ - ایجاد شرایط مناسب برای تجارت الکترونیکی

- رشد اینترنت در ایران بایستی در سیاست گذاریها بیشتر در نظر گرفته شود؛
- فراهم کنندگان بایستی پهنای باند با کیفیت مناسب را برای بازار اینترنت فراهم کنند؛
- بایستی کمپانی ها به ایجاد امنیت لازم برای استفاده از اینترنت برای تبادلات ایمن تشویق شوند و استانداردهای لازم در این زمینه معرفی گردند تا سرویس ها در سطح قابل پذیرش ارائه گردد.

۲ - مزایای استفاده از تجارت الکترونیکی در ایران

- مطرح شدن محصولات در سطح جهانی و در نهایت بالارفتن کیفیت محصولات؛
- کاهش موثرتر هزینه های عملیاتی بین عوامل بازرگانی (PARTNERS)، مشتریان و کانالاهای آن؛
- افزایش درآمد از طریق مشتریان جدید و کانالهای جدید همراه با محصولات و سرویس های جدید؛
- جلب رضایت مشتری؛
- صحت سفارشات ONLINE؛
- در نهایت امکان انجام خریدهای کوچک تا بستن قراردادهای کلان و کشوری.

۳ - انواع سرویس های تجارت الکترونیکی

سرویس های تجارت الکترونیکی را از نظر کاربرد می توان به چند دسته تقسیم بندی کرد. این سرویس ها به شرح زیر هستند:

- B2B، (BUSINESS TO BUSINESS): در این سرویس طرفین معامله شرکتها هستند؛
- B2C (BUSINESS TO CONSUMER): در این سرویس شرکتها با مشتریان در ارتباط هستند؛
- G2G (GOVERNMENT TO GOVERNMENT): روابط تجاری بین کشورها را دربر می گیرد و قوانین تجارت بین المللی را با توافق طرفین و ارائه راهکار شامل می شود؛
- C2B (CUSTOMER-TO-BUSINESS): طبق پیشنهاد مشتری سرویس موردنظر فراهم می گردد. مثل کرایه یک ماشین از نقطه ای مشخص با مبلغی تعیین شده از یک سایت اینترنتی؛
- C2C (CUSTOMER- TO-CUSTOMER): طرفین معامله افراد هستند. سرویس گیرنده فردی است که جنس یا کالایی را از شخص دیگر خریداری می کند. مثل آژانس های هواپیمایی و سمساریهای اینترنتی.

۴ - مسایل امنیتی در تجارت الکترونیکی

اینترنت به عنوان بستر انتقال اطلاعات در دنیای کنونی مطرح است. TCP/IP پروتکل انتقال اطلاعات در شبکه اینترنت است. با مطرح شدن اینترنت به طور گسترده، مسئله

امنیت اطلاعات قابل انتقال، به شکل مشخصی بستر فرستاده می شد. اطلاعاتی مثل، شماره کارت اعتباری، فرم پرداخت و غیره از جمله مسایلی بود که احتیاج به امنیت بیشتری داشت. به همین دلایل امنیت در تجارت الکترونیکی جایگاه مهمی داراست.

به چند روش می توان در اطلاعاتی مداخله کرد که بین دو کامپیوتر مبادله می گردد و این روشها عبارتند از [6,:9]

۱ - **استراق سمع:** اطلاعات توسط فردی خوانده می شود و می تواند بعداً مورد استفاده قرار گیرد. مثل شماره حساب یک فرد، در این حالت محرمانه بودن اطلاعات از بین می رود؛

۲ - **تغییردادن پیام:** امکان دارد پیام هنگام انتقال تغییر کند و یا کلاً عوض شود و سپس فرستاده شود. مثلاً سفارش کالا می تواند تغییر یابد؛

۳ - **تظاهرکردن:** ممکن است شخصی خود را به جای یک سایت معرفی کرده و همان اطلاعات را شبیه سازی کند و پس از دریافت مقادیر قابل توجه هیچ پاسخی به خریداران نداده و ناپدید گردد.

روشهای متفاوتی برای جلوگیری از این مسایل وجود دارد که یکی از آنها رمزدار کردن پیام است که خود به چند دسته تقسیم می گردد. دیگری درهم سازی و فشرده سازی پیام و تهیه DIGEST است. در امضای دیجیتالی عملاً تلفیقی از این روشها مورد استفاده قرار می گیرد. انواع روشهای رمزنگاری بدین شرح است:

● **رمزنگاری با کلید متقارن:** در این روش از یک کلید استفاده می شود. بدین شکل که یک کلید مشترک بین طرفین وجود دارد. اطلاعات با این کلید رمزدار شده و فقط توسط طرف مقابل که دارنده کلید است قابل بازگشایی است. مشکل این روش تبادل این کلید قبل از رمزدارکردن پیام است.

● **رمزنگاری با کلید نامتقارن یا کلید عمومی:** در این روش یک جفت کلید برای انتقال پیام استفاده می گردد. به این شکل که هرکاربر دارای یک کلید عمومی و یک کلید خصوصی است. کلید عمومی در یک دایرکتوری در اختیار هرکس می تواند قرار گیرد و کلید خصوصی هر فرد را، فقط خودش می داند. در ارسال پیغام از A به B، ابتدا A پیام را با کلید

اکثر شرکتها امروزه نیروی خود را بیشتر روی ارائه و فروش اطلاعات از طریق شبکه اینترنت متمرکز کرده اند.

در جامعه اطلاعاتی استفاده بهینه از حجم بالای اطلاعات و فراهم کردن سود بیشتر مورد نظر است.

خصوصی خود رمزدار کرده سپس با کلید عمومی پیام را ارسال می کند. در طرف مقابل B پیام را با کلید عمومی رمزگشایی کرده و سپس با کلید خصوصی خود رمز را باز می کند و پیغام را مشاهده می کند. اشکال این روش این است که شخص ثالثی مانند C می تواند خود را به جای A معرفی کرده و پیامی را با کلید خصوصی خود و سپس کلید عمومی رمزدار کرده وبرای B ارسال کند. در این روش B نمی تواند تشخیص دهد که پیغام ارسال شده حتماً از طرف A بوده است. امضای دیجیتالی به عنوان روشی برای جلوگیری از ایجاد این مشکل به وجود آمده است.

● **رمزنگاری بااستفاده از روش کلید عمومی با امضای دیجیتالی:**

امضای دیجیتالی همراه با کلید عمومی، موجودیتی است که به شخص طرف مقابل این امکان را می دهد تا تشخیص دهد کسی را که پیغام را فرستاده، همان کسی است که ادعا می کند، و پیغام دریافت شده همان پیغام ارسال شده است. (تصدیق اصالت).

در روش امضای دیجیتالی از کلید عمومی همراه با توابع HASH استفاده می شود.

کلید دارای یک تاریخ انقضا نیز هست که هرچه مدت اعتبارش کوتاهتر باشد اعتبار آن بالاتر است زیرا احتمال جعل آن بالا می رود. گیرنده پیغام امضای انجام شده را چک می کند تا از اصالت آن باخبر شود.

مراکزی که امضای دیجیتالی را در اختیار قرار می دهند خود از مراکز دیگری اعتبار گواهینامه را دریافت کرده اند. این مرکز موجودیتی است که اعتبار را برای یک فرد ایجاد می کند. چند نمونه از آنها XCERT، VENSIGN، THAWTE هستند که با دریافت وجه مشخصی این اعتبار را در اختیار قرار می دهند.

۵ - **مسایل مالی و پرداخت در تجارت الکترونیکی**

باتوجه به رشد اینترنت و مسئله خرید کالاها از اینترنت، مکانیسم های مختلفی برای پرداخت در برابر خرید موردنظر مطرح شد. در واقع پرداخت در تجارت الکترونیک، نیاز به مکانیسم های پرداخت ارزان و سریع دارد. در این راستا روشهای پرداختی گوناگون ایجاد شده اند، که هریک قابلیت خاص خود را دارد و در بعضی موارد شبیه به پول واقعی هستند. در اینجا انواع مکانیسم های پرداختی و شرکتهای وابسته به آنها آورده شده است. [10] (سیستم های پرداخت رایج در وب جهانی را از نظر ساختار فیزیکی نیز می توان دسته بندی کرد) سیستم هایی که از پول دیجیتالی (DIGITAL MONEY) استفاده می کنند:

- CYBERCOIN & CYBERCASH
- ECASH

سیستم هایی که از کارتهای اعتباری استفاده می کنند:

- CYBANK
- CYBERCASH & CYBERCOIN
- IKP, SET

سیستم هایی که از کارتهای هوشمند استفاده می کنند:

- MONDEX
- FETFARE
- VERIFONE

سیستم هایی که چک های الکترونیکی را فراهم می کنند:

- AXCEL CHECK

- CHECK FREE
- REDI-CHECK

سیستم هایی که ریز پرداختها را فراهم می کنند:

- MILLICENT
- MINI-PAY

به طور نمونه ECASH پروتکل پول الکترونیکی است که به وسیله DAVID CHAUM از شرکت DIGICASH توسعه یافته است. در ECASH، کاربر یک سری رشته های بلند از شماره ها را با نام TOKEN جمع آوری می کند که به عنوان پول شناخته می شود. این TOKEN ها درست مثل پول فیزیکی مبادله می گردد. این سیستم عدم انکار را برای کاربر پشتیبانی می کند، نیاز به سخت افزار خاصی نداشته و دارای هزینه است.

۶ - ابزار تبادلات الکترونیکی (XML)

XML (EXTENSIBLE MARKUP LANGUAGE) یک زبان نشانه گذاری برای ایجاد مستندات ساختار یافته است. XML شبیه به HTML است، با این تفاوت که XML ، قابل گسترش است. درواقع XML و HTML زیر مجموعه ای از SGML هستند. XML یک استاندارد باز، قابل گسترش، بین المللی و در دسترس است. XML یک زبان از پیش تعریف شده نیست بلکه قابلیت تعریف نشانه گذاریها و TAG های جدید را فراهم می سازد.

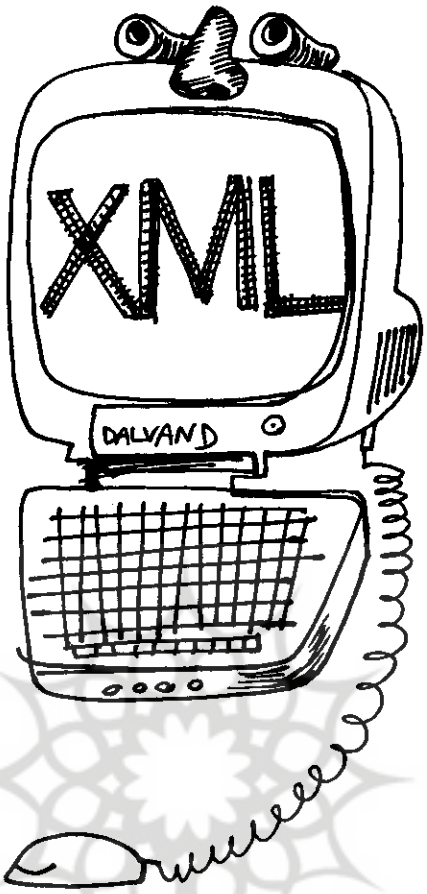
قبلاً از EDI برای تبادل داده بین دو کامپیوتر استفاده می شد که به دلیل محدودیتهایی که داشت کنار گذاشته شده و در حال حاضر از XML استفاده می شود. XML در مقایسه با EDI دارای مزایای زیر است:

- امکان تبادل داده تحت اینترنت؛
- هزینه پیاده سازی پایین تر؛
- سرعت بالای تبادلات.

۷ - استانداردها و تجارت الکترونیکی

استانداردها نقش مهمی را در توسعه یک ساختار ایفا می کنند. استانداردهای زیادی در زمینه های مختلف تجارت الکترونیکی مطرح هستند. مدیران IS بایستی با استانداردهای موجود آشنا بوده و قابلیت اجرای آنها را برای ارگانیسم خود ارزیابی کنند. استانداردها و پروتکل های تجارت الکترونیک در زمینه های مختلف عبارتند از:

- پروتکل های امنیتی (STT,S-HTTP,SSL و...)
- پروتکل های امنیتی - پرداختی (SEPP,IKP,SET)
- پروتکل های مالی - پرداختی



(JEPI,BIPS,OFX و...)

۱-۷ پروتکل های امنیتی: اخیراً هر کاربر اینترنت باید تبادلات را قبل از فرستادن پیام از طریق اینترنت به طور روشن محافظت کند. یک دسته از پروتکل های امنیتی، امنیت را برای لایه اینترنت فراهم می کنند. این پروتکل ها مثل ISAKMP,SKIP,IPSEC و غیره پروتکل های امنیتی لایه اینترنت هستند. سری دیگر از پروتکل های امنیتی، پروتکل های امنیتی لایه انتقال هستند مثل TLS,PCT,SSL و SSH. آخرین سری از پروتکل های امنیتی، پروتکل های امنیتی لایه کاربردی هستند. این پروتکل ها مثل SMTP,S-HTTP، امنیت را در لایه کاربرد ایجاد می کنند.

انتقال اطلاعات مهم مثل شماره کارت اعتباری اشخاص باید با امنیت کامل انجام گیرد. بافرض یک انتقال ایمن با پروتکل SSL,TCP/IP به عنوان پروتکل امنیتی لایه انتقال در زیر لایه کاربردی قرار گرفته و امنیت ارتباطات بین سرویس دهنده و سرویس گیرنده را برقرار می کند. SSL یکی از پروتکل های امنیتی است و به دلیل مزایای زیر برای سرویس تجارت الکترونیک مناسب است[3,7].

- مستقل از لایه کاربرد است؛
- SSl از تکنیک رمزنگاری خود به صورت قابل انعطاف عمل می کند؛
- تصدیق اصالت را برای طرفین معامله فراهم می سازد؛
- رمزنگاری و امضای دیجیتالی را به کار می برد؛
- قابلیت کار با FTP ،TOLMET ،HTTP را داراست.

پروتکل S-HTTP جایگزینی برای SSL محسوب می شود و اولین بار توسط EIT مطرح شد. این پروتکل به میزان SSL ، شناخته شده نبوده و فقط با HTTP سازگاری دارد.

SSL نیازهای امنیتی ذیل را برای سرویس تجارت الکترونیک برآورده می سازد. این نیازهای امنیتی عبارتند از:

- پنهان سازی (PRIVACY)

فرض کنید که پیغام های انتقال یافته از A به B رمزدار شده است. A از کلید عمومی مربوط به B برای کدکردن پیغام استفاده می کند. در این حالت B تنها کسی است که می تواند پیغام را رمزگشایی کرده و با استفاده از کلید خصوصی اش آن را بخواند.

- تصدیق اصالت (AUTHENTICITY)

گیرنده اطلاعات این امکان را پیدا می کند که هویت فرستنده را دریابد.

- صحت (INTEGRITY)

گیرنده این امکان را می یابد که هرگونه تغییر اطلاعات را شناسایی کند.

- عدم انکار (NONREPUDIATION)

فرستنده نمی تواند اطلاعات ارسالی را انکار کند و با قاطعیت می توان ادعا کرد که اطلاعات توسط فرستنده ارسال شده است.

- رمزنگاری با کلید نامتقارن یا عمومی

اطلاعات رمزدار شده و در طرف مقابل رمزگشایی می شود. (با روش جفت کلید)

- استفاده از امضای دیجیتالی.

فرستنده دارای یک کلید عمومی همراه با تاریخ انقضاست که آن را از یک کمپانی مخصوص مثل VERISIGN دریافت کرده است. با امضای پیغام، گیرنده می تواند آن را چک

کرده و صحت آن را ممیزی کند.

لایه های SSL: SSL شامل دو لایه SSL HANDSHAKE و SSL RECORD است.

SSL HANDSHOKE: به طور خلاصه در این لایه CLIENT با SERVER ارتباط برقرار کرده، کلید عمومی SERVER را دریافت کرده و هویت آن را در می یابد. سپس SERVER به شناسایی CLIENT می پردازد و در این زمان HANDSHAKING به پایان رسیده و در نهایت انتقال داده صورت می گیرد.

SSL RECORD: به طور مختصر بلاک های اطلاعاتی به RECORDهای SSL تقسیم بندی می شود. این لایه اقدام به فشرده سازی داده کرده و الگوریتم MAC را برای اطمینان از صحت داده استفاده می کند.

۲-۷ پروتکل های امنیتی پرداختی: باتوجه به اینکه تجارت الکترونیک باارزش میلیاردها دلار از طریق اینترنت صورت می گیرد، خرید از اینترنت بایستی باامنیت کامل پرداخت، روی شبکه های باز انجام پذیرد. پروتکل های IKP,SET (3KP,SEPP 2KP,1KP) امنیت پرداخت را در تبادلات تجارت الکترونیکی فراهم می کنند.(1) پروتکل IKP، از خانواده پروتکل های پرداختی امنیتی است که تبادلات بر پایه کارت اعتباری را بین مشتری و تاجر از نظر امنیتی پشتیبانی می کند. این پروتکل، پروتکلی باز است. این پروتکل برای دیگر شیوه های پرداختی مثل کارتهای بدهی، و چک های الکترونیکی و کارتهای هوشمند، قابل توسعه است. تکنیک رمزنگاری RSA همراه با صحت را به عنوان رمزنگاری کلید عمومی استفاده می کند. یک سیستم واقعی براساس این پروتکل، پروتکل SET است. SET توسط کمپانی های بزرگ VISA و MASTERCARD پشتیبانی شده و توسط IBM و چندین فروشنده در زمینه تکنولوژی اطلاعات توسعه یافته است. SET عملاً برای سیستم کارت اعتباری پیاده سازی شده و در حال استفاده است.

عملکرد پروتکل SET: SET، برای کاربر کیف الکترونیکی، گواهینامه دیجیتالی ایجاد می کند. SET، بعد از تصمیم گیری مشتری برای خرید وارد عمل می شود و مذاکرات قبل از خرید را در برنمی گیرد. نهادهایی که به نوعی در یک تراکنش کارت اعتباری درگیر هستند، شرکت کارت اعتباری، صادرکننده کارت، دارنده

تجارت الکترونیک دربرگیرنده مکانیسم های پرداختی مختلفی است که توسط شرکتهای گوناگون طراحی شده اند.

سیستم پرداخت بانک اینترنتی سیستمی است که تمام مراحل پردازش تجارت الکترونیک روی شبکه های عمومی را انجام می دهد.

کارت (خریدار)، تاجر و وصول کننده هستند. نهادهایی دیگری هم می توانند در این زمینه شرکت کنند که به نوعی سرویس دهنده هستند. عملکرد این پروتکل شامل مراحل زیر است:

- راه اندازی پرداخت (PINITREQ/PINITRES)؛
- سفارش خرید (PREQ/PRES)؛
- مجوزگیری (AUTHREQ/AUTHRES)؛
- تصرف پرداخت (CAPREQ/CAPRES)؛
- پرس و جوی دارنده کارت (INQREQ/INQRES) (اختیاری است).

۳-۷ پروتکل های مالی - پرداختی: تجارت الکترونیکی دربرگیرنده مکانیسم های پرداختی مختلفی است. این مکانیسم ها توسط شرکتهای متفاوتی مطرح و پیاده سازی شده اند. برای ایجاد سرویس های مالی یک سری مشخصات متحدالشکل ضروری است که تبادلات الکترونیکی داده بین موسسات مالی - بازرگانی و مشتریان از طریق اینترنت انجام گیرد. پروتکل OFX در این راستا مطرح شد تا فعالیتهای بانکداری، پرداخت صورتحساب، سرمایه گذاری و غیره را به طور مراحل خلاصه و مشخص بیان کند. این پروتکل به صورت یک سیستم CLIENT-SERVER عمل می کند روش ارتباط کاربر با موسسه مالی به صورت رد وبدل شدن درخواست REQUEST و پاسخ RESPONSE خواهد بود. انتقال داده توسط پروتکل HTTP صورت می گیرد. TAG های پیشنهادی به صورت عنصر ELEMENT و مجموعه ای از عناصر AGGREGATE خواهد بود [4,5].

سیستم پرداخت بانک اینترنتی BIPS درواقع یک معماری و اینترفیس استاندارد با سیستم های پرداختی بانک موجود را مطرح می کند [11]. این سیستم یک معماری عریض برای انجام تمام مراحل پردازش تجارت الکترونیکی روی شبکه های عمومی است. BIPS، دسترسی به چندین سیستم پرداختی را فراهم می کند که از جمله شبکه SWIFT (که در سال ۱۳۷۲ به شبکه بانکی ایران متصل شده)، CHIPS,FEDWIRE,ACH و سیستم هایی که در آینده مطرح خواهد شد را می توان نام برد.

پروتکل های NETCASH,ECASH,CYBERCASH و NETBILL برای انجام پرداختها از طریق اینترنت طراحی شده و پولهای الکترونیکی را پشتیبانی می کنند و هریک باتوجه به ویژگیهای خاص خود، کاربردهایی دارد [8].

منابع:

1 - Electronic Payment Systems,O'Mahony-Peirce, Tewari, 1997.
2 - IEEE Communication Magazine, Internet Commerce at Cisco Systems, September 1999.
3 - WWW. Netscape. Com/ssl.html, by brian lashley and andrzej tarski.
4 - http://www.microsoft.com/money/fi/ofx/what isofx.htm,2000.
5 - WWW. Ofx.net, last update May 13, 1999.
6 - hackers Proof: The Ultimate Guide to network Security, by lars klander, 1997.
7 - http://ei.cs.vt.edu/~wwwbtb/book/chap18/ssl.html
8 - http://www.digicash.com/publish/ecash-intro/ecash- intro.html,2000.
9 - Security requirements for Electronic Commerce, 10 May 1999.
10 -http://www.ict.tuwein.ac.at/eipan/cikersch/2000.
11 - http://www.fstc.org/press,2000.

● **آتوسا عباس نژاد: دانشجوی کارشناسی ارشد مهندسی صنایع و کارشناس مرکز تحقیقات مخابرات ایران.**