رهیافتی کاربردی برای امنیت تجارت الکترونیکی

محمود پرموزه[۱]، عبدالناصر درگلاله[۲]، مریم هنرمند [۳]
[۱] گروه کامپیوتر، عضو باشگاه پژوهشگران جوان، دانشگاه آزاد اسلامی واحد زاهدان، زاهدان، ایران، parmouze@gmail.com
[۲] دانشگاه آزاد اسلامی، واحد علوم وتحقیقات سیستان و بلوچستان، گروه کامپیوتر، زاهدان، ایران، n.dorgalale@gmail.com
[۳] عضو هیئت علمی، گروه کامپیوتر، دانشگاه آزاد اسلامی واحد زاهدان، honarmand@math.usb.ac.ir

چکیده - با وجود تمام مزایایی که تجارت الکترونیکی بهمراه دارد، نیازمند یک محیط امن برای انجام تراکنش‌ها و ارتباطات آنلاین برای جلوگیری از سوء استفاده از طریق سیستم‌های اطلاعاتی و کامپیوتری است. بهترین راهکار برای ایجاد فضای در امن تجارت الکترونیکی بررسی مشکلات موجود برای ایجاد امنیت و ارائه‌ی راهکارهای کاربردی به جای مطالعات و بررسی تئوری می‌باشد. در این مقاله به بررسی و شناسایی نیازهای امنیتی و مشاهده تهدیدها و آسیب پذیری‌های سیستم تجارت الکترونیکی با فناوریهای کاربردی پرداخته شده است. همچنین فناوریهای مناسب نظیر *PKI*[۱] و *PGP*[۲] برای ایجاد سیستم امنیتی معرفی شده است.

کلید واژه- امنیت تجارت الکترونیکی، PKI، PGP، معماری سه لایه، ebXml

۱- مقدمه

تجارت الکترونیکی خرید و فروش راحت در اینترنت است. فعالیت‌های تجاری در اینترنت به صورت نمایی درحال رشد است و یکی از نیازهایش امنیت است. تکامل سریع تکنولوژی محاسبات و ارتباطات و استاندارد سازی آن جهش بزرگی را در تجارت الکترونیک ایجاد کرده است. کاهش هزینه دسترسی، افزایش در سرعت انتقال و رسیدن آسان مشتریان و فروشندگان از جمله دلایل اصلی رشد این تجارت شده است.

عموما در تجارت الکترونیک چهار مورد زیر از دیدگاه مشتریان لحاظ می‌گردد [2]:

- فهرست محصولات
- کارت خرید
- امنیت تراکنش
- پردازش سفارش

مشتریان برای پرداخت یک گزینه را انتخاب کرده و نرم افزار باید توان رسیدگی به این پرداخت‌ها را داشته باشد. این پرداخت می‌تواند پول الکترونیکی، کارت اعتباری و یا هر نوع پرداخت الکترونیکی دیگری باشد.

۲- تهدیدهای امنیتی

نیاز به امنیت تجارت الکترونیکی مورد مطالعه، با مشتری شروع و با انجام تجارت پایان می‌یابد؛ پس در این "زنجیره تجارت" داراییهایی هستند که باید محافظت شوند و برای تضمین امنیت تجارت الکترونیکی که شامل سیستم کاربران، متن‌های انتقالی روی کانال‌های ارتباطی و سرورهای تجارت و وب است، امنیت هر قسمت باید به طور کامل مد نظر قرار گرفته شود. قطعا یکی از دارایی‌های بزرگ که باید محافظت شود، لینک‌های ارتباطی از راه دور است و البته تنها نگرانی در کامپیوتر و تجارت الکترونیک این مورد نیست. برای مثال، اگر ارتباطات از راه دور به صورت لینک‌های امن ساخته شود، اما هیچ اقدام امنیتی برای سرویس گیرنده انجام نگیرد باز هم امنیت زیر سوال قرار می‌گیرد[1].

۲-۱- تهدیدهای مشتریان

تا قبل از معرفی محتوای اجرایی وب، صفحات وب به طور عمده استاتیک بودند. کدهای HTML فقط توانایی لینک کردن صفحات مختلف را داشتند که شاید با این روش بتوان طوری

صفحات را لینک داد که کاربر احساس کند با محتوای متنوعی سروکار دارد.

- **محتوای فعال**

محتوای فعال اشاره به برنامه‌هایی دارد که به صورت شفاف در صفحات وب قرار گرفته شده‌اند. محتوای فعال می‌تواند اشکال گرافیکی در حال حرکت، دانلود، پخش صوتی و یا اجرای برنامه صفحه گسترده مبتنی بر وب باشد. محتوای فعال در تجارت الکترونیک نیز استفاده می‌شود. به طور مثال به جای خرید دستی می‌توانید یک سبد خرید اینترنتی داشته باشید و اقلام مورد نیازتان را در سبد قرار داده و در انتها توسط کارت خرید و یا روش پرداخت دیگری مبلغ محاسبه شده را پرداخت کنید. بهترین و شناخته شده‌ترین شکل محتوای فعال اپلت‌های جاوا، کنترل‌های اکتیویکس، جاوا اسکریپت و یک زبان سمت سرور است. از آنجائیکه ماژول‌های محتویات فعال در صفحات وب جاسازی شده، می‌توان آن‌ها را به طور کامل و شفاف به هرکسی و در هر جایی انتقال داد. از اینرو هر کسی می‌تواند محتوای مخرب در صفحات وب جاسازی کند، که به این تکنولوژی اسب-های تروجان می‌گویند که بلافاصله شروع به اجرای فعالیت‌های مخرب می‌کنند.

یکی دیگر از روش‌های نفوذ کاربران کوکی‌ها هستند.کوکی-ها که عمدتا به صورت یک فایل بر روی سیستم کلاینت ذخیره می‌شوند به راحتی می‌توانند توسط مخربان مورد حمله و تغییر قرار گیرند.

- **تغییر کد**

زمانی که داده‌ها ارسال می‌شود، در راه انتقال داده‌ها توسط مخربان ربوده شده و در بعضی مواقع مخربان داده‌های ربوده شده را تغییرداده و با تغییرات جدید دوباره ارسال می‌کنند.

- **جایگزین سیستم سمت سرور با یک سیستم ناشناس**

در بعضی از مواقع قربانی به اشتباه با سیستم جعلی در ارتباط است و همه اطلاعات را در اختیار سارقین اینترنتی قرار می‌دهد. در این حالت قربانی به تصور اینکه با طرف قرارداد خود در حال انجام عملیاتی از جمله معاملات الکترونیکی است همه اطلاعات را در اختیار سارقین قرار می‌دهد.

۲-۲- تهدیدهای کانال ارتباطی

اینترنت به عنوان زنجیره‌ی الکترونیکی در ایجاد ارتباط بین عوامل یک تجارت الکترونیکی است و برای ارتباط بین آن‌ها نیاز به کانال‌های ارتباطی است و این کانال‌های ارتباطی نیاز به امنیت دارند و اگر امنیت این کانال‌ها برقرار نباشد مهاجمین به راحتی به اطلاعات دسترسی پیدا خواهند کرد.

- **تهدیدهای تمامیت**

در بحث امنیت اطلاعات تمامیت به این معناست که داده‌ها نمی‌توانند توسط افراد غیر مجاز ایجاد، تغییر و یا حذف گردند. یکی از سیاست‌های امنیتی کانال ارتباطی، رمز نگاری داده‌های ارسالی است. حال اگر امنیت داده‌ها را در نظر نگیریم اطلاعات ربوده شده توسط سارقین به راحتی شناسایی می‌شوند.

- **تهدیدهای دسترسی پذیری**

دسترسی پذیری به این معناست که تمامی داده‌های موجود در هنگام نیاز در دسترس باشند. تغییر ظاهر و جازدن مخربان به جای نمایندگی‌های مجاز یکی از عوامل تهدیدهای امنیتی است که قربانی به اطلاعات غیر مجاز دسترسی پیدا می‌کند.

- **تهدیدهای سرور**

در زنجیره (مشتری- اینترنت - سرور) سرور سومین مکان دسترسی و همچنین در معرض خطر سرقت اطلاعات مشتریان و سازمان‌ها در تجارت الکترونیکی است. در نتیجه باید امنیت سرور از ورود مهاجمان تضمین باشد.

- **تهدیدهای سرور اصلی**

پاسخ به درخواست از مرورگرهای وب را از طریق پروتکل HTTP و اسکریپتهای CGI[۴] و همچنین چند نرم افزار سرور مانند FTP، پست الکترونیکی و نرم افزارهای دیگر صورت می‌گیرد. هرگونه خطا در هر یک از این عوامل امنیت را کاهش می‌دهد.

- **تهدیدهای بانک اطلاعاتی**

همه اطلاعات خصوصی کاربران در بانک اطلاعاتی روی سرور قرار دارد و هرگونه ناامنی در سرور بانک اطلاعاتی باعث فاش شدن اطلاعات می‌شود و همچنین امکان دارد سارق به اطلاعات احراز هویتی شخص دستیابی پیدا کند.

- **تهدیدهای رابط گذرگاه مشترک**

رابط گذرگاه مشترک (CGI)، بکارگیری انتقال اطلاعات از یک وب سرور به برنامه دیگری روی سرور مانند یک برنامه بانک اطلاعاتی است. از اسکریپت‌های CGI برای پردازش فرم‌های وب

یا انواع URLها استفاده می‌شود. برنامه‌های CGI ناامن نخستین راه نفوذ مهاجم به یک وب سایت هستند. حال اگر اشکالات امنیتی در CGI پیش بیاید و یا برنامه ناامن دیگری جایگزین این برنامه شود امنیت کاهش می‌یابد.

- **هک شدن کلمه عبور**

ساده‌ترین راه نفوذ به سیستم توسط مخربان حدس کلمه عبور می‌باشد و باید کاربران در انتخاب کلمه عبور نهایت دقت را انجام دهند.

۳- بکارگیری امنیت در تجارت الکترونیکی

مراحل طراحی امنیت شامل مدل کردن سیستم، شناسایی ویژگی‌های امنیتی برای محافظت، شناسایی مدل حریف و سپس بدست آوردن مسائل امنیتی زیر حملات مخربان است.

جزییات مدلسازی سیستم و شناسایی نیازهای امنیتی امکان پذیر است. اما غیر ممکن است آسیب‌های سیستم حریف را به درستی و با دقت بتوانیم مدل کنیم.

۳-۱- سیکل زندگی مهندسی امنیت

یک تفاوت واضح بین طراحی سیستم نرم افزاری و سیستم امنیتی وجود دارد. تا زمان طراحی نرم افزارها صحت و درستی برنامه‌های کاربردی اولویت مهم و اولیه است. در حقیقت در سیستم نرم افزاری هدف طراح تامین کردن سیستم ورودی مناسب برای کاربران است تا بتوانند خروجی مناسب دریافت کنند. اما در پوشش سیستم امنیتی طراح مجبور است تامین کند که خصوصیات سیستم در مقابل حملات محافظت می‌شوند.

پروسه طراحی و گسترش زیرساخت امنیت اطلاعات پروسه متوالی از آنالیز، طراحی، نظارت و سازش برای نیازهای قابل تغییر است.

سیکل زندگی مهندسی امنیت از مراحل زیر تشکیل شده است:

- **خصوصیات مورد نیاز امنیت و آنالیز ریسک**

فاز اول در سیکل مهندسی امنیت آنالیز ریسک است. مجموعه اطلاعات راجع به دارایی‌های سازمان‌ها که نیاز به محافظت دارد، همچنین مشاهده تهدیدهای روی دارایی‌ها و زیر ساخت عملیاتی موجود در این فاز جا دارند.

- **خصوصیات سیاست امنیتی**

این فاز استفاده "ویژگی نیازمندی‌های امنیت" و "ریسک گزارش تجزیه و تحلیل امنیت " به عنوان ورودی و تولید مجموعه‌ای از سیاست‌های امنیتی تجارت الکترونیک است.

- **خصوصیات زیرساخت‌های امنیتی**

این بخش آنالیز "خصوصیات نیازمندی‌های امنیتی" و "خصوصیات سیاست امنیتی" برای ادغام یک لیست از ابزارهای امنیتی که برای محافظت دارایی‌ها مورد نیاز هستند می‌باشد. در این فاز دیدگاه‌ها از محل و هدف ابزارهای امنیتی مشخص می‌کند.

- **بکارگیری زیرساخت‌های امنیتی**

این بخش سازماندهی، تهیه کردن، گسترش دادن و پیکربندی انتخاب زیر ساخت‌های امنیتی، در سطح سیستم است.

- **تست امنیت**

در این فاز آزمایش‌هایی در رابطه با اثر زیرساخت‌های امنیتی انجام می‌شود.

- **ارزیابی نیازمندی‌ها**

تغییرات در اهداف تجارت، محیط‌های عملیاتی و پیشرفت تکنولوژی ممکن است سیکل امنیتی را به نیازهای امنیتی جدیدی هدایت کند و نیاز به راه اندازی سیکل امنیتی جدیدی باشد.

۳-۲- نیازهای امنیتی

در طول این فاز نیازمندی‌های امنیتی، سیاست‌های امنیتی، زیر ساخت‌های امنیتی و تست بررسی می‌شود.

- **تعیین اعتبار**

هدف اصلی در تعیین اعتبار تایید هویت کاربران است. هویت یکی از فناوری‌های بنیادین در امنیت است. این فناوری بیش از سایر فناوری‌ها با کاربران سروکار دارد. البته هویت فقط مختص کاربران نیست و گاه ابزارهای شبکه نیز نیاز به تعیین هویت دارند. فناوری‌های هویت نخستین A از واژه لاتین (احراز هویت[۵]، مجاز شناسی[۶] ، حسابرسی[۷]) است. فناوری‌هایی نظیر گذر واژه‌های چند بار مصرف، RADIUS، TACACS، OTP، PKI، PGP، HIDS برای امنیت میزبان و رمزنگاری و نظیر آن‌ها را می‌توان برای اعتبارسنجی هویت کاربری بکار برد. البته هویت خود شبکه‌ها را می‌توان به وسیله‌ی عناصرمختلفی (نظیر IP، نام کاربری) بیان کرد.

- **پنهانی**

در تجارت آنلاین پنهان کردن اطلاعات قابل دسترس و قابل تغییر است. توانایی برای بدست آوردن آن‌ها توسط تعیین اعتبار و امکاناتی نظیر رمزنگاری انجام می‌شود. البته همیشه امنیت مبتنی بر پنهان کاری نیست به طور مثال در دنیای شبکه توسط ابزارهایی نظیر Nmap می‌توان نوع و نسخه‌های حفاظهای مورد استفاده را بدست آورد.

- **تمامیت**

تنها کاربران یا پروسه‌های مجاز قادر به تغییر و به روز رسانی داده‌ها خواهند بود. این ویژگی برای جلوگیری از دستکاری، یا حذف ناخواسته پیام‌ها می‌باشد. سرویس‌های ارتباطی تمامیت اطلاعات می‌کوشند تا داده‌های فرستاده شده در شبکه، در طول راه دچار دگرگونی یا گم نشود. بدون این سرویس‌ها، یک شخص غیر مجاز ممکن است یک بسته یا پیام را از شبکه بگیرد، آنرا تغییر دهد و دوباره در جریان اندازد، بدون اینکه تغییرات برای گیرنده بسته یا پیام آشکار شود. با تایید بسته و رمز نگاری پیام ها می‌توان بروز اشتباه تصادفی یا متقابلانه در هنگام ورود داده‌ها و نیز تخریب و تغییر پیام‌ها را کاهش داد.

- **عدم انکار**

تضمین اینکه کاربران توانایی انکار صحت اطلاعات و محتویات پیام‌های مبادله شده را نداشته باشند. یکی از فناوری-های موجود برای این کار امضای دیجیتالی است.

۳-۳- سیاست‌های امنیتی

سیاست امنیتی بیان رسمی و مکتوب از قوانینی است که باید توسط افراد و عواملی که به نوعی به فناوری و دارایی‌های اطلاعاتی سازمان دسترسی دارند، رعایت شود.

گام اول در تامین یک معامله تجارت الکترونیکی تنظیم مکتوب سیاست امنیتی است که به صورت آشکار نیازمندی‌ها را برای هر جز از سیستم و چگونگی فعل و انفعالاتشان مشخص می‌کند. اصولا در گام اول از سیاست، فناوری دخالت ندارد بلکه فعالیت‌های وسیع شبکه مد نظر است و بعد از مشخص کردن سیاست، فناوری مربوطه برای بکارگیری زیرساخت آن مورد استفاده قرار می‌گیرد.

سیاست امنیتی ممکن است مسائل زیر را پوشش دهد :

- کاربران به چه نوع سرویس‌هایی (به عنوان مثال؛ وب، FTP، SMTP) دسترسی دارند.
- حریم خصوصی کاربران چیست.
- چه اطلاعاتی باید رمزنگاری شود.
- چه داده‌هایی از مشتریان باید نگهداری شود. چقدر این اطلاعات حساس و نیاز به محافظت دارند.
- کارمندان سازمان‌ها به چه میزان و به کدام اطلاعات دسترسی داشته باشند.
- نقش و مسئولیت مدیران در اجرای امنیت چیست.
- چه کسی به سرور اصلی دسترسی داشته باشد.

در این فاز بیشتر تاکید بر سیاست‌های امنیتی است و تاکیدی بر بکارگیری فناوری نیست.

۳-۴- زیرساخت‌های امنیتی

زیرساخت‌های امنیتی پیاده‌سازی سیاست‌های امنیتی است. زیرساخت‌های امنیتی تکنولوژی، انتخاب یک تکنولوژی مناسب برای تجارت الکترونیکی است. به طور مثال اگر سیاست بکارگیری داشتن کلمه عبور برای هر فرد است در هنگام ثبت آن از کاربر ورود دو بار کلمه عبور را بخواهیم.

بعضی از کارها می‌تواند در این مرحله شامل موارد زیر باشد:

- مجبور کردن کاربر به استفاده از کلمه های عبور پیچیده.
- مسدود کردن ورودی‌های غیر مجاز از دیواره آتش.
- نیاز به گواهینامه‌های دیجیتالی برای تأیید هویت
- قابلیت اتصال به دسترسی از راه دور .
- دسترسی فیزیکی به سرور در هنگام ورود ثبت شود.

۳-۵- تست امنیت (بررسی تطابق)

تست امنیت برای بررسی اینکه زیرساخت‌های امنیتی تا چه حد با سیاست‌های امنیتی تبعیت می‌کند، صورت می‌گیرد. مهمترین دلیل برای این کار این است که دوام و مقاومت سیاست‌های امنیتی در برابر تهدیدهای واقعی تست شود.

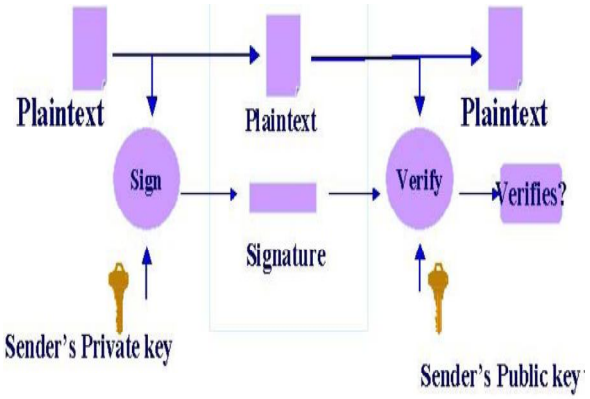
۴- بررسی فناوری‌های امنیتی

۴-۱- زیرساخت کلید عمومی (PKI)

PKI از فناوری‌های امنیت است و برای هویت کاربران کاربرد دارد. PKI مکانیزمی است که برای توزیع دیجیتال (که بیانگر هویت کاربران است) به کار می‌رود. گواهی‌های دیجیتال کلیدهای عمومی هستند که توسط مرکز صدور گواهی (CA[۸]) امضا شده‌اند. مراکز صدور گواهی تایید می‌کند که یک گواهی دیجیتال به یک شخص یا سازمان تعلق دارد. البته این فناوری به دلایلی مانند مدیریت دشوار آن و سختی استفاده برای کاربران با انتقاداتی مواجه شده است.

PKI اصولا در محل‌هایی مانند گواهی‌های TLD/SSL برای سرورها، ایمیل مطمئن و VPN سایت استفاده می‌شود.

بعضی از طرفداران تجارت الکترونیکی پیشنهاد به ایجاد PKI یکپارچه و بزرگ برای افزایش سرعت رشد تجارت الکترونیک دارند (شکل ۱).



شکل ۱: زیرساخت کلید عمومی PKI [2]

سیستمهای PKI به دو دسته باز و بسته تقسیم می‌شوند. سیستم PKI باز سیستمی است که زنجیره اطمینان آن می‌تواند شامل چند سازمان باشد. مشکل این سیستم‌ها از آنجا ناشی می‌شود که شما به سازمانی که هویت را تایید می‌کند اطمینان کامل داشته باشید. در سیستم‌های PKI بسته CA داخل خود سازمان است و تنها برای تایید هویت موجودیت‌های آن سازمان گواهی صادر می‌کند. PKI بسته بیشترین کاربرد را دارد و مشکلات اعتماد تایید هویت و تمایز وجود نام‌های یکسان کاربران را حل کرده است و عموما از PKI بسته استفاده می‌شود.

زیرساخت کلید عمومی (PKI) سرویس‌هایی نظیر امضای دیجیتال، تصدیق هویت، محرمانگی، صحت، عدم انکارپذیری، ارائه می‌دهد.

۴-۲- سرویس رمزنگاری PGP

PGP یک سرویس محرمانه‌ی قابل اعتماد و احراز هویت را فراهم می‌کند که برای ارسال ایمیل امن و ذخیره فایل استفاده می‌شود. PGP به طرز غیر قابل باور نکردنی در حال رشد است و به طور گسترده مورد استفاده قرار می‌گیرد. از دلایل اصلی استفاده آن الگوریتم‌های امن است [2].

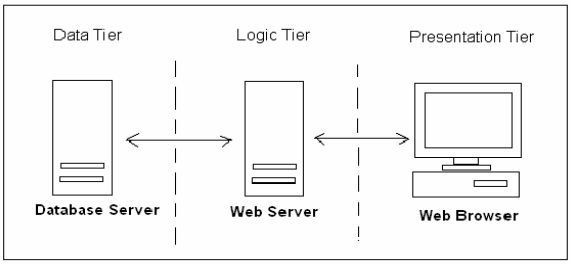
PGP سرویس‌های مهمی نظیر احراز هویت، محرمانگی، فشرده‌سازی، سازگاری با پست الکترونیکی دارد.

PGP از تکنیک رمزنگاری کلید استفاده می‌کند و از امنیت بالایی برخوردار است [5].

۴-۳- طراحی سه لایه‌ی وب

از آنجایی که مهاجمان برای دسترسی به محتوا ابتدا سرور وب را مورد تهاجم قرار می‌دهند برای جلوگیری از تسخیر سرور وب یکی از راهکارها، طراحی سه لایه وب است. در این روش سرورهای کاربردی و پایگاه داده از یکدیگر جدا شده اند.

یک معماری مناسب برای معماری سه لایه در [4] مطرح شده است؛ لایه اول presentation نامیده می‌شود که همان صفحه وب سمت کاربر است. لایه دیگر، لایه Logic نامیده می‌شود و همان کدهای اجرایی سمت سرور است و لایه سوم، لایه Data که شامل بانک اطلاعاتی می‌باشد (شکل۲).



شکل ۲: معماری سه لایه وب [4]

از مزایای این روش می‌توان به موارد زیر اشاره کرد:

- سادگی در تغییر و جایگزینی در هر لایه بدون تغییر دادن لایه‌های دیگر.

- بالارفتن سرعت بارگذاری به دلیل جداسازی صفحات کاربردی از بانک اطلاعاتی.
- بکار بردن سیاست‌های امنیتی مناسب برای هرلایه بطور جداگانه.

البته برای معماری سه لایه نیز می‌توان یک سری مسائل امنیتی به کار برد؛ ازجمله می‌توان به قرار دادن دیواره آتش در هر لایه اشاره کرد [7].

۴-۴- ebXml

ebxml نحوه انجام تجارت الکترونیک را بر اساس XML بیان می‌کند و چارچوبی را ایجاد می‌کند که شرکت‌ها می‌توانند در آن ثبت نام نموده و سپس شریک تجاری خود را از طریق آن پیدا کنند.

هدف ebxml فراهم کردن یک متد استاندارد برای تبادل پیام‌های تجاری در تجارت الکترونیکی است.

در [3] پنج راهکار مهم را برای بکارگیری امن تبادل پیام در اسناد تجارت الکترونیکی بیان کرده است. این راهکارها عبارتند از:

- فرمت امضای دیجیتالی برای اسناد XML
- رمزنگاری اسناد XML
- استفاده از تکنولوژی مدیریت کلید عمومی XKMS[9]
- استفاده از زبان نشانه گذاری امنیتی SAML[10]
- استفاده از زبان نشانه گذلری کنترل دستیابی XACML[11]

۵- نتیجه‌گیری

در این مقاله سعی به ترغیب برای بکارگیری فناوری‌های مشهور و جدید در امنیت شده است، که با بکارگیری فناوری‌ها و تحقیق در بازه‌های کاربردی مسائل امنیتی پرداخته شده است. اغلب امنیت را در قالب (اول محرمانگی، بعد یکپارچگی، بعد دسترسی پذیری) به عنوان راهکارهای امنیتی می‌دانند ولی تحقیقات کاربردی برای بکارگیری از فناوری‌های امنیتی مطرح نشده است. برای امنیت مقاوم در برابر خطا و حملات باید حداکثر توان را به ایجاد یک سیاست امنیتی و بکارگیری مناسب این سیاست‌ها و استفاده از ابزارهای امنیتی با حداکثر درجه امنیتی بکار گرفت.

در دنیای طراحی صفحات تجاری نیز یک برنامه نویس نباید ادعای مبنی بر امن بودن کد داشته باشد زیرا امنیت سرور وب مهم است و همچنین نباید متکی به سرورهای وب (مثلا غرور در استفاده از سرورهای آپاچی) بود و کد غیر امن بر روی سرور قرار داد.

تحقیقات سنتی و پرداختن به جزئیات ریاضی دیگر چندان کاربرد ندارد. پس باید با رویکردی کاربردی به مسائل امنیتی پرداخته شود و نقاط ضعف فناوری‌های موجود برای امنیت را مورد بررسی قرار داد.

مراجع

[1] A SENGUPTA," *e-Commerce security – A life cycle approach*", Centre for Distributed Computing, Kolkata 700 032, India, Printed in India, April/June 2005, pp. 119–140.
[2] Dr. Nada M. A. Al-Slamy ," *E-Commerce security* ", Alzaytoonah University MIS Dept. Amman, Jordan 962, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.5, May 2008
[3] Dongkyoo Shin, Dongil Shin, Sukil Cha, and Seyoung Kim," *A Study on the Secure ebXML Transaction Models* ", World Academy of Science, Engineering and Technology 46 2008
[4] Gagnesh Arora," *Web Based Client Server Technology – A Three Tier Architecture* ", Ansal Institute of Technology, Gurgaon, (Haryana), India
[5] Alexander Bautista ,*PGP(Pretty Good Privacy)*, 9.27.11
[6] Stefan Dumbrava, Doru Panescu and Mihaela Costin, *A Three-tier Software Architecture for Manufacturing Activity Control in ERP Concept, International Conference on Computer Systems and Technologies - CompSysTech*' 2005
[7] Xue Liu, Jin Heo,Lui Sha, University of Illinois at Urbana-Champaign," *Modeling 3-Tiered Web Services*"

زیرنویس‌ها

[1] public key Infrastructure
[2] Pretty Good Privacy
[3] three-Tiered Web Services
[4] common gateway interface
[5] Authentication
[6] Authorization
[7] Accounting
[8] Certificate Authority
[9] XML Key Management Specification
[10] Security Assertion Markup Language
[11] XML Access Control Markup Language