امنیت در خدمات گزارشگری مالی مبتنی بر XML در اینترنت

دکترمحمد عرب‌مازاریزدی
دانشیار دانشگاه شهیدبهشتی
الهام حسنی‌آذر داریانی
دانشجوی کارشناسی ارشد حسابداری

بسیاری از شرکت‌ها در تلاش هستند که توان نفوذ اطلاعات مالی خود را از طریق ایجاد وب سایت شرکت و ارائه چنین اطلاعاتی به کارکنان، سرمایه گذاران و تحلیلگران مالی افزایش دهند. زبان گزارشگری مالی توسعه‌پذیر (XBRL) ایجاد شد تا ابزار مؤثر و کارآمد برای تهیه و تبادل اطلاعات مالی در اینترنت در اختیار کاربران قرار دهد. زبان گزارشگری اطمینان بخشی توسعه‌پذیر (XARL) نیز طراحی شد تا تأییدکنندگان اطلاعات مالی بتوانند صحت اطلاعات منتشر شده در اینترنت را تایید کنند و به کاربران و شرکت‌ها اطمینان دهند که می‌توانند به چنین اطلاعاتی اتکا کنند.

خدمات XBRL و XARL روش‌های تبادل پیام مبتنی بر اینترنت هستند. اینترنت ماهیتاً ناامن است. بدون امنیت مناسب امکان استفاده از حداکثر توان خدمات XBRL و XARL وجود ندارد. روش‌های امروزی امنیت شامل ترکیبی از شناسه‌ها و رمز عبور کاربر و امنیت نقطه به نقطه، است. دسترسی به فنون کنترل مبتنی بر شناسه و رمز عبور کاربر می‌تواند از دسترسی بدون مجوز به پرونده‌ها و داده‌ها حفاظت کند اما نمی‌تواند صحت اطلاعات را تضمین نماید. این نوع امنیت برای حفاظت از اطلاعاتی کافی نیست که از چندین مرحله می‌گذرد. بنابراین روش‌های امنیت دیگری برای جبران این محدودیت‌ها لازم است.

این مقاله، امنیت در خدمات گزارشگری مالی را مورد توجه قرار می‌دهد. اول خدمات وب را شرح می‌دهد و خدمات گزارشگری مالی مانند XBRL و XARL را به عنوان خدمات وب توضیح داده و پس از آن به بحث درباره تهدیدها و محدودیت‌های فنون امنیت رایج می‌پرازد. سپس الزامات امنیت را شناسایی می‌کند که به منظور فراهم کردن خدمات XBRL و XARL قابل اعتماد و قابل اتکا باید در نظر گرفته شود. بالاخره مقاله معماری امنیت خدمات وب را به عنوان سازوکار امنیت مناسب برای خدمات گزارشگری مالی پیشنهاد می‌دهد.

XBRL، XARL، امنی ، صحت اطلاعات، خدمات وب

پیشرفت‌های سریع در رایانه و فناوری ارتباطات، روش‌های کسب و کار و روش انتشار اطلاعات مالی را متحول کرده است. بسیاری از سازمان‌ها در حال حاضر در تلاش‌اند تا اطلاعات مالی را در اینترنت ارائه کنند تا امکان دسترسی کاربران به اطلاعات و همچنین، امکان تبادل موثر و به موقع اطلاعات بین تهیه‌کنندگان و ذی‌نفعان متعدد افزایش یابد. با این وجود، این امر اغلب به بریدن و چسباندن (یا Cut & Paste) یا کپی‌برداری صرف، محدود شده و بدلیل فقدان قالب‌های پذیرفته شده عمومی و مشترک برای ارائه اطلاعات مالی، پرهزینه و همراه با خطا نیز هست.

زبان گزارشگری مالی توسعه‌پذیر(XBRL)[1] به منظور غلبه بر این محدودیت‌ها ایجاد شد. این زبان، اطلاعات مالی را با روشی استاندارد شده در زمینه تهیه، انتشار و تبادل اطلاعات مالی، ارائه می‌کند. همچنین استقلال از نوع فناوری سخت و نرم افزاری به‌کار رفته، توانایی مبادله اطلاعات بین سیستم‌های رایانه‌ای در محیط‌های گوناگون، تهیه کارآمد صورت‌های مالی و استخراج کارآمد اطلاعات مالی برای اهداف تجزیه و تحلیل، از ویژگی‌های برجسته آن به‌شمار می‌رود. Hoffman and Strand, 2001 و Boritz and No, 2003a) زبان دیگری نیز برای اطمینان بخشی در مورد صحت اطلاعات مورد مبادله از طریق XBRL، ایجاد شد که اصطلاحاً **زبان گزارشگری اطمینان بخشی توسعه‌پذیر XARL**[2] خوانده می‌شود. وجود XARL موسسات ارائه خدمات اطمینان‌بخشی و تضمین کیفیت را قادر می‌سازد تا صحت اطلاعات توزیع شده مبتنی بر XBRL در اینترنت را تایید و به کاربران و شرکت‌ها کمک کنند تا به این قبیل اطلاعات مالی اتکا کنند. (Boritz and No, 2003b)

با وجود تمایل شرکت‌ها برای استفاده از امکانات XBRL، هنوز هم نگرانی زیادی در مورد امنیت اطلاعات مالی در اینترنت وجود دارد. اینترنت ناامن است و بدون برقراری امنیت مناسب، اطلاعات مالی مورد انتشار و مبادله در اینترنت، مخصوصاً وب، در معرض محدودیت و دستکاری است. بنابراین موضوع امنیت به منظور فراهم نمودن امکان انتقال الکترونیک و در عین حال قابل اعتماد و قابل اتکا کردن اطلاعات مالی در اینترنت باید مورد توجه قرار گیرد. این مقاله، به موضوع امنیت در ارائه خدمات گزارشگری مالی مبتنی بر XML در اینترنت اختصاص یافته است.

XBRL و XARL الگوهای جدید برای گزارشگری مالی در اینترنت

زبان نشانه‌ای توسعه پذیر (XML)[3]: تکامل اسناد الکترونیکی در اینترنت

ظهور وب تامین‌کنندگان اطلاعات را قادر ساخته تا به آسانی و ارزانی اسناد الکترونیک را برای کاربران اینترنت منتشر کنند. امروزه همه این واقعیت را پذیرفته‌اند که وب، کانال اصلی انتقال اطلاعات از فردی به فرد دیگر، از واحد تجاری به مشتری، و از واحد تجاری به واحد تجاری دیگر است. زبان XML توسط کنسرسیوم شبکه جهانی در سال ۱۹۹۶ به منظور توسعه فناوری وب ایجاد شد (Bosak and Bray,1999) تا تبادل کارآمد اطلاعات را در وب امکان‌پذیر سازد.

زبان نشانه‌ای XML توان و انعطاف‌پذیری لازم برای

نمایشگر ۱ـ تهدیدهای امنیت در خدمات گزارشگری مالی

عنوان تهدید	چگونگی تهدید امنیتی
دستکاری پیام	دستکاری پیام، نوعی حمله است که محتوای پیام کدگذاری شده XML (یا به عبارت دیگر اسناد XBRL یا XARL) را تغییر می‌دهد تا جریان اطلاعات بیان شده توسط پیام را مختل کند. برای نمونه، مهاجم ممکن است بخشی از پیام XML را تغییر دهد، یا اطلاعات اضافی در پیام XML درج کند، یا بخشی از پیام XML را حذف کند.
افشا پیام	افشای پیام، نوعی حمله است که از طریق آن کاربر بدون مجوز، امکان دسترسی به اطلاعات یک پیام یا بخشی از یک پیام را به‌دست می‌آورد.
جایگزینی پیام	گرفتن پیام‌ها و تغییر ظاهر بخش‌هایی از آن را در برمی‌گیرد. برای نمونه، یک مهاجم، سند XARL را می‌گیرد که برنامه تامین‌کننده به برنامه درخواست‌کننده فرستاده است، و آن را با سند دیگری جایگزین می‌کند. بنابراین هر دو برنامه تصور خواهند کرد که در حال برقراری ارتباط با یکدیگر هستند و ممکن است هرگز ندانند که ارسال سند واقعی قطع شده و محتوای آن تغییر داده شده است.
جعل IP	روشی فنی است که برای به‌دست آوردن امکان دسترسی غیرمجاز به سیستم مورد استفاده قرار می‌گیرد. در این روش، فرد مهاجم یک پیام XML را با نشانی IP جعلی به سیستم می‌فرستد. که ظاهراً نشان می‌دهد پیام از حوزه‌های مورد اعتماد می‌آید. برای مثال، با فرستادن یک پیام درخواست سرویس XARL با نشانی IP یک درخواست‌کننده سرویس مورد اعتماد، مهاجم ممکن است اسناد XARL را از تامین‌کننده سرویس XARL به‌دست آورد.
امتناع از خدمت	امتناع از ارائه خدمت (DOS) نوعی طرح حمله است که کاربران قانونی را از استفاده از یک خدمت باز می‌دارد یا ارتباط را با رایانه یا شبکه‌ای برقرار می‌کند که قادر به تامین خدمات معمول نیست. حمله از نوع DOS در واقع نوعی نقض امنیت سیستم است که در آن معمولاً سرقت یا تغییر اطلاعات صورت نمی‌گیرد. با این وجود، این حمله می‌تواند به در دسترس قرار دادن اطلاعات نامربوط منجر شود. نوعی قصور در ارائه خدمات که می‌تواند سبب هدر رفتن زمان و پول زیادی شده و حتی در مواردی سبب از دست رفتن حیثیت و شهرت سازمان‌ها یا کاربران شود.
وارسی بسته	گرفتن و خواندن یک پیام یا همه پیام‌های موجود در ترافیک شبکه یا کانال ارتباطی است. با استفاده از ابزار بررسی بسته، مهاجم می‌تواند شناسه‌ها و رمزهای عبور کاربران را به هنگام انتقال پیام‌های XML به‌دست آورد.
ویروس رایانه‌ای	ویروس رایانه‌ای یک کد(یا برنامه) مخرب است که می‌تواند سیستم‌های رایانه‌ای را مختل کند و انواع کارها از قبیل حذف پرونده‌ها، تخریب سیستم و باز کردن سیستم را برای سارقان داده‌ها انجام دهد. ویروس رایانه‌ای ویروس نامیده می‌شود زیرابرخی از خصوصیات ویروس‌های زیستی، مثل انتقال کدمخرب از یک رایانه آلوده به رایانه دیگر را دارا می‌باشد.

نرم‌افزارهای کاربردی تحت وب و سایر بسته‌های نرم‌افزاری واحدهای تجاری را افزایش داده (Elliotte, Halfhill, 1999, 2001)، تبادل موثر و کارآمد را تسهیل کرده و جستجوهای مفهومی‌تری را ممکن ساخته است. از آنجا که XML محتوای اطلاعات را از طریق کدگذاری اطلاعات با الصاق برچسب‌های خاصی(Tag) در اختیار کاربر می‌گذارد که محتوا و ساختار آن را شرح می‌دهد، در نتیجه، جستجوها می‌توانند نتایج مربوط‌تر و صحیح‌تری ایجاد کنند. علاوه بر این، کاربر می‌تواند داده‌ها را به اشکال مختلف با استفاده از اطلاعات مربوط به ساختار آنها در XML مشاهده کنند. بالاخره XML استانداردی باز و سیستم مستقل است که شیوه جامعی را برای قالب‌بندی و ارائه داده‌ها ایجاد می‌کند.

زبان XBRL در واقع اقتباس حرفه مالی از XML برای گزارشگری مالی است. در XBRL، به تمام داده‌های مالی برچسب‌هایی زده می‌شود که آنها را به‌عنوان دارایی، بدهی،

سرمایه، سود و غیره از هم متمایز می‌سازد. بنابراین کاربران می‌توانند به آسانی، داده‌ها را همراه با برچسب‌هایی مثل وجوه نقد استخراج یا تغییر شکل دهند، و به کمک نرم‌افزارهای کاربردی تحلیلی، تجزیه و تحلیل کنند. برای مطالعه بیشتر درباره XBRL به مقالات هافمن و استراند(Hoffman and Strand, 2001) یا بورتیز و نو (Bortiz and No,2003a) مراجعه کنید.

صحت اطلاعات مالی مندرج در یک سند XBRL به قابلیت اتکای پردازش‌های مورد استفاده برای ایجاد سند، ماهیت و میزان مطمئن بودن فرایندهای انجام شده روی آن اطلاعات و مقدار امنیت برقرار شده برای حفاظت از صحت اطلاعات بستگی دارد. زبان گزارشگری اطمینان‌بخشی توسعه‌پذیر (XARL)، صورت توسعه یافته‌ای از XBRL مبتنی بر XML است که ارائه‌کنندگان خدمات اطمینان‌بخشی و تضمین کیفیت را قادر می‌سازد تا صحت اطلاعات دارای برچسب XBRL منتشر شده در اینترنت را تایید و گزارش کنند. این زبان به کاربران و شرکت‌ها نیز کمک می‌کند تا به این قبیل اطلاعات مالی اعتماد کنند. در صورت وجود زیرساخت مناسب، XARL می‌تواند روشی را برای ایجاد اطمینان نسبت به صحت اطلاعات مالی مندرج در اسناد XBRL فراهم کند.

زبان XARL نیز مثل XBRL عناصر نشان‌دهنده اطلاعات مربوط به فرایند اطمینان‌بخشی و اجزای پشتیبان آن را برای ترکیب با XBRL تعریف می‌کند تا به کاربران اجازه دهد درباره میزان اعتمادی قضاوت آگاهانه‌ای داشته باشند. که به هر یک از اقلام داده‌های دریافت شده می‌کنند. به عبارت دیگر، یک سند XARL شامل برچسب‌هایی است که نوع تضمین، تاریخ اطمینان‌بخشی، امضای دیجیتالی حسابرس، قابلیت اتکای سیستم و غیره را نشان می‌دهد. بحث بیشتر درباره XARL را می‌توان در مقاله بوریتز و نو یافت. (Boritz and No, 2003b and 2004a

شرکت سهامی عام "الف" را در نظر بگیرید که می‌خواهد صورت‌های مالی را به بستانکاران، سرمایه‌گذاران و تحلیلگران ارائه دهد و یک شرکت خدمات اطمینان بخشی به‌نام "ب" را در این زمینه به‌کار می‌گیرد تا صحت اطلاعات منتشر شده را تضمین کند.

بعد از اینکه شرکت "الف" اطلاعات مالی را با استفاده از سیستم حسابداری داخلی خود تهیه می‌کند، سند XBRL برپایه

نمایشگر ۲ـ الزامات امنیت برای خدمات گزارشگری مالی

الزامات امنیت	شرح
محرمانه بودن	زمانی که فرستنده اسناد XBRL و XARL را از طریق اینترنت به گیرنده انتقال می‌دهد، اسناد محرمانه باقی می‌ماند. به عبارت دیگر، فقط فرستنده و گیرنده مورد نظر می‌توانند پیام را بخوانند. وقتی فرستنده اسناد XBRL و XARL را از طریق اینترنت به گیرنده انتقال می‌دهد، اسناد تغییر داده نمی‌شوند. به عبارت دیگر اسناد XBRL و XARL دقیقاً به همان صورت که توسط فرستنده منتقل شده توسط گیرنده مورد نظر دریافت می‌شود.
تاییداعتبار	زمانی که اسناد XBRL و XARL توسط کاربر یا سیستم دریافت می‌شود فرستنده و گیرنده همان کسانی هستند که ادعا می‌کنند.
عدم انکار	زمانی که اسناد XBRL و XARL به گیرنده فرستاده می‌شود فرستنده بعداً نمی‌تواند ارسال اسناد را انکار کند و بالعکس، گیرنده بعداً نمی‌تواند دریافت اسناد را انکار کند.
مجوز(کنترل دسترسی)	فقط کاربران دارای مجوز قادرند که به اسناد XBRL و XARL دسترسی داشته باشند.
مدیریت کلید	رمزگذاری به منظور نگهداری محرمانه اطلاعات منتقل شده در اینترنت مورد استفاده قرار می‌گیرد. رمزگذاری استفاده از کلیدهای رمز خصوصی و یا عمومی برای رمزدار کردن انتقالات است. اطمینان از ایجاد درست، ذخیره‌سازی، استفاده و از بین رفتن کلید رمز مهم است. لازم است در ردیابی‌های حسابرسی نیز دسترسی‌ها و اقدامات کاربر ردیابی شود.
ردیابی‌های حسابرسی	ردیابی‌های حسابرسی مجموعه‌ای از سوابق رویدادهای مرتبط با دسترسی و فعالیت‌های کاربر است. ردیابی‌های حسابرسی می‌تواند مسئولیت پاسخ‌گویی کاربر را از طریق ردیابی فعالیت‌های کاربر افزایش دهد، رویدادهای سیستم را بعد از وقوع مساله بازسازی، مسائل را بررسی و مزاحم‌های سیستم را شناسایی کند.

فهرست طبقه‌بندی شده XBRL ایجاد می‌شود. فهرست طبقه‌بندی شده XBRL از سازمان XBRL (XBRL.ORG) قابل دریافت است. تایید نرم‌افزار برای کنترل این موضوع صورت می‌گیرد که سند، یک سند معتبر XBRL است، سپس سند تایید شده XBRL در وب سایت شرکت یا سرویس‌دهنده FTP قرار می‌گیرد. در همان حال، سند مزبور به شرکت ارائه کننده خدمات اطمینان‌بخشی در اینترنت، با استفاده از امکانات امنیتی مناسب، فرستاده می‌شود.

حالا زمانی‌که کاربران به اطلاعات سند XBRL برای تجزیه وتحلیل نیاز دارند، ویرایش مطمئن آن را از شرکت تضمین کننده کیفیت اطلاعات (شرکت "ب") دریافت می‌کنند. حالا با دریافت نسخه‌ای مطمئن، اگر بخواهند به آسانی می‌توانند سند را به HTML، صفحه گسترده یا پایگاه داده‌ها تبدیل کنند.

اگرچه کاربران می‌توانند اسناد XBRL را از وب سایت شرکت تضمین‌کننده صحت اطلاعات یا هر منبع دیگری بدست آورند، اما همواره درباره صحت چنین اسنادی ابهام وجود دارد، زیرا برچسب‌های XBRL می‌توانند به اشتباه به‌کار برده شده و یا بدون مجوز قانونی مناسبی تغییر یابند. بنابراین کاربران باید برای بدست آوردن اطلاعات مالی قابل اتکا، این قبیل اسناد را از طریق شرکت واسطه تضمین کیفیت بدست آورند. این شرکت‌های واسطه، روش‌های اطمینان‌بخشی مختلفی چون تایید قابلیت اتکای فرایندهای تولید اطلاعات، انجام روش‌های تحلیل‌داده‌ها و بررسی صحت برچسب‌های XBRL را انجام می‌دهند. این شرکت‌ها یک سند XARL را از طریق درج اطلاعات مطمئن (مرتبط با عناصر گزارشگری واحد تجاری موجود در سند XBRL منتشر شده شرکت)، مطابق با عناصر طبقه‌بندی شده XARL ایجاد می‌کنند. فهرست طبقه‌بندی شده XARL از سازمان XARL در اینترنت قابل دریافت است. کاربران نیازمند اطلاعات مالی مطمئن و قابل اتکا می‌توانند اسناد XBRL و XARL را از شرکت‌های واسطه تضمین کیفیت درخواست کنند.

سیستم تایید در شرکت واسطه (شرکت ب)، پس از دریافت درخواست اطلاعات، درصورتی که کاربران مجاز به دریافت اطلاعات باشند، اسناد XBRL و XARL را برای کاربران می‌فرستد. سند XARL به‌طور دیجیتالی توسط شرکت واسطه "ب" با استفاده از کلید خصوصی امضا می‌شود و در صورت امکان، رمزگذاری با کلید عمومی کاربر نیز صورت می‌گیرد تا فقط

توسط او قابل استفاده باشد. سپس اسناد XBRL و XARL رمزگذاری شده برای کاربر ارسال می‌شود.

کاربر با استفاده از کلیدهای اختصاصی و عمومی ایجاد شده توسط شرکت واسطه "ب" اسناد XBRL و XARL را رمزگشایی کرده و برای اهداف خود از آنها استفاده می‌کند. او همچنین می‌تواند اعتبار اسناد XBRL و XARL را از طریق تایید امضای بیمه‌کننده تایید کند. زیرا امضای دیجیتالی داده‌ها یک عنصر غیر قابل جعل است. امضای دیجیتالی صحت سند و هویت فرستنده را تایید می‌کند که امضای او در سند پیوست می‌شود. اگر کاربران بخواهند سند را به HTML، یک صفحه گسترده یا پایگاه داده‌ها تبدیل کند، می‌توانند با صفحات مناسب ایجاد شده توسط خودشان یا سایر نرم‌افزارها این کار را انجام دهند.

به‌طور خلاصه، XBRL می‌تواند روش استانداردی را برای تهیه، انتشار و تبادل اطلاعات مالی فراهم کند. محیط XARL هم مدرکی را فراهم می‌سازد که کاربران اطمینان یابند اطلاعات کدگذاری شده XBRL نه تنها توسط حسابرسان، حسابرسی شده بلکه دستکاری نیز نشده است. بنابراین عدم اطمینان درباره اطلاعات مالی به میزان زیادی کاهش می‌یابد.

موضوع امنیت در اینترنت

موضوع امنیت در اینترنت به‌دلیل این واقعیت از اهمیت زیادی برخوردار است که اینترنت شبکه عمومی غیرقابل اتکا و ناامنی است. ناامنی ذاتی اینترنت، مزاحمان و سارقان داده‌ها را به خود جلب می‌کند. بنابراین خدمات گزارشگری مالی مبتنی بر وب ناامن است. برخی از تهدیدهای عمده امنیت در خدمات گزارشگری مالی تحت وب عبارت از: دستکاری در پیام، افشای پیام محرمانه، جایگزینی پیام، امتناع از ارائه خدمت، وارسی بسته[۴] و حملات ویروس‌ها است. (Bosworth and Kabay, 2000) در **نمایشگر ۱** این تهدیدها بطور خلاصه ارائه شده است.

خدمات گزارشگری مالی، مجموعه‌ای از اطلاعات مالی را برای تعداد زیادی از کاربران از طریق سیستم‌های توزیع شده و در عین حال ناهمگون، فراهم می‌آورند. با این وجود، ویژگی‌های امنیتی این سیستم‌ها باید به گونه‌ای باشد که اطمینان دهد چنین خدماتی فقط به گیرندگان مجاز، فرصت دسترسی به این اطلاعات مالی را می‌دهد و در صورت لزوم، هویت کاربر را تایید می‌کند. کاربران خدمات گزارشگری مالی، باید بتوانند صحت اطلاعات فراهم‌شده را تایید، پیام را بطور محرمانه دریافت و هویت تامین‌کنندگان این خدمات را تایید و تعیین کنند که آیا تامین‌کننده خدمات گزارشگری مالی، مجوز ارائه این خدمات را دارد؟

نمایشگر ۳ـ استانداردهای امنیت XML

استاندارد امنیت	شرح
رمزگذاری XML	رمزگذاری XML به منظور فراهم کردن روشی برای انتقال سند XML ایجاد شد تا سند فقط توسط گیرندگان مورد نظر قابل خواندن باشد. استاندارد یا مشخصه رمزگذاری XML، قالب، مدل داده‌ها و ساختار دستوری محتوای رمزگذاری را با در نظر گرفتن این موضوع تعریف می‌کند که گیرنده اطلاعات مورد نظر به نظام کشف رمز مجهز است. با رمزگذاری، کاربران علاوه بر کل اسناد XML، می‌توانند بخش‌های خاصی از سند را نیز رمزگذاری کنند.
امضاء XML	امضا XML مشخصه طراحی شده‌ای است که الزامات خاصی را برای امضاهای دیجیتالی مورد استفاده در اسناد XML در نظر می‌گیرد. امضای XML ساختار دستوری مورد نیازی را برای امضای عناصر خاصی از سند به جای همه آن، اضافه کردن بیش از یک امضا به یک سند و برخورد با مسئله تغییرات احتمالی داده‌های امضا شد، تعریف می‌کند.
زبان نشانه‌ای تخصیص امنیت (SAML)	زبان نشانه‌ای تخصیص امنیت، یک سازوکار مبتنی بر XML است که اعتبار و مجوز اطلاعات را مبادله می‌کند. زبان SAML روشی عمومی را برای اشتراک خدمات امنیتی بین بخش‌های مختلف فراهم می‌کند و نیز به بخش‌های مختلف اجازه تبادل موضوعات مرتبط با امنیت، اعتبار، مجوز و نمایه اطلاعات را صرف‌نظر از سیستم‌های امنیتی مورد استفاده، می‌دهد.
زبان نشانه‌ای کنترل دسترسی توسعه‌پذیر (XACML)	زبان نشانه‌ای کنترل دسترسی توسعه‌پذیر (XACML) مشخصه‌ای است که همراه با SAML مورد استفاده قرار می‌گیرد. این زبان روشی را برای استاندارد کردن سیاست‌های کنترل دسترسی فراهم می‌کند که برای اسناد XML ایجاد و به‌کار برده می‌شوند.

کنترل‌های دسترسی مبتنی بر شناسه و کلمه عبور کاربر، برای خدمات گزارشگری مالی کافی نیست زیرا چنین کنترل‌هایی فقط اطمینان می‌دهد که کاربران مجاز قادرند به سرویس‌ها دسترسی داشته باشند اما نمی‌تواند سایر اطمینان‌هایی را تامین کند که تامین‌کنندگان و کاربران نیاز دارند. از روش‌هایی مثل رمزگذاری و رمزگشایی پیام‌های مورد مبادله بین بخش‌های مختلف در شبکه‌های عمومی، مانند اینترنت، استفاده می‌شود تا پیام‌ها را از دسترسی غیرمجاز درهنگام عبور حفظ کند.

امروزه با استفاده از گواهی‌های دیجیتالی مانند گواهینامه X.509، به‌عنوان بخشی از فرایند تایید، می‌توان اعتبار فرستنده و گیرنده پیام را تایید کرد. پروتکل دیگر برای انتقال امن داده‌ها در وب، S-HTTP[5] یا HTTP امن است.

هرچند با امکانات موجود هم در صورت وجود زیر ساخت‌های مناسب، می‌توان ارتباط امنی را برای انتقالات محیط XBRL فراهم سازند، اما برای تامین امنیت کافی نیستند. در خدمات گزارشگری مالی، پیام XML ممکن است قبل از رسیدن به مقصد، از میان رابط‌های متعددی عبور کند. بنابراین برقراری امنیت نقطه به نقطه در میان آن رابط‌ها، دشوار و پرهزینه است.

بنابراین اگر تامین‌کننده سرویس مالی بخواهد فقط بخش خاصی از سند را رمزگذاری کند(برای مثال، عنصر وجوه نقد در ترازنامه)، رمزگذاری فقط آن بخش از طریق امکانات معمول و موجود، دشوار خواهد بود.

همان طور که پیش از این توضیح داده شد، در خدمات گزارشگری مالی تحت XBRL در خصوص تبادل پیام‌های XML کدگذاری شده، باید ساز و کاری فراهم شود که الزامات اولیه امنیت لایه پیام را برآورده کند. برای نمونه، گیرنده پیام باید قادر باشد که از صحت پیام اطمینان، پیام را بطور محرمانه دریافت و هویت فرستنده را تعیین کند. ویژگی‌های امنیتی خاصی برای ارزیابی چگونگی انتقال الکترونیکی و قابل اعتماد و قابل اتکا بودن پیام‌های XML کدگذاری شده باید فراهم شود (Greenstein and Vasarhelyi,2002) **نمایشگر ۲** این الزامات را به‌طور خلاصه بیان می‌کند. برای خدمات گزارشگری مالی امن، موضوع امنیت باید مورد توجه قرارگیرد و برای این کار دامنه‌ای از ساز و کارهای امنیت مبتنی بر XML مورد نیاز است.

تلاش‌های بسیاری به منظور ایجاد اطمینان درباره امنیت در اینترنت به‌خصوص برای خدمات وب صورت گرفته است. این روش‌ها، راه حل‌هایی برای ایجاد امنیت لایه پیام مبتنی بر XML پدید آورده و از این رو می توانند برای خدمات گزارشگری مالی تحت وب مورد استفاده قرار گیرند. **نمایشگر ۳** این استانداردهای امنیتی را به‌طور خلاصه ارائه می‌کند.

اگرچه این استانداردهای امنیتی می‌توانند اطمینان‌های اولیه‌ای درباره گزارشگری مالی اینترنتی فراهم آورند، اما ترکیب و اجرای تمامی این راه حل‌های امنیتی به‌دلیل پیچیدگی محیط واحد تجاری و الزامات زیربنایی، دشوار است. علاوه بر این، پیوندهای ضعیف موجود در شبکه امنیتی، می‌توانند امنیت زیربنای موجود را از بین ببرد.

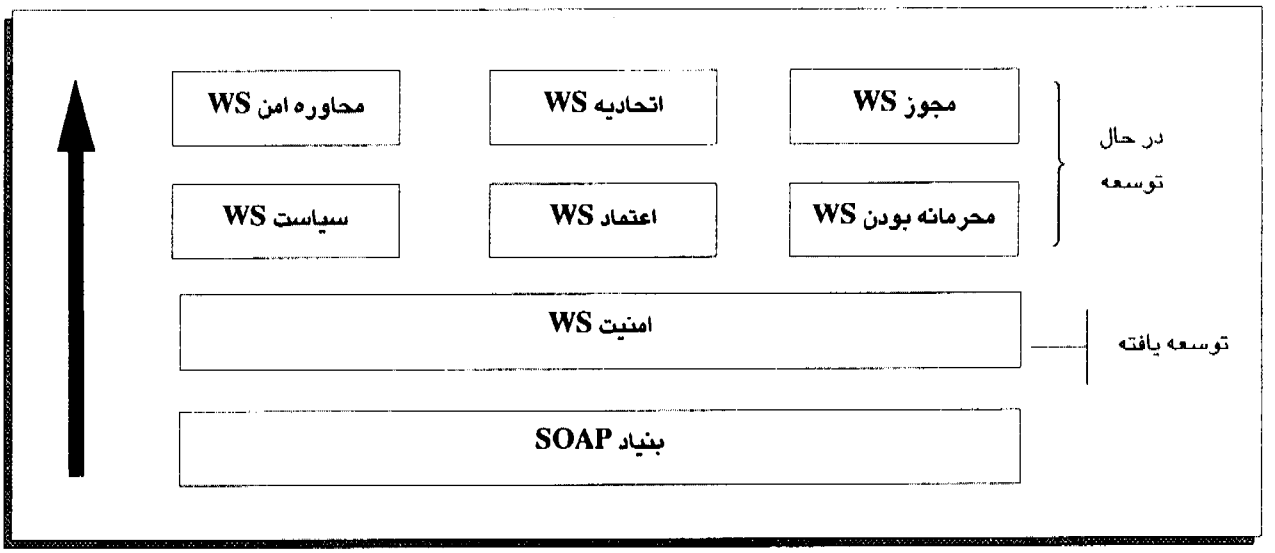
معماری امنیت خدمات وب (یا WSSA) شامل مجموعه‌ای از استانداردهای مورد توافق و نظر گروه شرکت‌های IBM، Microsoft و Verisign است. این استانداردها هنگام تبادل داده‌ها به‌عنوان بخشی از سرویس وب، بر موضوع برقراری امنیت حاکم است. (MSDN, 2003b) معماری WSSA کیفیت تبادل پیام را از طریق اطمینان بخشی، تایید صحت، تایید اعتبار، بررسی مجوز و برقراری اعتماد، بهبود می‌بخشد. (MSDN, 2002) از آنجا که WSSA امنیت نقطه به نقطه را ممکن ساخته و امنیت خدمات وب را مورد توجه قرار داده است، سازوکاری مناسب برای دستیابی به الزامات امنیت برای خدمات گزارشگری مالی نیز می باشد.

معماری WSSA دارای چندین مشخصه است: امنیت، سیاست، اعتماد، محرمانه بودن، محاوره امن، اتحادیه WS و مجوز WS. **نمایشگر ۴** رابطه مشخصه‌های WSSA را نشان می‌دهد.

اطمینان، صحت و تایید اعتبار حداقل الزامات برای کنترل امنیت سرویس XARLمی باشند. امنیت، سیاست و اعتماد ابزاری را برای ایجاد اطمینان درباره اختصاصی بودن، صحت و تأیید اعتبار خدمات گزارشگری مالی فراهم کرده و در عین حال، این امکان را فراهم می‌کند که با سایر خدمات وب ارتباط برقرار کنند.

روش‌های معماری مختلفی وجود دارد که می توان از آنها برای اجرای خدمات XBRL و XARL استفاده کرد. **بوریتز و نو** (Boritz and No, 2004b) الزامات زیربنایی را در مورد امکان اجرای خدمات گزارشگری مورد توجه قرار داده‌اند.

نمایشگر ۴ـ رابطه مشخصه‌های امنیتی در WSSA



فرض کنید شرکت سهامی عام "الف" از گزارشگری تحت محیط XBRL استفاده می‌کند. شرکت تضمین کیفیت "ب" که خدمات اطمینان بخشی گزارش‌های محیط XBRL را ارائه می‌دهد نقش واسطه انتقال این اطلاعات را ایفا می‌کند. فرض کنید که کاربری بنام "ج" نیز می‌خواهد صورت‌های مالی شرکت "الف" را برای تصمیم‌گیری در زمینه سرمایه‌گذاری تجزیه و تحلیل کند.

شرکت "الف" اطلاعات مالی را با استفاده از سیستم حسابداری داخلی خود تهیه کرده و یک سند XBRL را با درج اطلاعات مالی مبتنی بر سرفصل‌های طبقه‌بندی شده خاص شرکت و عناصر فهرست طبقه‌بندی شده XBRL ایجاد می‌کند. سند XBRL به‌عنوان یک پیام کدگذاری شده از طریق اینترنت منتقل می‌شود و به‌طور دیجیتالی توسط سازمان XBRL با استفاده از علایم امنیتی همچون Keberos Ticket[6] یا گواهینامه X.509 (امنیت WS) امضا می‌شود. سند XBRLایجاد شده به‌طور خودکار کنترل می‌شود که آیا XBRL صحیح است. سپس سند XBRL تایید شده در پایگاه داده‌های شرکت قرار می‌گیرد.

شرکت تضمین کیفیت اطلاعات "ب" سند XBRL را از شرکت "الف" می‌گیرد. هر زمان که برنامه تامین‌کننده خدمات XBRL در شرکت "الف" درخواستی را در زمینه تایید اعتبار اطلاعات از برنامه اطمینان بخشی شرکت "ب" داشته باشد، برنامه موجود در شرکت "ب" درخواست را با استفاده از علائم امنیتی رمزگذاری می‌کند. سپس در صورتی که شرکت "ب" برای دریافت اطلاعات مجاز شناخته شود برنامه شرکت "الف" با برنامه شرکت "ب" ارتباط برقرار می‌کند. سند XBRL به‌طور دیجیتالی توسط شرکت "الف" با استفاده از علائم امنیتی امضا می‌شود. برای نمونه، سند XBRL کدگذاری شده به‌طور دیجیتالی و با استفاده از کلید خصوصی امضا می‌شود و با کلید عمومی مورد استفاده در شرکت "ب" رمزگذاری می‌شود. شرکت خدمات اطمینان بخشی "ب" با استفاده از کلیدهای مزبور سند XBRL را رمزگشایی می‌کند. سپس شرکت "ب" رویه‌های اطمینان بخشی را در مورد اطلاعات دریافتی از "الف" انجام می‌دهد و یک سند XARL را از طریق درج اطلاعات مطمئن مربوط به شرکت "الف" (با استفاده از اطلاعات موجود در سند XBRL آن شرکت) ایجاد می‌کند. این سند XARL با استفاده از علایم امنیتی امضا می‌شود. بررسی صحت سند XARL ایجاد شده به‌طور خودکار انجام می‌شود. سپس سند تایید شده در پایگاه داده‌های شرکت "ب" قرار می‌گیرد. زمانی که کاربری بنام "ج" به اطلاعات مندرج در سند XBRL برای تجزیه و تحلیل خود نیاز دارد، برنامه درخواست کننده خدمت XBRL موجود نزد "ج" درخواست خود را به برنامه تامین‌کننده خدمات XBRL موجود در شرکت "الف" می‌فرستد. دریافت اطلاعات مزبور کانال‌های اطمینان بخشی شرکت واسطه را به‌طور خودکار طی می‌کند تا نهایتاً اطلاعات قابل اعتماد در فرمت XARL به‌دست کاربر برسد. اگرچه "ج" می‌تواند سند XBRL را به‌طور مستقیم از شرکت "الف" هم به‌دست آورد اما این کار او را در معرض خطر دریافت اطلاعات غیرقابل اتکا قرار می‌دهد.

بالاخره "ج" با استفاده از کلیدهای خصوصی و عمومی فراهم شده، به‌وسیله شرکت واسطه "ب"، اطلاعات دریافتی را

رمزگشایی می‌کند. اگر "ج" بخواهد معتبر بودن شرکت " ب" را تایید کند، می‌تواند این کار را نیز انجام دهد. سپس "ج" صورت‌های مالی معتبر دریافتی را برای تجزیه و تحلیل مورد استفاده قرار می‌دهد. برای مثال، صورت‌های مالی را در Excel قرار می‌دهد و نسبت‌های مالی را محاسبه می‌کند.

دریافت سند XARL اگر با استقرار برنامه ویژه‌ای بین برنامه درخواست‌کننده و برنامه سرویس‌دهنده همراه شود، اطلاعات مالی موجود در مدل Excel کاربر "ج" می‌تواند به‌طور مستمر بهنگام شود. همچنین "ج" می‌تواند به‌طور همزمان از خدمات گزارشگری مالی و سایر خدمات تحت وب مانند مظنه قیمت سهام و خدمات سرمایه‌گذاری در سهام استفاده کند. همچنین با استقرار برنامه یاد شده، "ج" می‌تواند از سرویس XARL و سایر خدمات وب به‌طور خودکار و مستمر استفاده کند.

امروزه شرکت‌های زیادی در صددند تا اطلاعات مالی خود را با استفاده از اینترنت در عرصه وسیع‌تری منتشر کنند. آنها همزمان از شبکه‌های درون شرکتی یا اینترانت‌ها نیز استفاده می‌کنند. با اتصال اینترانت‌ها به اینترنت و ایجاد وب سایت شرکت‌ها اطلاعات مالی را در اختیار ذی‌نفعان قرار می‌گیرد. کاربران اطلاعات مالی می‌توانند به آسانی و به موقع اطلاعات مورد نیاز را به‌دست آورند. با این وجود، داده‌ها باید دوباره توسط کاربران جستجوگر برای تجزیه و تحلیل آنها ثبت یا برش و الصاق شوند زیرا قالب‌های پذیرفته شده عمومی و مشترکی برای شرح داده‌های گزارش شده واحد تجاری وجود ندارد. زبان گزارشگری مالی توسعه پذیر(XBRL) برای غلبه بر این محدودیت و فراهم نمودن ابزار موثر و کارآمد برای تهیه و تبادل اطلاعات مالی در اینترنت ایجاد شد. زبان گزارشگری اطمینان‌بخشی توسعه پذیر(XARL) به منظور حسابرسی و تایید اعتبار و صحت اطلاعات مورد گزارش در محیط XBRL نیز ابداع کمک‌کننده بعدی بود. به کمک XARL به کاربران و شرکت‌ها اطمینان داده می‌شود تا به اطلاعات XBRL دریافتی اعتماد کنند. این دو پدیده یعنی XBRL و XARL در کنارهم می‌توانند روش استانداردی را برای تهیه، انتشار و تبادل اطلاعات مالی فراهم کنند و همچنین صحت اطلاعات توزیع شده در اینترنت را تضمین کنند.

1- eXtensible Busines Reporting Language(XBRL)

2- eXtensible Assurance Reporting Language(XARL)

3- eXtended Markup Language(XML)

4- Packet Sniffing

(سخت افزار یا نرم‌افزاری است که بسته‌های ارسالی در یک شبکه را بررسی می‌کند).

7- Secure Hypertext Transfer Protocol

(این پروتکل امنیت انتقال اطلاعات را در اینترنت تضمین و امنیت پیام به پیام را تامین می کند)

۸- پروتکل اعتبار شبکه‌ای که توسط دانشگاه MIT ابداع شد. پروتکل Keberos هویت کاربرانی را تایید یا رد می‌کند که می‌خواهند با شبکه ارتباط برقرار کنند و توسط کلید رمز، ارتباطات آنها را رمزدار می‌کند.

1- Boritz, J.E., No, W.G., 2003a. Business Reporting with XML: XBRL (Extensible Business Reporting Language). The Internet Encyclopedia. John Wiley, New York.

2- Boritz, J.E., No, W.G., 2003b. Assurance Reporting for XBRL: XARL(Extensible Assurance Reporting Language). Trust and Data Assurances in Capital Markets: The Role of Technology Solutions. Research Monograph sponsored by Pricewaterhouse Coopers, pp.17-31.

3- Boritz, J.E., No, W.G., 2004a. Assurance Reporting for XML-Based Information Services: XARL (Extensible Assurance Reporting Language). Canadian Accounting Perspectives 3(2), 207-233.

4- Boritz, J.E., No, W.G., 2004b. Infrastructure Requirements for Assurance Reporting with XARL (Extensible Assurance Reporting Language), Manuscript, University of Waterloo.

5- Bosak, J., Bray, T., 1999. XML and the Second Generation Web. Retrieved March 3, 2003, from:<http://www.sciam.com>.

6- Bosworth, S., Kabay, M.E., 2002. Computer Security Handbook, fourth ed. John Wiley & Sons Inc., New York.

7- Elliotte, R.H., 2001. XML Bible, second ed. John Wiley & Sons Inc., New York.

8- Greenstein, M., Vasarhelyi, M., 2002. Electronic Commerce: Security, Risk Management, andControl. McGraw Hill Irwin, New York.

9- Halfhill, T.R. 1999. XML: The Next Big Thing. Retrieved March 20, 2003, from <http://domino.research.ibm.com/comm >.

10- Hoffman, C., Strand, C., 2001. XBRL Essentials. AICPA, New York.

11- MSDN., 2003b. Secure, Reliable, Transacted Web Services: Architecture and composition. Retrieved February 9, 2004, from <http://msdn.microsoft.com/ >.

12- MSDN, 2002. Security in a Web Services World: A proposed Architecture and Roadmap. Retrieved February 17, 2004, from <http://msdn.microsoft.com>.