فصلنامه علمی-ترویجی پدافند غیرعامل

سال سوم، شماره ۴، زمستان ۱۳۹۱، (پیاپی ۱۲): صص ۴۵-۵۳

بررسی مدل‌های کنترل دسترسی در XML

احسان سرگلزایی[۱]، مجید غیوری[۲]

تاریخ دریافت: ۹۱/۰۹/۰۲
تاریخ پذیرش: ۹۱/۱۰/۰۴

چکیده

امروزه حجم زیادی از اطلاعات بر روی وب قرار داردکه بخش قابل توجهی از این اطلاعات در قالب XML ظاهر شده است. یکی از مزیت‌های اصلی استفاده از XML ، نمایش داده‌های غیرساخت‌یافته است که قابلیت‌های بسیاری را در اختیار کاربران می‌گذارد. ویژگی غیرساخت‌یافته بودن اطلاعات و انعطاف‌پذیری XML باعث فراگیرشدن استفاده از آن شده و در بانک‌های اطلاعات نیز مورد توجه قرار گرفته است. بنابراین، برقراری امنیت در مستندات XML یک نیاز جدی می‌باشد. داده‌ها به هر شکلی که ذخیره شوند باید از تهدیدهای ممکنمحافظت گردند. برای جلوگیری از تهدیدها، روش‌ها و مدل‌های گوناگونی در بانک‌های اطلاعات طرح‌ریزی و پیاده‌سازی شده است. این مدل‌ها خود نیز مبتنی بر روش‌های مختلفی می‌باشد که در بانک‌های اطلاعات گوناگون به‌کار گرفته می‌شوند.یکی از مهم‌ترین این مدل‌ها، مدل کنترل دسترسی می‌باشد.در این مقاله، مدل‌های کنترل دسترسی روی سندهای XMLبررسی و مقایسه شده است.

کلیدواژه‌ها: داده‌های غیرساخت‌یافته، کنترل‌دسترسی، مدل‌های کنترل‌دسترسی XML، امنیت

۱- کارشناس ارشد امنیت اطلاعات، دانشگاه صنعتی مالک اشتر ehsan.sargolzai@gmail.com - نویسنده مسئول
۲- استادیار و عضو هیئت علمی دانشگاه جامع امام حسین(ع)

۱- مقدمه

«اطلاعات ساخت‌یافته» اطلاعاتی هستند که دارای ساختار مشخصی هستند. بانک‌های اطلاعات رابطه‌ای، نمونه خوبی از بانک‌های اطلاعات ساخت‌یافته هستند. در مقابل، اطلاعات نیمه‌ساختاریافته، ساختار مشخصی ندارند و خودتعریف می‌باشند. سندهای XML نیز نیمه‌ساختاریافته‌اند.هر چند داده‌های ساخت‌یافته و غیرساخت‌یافته هر دو می‌توانند در قالب XML ذخیره شوند؛ اما نمایش داده‌های غیر ساخت‌یافته به صورت XML قابلیت‌های بسیاری را در اختیار کاربران می‌گذارد. ویژگی غیرساخت‌یافته بودن اطلاعات و انعطاف‌پذیری XML و همچنین همه‌گیر شدن استفاده از آن باعث شده است که در بانک‌های اطلاعات نیز مورد توجه قرار گیرد. در این میان، دسترسی به اطلاعات و امنیت اطلاعات مبادله‌شده بسیار مورد توجه می‌باشد.

جهت برقراری امنیت در بانک اطلاعات XML مدل‌ها، مکانیزم‌ها و روش‌هایی وجود دارد. در حال حاضر بخش قابل توجهی از مدل‌هایی که در برقراری امنیت در بانک اطلاعات XML استفاده می‌شود، مدل‌های کنترل دسترسی می‌باشند. بیشتر کنترل‌های دسترسی مرسوم، شامل لیست‌های کنترل دسترسی [۴]، لیست‌های قابلیت [۷] و ماتریس‌های کنترل دسترسی [۴] هستند. هنگامی که درباره امنیت یک سیستم صحبت می‌شود، "کنترل دسترسی" جنبه‌های بسیاری را شامل می‌شود. کنترل دسترسی باید ساده و قابل فهم باشد و بتواند امنیت دسترسی به داده‌های مستقر در یک مکان را پشتیبانی نماید. همچنین در بسیاری از سیستم‌ها همچون سیستم‌های تراکنش تجاری و بایگانی‌های پزشکی که شامل داده‌های حساس می‌باشند، کنترل دسترسی در پایین‌ترین سطح (عنصر و یا صفت) مورد نیاز است.

کارهای زیادی برای توصیف کنترل دسترسی روی مستندات XML انجام شده است. برخی از این کوشش‌ها عبارت‌اند از: تعریف و اجرای خط‌مشی‌های کنترل دسترسی بر روی منابع XML [۸]، کنترل دسترسی به مستندات XML توسط تعیین سطوح مجوزها و خط‌مشی‌های انتشار مجوزها [۹]، توصیف کنترل دسترسی برای اسناد XML که ارتباط معنایی با هم دارند [۱۰] و تعریف یک سیستم کنترل دسترسی در پایین‌ترین سطح برای مستندات XML [۱۱]. کنترل دسترسی در پایین‌ترین سطح، شامل توصیف موضوع‌های مجوز (کاربران یا گروه‌های کاربری و یا کامپیوترها)، اشیاء مورد دسترسی (المان‌ها و محتوای المان‌ها) و تعیین مجوزهای دسترسی می‌باشد. تمرکز در این کار عموماً بر روی توصیف یک زبان برای تعیین محدودیت‌های کنترل دسترسی به مستندات XML و همچنین توصیف انواع مختلف خصوصیات و خط‌مشی‌های مرتبط با آن می‌باشد.

۲- امنیت در بانک اطلاعات

هنگامی که صحبت از بانک اطلاعات امن به میان می‌آید معمولاً سه هدف محرمانگی[1]، جامعیت[2] و دسترس پذیری[3] مطرح می‌شود. برای رسیدن به این اهداف بایستی سیاست‌های امنیتی واضح و مشخصی تدوین گردد. به‌عبارت دیگر، باید به‌طور کامل و صریح روشن گردد که چه بخش یا بخش‌هایی از داده‌ها باید محافظت شوند و چه کاربرانی اجازه دسترسی به چه قسمت‌هایی از داده‌ها را دارند.

برای برقراری امنیت در سیستم بانک‌اطلاعات، ابتدا با کمک مکانیزم‌های تصدیق هویت کاربر، مثل کلمهٔ عبور، اطمینان حاصل می‌کنیم که کاربر واردشده به سیستم، یک کاربر مجاز می‌باشد. در مرحله بعد، هنگامی که مطئمن شدیم کاربری که وارد سیستم شده اجازه ورود داشته است، با مکانیزم‌های کنترل دسترسی، فقط مجوزهای دسترسی به داده‌های به‌خصوصی که می‌تواند به آنها دسترسی داشته باشد را به او تخصیص می‌دهیم. اما این کاربر مجاز ممکن است روی همان داده‌های مجاز، خود نیز تغییرات غیر مجاز انجام دهد. مقابله با چنین تهدیداتی به تضمین جامعیت سیستم برمی‌گردد که با قرار دادن قیود جامعیت، استفاده از مکانیزم‌هایی مثل assertion، trigger و.... از داده‌های بانک‌اطلاعات مراقبت می‌نمائیم.

در بانک‌های اطلاعات نامتمرکز، بخشی از امنیت بانک به تبادل اطلاعات و ذخیره‌سازی آنها بستگی دارد. رمزنگاری، امنیت کانال‌های ارتباطی را برقرار می‌کند. ایده اصلی رمزنگاری داده‌ها، استفاده از الگوریتم‌های رمزنگاری و نیز یک کلید رمزنگاری مخصوص مدیر بانک اطلاعات استکه به صورت امن نگاه داشته می‌شود. در بانک‌های اطلاعات XML و به‌خصوص بانک‌های نامتمرکز، اغلب به‌دلیل ذخیره‌سازی اطلاعات به فرمت رشته، عمل رمزنگاری داده‌ها جهت انتقال و همچنین ذخیره‌سازی بسیار الزامی می‌باشد

۳- مفاهیم کنترل دسترسی XML

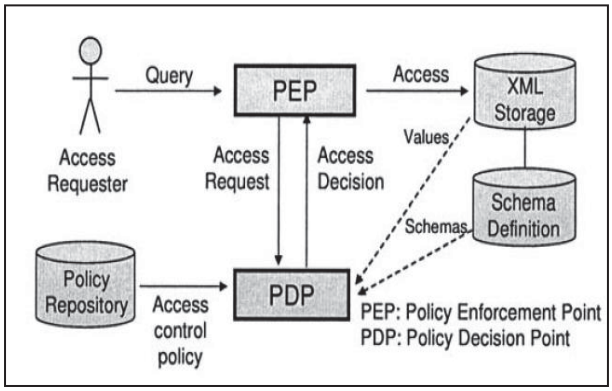
در این قسمت، ابتدا مفاهیم کلی کنترل دسترسی XML آورده می‌شود.

۳-۱- معماری کلی کنترل دسترسی XML

در شکل (۱) معماری کلی کنترل دسترسی XML آورده شده است. یک درخواست‌دهنده درخواست خود را به PEP(نقطه اِعمال سیاست) ارسال می‌کند. در ادامه، PEP از PDP (نقطه تصمیم‌گیری سیاست) می‌خواهد که تصمیم مجوزدهی در مورد درخواست مذکور را به وی اعلام کند. PDP، سیاست‌هایی که برای تصمیم‌گیری در مورد این

1- Secrecy
2- Integrity
3- Availability

درخواست مورد نیاز هستند را از انباره سیاست بازیابی می‌کند. سپس بـر اسـاس شـمای داده‌هـا و اشـیای درخواسـتی در پـرس‌وجـو و سیاست‌های مربوطه، تصمیم نهایی را به PEP اعلام می‌کند. در انتهـا PEP با توجه به تصمیمی که از PDP دریافت کرده اسـت، دسترسـی به داده‌های درخواستی را تعیین می‌کند.



شکل ۱- معماری کلی کنترل دسترسی XML

۳-۲- سیاست کنترل دسترسی

براساس قوانین سیاست کنترل دسترسی مشخص می‌شـود کـه چـه نهادهایی (مثلاً یک کـاربر انـسانی، یـک سیـستم و غیـره) روی چـه اشیائی، چه مجوزهای دسترسی‌ای (مثلاً مجـوز خوانـدن، نوشـتن، و غیره) دارند.

۳-۳- نهادها

نهادها معمولاً بر اساس شناسه‌شان شناخته می‌شوند. موقعیـت‌هـا را می‌توان با استفاده از آدرس IP یـا آدرس نمـادین نـشان داد. نهادهـا می‌توانند در یک سلسله‌مراتب نیز سـازماندهی شـوند، بـه‌طـوری‌کـه مجوزدهی برای یک نهاد بالاتر در سلسله‌مراتب می‌تواند به گـره‌هـای پایین‌تر از خود نیز انتشار یابد.

۳-۴- اشیاء مجوزدهی

یک شئ می‌تواند یک شما، یک سند، و یا یک زیرسـند باشـد. بـرای شناسایی شما و سند، می‌توان از یکی از روش‌های نام فایـل، شناسـه منبع عام (URI)[1]، یـا شناسـه شـئ (در پایگـاه داده) اسـتفاده کـرد. اشیای زیرسند را می‌توان با استفاده از عبارات مسیر XPath شناسایی کرد. شئ‌هایی که کنترل دسترسی را بر روی آن‌ها اعمال مـی‌کننـد، شامل مستنداتی هستند که با یک شِمای XML مطابقت دارند.

۳-۵- عملیات دسترسی

دو نوع عمل دسترسی خواندن و نوشتن (به‌روزرسانی، ایجاد، حـذف) روی اشیاء وجود دارد. بیشتر مدل‌ها تنها از عمل خوانـدن پـشتیبانی می‌کنند.

۳-۶- مجوزدهی در سطح شِما و سند

دو نوع مجوزدهی داریـم: ۱- مجـوزدهی در سـطح سـند کـه در آن، مجوزدهی فقط روی یک سند خاص انجام می‌شود. ۲- مجوزدهی در سطح شِما که در آن، مجـوزدهی روی مجموعـه‌ای از سـندها انجـام می‌شود. بنابراین، مجوزهایی که برای یک شِما وجود دارند، برای تمام سندهای منطبق با آن شِما نیز قابل اِعمال هستند.

۳-۷- انتشار

در یک سند XML، انتشار[2] بدین معنی است که آیا مجوزهـای یـک عنصر، فقط محدود بـه آن عنـصر و صـفت‌هـایش اسـت(مجـوزدهی محلی[3]) یا اینکه مجوزها برای تمام محتوای عنصر (یعنی صـفت‌هـا و زیرعناصر آن عنصر) قابل اِعمال است؟ (*مجوزدهی بازگشتی*[4])

برخـی از مـدل‌هـا، انتـشار را فقـط بـرای مجوزهـای منفـی در نظـر می‌گیرند که به آن، سازگاری روبه پایین نیز گفتـه مـی‌شـود. یعنـی، فقط مجوزهای منفی یک عنصر، به تمام صـفت‌هـا و زیرعنـصرهایش انتشار می‌یابند. برخی از مـدل‌هـا، انتـشار رو بـه بـالا را نیـز مطـرح می‌کنند که در آن، مجوزهای یک گـره در درخـت XML، بـه طـرف والدهایش منتشر می‌شود. چهار سیاست انتشار که در مدل‌ها استفاده می‌شوند، عبارت‌اند از: ۱- عـدم انتـشار: کـه در آن مجوزهـا منتـشر نمی‌شوند (مجوزدهی محلی). ۲- عدم لغـو: مجوزهـای یـک گـره بـه زیرگره‌هایش منتشر می‌شود اما این انتشار، مجوزهای زیرگره‌ها را لغو نمی‌کند. ۳- لغو مجوز عام‌تر توسط مجـوز خـاص‌تـر: مجـوز گـره n، مجوزهای ناسازگاری مربوط به اجدادش را لغو می‌کند. ۴- لغو مسیر: مجوزها فقط برای گره‌های روی یک مسیر مشخص لغو می‌شوند.

۳-۸- ترکیب قوانین و مشکل ناسازگاری مجوزها

گاهی اوقات نتایج مجوزدهی دو یا چند قانون کنترل دسترسی، باعث ناسازگاری[5] می‌شـوند. مـدل‌هـای کنتـرل دسترسـی در مواجهـه بـا ناسـازگاری از سیاسـت‌هـای رفـع ناسـازگاری اسـتفاده مـی‌کننـد: ۱- سیاست هر کدام خاص‌تر باشد، مقدم است: برای مثال، مجوزدهی در سـطح سـند، مقـدم بـر مجـوزدهی سـطح شِـما اسـت. ۲- «سیاست منفی‌ها» مقدم‌اند: در ایـن سیاسـت، مجوزهـای منفـی همیشه مقدم بر مجوزهای مثبت هستند. اغلب مدل‌ها از این سیاست استفاده می‌کنند. ۳- سیاسـت مجـوز قـوی، مجـوز ضـعیف را باطـل می‌کند: به هر قـانون، یـک اولویـت تخـصیص داده مـی‌شـود و از دو

1- Universal Resource Identifier (URI)

2- Propagation
3- Local Authorization
4- Recursive Authorization
5- Conflict

مفهوم ضعیف و قوی برای قوانین استفاده می‌شود. یک قانون قوی، قانون ضعیف را باطل می‌کند.
علاوه بر مشکل ناسازگاری، مواردی نیز ممکن است وجود داشته باشد که برای یک عمل دسترسی، نه مجوز مثبت و نه مجوز منفی وجود داشته باشد. به این مشکل، ناکامل بودن گفته می‌شود. دو سیاست برای برخورد با این مشکل داریم: ۱- سیاستِ باز؛ که در آن، مجوز پیش‌فرض، مجوز مثبت است. ۲- سیاست بسته؛ که در آن، مجوز پیش‌فرض، مجوز منفی است.

۴- مدل‌های کنترل دسترسی در بانک اطلاعات XML

یکی از اصول سیستم پایگاه داده‌ها، مدیریت کنترل دسترسی می‌باشد. مدیریت کنترل دسترسی در بانک‌های اطلاعات توسط سرویس‌دهنده‌ها انجام می‌شود. کنترل دسترسی بنابر عوامل مختلف به‌سرعت تحول یافته است. مدل‌های کنترل دسترسی را می‌توان به دو گروه سنتی و توسعه‌یافته تقسیم‌بندی نمود. در گروه سنتی، دو مدل کنترل دسترسی محتاطانه[1] و الزامی[2] قرار دارند که پایه و زیربنایی برای سایر مدل‌ها به‌حساب می‌آیند. مدل‌های گروه توسعه‌یافته، مدل‌هایی می‌باشند که بر پایه مدل‌های سنتی بنا شده و آنها را به نوعی توسعه داده و مشکلاتشان را رفع نموده‌اند. مدل‌های کنترل دسترسی در تعریف قوانین (تعریف نهادها، اشیا، و مجوزها) با یکدیگر تفاوت دارند.
در ادامه، به بیان اجمالی مدل‌های کنترل دسترسی می‌پردازیم.

۴-۱- مدل کنترل دسترسی محتاطانه

در این مدل، دسترسی کاربران به بانک اطلاعات، براساس هویت کاربران (ID) و قوانینی به نام اجازه ورود (مجوز) کنترل می‌شود [۱]. در اینجا برای هر کاربر (یا گروهی از کاربران) نوع دسترسی‌های آنها به هر شئ موجود در بانک مشخص می‌شود. نوع این اشیاء بستگی به بانک اطلاعات دارد. در مدل رابطه‌ای، اشیاء می‌توانند رابطه‌ها (جداول)، دیدها، صفت‌ها و در صورت لزوم، رکوردها؛ در مدل شئ‌گرایی می‌توانند شامل کلاس‌ها، اشیاء و متدها، و در بانک اطلاعات XML می‌توانند مستندات، مسیرها و عناصر باشند. کنترل‌های قابل اجرا بر روی اشیاء معمولاً در دو سطح صورت می‌گیرد: یکی در سطح حساب کاربری که امتیاز توسط مدیر بانک اطلاعات اعطا می‌شود و دیگری در سطح اشیاء که امتیاز اعطاءشده فقط برای بخشی از شئ خاص می‌باشد. بر این اساس، معمولاً انواع مجوزهایی که به یک کاربر داده می‌شود به صورت زیر است:
در سطح داده‌ها:
مجوز read : اجازه خواندن داده‌ها را می‌دهد ولی اجازه تغییر داده‌ها را نمی‌دهد.
مجوز insert : اجازه درج داده جدید را می‌دهد.
مجوز update : اجازه تغییر داده‌ها را می‌دهد.
مجوز delete : اجازه حذف داده‌ها را می‌دهد.
در سطح شِما:
مجوز index: اجازه ایجاد یا حذف شاخص‌ها را می‌دهد.
مجوز resource: اجازه ایجاد رابطه‌های جدید را می‌دهد.
مجوز alteration: اجازه اضافه یا حذف صفات رابطه را می‌دهد.
مجوز drop: اجازه از بین بردن رابطه‌ها را می‌دهد.
معمولاً یک مجوز به صورت سه‌تایی (subject, mode, object) نمایش داده می‌شود که بیان‌کننده روش دسترسی (mode) یک کاربر یا فرآیند (subject) به یک شئ (object) می‌باشد. بنابراین هر درخواستی که از طرف کاربر داده می‌شود، ابتدا مجوز آن بررسی شده و در صورت وجود سه‌تایی مربوطه، اجازه دسترسی داده می‌شود. در این مدل، دو نوع خط‌مشی تعریف می‌شود:

۱) **خط‌مشی بسته:** در این نوع خط‌مشی، دسترسی‌هایی اجازه داده می‌شود که مجوز صریح آنها موجود باشد و تصمیم پیش فرض این است که دسترسی رد شود. اکثر سیستم‌ها از سیاست‌های بسته پشتیبانی می‌کنند.
۲) **خط‌مشی باز:** در این خط مشی، مجوز منفی داده می‌شود و در صورت وجود آن، اجازه دسترسی داده نمی‌شود و تصمیم پیش‌فرض (در صورت عدم وجود مجوز منفی) این است که دسترسی قبول شود. سیاست باز فقط در سیستم‌هایی استفاده می‌شود که به حفاظت محدود نیاز دارند و اکثر دسترسی‌ها اجازه داده می‌شود.

۴-۲- مدل کنترل دسترسی الزامی

برای حل مشکلات بالقوه موجود در روش کنترل دسترسی محتاطانه، از روش کنترل دسترسی الزامی استفاده می‌شود [۱]. معروف‌ترین مدل کنترل دسترسی الزامی، مدل Bell-LaPadula است. در این مدل، پدیده‌های سیستم به چهار دسته زیر تقسیم می‌شوند:
شئ: پدیده‌های فعالی که اطلاعات را نگهداری می‌کنند؛ مانند جداول، رکوردها، صفت‌ها، دیدها، اشیاء و کلاس‌ها.
فرایند: پدیده‌هایی که درخواست‌های دسترسی به اشیاء را می‌دهند، مانند کاربران و برنامه‌ها.
کلاس‌های امنیتی[3]: سطوح امنیتی دسترسی به هر شئ را مشخص می‌کنند که به صورت‌های خیلی محرمانه (TS)، محرمانه (S)، سری (C)، و طبقه‌بندی‌نشده (U) تعریف می‌شوند و ترتیب آنها به‌صورت $TS > S > C > U$ است.
حساسیت[4]: حساسیت هر فرآیند در رابطه با یک کلاس امنیتی

1- Discretionary
2- Mandatory
3- Security Classes
4- Clearance

نمایش داده می‌شود. در این روش، کلاس دسترسی را به‌صورت زوج‌های مرتب از سطوح امنیتی و مجموعه گروه‌ها نمایش می‌دهند (S,G1).

کلاس‌دسترسی C1 پایین‌تر از کلاس‌دسترسی C2 است (C1 =< C2) اگر و فقط اگر سطح امنیت C1 بزرگتر یا مساوی سطح امنیت C2 و گروه‌های C1 شامل همه گروه‌های C2 باشند. دو کلاس C1 و C2 را غیر قابل مقایسه گویند اگر نه C1 =< C2 و نه C2 =< C1 برقرار باشد.

سطح امنیت از کلاس دسترسی یک شئ نشان‌دهنده حساسیت اطلاعات آن شئ می‌باشد. همچنین نشان‌دهنده پتانسیل خرابی است که از یک دسترسی غیر مجاز به اطلاعات می‌تواند نتیجه شود. سطح امنیت کلاس دسترسی یک کاربر، نشان‌دهنده قابل‌اعتمادبودن کاربر است که اطلاعات حساس را برای کاربران غیر مجاز فاش نمی‌کند. کاربران با کلاس دسترسی مربوط به خود با سیستم ارتباط برقرار می‌کنند و می‌توانند تراکنشی با کلاس دسترسی خود یا کمتر از آن به سیستم بدهند. به‌طور نمونه، کاربر با کلاس (S,0) می‌تواند تراکنش‌هایی با کلاس‌های دسترسی (S,0) و (C,0)و (U,0) به سیستم بدهد.

مدل Bell-LaPadula دو محدودیت زیر را در تمام دسترسی‌ها به اشیاء بانک اطلاعات قائل است:

۱. فرایند S اجازه دسترسی خواندن به شیء O را دارد اگر:

$$Class(S) >= Class(O)$$

به‌عنوان مثال، کاربر X با حساسیت TS، می‌تواند جدولی با حساسیت C را بخواند. اما کاربر Y با حساسیت C، اجازه خواندن از جدولی با حساسیت TS را ندارد.

۲. فرایند S اجازه نوشتن بر روی شیء O را دارد اگر:

$$Class(O) >= Class(S)$$

ضعف اصلی سیاست‌های الزامی، دشواری کنترل آنها است؛ زیرا احتیاج به تعریف و استفاده از طبقه‌بندی اشیاء، کاربران و برنامه‌ها دارند. این کار ممکن است همیشه میسر نباشد. به‌علاوه، دسترسی‌های تعیین شده، فقط بر اساس طبقه‌بندی اشیاء و تراکنش‌های موجود در سیستم است و هیچ امکانی به کاربران برای واگذاری یا پس‌گرفتن مجوز به دیگر کاربران داده نمی‌شود.

در ادامه، به چند مورد از مدل‌های گروه توسعه‌یافته که بر پایه مدل‌های سنتی بنا شده‌اند، می‌پردازیم.

۴-۳- مدل کنترل دسترسی دامیانی و سایرین

۴-۳-۱- خط‌مشی کنترل دسترسی

مجوزدهی با استفاده از پنج‌تایی <subject, object, action, sign, type> مشخص می‌شود که در آن، Subject ∈AS: نهادی است که مجوزدهی باید برایش انجام شود. Object: می‌تواند یک URI∈Obj یا یک URI:PE باشد که در آن، URI ∈Obj و PE یک عبارت مسیر است. Action: تنها می‌تواند خواندن باشد. Sign ∈ {+,-}: نشان‌دهنده مجاز یا عدم مجاز بودن دسترسی است. type ∈ {LDH, RDH, L, R, LD, RD, LS, RS}: نوع مجوزدهی و سیاست انتشار را مشخص می‌کند.

نهادها: در این مدل، نهادها می‌توانند بر اساس شناسه خود و موقعیت‌شان شناسایی شوند. یک نهاد با سه‌تایی <user-id, IP-address, sym-address> شناسایی می‌شود. user-id، شناسه کاربری‌ای است که کاربر با آن به سیستم متصل شده است. IP-address آدرس IP و sym-address، آدرس نمادینی ماشینی است که کاربر از آن به سیستم متصل شده است.

اشیاء: مجموعه‌ای از URI ها است که به سندهای XML یا DTD ارجاع دارند. ارجاع به عناصر و صفت‌ها نیز با استفاده از عبارات مسیری انجام می‌شود.

عملیات: این مدل فقط از عمل خواندن پشتیبانی می‌کند.

علامت: دو نوع علامت مثبت و منفی را داریم که علامت مثبت، نشانه مجاز بودن، و علامت منفی، نشانه عدم مجاز بودن نتیجه مجوزدهی هستند.

نوع: این فیلد، نوع مجوزدهی و سیاست انتشار را مشخص می‌کند. L و R به‌ترتیب نشان‌دهنده محلی یا بازگشتی بودن مجوزدهی، و D نشان‌دهنده مجوزدهی در سطح شما است. عدم ذکر D، نشاندهنده مجوزدهی در سطح سند است. این مدل، از سیاست «هر کدام خاص‌تر باشد مقدم است» استفاده می‌کند. برای انعطاف‌پذیری مدل در موارد ناسازگاری، از دو مفهوم نرم(S) و سخت(H) استفاده می‌شود و در صورت ناسازگاری دو قانون، مجوز سخت می‌تواند مجوز نرم را باطل کند. مثلاً LDH به معنی محلی بودن، در سطح شِما بودن، و سخت بودن مجوز است.

۴-۳-۲- اجرای کنترل دسترسی

وقتی درخواست دسترسی به یک شئ صادر می‌شود، باید مشخص شود که آیا مجوز دسترسی به شئ یا بخش‌هایی از شئ مورد نظر وجود دارد یا نه. با بررسی مجاز بودن، سیستم یک view از سند مربوط به درخواست ایجاد می‌کند و به کاربر ارائه می‌دهد. این view، به‌ترتیب بعد یک فرایند برچسب‌زنی درخت، و یک فرایند تبدیل به‌دست می‌آید.

با داشتن درخواست و URI سند XML مربوط به درخواست، فرایند برچسب‌زنی درخت، درخت متناظر با URI را تشکیل می‌دهد. سپس برای هر گره درخت، مجاز یا نامجاز بودن نهاد درخواست‌دهنده در دسترسی به آن گره را با توجه به نوع مجوزهایی که برایش وجود دارد، مشخص می‌کنیم. الگوریتم دارای چهار گام زیر است:

گام ۱، بازیابی مجوزها: مجموعه مجوزهای A که مربوط به URI سند و نهاد درخواست‌دهنده می‌شوند را بازیابی می‌کنیم.
گام ۲، برچسب‌زنی اولیه: برای هر مجوز، مجموعه گره‌های N را به‌دست می‌آوریم. برای هر $n \in N$ ، با توجه به مثبت یا منفی بودن sign، subject را به لیست مجوز دسترسی یا لیست عدم دسترسی اضافه می‌کنیم. در مواردی که ممکن است علامت‌های متفاوتی برای هر نوع مجوزدهی به‌وجود آید، از یک سیاست رفع ناسازگاری استفاده می‌کنیم تا در نهایت برای هر نوع، فقط یک علامت داشته باشیم.
گام ۳، انتشار برچسب: برچسب هر گره بر اساس دو قاعده زیر به صفت‌ها و زیرعناصر انتشار می‌یابند: ۱- مجوزهای یک گره، بر مجوزهای اجداد خود مقدم‌ترند، و۲- مجوزهای سطح سند، بر مجوزهای سطح شِما مقدم‌ترند، مگر اینکه مجوزهای سطح نمونه نرم، یا مجوزهای سطح شِمای سخت تعریف شده باشند. گره‌هایی که بدون علامت هستند، علامت منفی می‌گیرند (به‌دلیل سیاست بسته).
گام ۴، محاسبه view: وقتی زیردرخت مربوط به درخواست، به‌طور کامل علامت‌گذاری شد، view با هرس کردن تمام زیردرخت‌هایی از درخت اولیه که دارای گره‌هایی با علامت منفی هستند، به‌دست می‌آید.

۴-۴- مدل کنترل دسترسی کودو و سایرین

بیشتر مدل‌های کنترل دسترسی، وقتی درخواست دسترسی صادر می‌شود، در همان زمان، عمل ارزیابی سیاست انجام می‌شود. این عمل در برخی موارد ممکن است زمان‌بر باشد. برای حل این مشکل، کودو و سایرین [۱۲] مدل تحلیل ایستایی را ارائه کرده‌اند که می‌توان تحلیل پویا را در صورت نیاز به‌عنوان یک متمم در کنار این تحلیل استفاده کرد. یعنی، برای پاسخ به یک پرس‌وجو، ابتدا از تحلیل ایستا برای ارزیابی مجوزهای درخواست‌شده در آن استفاده می‌کنیم. اگر با استفاده از تحلیل ایستا نتوانستیم تصمیم‌گیری کنیم، از تحلیل پویا (دیگر مدل‌ها) استفاده می‌کنیم. خط‌مشی این مدل برگرفته از مدل کنترل دسترسی مبتنی بر تابع می‌باشد.

۴-۴-۱- خط‌مشی کنترل دسترسی

مجوزدهی با استفاده از سه‌تایی <Subject, Permission Action, Object> مشخص می‌شود. نهاد یک پیشوند دارد که به نوع آن اشاره می‌کند، همچون شناسه شخص (uid)، نقش (role) و گروه (group). علامت "+" برای قاعده اعطاء و علامت "-" برای قاعده لغو به‌کار می‌رود. از Xpath برای مشخص کردن اشیاء در مجوزها استفاده می‌شود؛ با این محدودیت که از توابع پشتیبانی نمی‌شود. در این مدل فقط از عمل خواندن پشتیبانی می‌شود. از مجوزهای منفی و مثبت نیز برای مدیریت استثناها استفاده می‌شود. این مدل، تمایزی بین مجوزهای سطح شِما و مجوزهای سطح سند قایل نمی‌شود.
این مدل، از مجوزهای محلی و بازگشتی نیز پشتیبانی می‌کند. برای حل مشکل برخورد نیز می‌توان از سیاست‌های «منفی‌ها مقدم‌اند یا مثبت‌ها مقدم‌اند» استفاده کرد. به‌دلایل امنیتی، ارائه‌دهندگان مدل، سیاست اول را برای مدلشان انتخاب می‌کنند. وقتی مجوزی وجود نداشته باشد، از سیاست بسته استفاده می‌شود.

۴-۴-۲- اوتوماتای حالت متناهی غیرقطعی(NFA)

اساس این مدل، مبتنی بر اوتوماتا است.
تعریف: یک اوتوماتای حالت متناهی غیرقطعی M با پنج‌تایی $(\Omega, Q, Qinit, Qfin, \delta)$ نشان داده می‌شود که در آن،
Ω، الفبای زبان است.
Q، یک مجموعه متناهی از حالت‌های M است.
$Qinit \subseteq Q$، مجموعه حالت‌های اولیه M است.
$Qfin \subseteq Q$، مجموعه حالت‌های نهایی M است.
$\delta : Q \times \Omega \rightarrow Q$، تابع گذار حالت M است.
L(M)یا زبان M، مجموعه رشته‌هایی است که M می‌پذیرد.
با داشتن یک عبارت XPathمثل r که دارای شرط نیست، می‌توان NFA معادلش را ساخت. این NFA، یک مسیر را پذیرش می‌کند، اگر و تنها اگر آن مسیر با r منطبق باشد. اگر r دارای شرط باشد، دو NFA (خوش‌بینانه و بدبینانه)[1] برای آن ایجاد می‌کنیم، که به‌ترتیب در اولی فرض می‌شود که تمام شرط‌ها برآورده می‌شوند و در دومی فرض می‌شود که تمام شرط‌ها برآورده نمی‌شوند.

۴-۴-۳- الگوریتم این مدل بدین صورت است:

گام ۱، ایجاد اوتوماتای شِما: برای شِمایی که سند بر اساس آن ساخته شده، یک اتوماتای شِمای MG ایجاد می‌شود. این NFA، فقط مسیرهایی را می‌پذیرد که بر اساس شِما مُجاز هستند.
گام ۲، ایجاد اوتوماتای کنترل دسترسی از روی سیاست‌های کنترل دسترسی: برای هر نقش در سیستم، اوتوماتای کنترل دسترسی M به‌صورت زیر به‌دست می‌آید:

$$L(M) = (L(M[r1]) \cup \ldots \cup L(M[rm])) \setminus (L(M[r1']) \cup \ldots \cup L(M[rm']))$$

r_i ها عباراتی هستند که در قوانینی آمده‌اند که به نقش مذکور، مجوز دسترسی می‌دهند (مجوزی با علامت +). r_i' ها عباراتی هستند که در قوانینی آمده‌اند که به نقش مذکور، مجوز دسترسی نمی‌دهند (مجوزی با علامت -).\ نیز نشان‌دهنده تفریق دو مجوعه است. در

1- Overestimate & Underestimate

اینجا فرض بر این است که در هر دو دسته عبارات، از هیچ شرطی استفاده نشده است. همان‌طور که در قسمت قبل ذکر شد، اگر در عبارات مذکور از شرط استفاده شده باشد، باید دو اتوماتا ایجاد شود.

گام ۳، ایجاد عبارات منظم پرس‌وجو (Er): در یک پرس‌وجو به زبان XQuery، عبارات Xpath ای که در پرس‌وجو آمده‌اند باید به عبارات منظم معادل‌شان تبدیل شوند. اگر در عبارتی از متغیر استفاده شده باشد، آن را با عبارت معادلش جایگزین می‌کنیم. برای عبارات مسیر ذکر شده در RETURN، زیردرخت‌های عناصر ذکر شده نیز برگردانده می‌شوند.

گام ۴، مقایسه اوتوماتای کنترل دسترسی با عبارات منظم پرس‌وجو: با داشتن عبارت rXPath سه حالت زیر را داریم:

۱. **همیشه مجاز:** اگر هر مسیری را که عبارت منظم پرس‌وجوی Er و اوتوماتای شِمای M_G پذیرش می‌کنند، اوتوماتای کنترل دسترسی (بدبینانه) نیز پذیرش کند.

۲. **همیشه غیرمجاز:** اگر هیچ مسیری توسط عبارت منظم پرس‌وجوی Er، و اوتوماتای شِمای M_G، و اوتوماتای کنترل دسترسی (خوش‌بینانه) پذیرش نشود.

۳. **نتیجه به‌طور ایستا نامشخص است، اگر هیچ‌یک از حالات فوق رخ ندهد.**

مزیت عمده تحلیل ایستا این است که می‌توان پرس‌وجوها را بر اساس عبارات مسیر استفاده‌شده در آنها بازنویسی کرد. اگر پرس‌وجو حاوی مسیری باشد که بر اساس گام (۴) به‌عنوان همیشه غیرمجاز تشخیص داده شده است، می‌توان آن را بدون ارزیابی از پرس‌وجو حذف کرد. همچنین اگر مسیری در پرس‌وجو وجود داشته باشد که بر اساس گام ۴ به‌عنوان همیشه‌مجاز تشخیص داده شده است، می‌توان آن را بدون ارزیابیبه درخواست دهنده برگرداند. آن دسته از عبارات مسیر که به‌طور ایستا نمی توان برایشان تصمیم‌گیری کرد را می‌توان به‌طور پویا در زمان اجرا ارزیابی کرد.

۴-۵- دیگر مدل‌های کنترل دسترسی XML

مدل لیست کنترل دسترسی[1] [۴] و مدل قابلیت[2] [۵]، دو مدل قدیمی برای کنترل دسترسی در زمان اجرا هستند. در مدل لیست کنترل، دسترسی مجوزها برای اشیاء تعیین می‌گردند. در مقابل، در مدل قابلیت، مجوزها برای موضوعاتی (کاربرانی) که قصد دسترسی به اشیاء را دارند تعیین می‌گردند.این دو مدل را می‌توان به‌سادگی جهت بانک‌های XML استفاده کرد. به این منظور کافیست که هر سند و یا هر المان یا زیرالمان یک سند را یک شئ درنظر گرفته و بدین ترتیب خط‌مشی مربوطه را ایجاد و کنترل دسترسی را اِعمال کرد.

در [۳]مدل XACS(Xml Access Control System)آمده است که در آن، هنگامی که کاربران در حال جستجوی سندهای Xml هستند، برای اجازه دسترسی آنها به سندهای Xml خاص، داده‌ها تنها با توجه به سطح هویتشان تهیه می‌شود. به‌منظور انجام این‌کار، XACS بخش‌های خاصی از اسناد که غیرقابل دسترس هستند را حذف می‌کند و قطعات در دسترس را بسته به میزان اختیار اتکاربران انتقال می‌دهد.

در [۱۳،۷] مدل کنترل دسترسی مبتنی بر نقش[3] آورده شده است. مدل مبتنی بر نقش برای شبیه‌سازی دیگر مدل‌ها استفاده شده است. این مدل همچنین الگوهای اختیاری بیشتری را برای دسترسی به داده‌ها در اختیار مدیر سیستم قرار می‌دهد [۱۵،۱۴]. مدل کنترل دسترسی مبتنی بر نقش، اولین بار توسط آقای رابیتی و همکارانش جهت استفاده در بانک‌های اطلاعات شئ‌گرا مطرح گردید [۱۶]. این مدل به‌راحتی قابل انطباق با مستندات XML و همچنین بانک اطلاعات XML می‌باشد.

در [۶] مفهوم Observation-based Fine Grained (OFGAC) Access Controlآمده است که در آن، دسترسی داده‌ها در سطوح مختلفی از انتزاع، با توجه به سطح حساسیت‌شان می‌باشد. بنابراین، کاربران غیرمجاز قادر نیستند به محتوای واقعی یک صفت یا عنصر حاوی اطلاعات جزئی پی ببرند. در حالی که با توجه به حقوق دسترسی خود، مجاز به گرفتن یک view از آن می‌باشند که توسط یک ویژگی خاص ارائه شده است.

ایده ایجاد کنترل دسترسی رسا و با معنی در [۹ ، ۱۷] پیشنهاد شده است. این روش‌ها برای جستجوی گره‌های دسترسی کنترل‌شده یا رفع چک کردن دسترس‌پذیری غیر ضروری در زمان اجرا مؤثر هستند. این تحقیقات تلاش می‌کنند تا کارائی کنترل دسترسی رسا را بهبود بخشند. امّا از آنجا که معمولاً روی بهینه‌سازی مبتنی بر مستندات تمرکز دارند [۱۸]، بانک‌های اطلاعات XML با تکرار به‌روزرسانی مستندات یا قواعد کنترل دسترسی ممکن است متحمل هزینه‌های غیر قابل قبول شوند. مدل کنترل دسترسی مبتنی بر تابع، یک مدل رسا و با معنی می‌باشد. این مدل قابل کاربرد در مدل‌های کنترل دسترسی موجود برای مستندات XML می‌باشد. نوآوری این مدل، کنترل دسترسی در مقیاس‌پذیری و کارائی بالا می‌باشد. ایده کلیدی در این مدل، کد کردن قواعد کنترل دسترسی و همچنین یک مجموعه از توابع دستور که جداگانه ارزیابی دسترسی واقعی را اجرا می‌کنند، می‌باشد. علاوه براین، توابع دستور برای نگهداری در حافظه و تسهیل در به‌روزرسانی گروه‌بندی شده‌اند. مدل‌های کنترل دسترسی محتاطانه، لیست کنترل دسترسی و کنترل دسترسی مبتنی بر نقش، کنترل دسترسی رسا و با معنی را برروی مستندات XML فراهم می‌نمایند. این رویکردها معمولاً اعطا و لغو مشخصه‌های

1- Access Control List (ACL)
2- Capability
3- Role-Based Access Control: RBAC

کنترل دسترسی، مکانیزم انتشار که به‌وسیله آن عنصرهای تولیدشده احکام را از پدرشان به ارث می‌برند، و روش‌های حل برخورد داده‌ها به علت همپوشانی را توسط کنترل دسترسی چندگانه پشتیبانی می‌کنند [۱۹، ۲۰]. از آنجا که این مدل‌ها کنترل دسترسی را به‌وسیله پیمایش مستندات XML در زمان اجرا انجام می‌دهند، اجرای این مدل‌ها هزینه‌های محاسبات سنگینی را تحمیل می‌کنند، به‌خصوص برای مستندات XML دارای لایه‌های بسیار زیاد با قواعد حجیم کنترل دسترسی با معنی.

مدل‌های کنترل دسترسی مبتنی بر ایده view امنیتی[۲۲]: view امنیتی از یک سند XML، یک view از سند XML به‌همراه اطلاعاتی که یک گروه کاربری مجاز است بخواند و همچنین یک view ازDTD را به آن گروه ارائه می‌دهد. viewDTD برای این است که view سند، بر اساس آن مجاز بشود. هر سند فقط یک view امنیتی دارد. کاربران مجاز، روی view پرس‌وجو اجرا می‌کنند.

مدل کنترل دسترسی مبتنی بر نگاشت بیتی، کنترل دسترسی را در سطوح مختلف بانک اطلاعات XML برقرار می‌کند [۲۱]. این مدل که توسط آقای یون و همکارانش مطرح گردید از یک رویکرد نگاشت بیتی سه بُعدی برای کنترل دسترسی به اطلاعات مستندات XML استفاده می‌کند.

۵- مقایسه مدل‌های کنترل دسترسی

در این قسمت، مزایا و معایب مدل‌های کنترل دسترسی ذکر شده که به صورت خلاصه آورده شده است.

جدول ۱- مقایسه مدل‌های کنترل دسترسی XML

مدل کنترل دسترسی	مزایا	معایب
مدل کنترل دسترسی دامیانی و سایرین	• سرعت بالا در بررسی مجوزها • قابلیت توسعه • دارا بودن معماری باز جهت توسعه	• عدم استفاده تحلیل ایستا برای ارزیابی مجوزهای درخواست‌شده • فقط از عمل خواندن پشتیبانی می‌شود.
مدل کنترل دسترسی کودو و سایرین	• می‌توان پرس‌وجوها را بر اساس عبارات مسیر استفاده شده در آنها بازنویسی کرد. • قابلیت توسعه	• عدم پشتیبانی از ساختارهای سلسله‌مراتبی • فقط از عمل خواندن پشتیبانی می‌شود. • در مواردی که سیاست‌های کنترل دسترسی به‌طور پویا تغییر می‌کنند، کمک زیادی در کاهش زمان اجرا نمی‌کند. • در استفاده از Xpath برای مشخص کردن اشیاء در مجوزها از توابع پشتیبانی نمی‌شود. • پرس‌وجوهای بازگشتی را نمی‌توان اداره کرد زیرا عبارت منظم معادلشان تعریف نمی‌شود.
مدل لیست کنترل دسترسی	• سادگی مدل • بررسی سریع مجوزها برای یک سند و یا یک المان یا زیرالمان	• برای به‌دست آوردن همه مجوزهای یک کاربر، باید تمامیلیست‌های کنترل دسترسی بررسی شود • کارایی پس‌گرفتن مجوزها بر اساس حذف کاربر یا شئ ضعیف می‌باشد. • بزرگ شدن لیست در بانک‌های اطلاعات حجیم • عدم پشتیبانی از مسیرهای شامل // ، * و گزاره‌ها • در عمل از کارایی پایینی برخوردار می‌باشد • در بانک‌های XML نامتمرکز به‌راحتی قابل استفاده نمی‌باشد.
مدل مبتنی بر نقش	• سادگی و قابل فهم بودن مدل • اعمال محدودیت برای کاربران و نقش‌ها • امکان استفاده از نقش‌های پارامتریک • بررسی سریع مجوزهای یک کاربر	• پیچیدگی گراف نقش برای بانک‌های اطلاعات با داده‌های زیاد • نیاز به حافظه زیاد جهت محاسبات • امکان ایجاد پیچیدگی در مدل توسط محدودیت‌ها • داشتن مشکل با مسیرهای شامل // ، * و گزاره‌ها • در بانک‌های XML نامتمرکز به راحتی قابل استفاده نمی‌باشد.
مدل مبتنی برتابع	• پیاده‌سازی آسان در نرم‌افزارهای کاربردی • سرعت بالا در بررسی مجوزها • قابلیت توسعه مدل • پشتیبانی از مسیرهای شامل // ، * و گزاره‌ها • دارا بودن معماری باز جهت توسعه • ایجاد کنترل دسترسی در پایین‌ترین سطح	• پیاده‌سازی سیاست‌ها در توابع • وابستگی به زبان برنامه‌نویسی • عدم قابلیت حمل • انعطاف‌پذیری پایین • استفاده مستقیم از حافظه اصلی • عدم استفاده در بانک‌های XML نامتمرکز
مد مبتنی بر نگاشت بیتی	• کارایی بالا در پس گرفتن مجوزها براساس حذف کاربر، سند، المان ویا زیرالمان • سرعت بالا در بررسی مجوزها • قابلیت توسعه • پشتیبانی از مسیرهای شامل // ، * و گزاره‌ها • ایجاد کنترل دسترسی در پایین‌ترین سطح • قابل استفاده در بانک‌های XML نامتمرکز	• حجیم شدن مکعب دسترسی در بانک‌های اطلاعات با داده‌های بسیار زیاد

۶- نتیجه

امنیت در بانک‌های اطلاعات و به‌تبع آن در بانک اطلاعات XML، براساس مدل‌های کنترل دسترسی ایجاد می‌گردد. در این مقاله به بررسی اجمالی امنیت و چند مدل کنترل دسترسی مهم در بانک اطلاعات XML پرداختیم. مدل‌های کنترل دسترسی سنتی محتاطانه و الزامی که پایه و مبنایی برای سایر مدل‌های کنترل دسترسی محسوب می‌شوند آورده شدند. مدل کنترل دسترسی دامیانی و سایرین که خیلی از مدل‌ها از این مدل نشأت گرفته‌اند و همچنین مدل کنترل دسترسی کودو و سایرین که مدل تحلیل ایستا می‌باشد آورده شد و در ادامه، چند مدل کنترل دسترسی دیگر معرفی شدند و ملاحظه شد هر یک از این مدل‌ها، جهت استفاده در بانک‌های اطلاعات XML دارای مزایا و معایبی هستند که به‌طور خلاصه در یک جدول، مقایسه‌ای اجمالی بین این روش‌ها آورده شد. بسیاری از مسایل در این زمینه وجود دارند که می‌توان به‌عنوان کارهای آتی بر روی آن به تحقیق پرداخت؛ از جمله، ارائه مدل‌های کنترل دسترسی XML کارا و سریع.

مراجع

۱. حق جو، مصطفی؛ صفائی، علی‌اصغر؛ «بانک اطلاعات علمی- کاربردی»، ج ۲، تهران، انتشارات دانشگاه علم و صنعت ایران، (۱۳۸۷).

2. Tim Bray, Jean Paoli, C. M. Sperberg-McQueen, Eve Maler. "Extensible Markup Language (XML) 1.0". World Wide Web Consortium (W3C). http://www.w3c.org/TR/REC-xml. Fourth Edition, 29 September (**2006**). (Visited on 2008-02-09).
3. S. M. Jo and K.Y. Chung, "Access Control Mechanism for XML Document", Proceedings of the International Conference on IT Convergence and Security 2011, Lecture Notes in Electrical Engineering, (**2012**), Vol. 120, Part 2, 81-90, DOI: 10.1007/978-94-007-2911-7_7.
4. R.S. Sandhu, E. J. Coyne, H.L. Feinstein, and C.E. Youman. "Role-Based Access Control Models". IEEE Computer, Volume 29, No 2, pp.38-47, February (**1996**).
5. L. Gong. "A Secure Identity-Based Capability System". Proc. IEEE Symposium on Security and Privacy, pp.56-65, (**1989**).
6. R. Halder and A. Cortesi, "Observation-Based Fine Grained Access Control for XML Documents", Computer Information Systems – Analysis and Technologies, Communications in Computer and Information Science, (**2011**), Vol. 245, Part 8, 267-276, DOI: 10.1007/978-3-642-27245-5_32.
7. J. Wang and S. L. Osborn, "A Role Based Approach to Access Control for XML Databases", SACMAT'04 of ACM, page 70-77, June (**2004**).
8. E. Bertino, S. Castano, E. Ferrari, M. Mesiti, "Specifying and Enforcing Access Control Policies for XML Document Sources", World Wide Web, pp. 139-151, Vol. 3, (**2000**).
9. E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, P. Samarati, "Controlling Access to XML Documents", In IEEE Internet Computing, pp. 18-28, Vol. 5, No. 6, (**2001**).
10. V. Parmar, S. Hongchi, S Chen, "XML Access Control for Semantically Related XML Documents", In Proceedings of the 36th Annual Hawaii International Conference, pp. 288–297, (**2003**).
11. E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, and P. Samarati "A Fine-Grained Access Control System for XML Documents". ACM TISSEC, pp.169-202, (**2002**).
12. M. Murata, A. Tozawa, M. Kudo, S. Hada, "XML access control using static analysis", ACM Transaction Information System Security 9(3), pp. 292–324, (2006).
13. R. Sandhu, E. Coyne, H. Feinstein, C. Youman. "Role-Based Access Control Models". IEEE Computer, 29:38–47, Feb. (**1996**).
14. R. Sandhu, V. Bhamidipati, Q. Munawer. "The ARBAC97 model for role-based administration of roles". ACM Transaction on Information and Systems Security, 2(1):105–135, Feb. (**1999**).
15. S. Osborn, R. Sandhu, Q. Munawer. "Configuring role-based access control to enforce mandatory and discretionary access control policies". ACM Trans. Information and System Security, 3(2):1–23, (**2000**).
16. F. Rabitti, E. Bertino, W. Kim, and D. Woelk. "A model of authorization for next-generation database systems". ACM Trans Database Syst, 16(1):88–131, (**1991**).
17. T. Yu, D. Srivastava, L.V.S. Lakshmanan, and H.V. Jagadish, "Compressed Accessibility Map: Efficient Access Control for XML". VLDB, pp.478-489, (**2002**).
18. S. Cho, S. Amer-Yahia, L.V.S. Lakshmanan, D. Srivastava, "Optimizing the secure evaluation of twig queries". VLDB, pp.490-501, (**2000**).
19. E. Bertino and E. Ferrari. "Secure and selective dissemination of XML documents". ACM TISSEC, 5(3):290–331, (**2002**).
20. A. Gabillon, E. Bruno, "Regulating Access to XML Documents". Working Conference on Database and Application Security, pp.219-314, (**2001**).
21. A. Gummadi, J. P. Yoon, B. Shah, V. Raghavan, "A bitmap-based access control for restricted views of XML documents", ACM Workshop on XML Security, pp. 60-68, October (**2003**).
22. W. Fan, C.Y. Chan, M. Garofalakis, "Secure XML querying with security views", In Proc. of the 2004 ACM SIGMOD International Conference on Management of Data, (**2004**).

Investigation of Access Control Models in XML

E. Sargolzaei[1]
M. Ghayoori[2]

Abstract

Nowadays, there is a large amount of information on the web and a significant portion of this amount of information has been appeared in the form of XML. One of the main advantages of using XML is to show the non-structured data which presents many capabilities for users. Being Non-Structured and the flexibility of XML make it a common method for use and a notable procedure in the security of databases. Therefore, security at XML documents is an important requirement. Data stored at any format must be protected from any possible attack. In order to prevent from such attacks, various methods and models have been designed and implemented. These models are based on different methods that are applied in various data bases. One of the most important models is the access control model. In this paper, the access control models for XML documents have been investigated and compared .

Key Words: *Non-Structured Data, Access control, XML Access Control Models, Security*

1- Malek Ashtar University of Technology, M.S in Information Security (ehsan.sargolzai@gmail.com) -Writer in Charge
2- Imam Hossein Comprehensive University, Assistant Professor and Academic Member