مجله‌ی علمی پژوهش در علوم رایانه، شماره ۲۲، تابستان ۱۴۰۰، ص ۱۲ – ۱

ISSN: 2745-3673
http://www.Rcsj.ir

مجله علمی پژوهش در علوم رایانه (سال ششم)
شماره ۲۲ / تابستان ۱۴۰۰ / ص ۱۲ – ۱

امنیت در تجارت الکترونیک

فاطمه بهرامی ضیابری[۱]، سعید زاهدی[۲]

[۱] کارشناسی ارشد مهندسی تجارت الکترونیک واحد لاهیجان.
[۲] استاد گروه مهندسی کامپیوتر دانشگاه فردوسی مشهد.

نام نویسنده مسئول:
فاطمه بهرامی ضیابری

تاریخ دریافت: ۱۴۰۰/۳/۱۵
تاریخ پذیرش: ۱۴۰۰/۵/۳۱

چکیده

با توجه به پیشرفت سریع فناوری اطلاعات و جایگزینی تجارت آنلاین (تجارت از طریق اینترنت) با تجارت سنتی، مسائل امنیتی، اللخصوص برای کسب وکارها در محیط تجارت الکترونیک، اهمیت بسیاری پیدا کرده است. در تعریف امنیت میتوان گفت که امنیت به مجموعهٔ تدابیر، روشها و ابزار برای جلوگیری از دسترسی و تغییرات غیرمجاز در نظام رایانه ای گفته می شود و امنیت اطلاعات به حفاظت از اطلاعات و به حداقل رساندن خطر افشای آنها در بخش های غیرمجاز اشاره می کند. در تجارت الکترونیک به منظور شکل گیری و سرویس دهی، نیازمند محیطی هستیم که از طریق آن افراد مختلف بتوانند داد و ستد خود را انجام بدهند.این محیط که در اینجا همان برنامه های تحت وب می باشند، خود نیازمند بستری جهت قرارگیری می باشند. حال در اینجا نیاز به ارائه سرویس ها مطرح می شود که خود این امر در برگیرنده مباحث نرم افزاری چون سیستم عامل، سرویس دهنده وب و مباحث سخت افزاری چون سرویس دهندگان و ساختار آنها می باشد. البته مسئله ی بسیار مهم و حیاتی در این سیستم ها بر قراری امنیت در این سیستم ها می باشد. پیشرفت مداوم تکنولوژی در جوامع کنونی منجر به گسترش استفاده از شیوه های خرید آنلاین و خرید های اینترنتی شده است اما یکی از ایراد این روش این است که منجر به بی دقتی و تنبلی کاربران در مورد اطلاع پیدا کردن از صحت فروشنده و حفاظت از اطلاعات شخصیشان شده است. بدین ترتیب در هر کسب و کار اینترنتی که شکل می گیرد نیاز است که در ابتدا مطالعات وسیعی در زمینه های امنیتی هم چنین افزایش آگاهی در خصوص قوانین و سیاست های امنیتی صورت پذیرد تا کاربران نیز به توانند با اطمینان خاطر مضاعف به این کسب و کار ها اعتماد کنند و از آن ها بدون وجود هیچ گونه دغدغه ایی بهره مند بشوند.

واژگان کلیدی: تجارت الکترونیک – امنیت – تکنولوژی - فن آوری اطلاعات.

مجله‌ی علمی پژوهش در علوم رایانه، شماره ۲۲، تابستان ۱۴۰۰، ص ۱۲-۱

ISSN: 2745-3673
http://www.Rcsj.ir

مقدمه

امروزه برای موفقیت در جهش صادراتی، مستلزم شناسایی تحولات جهشی، مانند تجارت الکترونیک در عرصه تجارت بین المللی می باشد (خدادا حسینی و فتحی ۱۳۸۱) همچنین این مسئله باید مد نظر قرار داده شود که تجارت الکترونیک و جهانی شدن آن دو پدیدخه ی مهم و بحث برانگیز در دنیای امروزه می باشد که فرصت های زیادی را برای بنگاه های موجود در این حیطه ایجاد می کند و بنگاه ها با بهره گیری از این فرصت ها می توانند موفقیت خود را در بازار های جهانی تضمین کنند. (صباغ کرمانی و اسفیدانی، ۱۳۸۴)

البته این نکته نیز حائذ اهمیت می باشد که به دلیل تحولات گسترده ای که در سال های گذشته در عرصه تجارت الکترونیک رخ داده است، شاهد می باشدم که سازمان های بسیار ی به حیطه سرمایه داران بزرگ اضافه شده و پا به عرصه تجارت الکترونیک می گذارند، ولی بسیار ی از آنان با شکست و نا کامی مواجه می شوند. بنابراین با وجود رشد سریع تجارت الکترونیک، محدودیت های موجود مانع رشد سریع این تجارت می گردد. مورد دیگری که در این گونه از تجارت ها باید مد نظر قرار داد این است که اطلاعات در سیستم های رایانه ای مجزا از یکدیگر هستند، یعنی حالتی کاملاً ایستا را دارند، بنابر این حفظ امنیتی آن کار دشواری نیست ؛ ولی با اتصال گسترده ی رایانه ها و پیدایش شبکه های ارتباطی دیگر ازلاعات که امروزه مهم ترین کالای این عرصه می باشد تنها مقیم یک رایانه ی خاص نیست و در پهنای شبکه های گستر ده ی اطلاعاتی مرتب در حال جابهجایی می باشد. (جعفری ۱۳۸۵)

همین مسئله منجر گردیده است که در جهان کنونی مسئله ی حفظ ازلاعات به یک چالش جدی در پیش روی ما تبدیل گردد، همچنین به دلیل افزایش استفاده از ایمیل ها برای تبادل اطلاعات و معاملات آنلاین در سازمان ها موجب افزایش نیاز به ارتباطات با امنیت بالا گردیده است. بخصوص که کلاهبرداری ها و سایر روش های هک در این فضا ها روز به روز پیشرفته تر و هوشمندانه تر شده است.

در نتیجه اگر شرکتی بخواهد خود را به سیستم تجارت الکترونیک مجهز نماید و خواهان دستیابی به پتانسیل واقعی در حوزه ی تجارت الکترونیک باشد ابتدا باید بتواند زیر ساخت های لازم و مطرح در این حوزه را مد نظر قرار دهد در تجارت الکترونیک به دلیل استفاده از محیط های شبکه ای برای اینگونه تجارت ها میزان ریسک بسیار بالا می باشد که تأمین امنیت این شبکه ها برای جلوگیری یا به حداقل رساندن این ریسک امری ضروری به نظر می رسد. (جاج ملک و توکلی، ۲۰۱۶)

با توجه به این مسئله که نقش فناوری ازطلاعات یک نقش محوری در حوزه ی دارایی های ارزشمند هر سازمان می باشد می توان گفت که امنیت اطلاعات به یکی از مولفه های کلیدی در مدیریت و برنامه ریزی در شهر های مدرن تبدیل گشته است. پس می توان امنیت را پایه ی یکپارچگی و رشد کسب و کار الکترونیکی به شمار آورد. (کرونین، ۱۹۹۵)

حفظ امنیت اطلاعات یکی از مؤلفه های اساسی در مدیریت و برنامه ریزی شرکت های مدرن می باشد به علاوه لازم به ذکر است که مدیریت امنیت اطلاعات، به منظور حفاظت از شرکت ها در برابر طیف وسیعی از تهدید ها به منظور اطمینان از تداوم یافتن کسب و کارشان و همچنین به حداقل رساندن اسیب ها بسیار حائذ اهمیّت می باشند. البته امنیت یک سیستم را از طریق در نظر گرفتن عوامل فیزیکی مانند سخت افزار، منطقی از قبیل نرم افزار و قدرت امنیت سازمانی، می توان برقرار کرد. پس تجزیه و تحلیل حمله های داخلی و خارجی محتمل نیز جنبه ی مهمی از برقرار امنیت اطلاعاتی را در بر می گیرد. (نجف زاده ۲۰۱۱)

با توجه به مفاهیم مطرح شده در عنوان مقاله هدف اصلی در پژوهش حاضر امنیت و نحوه ی برقراری آن در تجارت الکترونیک می باشد. که با توجه به این هدف، ابتدا به تعریف تجارت الکترونیک و مفهوم امنیت و هم چنین امنیت در تجارت الکترونیک می پردازیم و سپس به بررسی انواع امنیت در تجارت الکترونیک و سیاست های اتخاذ شده در این زمینه و نحوه ی مدیریت امنیت در تجارت الکترونیک خواهیم پرداخت.

مجله‌ی علمی پژوهش در علوم رایانه، شماره ۲۲، تابستان ۱۴۰۰، ص ۱۲-۱

ISSN: 2745-3673
http://www.Rcsj.ir

تعریف تجارت الکترونیک

به دلیل گستردگی حوزهٔ تجارت الکترونیک، برای آن تعاریف بسیاری بیان شده است که از مجموع آنها میتوان دریافت که تجارت الکترونیک کاربردهای وسیعی را دارا می باشند. گفتنی است بیش از ۳۰ نوع فناوری موجود می باشد که از آنها در تعریف تجارت الکترونیک استفاده شده است و این موضوع گستردگی تجارت الکترونیک را نشان میدهد. (Niranjanamurthy, M., & Chahar, D,2013)

تجارت الکترونیک تعاریف متعددی دارد که چند نمونه ی آن به شرح زیر می باشد :

۱- انجام هر گونه امور تجاری وبازرگانه از طریق شبکه ی جهانی اینترنت را تجارت الکترونیک می گویند که این امور می تواند شامل مواردی از جمله عمده فروشی و خرده فروی در کالاهای فیزیکی و غیر فیزیک و هم چنین ارائه ی سرویس های مختلف به مشتریان و امور تجاری دیگر می باشد.

۲- تجارت الکترونیک نامی عمومی می باشد برای گستره هایی از نرم افزار ها و سیستم ها که خدماتی از جمله جست و جوی ازلاعات، مدیریت تبادلات، بررسی وضعیت اعتبار، اعطای اعتبار، برداخت به صورت آنلاین گزارشگیری و موارد دیگری را شامل می گردد در واقع این سیستم ها زیر بنای اساسی فعالیت های مبتنی بر اینترنت را فراهم می کنند. (سرمدی و میرایی ؛۱۳۸۳)

۳- تجارت الکترونیک عبارت است از مبادله، تجارت بدون استفاده از کاغذ که در آن نوآوری هایی همانند مبادلهء الکترونیکی داده ها، پست الکترونیک، تابلو اعلانات الکترونیک، انتقال الکترونیک وجه و سایر فنآوریهای مبتنی بر شبکه بکار گرفته می شود. تجارت الکترونیک نه تنها عملیاتی را که در انجام معاملات بطور دستی و با استفاده از کاغذ صورت میگیرد را به حالت خودکار درمیآورد بلکه سازمانها را یاری میکند که به یک محیط کاملاً الکترونیک وارد شوند و روش های کاری خود را تغییر دهند. هر نوع فعالیتی که هدف تجاری داشته باشد و در یک قالب الکترونیکی صورت گیرد را می توان تجارت الکترونیک نامید. به عبارت دیگر تجارت الکترونیک، تجارتی می باشد که از وسایل الکترونیکی از جمله کامپیوتر برای انجام آن استفاده می شود. تجارت الکترونیک شامل بخشهای گوناگونی از جمله : مبادله الکترونیکی سهام و وجوه، مبادله الکترونیکی مطالب کالاها و خدمات نامه های الکترونیکی، طرح های تجاری، بازاریابی های مستقیم تبلیغات، قبول سفارشات و.. . را شامل می شود. (سیامک قاجاری، ۱۳۷۴)

بسیاری ازسازمان ها و شرکت هایی که به تجارت الکترونیک روی آورده اند به دنبال ترقی و پیشرفت در این عرصه و رسیدن به نقطه ایده آل خود هستند که برای دست یابی به این نقطه در ابتدا لازمه است که ۵ گام زیر را به درستی در روند تجاری خود طی کنیم که این ۵ گام عبارت اند از :

گام اول) در مرحله اول شرکت یا سازمان متقاضی تجارت الکترونیک باید سعی کند که یک سایت ساده که شامل اطلاعات و داده های محصولات و خدمات تولیدی اش می باشد را ایجاد کند و در اختیار مشتریان خود را قرار بدهند . در حقیقت، مرحله اول به معنای ایجاد ویترینی بر روی شبکه های سراسری مانند وب برای بازدیدکنندگان می باشد تا اطلاعات مورد نظر خود را از طریق این صفحات دریافت نمایند. بعنوان مثال اگر شبکه داخلی کشوری و یا سازمانی راه اندازی شده باشد می توان تجارت را بدون استفاده از اینترنت راه اندازی نمود.

گام دوم) در این گام توسعه و گسترش گام اول مد نظر می باشد. در این مرحله سایت شرکت تبدیل به یک پایگاه داده دیتا بیس می گردد و برای نگهداری اطلاعات به کار گرفته می شوند. در این مرحله، اطلاعات در همه محصولات و خدمات و شرح آن ها به طور کامل در بانک اطلاعات قرار می گیرد و کاربران امکان ارسال سفارش خرید خود را از طریق این وب سایت، خواهند داشت، اما هنوز زیرساخت های لازم برای پرداخت اینترنتی ایجاد نشده است و پرداخت پول به همان روش سنتی انجام می گیرد. این روش ها را بعضی از سازمان ها بعنوان روشی امن برای خود برمی گزینند اما این کار در واقع به نوعی بی بهره ماندن از فناوری موجود می باشد.

گام سوم) گام سوم شامل ایجاد تعامل میان کاربران و سایت شرکت ها می باشد. در این مرحله، کاربران امکان ارتباط با مدیر سایت را خواهند داشت که این ارتباط از طریق ایمیل، چت ویدئو کنفرانس و دیگر ابزار ارتباط الکترونیکی دیگر می باشد

ISSN: 2745-3673
http://www.Rcsj.ir

که از مزیت های این روش این است که کاربران در مدت زمان بسیار کوتاهی پاسخ خود را از مدیر سایت دریافت می کنند و امکان پرسش و پاسخ به صورت آنلاین در میان فروشنده و خریدار و نیز بحث در مورد کالا و یا خدمات ایجاد می گردد ضروری است که. این تعاملات از دیدگاه کاربران یک رابطه امن و کاملا خصوصی تلقی می گردد. چرا که این ارتباط یک ارتباط مجازی بوده و کوچک ترین مسایل از دید مشتری پنهان نخواهد ماند.

گام چهارم) در این گام، امکان پرداخت اینترنتی برای کاربران فراهم می گردد و مشتریان پس از ارسال فرمهای سفارش خرید و دریافت کالا، وجه موردنظر را از طریق پایانه های فروش بانک ها و مؤسسات مالی طرف قرارداد برای فروشنده ارسال می کنند که این حمل و نقل پول به صورت بسیار امن از طریق شبکه برای مشتریان فراهم می شود این خریدها اگر بصورت محدود باشد می توان با استفاده از پروتکلهای امنیتی در اینترنت نیز آن را انجام داد. اما تقریبا تمامی تجارتهای کلان که بصورت الکترونیکی هستند روی اینترنت انجام نمی شوند.

گام آخر) گام آخر به مرحله یکپارچگی معروف می باشد. در این مرحله، سیستم های واسطه ای میان فروشنده و خریدار با سیستم های موجود در سازمان و یا شرکت به حالت یکپارچگی کامل در می آیند. بدین معنا که اگر کالایی فروخته شود، موجودی کالاهای فروش رفته به میزان خریداری شده از موجودی انبار کسر شده و همزمان دستور خرید جدیدی برای جایگزین کردن کالای فروش رفته به انبار ارسال گشته و در خرید های بعدی موجودی انبار بلافاصله به نمایش در می آیند. این مرحله از مجموعه مراحل تجارت الکترونیک کاملترین مرحله در تجارت الکترونیکی می باشد که در آن نتیجه همه عملیات مربوط به داد و ستد در همه سیستمهای سازمان منعکس می گردد. این کار زیر ساخت شروع بکار سیستمهایی همانند مدیریت ارتباط با مشتری (CRM) می باشد. (حسینی و همکاران ۲۰۰۹)

تعریف امنیت:

امنیت به معنای کیفیت یا حالت امن بودن،رهایی از خطر،ترس و احساس نگرانی و تشویش می باشد.این تعریف در دنیای تجارت الکترونیک نیز صادق می باشد و حفظ و بقای آن در چهار اصل خلاصه گردیده است:

محرمانگی : اطلاعات فقط و فقط باید توسط افراد مجاز قابل رویت باشد.

تمامیت : یک سیستم متشکل از عناصری است که در کنار هم برای رسیدن به هدف مشخصی همکاری می کنند.حفظ تمامیت به معنای پیشگیری از بروز مشکل در این همکاری و پیوسته نگه داشتن عناصر یک سیستم می باشد. در و اقع باید سعی گردد که داده ی فرستاده شده در طول راه دچار تغییر نشود و بسته ی فرستاده شده تماما و به درستی به دست گیرنده برسد.

دسترس پذیری : اطلاعات بایستی به هنگام نیاز توسط افراد مجاز قابل رویت باشد و سیستم های امنیتی به گونه ای طراحی شوند که در صورت نیاز بدون وقفه اطلاعات قابل حصول باشند.

عدم انکار : به هنگام انجام کاری و یا دریافت اطلاعات یا سرویسی، شخص انجام دهنده یا گیرنده نتواند آن اطلاعات یا را انکار کند.

امنیت به طور کلی به معنای از حفاظت در برابر حملات عمدی و غیرعمدی توسط سرویس ها و اشخاص در برابر آنچه که برای ارزشمند است می باشد . در واقع امنیت اطلاعات، پاسداری از حریم خصوصی افراد است که که معادل اطلاعات خصوصی، مبادلات تجاری، مبادلات مالی، ارتباطات شخصی، اقامتگاه شخصی و وضعیت فیزیکی و جسمانی فرد می باشد.(*Rane, P. B., & Meshram, B. B. 2012*)

امنیت در تجارت الکترونیک

با توجه به پیشرفت سریع فناوری اطلاعات و جایگزینی تجارت آنلاین (تجارت از طریق اینترنت) با تجارت سنتی، مسائل امنیتی، اللخصوص برای کسب وکارها در محیط تجارت الکترونیک، اهمیت بساری پیدا کرده است. در تعریف امنیت میتوان گفت که امنیت به مجموعۀ تدابیر، روشها و ابزار برای جلوگیری از دسترسی و تغییرات غیرمجاز در نظام رایانه ای گفته می شود

ISSN: 2745-3673
http://www.Rcsj.ir

و امنیت اطلاعات به حفاظت از اطلاعات و به حداقل رساندن خطر افشای آنها در بخش های غیرمجاز اشاره می کند. (قاسمی شبانکاره، مختاری و امینی لاری، ۱۳۸۶).

مفهوم امنیت در تجارت الکترونیک در حوزه های وسیعی مطرح گردیده است.در بررسی امنیت هر سیستمی، بنا بر اصول مشخص شده در استانداردها، در ابتدا باید دارایی های سیستم مشخص شده و سپس ارزش گذاری شوند و بعد از آن خطرات دارایی ها مورد بررسی قرار بگیرد و مطابق با هر خطر راه کاری ارائه گردد. در بررسی هرکدام از این موارد و به منظور ارائه ی راه کارهای مناسب ابتدا باید خطراتی که آنها را تهدید می کنند، را به خوبی بشناسیم و آنها را به دقت مورد تحلیل و بررسی قرار بدهیم.

در جهان کنونی امنیت شبکه یک مساله مهم برای ادارات و شرکت های دولتی و سازمان های کوچک و بزرگ می باشد. تهدیدهای پیشرفته از سوی تروریست های فضای سایبر، کارمندان ناراضی و هکرها، رویکردی سیستماتیک را برای امنیت شبکه ایجاد می کند. در بسیاری از صنایع، امنیت به شکل پیشرفته نه یک انتخاب بلکه یک ضرورت می باشد. این رویکرد هم یک راهبرد فنی است که ابزار و امکان مناسبی را در سطوح گوناگون در زیرساختار شبکه قرار داده و هم یک راهبرد سازمانی می باشد که این مسئله خواستار مشارکت همگانی است. (*Marchany, R. C., & Tront, J. G. 2002, January*)

رویکرد امنیتی طبقه بندی شده بر روی نگهداری ابزارها و سیستم های امنیتی و روال ها در پنج لایه در محیط فناوری اطلاعات متمرکز می شود. محافظت از اطلاعات اختصاصی به منابع مالی نامحدودی نیازمند است. در یک دنیای ایده آل، بودجه و منابع کافی برای پیاده سازی همه ابزارها و سیستم های مورد بحث موجود می باشد. اما خب متاسفانه ما در چنین دنیایی زندگی نمی کنیم. بدین ترتیب، باید شبکه ها را ارزیابی نماییم (چگونگی استفاده از آن، طبیعت داده های ذخیره شده، کسانی که نیاز به دسترسی دارند، نرخ رشد آن و ...) و سپس ترکیبی از سیستم های امنیتی را که بالاترین سطح محافظت را ایجاد می نمایند را، با توجه به منابع موجود پیاده سازی کنیم. یکی از مهم ترین فعالیت های مدیر شبکه، تضمین امنیت منابع شبکه می باشد. دسترسی غیر مجاز به منابع شبکه و یا ایجاد آسیب عمدی یا غیر عمدی به اطلاعات، امنیت شبکه را مختل می نماید. از طرف دیگر امنیت شبکه نباید آنچنان باشد که کارکرد عادی کاربران را با مشکل مواجه کند. (زرگر ؛۲۰۰۷)

برای تضمین امنیت اطلاعات و منابع سخت افزاری شبکه، از دو مدل امنیت شبکه استفاده می شود. این مدل ها عبارتند از: امنیت در سطح اشتراک[1] و امنیت در سطح کاربر[2] در مدل امنیت در سطح اشتراک، این عمل با انتساب اسم رمز یا پسورد[3] برای هر منبع به اشتراک گذاشته تامین می شود. دسترسی به منابع مشترک فقط هنگامی برقرار می گردد که کاربر اسم رمز صحیح را برای منبع به اشتراک گذاشته شده را به درستی بداند(پورسلیمی ؛۲۰۱۵)

تفاوت این دو مدل در آن است که در مدل امنیت در سطح اشترلک، اسم رمز به منبع نسبت داده شده و در مدل دوم اسم رمز و کلمه عبور به کاربر نسبت داده می شود. بدیهی است که مدل امنیت در سطح کاربر بسیار مستحکم تر از مدل امنیت در سطح اشتراک است. بسیاری از کاربران به راحتی می توانند اسم رمز یک منبع را به دیگران بگویند. اما اسم رمز و کلمه عبور شخصی را نمی توان به سادگی به شخص دیگری منتقل کرد.(زرگر ؛۲۰۰۷)

تجارت الکترونیکی که در اینجا مد نظر می باشد تجارت الکترونیکی می باشد که، به منظور شکل گیری و سرویس دهی، نیازمند محیطی است که از طریق آن افراد مختلف بتوانند داد و ستد خود را انجام دهند.این محیط که در اینجا همان برنامه های تحت وب می باشند، خود نیازمند بستری جهت قرارگیری هستند. حال نیاز به ارائه سرویس مطرح می گردد که خود در برگیرنده مباحث نرم افزاری چون سیستم عامل، سرویس دهنده وب و مباحث سخت افزاری چون سرویس دهندگان و ساختار آنها می باشد. (کفاش پور و دهنوی ۲۰۱۱) در بحث تجارت الکترونیک عواملی از قبیل برنامه های تحت وب، سرویس دهنده، بستر ارتباطی و دریافت کننده که عمدتا مشتری می باشد، بایستی در کنار هم قرار گیرند تا یک تجارت الکترونیک شکل گیرد که بحث مهمی که در تجارت الکترونیک مطرح می باشد برقراری امنیت به ویژه امنیت اطلاعاتی در این نوع تجارت است. برقراری امنیت در تجارت الکترونیک عامل مهمی در پیشرفت این نوع تجارت می باشد.

---

[1] (Share-Level)
[2] (User-Level)
[3] Password

ISSN: 2745-3673
http://www.Rcsj.ir

انواع امنیت در تجارت الکترونیک

در تجارت الکترونیک به منظور شکل گیری و سرویس دهی، نیازمند محیطی هستیم که از طریق آن افراد مختلف بتوانند داد و ستد خود را انجام بدهند.این محیط که در اینجا همان برنامه های تحت وب می باشند، خود نیازمند بستری جهت قرارگیری می باشند. حال در اینجا نیاز به ارائه سرویس ها مطرح می شود که خود این امر در برگیرنده مباحث نرم افزاری چون سیستم عامل، سرویس دهنده وب و مباحث سخت افزاری چون سرویس دهندگان و ساختار آنها می باشد. (حسینی و همکاران ؛۲۰۰۹) البته مسئله ی بسیار مهم و حیاتی در این سیستم ها بر قراری امنیت در این سیستم ها می باشد، که امنیت در برقراری تجارت الکترونیک موفق، شامل مراحل زیر می باشد:

امنیت شبکه[۴]: امنیت شبکه شامل سیاست ها و اقدامات اتخاذ شده جهت نظارت و جلوگیری از دسترسی های غیر مجاز، سوء استفاده و هک شدن است. به عبارتی دیگر به هر گونه فعالیتی مبنی بر محافظت از استفاده و یکپارچگی شبکه و داده ها، امنیت شبکه گفته می شود. شبکه های کامپیوتری می توانند همانند شبکه های شرکتی خصوصی باشند و یا این که به صورت عمومی باشند و در دسترس عموم قرار بگیرند.

امنیت میزبان[۵]: در این سطح امن سازی رایانه ها به نحوی انجام می شوند که رایانه را به عنوان یک موجودیت مستقل در شبکه در نظر می گیریم ولی مدیریت این امنیت را از طریق درگاه های خاصی در شبکه اعمال می کنیم در واقع امنیت این رایانه ها در صورت اتصال به شبکه از طریق سامانه های خاص و اعمال سیاست های امنیتی مناسب و به صورت متمرکز انجام می پذیرند و برای رایانه های سینگل، این امنیت به صورت انحصاری و محدودتری قابل اجرا می باشند.

امنیت سرویس دهنده وب : مقوله امنیت وب[۶] سایت از اهمیت بالایی برخوردار می باشد. باید در طراحی وب سایت از نقطه شروع تا پایان امنیت وب سایت اعمال گردد و همچنین پس از پایان طراحی وب سایت باید امنیت وب سایت بصورت کاملا تخصصی توسط کارشناسان طراحی وب سایت رصد بشود, زیرا با توجه به گسترده بودن دنیای تجارت الکترونیک و حضور اکثریت رقبا در این دنیای مجازی امکان حملات مخربانه از سوی رقبا و یا هکر ها بسیار زیاد می گردد. مهمترین بخش شناسایی نوع حملات می باشد. کافیست طراحی وب با مدنظر قرار دادن تهدیدها انجام شود تا درمقابل آنها ایمن بگردد. تست های نفوذ متعدد و همچنین پیاده سازی استاندارد های امنیتی، راه کار توصیه شده ما در امنیت وب است. در بسیاری از موارد، شریان انتقال اطلاعات را با استفاده از پروتکل های رایج (همانند SSL) را می توان به راحتی امن ساخت.

امنیت سیستم عامل[۷]: در یک حالت کلی به مجموعه اقداماتی گفته می شود که به منظور جلوگیری از بروز مشکلات امنیتی در بستر شبکه صورت می گیرد. این مجموعه اقدامات می تواند بصورت راهکارهای متعددی در غالب سرویس های سخت افزاری و نرم افزاری پیاده سازی بشوند. لازم به ذکر است که معمولا بسیاری از روشهای تامین امنیت توسط رول ها[۸] انجام می شوند.

دیوارهای آتش[۹]:در سامانه دیوار آتش سعی می شود که از سیستم مدیریت پورت ها استفاده بشود. این سیستم به این گونه کار می کند که پورت های مورد نیاز برای ارسال و یا دریافت اطلاعات را به صورت موقت باز می کند و در نهایت پس از اتمام دستور العمل تبادل اطلاعات آن را می بندد. با این کار دسترسی هکرها و یا سایر نفوذگرهای شبکه محدود می گردد.

یک خط مشی توام با آموزش[۱۰]: خط مشی های امنیتی در بر گیرنده تنظیمات سیستم ها و شبکه هایی هستند که شامل نصب نرم افزارها و سخت افزارها و اتصالات شبکه ای می شوند. خط مشی ها امنیتی نحوه شناسایی افراد، سطوح دسترسی کاربران، و نحوه انجام گرفتن عملیات بازرسی را تشریح و تعریف می کنند. اینگونه خط مشی ها همچنین در برگیرنده رمزنگاری

---

[4] Network Security
[5] Host Security
[6] Web Server Security:
[7] OS Security
[8] (Roles)
[9] Firewall:
[10] Security Policy

ISSN: 2745-3673
http://www.Rcsj.ir

و نرم افزارهای آنتی ویروس، روش های انتخاب رمز عبور، نحوه از بین رفتن اعتبار حساب ها کاربری، تعداد ورودهای نا موفق و چیزهایی مشابه آن هستند. (کلیدر و همکاران ۲۰۱۵)

در مبحث تجارت الکترونیک مواردی از جمله برنامه‌های سرویس دهنده، برنامه‌های تحت وب و بسترهای ارتباطی و دریافت کننده هایی که اکثرا شامل مشتری ها میباشند، بهتر است در کنار یکدیگر قرار بگیرند تا تجارت الکترونیک موفقی پایه ریزی بشود و اگر این محور را به شکل یک سیستمی ایجاد بکنیم خواهیم توانست کلیه این موارد را در مفهوم کلی ۱ – تولید، ۲- ارائه، ۳- انتقال، ۴- دریافت محصولات و یا کالا در اختیار داشته باشیم. برای درک بهتر به توضیحات مربوط به هر کدام بصورت جدا گانه می پردازیم.

امنیت در تولید : در مفهوم تولید، بیشتر با یکسری از برنامه های تحت وب و بانکهای اطلاعات در ارتباط می باشیم. فارغ از این موضوع که این برنامه ها توسط تیمی مشخص به منظور انجام یک داد و ستد اینترنتی به وجود آمده اند و یا به‌صورت آماده در قالب بسته های نرم افزاری تهیه شده اند، تهدیداتی متوجه‌آنها می باشد.این تهدیدات عمدتاً به منظور به دست‌آوردن اطلاعاتی محرمانه و یا ایجاد تغییری در سیستم، به منظور جعل هویت، دستکاری مبلغ کل‌در راستای‌کاهش آن و یا حتی‌تغییری در صفحه اصلی به منظور تخریب اعتبار آن مجموعه هستند.

امنیت در ارائه : عواملی که در مفهوم ارائه نقش دارند، عمدتا بسترهایی می باشند که عوامل مفهوم تولید به منظور فعالیت بر روی آن سوار می‌شوند. سیستم عامل، سرویس دهنده وب، سرویس دهنده بانک اطلاعاتی، سخت افزارهای مورد استفاده و... از جمله عواملی هستند که می توانیم در اینجا نام ببریم. بیشتر تهدیدهایی که عوامل ارائه را در معرض خطر قرار می‌دهد مربوط به ضعف تکنولوژی هستند و موارد دیگر در جایگاه‌های بعدی قرار می گیرند.

امنیت در انتقال :در بحث انتقال، که تنها با بستر ارتباطی سروکار دارند، از جمله مهمترین خطراتی که آن را تهدید می کند شامل، شنود اطلاعات مهم توسط یک فرد غیر مجاز می باشد. حال این شنود می تواند منجر به افشاء اطلاعات کارت اعتباری و یا شناسه کاربری شود و یا می‌تواند از طریق شنود شناسه نشست، هکر بتواند کنترل ارتباط را بدست بگیرد و با جعل هویت خود شروع به کار کند.

امنیت در دریافت : در مفهوم دریافت، به طور کلی با کاربران سیستم در ارتباط هستیم.اما در اینجا نیز همچون نواحی پیشین، خطرات و معضلاتی وجود دارد :

الف) انکار سفارش : این تهدید شاید در دنیای تجارت الکترونیک پیشرفته امروز اندکی بی معنا باشد. اما در ایران در برخی از سیستم ها که سفارش به صورت اینترنتی انجام می پذیرد و دریافت هزینه همزمان با تحویل کالا در محل مشتری انجام می گیرد، می تواند تهدیدی جدی به حساب آید، چرا که هیچ سیستمی به طور پیش فرض به منظور اثبات این موضوع که چه شخصی سفارش دهنده بوده است موجود نمی باشد.

ب) انکار دریافت کالا : این تهدید به طور عمده ای می تواند در نقل و انتقالات اینترنتی وجود داشته باشد به طوریکه دریافت کننده همواره دریافت سرویس و یا کالا را انکار کند.

ج) کلاه برداری : کلاه برداری های اینترنتی روش های بسیار زیادی دارند، اما آن دسته که در ارتباط با تجارت الکترونیک می باشد، شامل فریب دادن کاربران و دریافت اطلاعات کارت اعتباری آنها و یا دریافت هزینه ای بیشتر از قیمت کالا یا سرویس هستند. (طباطبایی؛ ۲۰۱۵)

سیاستهای امنیتی در تجارت الکترونیک

نیاز به نگرش جامع در زمینهٔ امنیت و همچنین الزامات امنیتی، در تجارت الکترونیک از دیدگاه وان سولمز (۲۰۰۱،) ؛ مورد مطالعه قرار گرفته است. زوکاتو (۲۰۰۲) نیز در این زمینه نگرش جامعی را ارائه داده و جنبه های مختلف و روابط آنها را در مواجهه با ابعاد مختلف امنیت، مورد بررسی قرار داده است () تشخیص الزامات توسط منابع کسب وکار، محیط و مدیریت ریسک، را پیشنهاد داده است و از آنجایی که فعالیت مهم در بخش مهندسی الزامات امنیتی، گردآوری آنها از منابع مختلف در

ISSN: 2745-3673
http://www.Rcsj.ir

یک مجموعه می باشد ؛ برای تشخیص چگونگی امنیت سیستم، باید الزامات براساس اهمیت و امکانپذیری آن طبقه بندی شوند(وان سولمز ۲۰۰۱)

البته باید در نظر داشت که با توجه به تهدیدهای زیادی که امروزه در محیط های سایبری وجود دارد، سازمانها به کنترلهای امنیتی برای محافظت از اطلاعات با ارزش خود نیازمند هستند. براساس دیدگاه هون و الوف (۲۰۰۲،) بدون تردید یکی از بخش های مهم کنترلی در حوزه سیاست امنیت اطلاعات می باشد. در همین راستا، وایتمن، تاوزند و آلبرتز بیان کردند که توسعهٔ سیاست امنیت اطلاعات، اولین گام در جهت آماده شدن سازمان در برابر حملات منابع داخلی و خارجی می. از طرفی دیگر، به منظور اثربخشی مدیریت امنیت، باید عوامل فنی و اجتماعی به طور همزمان مد نظر قرار داده شوند. درواقع در سیاست های امنیتی، این عناصر را در برنامهٔ منسجمی که سازمان برای اجرای امنیت به کار میبرد، ادغام می کنند. (اسمیت ؛۲۰۱۰)

با افزایش تجارت الکترونیک در فضای جهانی، اهمیت پرداختن به مبحث امنیت سایبری در خصوص انجام معاملات در فضای الکترونیک دو چندان گشته است. جریان اطلاعاتی که در فضای سایبر وجود دارد، هم اکنون توسط اکثر صاحبان مشاغل و تجار به عنوان منبع کسب اطلاعات مورد استفاده قرار می گیرند. (*jing,2009*)

سیاست پیشنهادی بروکینگز[11] برای مقابله با تهدیدات تجارت الکترونیک

سیاست های امنیت سایبری در تعامل با سیاست های تجاری می تواند محیط امنی را در تجارت دیجیتال به وجود آورند و رشد تجارت الکترونیکی را سرعت می بخشد. از همین رو موسسه مطالعات سیاست گذاری بروکینگز سیاست هایی را در راستای تحقق این امر پیشنهاد داده است که عبارت اند از :

دسترسی به داده ها: با پیچیده تر شدن الزامات امنیت سایبری، استفاده از مکانیسم های تحلیلی برای نظارت بر شبکه نقش مهم تری را برای تحلیل ریسک ها و ناهنجاری های شبکه افزایش می یابد . درصورتی که داده ها محدود تر بشوند و در اختیار همگان قرار نگیرند، در فضای بین المللی شرکت ها نمی توانند از حجم بالایی از اطلاعات در تحلیل های خود استفاده کنند.

محدود ساختن داده ها باعث می شود تا ریسک و هزینه دریافت اطلاعات افزایش پیدا کند در مقابل جریان اطلاعات در مرز ها، امنیت تجارت دیجیتال و در نتیجه میزان استفاده از آن را نیز مورد افزایش قرار می دهد.

اشتراک گذاری اطلاعات: به اشتراک گذاری اطلاعات مربوط به تهدیدات و آسیب پذیری ها برای ارتقاء آگاهی ها، بهبود واکنش ها و تحقق اهداف، در زمان واقعی و بدون تاخیر به یکی از خصیصه های اصلی سیاست های امنیت سایبری تبدیل شده است.

مسائل مربوط به امانت داری و حفظ محرمانگی در انتشار اطلاعات خصوصی و اطلاعات طبقه بندی شده درون مرزها موجب دشوار شدن تعامل با دولت ها و سازمانهای داخلی می شود. ایجاد موافقت نامه های تجاری که شامل تعهدات ایجاد سازوکار های اشتراک گذاری اطلاعات بخش های عمومی و خصوصی هستند که می تواند باعث تسهیل اشتراک گذاری اطلاعات گردد.

استاندارد های امنیت سایبری: استانداردهای امنیت سایبری می توانند رویکرد مشترکی را بر مبنای بهترین عملکرد برای نشان دادن ریسک های فضای سایبری ایجاد کنند. به عنوان مثال سازمان بین المللی استاندارد و کمیسیون بین المللی الکتروتکنیک بخش هایی از استانداردهای مرتبط با امنیت سایبری را ارتقاء می بخشند.

این استانداردها زمانی هستند که صرفا یک رویکرد واحد را مورد استفاده قرار ندهند و دارای یک چارچوب خاص مبتنی بر قواعد تجارت و حاکمیت برای طراحی شاخصه های امنیت سایبری، در نهایت سازگاری با عملکرد تجاری و نشان دادن ریسک پذیری در این زمینه داشته باشند.

[11] Brookings

ISSN: 2745-3673
http://www.Rcsj.ir

گواهی های انطباق با استانداردهای امنیت سایبری: صدور گواهینامه های انطباق می تواند برای تجار این اطمینان را ایجاد کنند که تجارت دیجیتال آنان در فضای سایبری امنی صورت می گیرد. موافقت نامه های تجاری می توانند در راستای حمایت از "رژیم ارزیابی انطباق" بوده و به دنبال این باشند که دولت ها به بازیگران اقتصادی که استانداردهای امنیت سایبری برای تجارت را رعایت می کنند مجوز صادرات و واردات را اعطا کنند .

رویکرد مبتنی بر ریسک نسبت به امنیت سایبری: براساس قوانین سازمان همکاری و توسعه اقتصادی [۳] امنیت سایبری باید با در نظر گرفتن منافع قانونی دیگران، کاهش دادن ریسک تا یک سطح قابل قبولی، متناسب با مزایای انتظاری اقتصادی و اجتماعی فعالیت های اقتصادی را مورد هدف قرار دهند.

در رابطه با انطباق کشورها با استانداردهای بین المللی، در ابتدا باید اثرات این تطابق با توجه به شرایط ویژه کشورها مورد بررسی قرار گیرند. ایران نیز با توجه به اهمیت حفظ محرمانگی پاره ای از اطلاعات اقتصادی در شرایط تحریم لازم می باشد تا در رابطه با انتشار اطلاعات تجارت الکترونیک خود حساسیت بیشتری به خرج دهند و در مورد اجرای استاندارد های یاد شده محتاط تر عمل نماید. (موسوی ؛ ۱۳۹۴)

مدیریت امنیت در تجارت الکترونیکی

امروزه به دلیل گسترش استفاده از اینترنت، بخصوص در طی دو دهه اخیر، جهان تجارت شاهد انقلاب تکنولوژیکی بوده که به عنوان تجارت الکترونیک شناخته شده است. یکی از مهم ترین مسائل مربوط به تجارت الکترونیک بحث امنیت و چگونگی مدیریت آن می باشد. هنگامی که خریدار از امنیت سایت مورد استفاده برای انجام معاملات الکترونیکی اطمینان نداشته باشد، از آن برای انجام معاملات الکترونیکی خود استفاده نمی کند. از این رو برقراری امنیت و مدیریت آن در سیستم تجارت الکترونیک با رویکردی منظم در مدیریت ریسک امری ضروری است. در اکثر موارد هزینه جلوگیری از مشکلات امنیتی، بسیار کمتر از هزینه های ترمیم، بعد از قربانی شدن، می باشند. امروزه به دلیل استفاده از گواهینامه های دیجیتال هویت قطعی و ایمنی لازم تا حدی که اعتماد میان طرفین را براقرار کند، به وجود آمده است.(محبوبه بحری و همکاران ۱۳۹۳)

شکل ۱. اشتباهات رایج در مدیریت امنیت تجارت الکترونیکی

ISSN: 2745-3673
http://www.Rcsj.ir

نتیجه گیری

پیشرفت مداوم تکنولوژی در جوامع کنونی منجر به گسترش استفاده از شیوه های خرید آنلاین و خرید های اینترنتی شده است اما یکی از ایراد این روش این است که منجر به بی دقتی و تنبلی کاربران در مورد اطلاع پیدا کردن از صحت فروشنده و حفاظت از اطلاعات شخصیشان شده است. بدین ترتیب در هر کسب و کار اینترنتی که شکل می گیرد نیاز است که در ابتدا مطالعات وسیعی در زمینه های امنیتی هم چنین افزایش آگاهی در خصوص قوانین و سیاست های امنیتی صورت پذیرد تا کاربران نیز به توانند با اطمینان خاطر مضاعف به این کسب و کار ها اعتماد کنند و از آن ها بدون وجود هیچ گونه دغدغه ایی بهره مند بشوند.

همچنان محققان عصر حاضر پیشنهاد می کنند که خریداران اینترنتی باید برای حفظ و مراقبت از اطلاعات شخصی خود انگیزه و دانش کافی را داشته باشند و هم چنین در این گونه از تجارت ها حضور هکر ها و سوء استفاده کنندگان را نباید نادیده گرفت. علاوه بر این امنیت در تجارت الکترونیک دارای ابعاد مختلفی می باشد که این ابعاد عبارت اند از: ممانعت از تغییر در صحت داده های منتقل شده در تجارت.؛ عدم امکان انکار توافقات و عملیات انجام شده از سوی فروشنده و خریدار؛ محرمانگی و ممانعت از افشای غیر مجاز اطلاعات.، حفاظت از حریم و اطلاعات شخصی افراد.؛ ممانعت از حذف داده ها و بازیابی به موقع آنها.، تایید کردن منبع داده ها.

به طور کلی مجرمان و هکر های سایت های اینترنتی با استفاده از نقاط آسیب پذیره هر سایت های تجاری و همچنین اشتباهات صورت گرفته از طریق کاربران اینگونه از سایت ها در زمان خرید از سایت ها نا امن و غیر معتبر و همچنین ویروسی کردن سیستم و ارائه ی اطلاعات جزئی و غیر ضروری به این گونه از سایت ها منجر می شوند تا امنیت اینگونه از سیستم تجارت های الکترونیکی به مخاطره بیوفتد در نتیجه به مرور زمان ناامنی را برای کاربران استفاده کننده از این گونه تجارت ها به وجود می آورند و فرایند ترقی و پیشرفت تجارت الکترونیک را به مخاطره می اندازند.

ISSN: 2745-3673
http://www.Rcsj.ir

منابع و مراجع

[۱] زرگر, و محمود. (۲۰۰۷). امنیت در تجارت الکترونیکی. مجلس و راهبرد, ۵۵(۱), ۱۰۱-۱۲۰.
[۲] پورسلیمی. (۲۰۱۵). تجارت الکترونیک و امنیت.
[۳] طباطبایی, و سیّدحسین. (۲۰۱۵). بررسی تطبیقی کلاهبرداری رایانه‌ای با کلاهبرداری سنتی با نگاه به امنیت تجارت الکترونیکی. پژوهشهای حقوق جزا و جرم شناسی, ۳(۶), ۱۳۷-۱۵۹.
[۴] کلیدری, یگانه, فکور ثقیه, امیر محمد, حدادیان, و سیما. (۲۰۱۵, *September*). اثر اعتماد بر جذب مشتریان بانکداری الکترونیکی از طریق بالا بردن امنیت و حفظ حریم خصوصی مشتری. سومین جشنواره ملی بانک ها و موسسات مالی.
[۵] قناد, و فاطمه. (۲۰۰۹). ویژگی ها و روش های عملی تجارت الکترونیکی. حقوق اسلامی, ۲۰, ۱۴۹-۱۷۱.
[۶] کفاش پور, آذر, و محمد حسین دهنوی. (۲۰۱۱). تاثیر فرهنگ بر تجارت الکترونیک. پژوهش و توسعه فناوری-دانش و فناوری, ۲.
[۷] عسگری. (۲۰۱۱). تجارت الکترونیک و آمادگی الکترونیکی. دانش حسابرسی, ۱۱(۴), ۲۲-۳۷.
[۸] نجف‌زاده. مدیریت و تجارت الکترونیک. مجله علمی ترویجی انجمن مهندسان مکانیک ایران, ۲۲(۶), ۶۵-۶۸.
[۹] حاج ملک, توکلی, و احمد. (۲۰۱۶). ارزیابی سطح امنیت در تجارت الکترونیک با استفاده از آنتروپی شانون و تئوری دمپستر. شافر. مدیریت فناوری اطلاعات, ۸.
[۱۰] سهیل سرمدسعیدی و وحیدرضا میرابی، تجارت الکترونیکی، کیمیا،۱۳۸۳.
[۱۱] سیامک قاجار، ادله اثکات در محیطهای دیجیتال، دبیرخانه شورای عالی انفورماتیک، چاپ محدود، ۱۳۷۴
[۱۲] خدادادحسینی, سیدحمید, شیرخدایی, کردنائیج, و اسدالله. (۲۰۰۹). عوامل مؤثر بر اعتماد مشتری در تجارت الکترونیک (مدل *C2B*). پژوهش‌های مدیریت در ایران, ۱۳(۲), ۹۳-۱۱۸.
[۱۳] شکورنیا, اسدالهی, پوراندخت, الهام‌پور, حسین, خدادای, و علی. (۲۰۱۱). بررسی نظرات دانشجویان دانشگاه علوم پزشکی جندی‌شاپور اهواز دربارهٔ وضعیت موجود و مطلوب مشاوره و راهنمایی تحصیلی. مجله علمی پزشکی جندی شاپور, ۱۰(۵), ۴۶۹-۴۷۹.
[۱۴] کرمانی, د. م. ص., دکتر مجید صباغ, اسفیدانی, و محمد رحیم. (۲۰۰۵). بررسی تأثیر عوامل رقابتی بر جهانی شدن و تجارت الکترونیک. تحقیقات اقتصادی, ۴۰(۳).
[۱۵] موسوی محمدعلی, و سقای بی ریا حکیمه. موسسات سیاستگذاری امریکا و اسلام: مطالعه موردی رند و بروکینگز.
[۱۶] ۱۳۸۶ شهریور۱۴-سرمایه
[۱۷] فصلنامه اطلاع رسانی-دوره ۱۸ شماره ۱و ۲
[۱۸] ۱۳۸۶ شهریور۱۴-سرمایه
[۱۹] ماهنامه شبکه-شماره ۵۲
[۲۰] دانستنیهای کامپیوتر-الکترونیک و مخابرات-جمعه ۲۸خرداد ۱۳۸۴
[۲۱] دانشجویان بانک مقالات علمی به زبان فارسی تجارت الکترونیک (فلسفه سیستم عامل لینوکس-معرفی مجوز *GNU - GPL* یا پروانه جامع همگانی گنو)-یکشنبه ۲۶ شهریور ۱۳۸۵
[22] Niranjanamurthy, M., & Chahar, D. (2013). The study of e-commerce security issues and solutions. International Journal of Advanced Research in Computer and Communication Engineering, 2(7), 2885-2895.

ISSN: 2745-3673
http://www.Rcsj.ir

[23] Marchany, R. C., & Tront, J. G. (2002, January). E-commerce security issues. In Proceedings of the 35th Annual Hawaii International Conference on System Sciences (pp. 2500-2508). IEEE.
[24] Kesh, S., Ramanujan, S., & Nerur, S. (2002). A framework for analyzing e-commerce security. Information Management & Computer Security.
[25] Jing, Y. (2009). On-line Payment and Security of E-commerce. In Proceedings. The 2009 International Symposium on Web Information Systems and Applications (WISA 2009) (p. 46). Academy Publisher.
[26] Yenisey, M. M., Ozok, A. A., & Salvendy, G. (2005). Perceived security determinants in e-commerce among Turkish university students. Behaviour & Information Technology, 24(4), 259-274.
[27] Rane, P. B., & Meshram, B. B. (2012). Transaction security for e-commerce application. International Journal of Electronics and Computer Science Engineering, 1(3), 1720-1726.
[28] Jaafari, K., Ruiz, T., Elmaleh, S., Coma, J., & Benkhouja, K. (2004). Simulation of a fixed bed adsorber packed with protonated cross-linked chitosan gel beads to remove nitrate from contaminated water. Chemical engineering journal, 99(2), 153-160.
[29] Abe, F., Akimoto, H., Akopian, A., Albrow, M. G., Amendolia, S. R., Amidei, D., ... & Handler, R. (1995). Observation of top quark production in p p collisions with the Collider Detector at Fermilab. Physical review letters, 74(14), 2626.
[30] Peykam, A., & Salimifard, K. (2016). A Framework for Analysis of Inter-organizational Factors Affecting on the Security of Information Systems using FAHP Approach. IT Management Studies, 4(16), 147-176.
[31] Von Solms, B. (2001). Information security—a multidimensional discipline. Computers & security, 20(6), 504-508.
[32] Smith, D. J. (2010). A culture of corruption. Princeton University Press.