مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
سال سوم، شماره ۱، بهار ۱۳۹۴،ص ۶۷-۵۳

یک مدل کنترل دسترسی جدید مبتنی بر مذاکره اعتماد با استفاده از معماری XACML

علی کریمی[1*]، محمود صالح اصفهانی[2]، محمدرضا حسنی آهنگر[3]

۱-دانشجوی دکتری، دانشگاه جامع امام حسین(ع)

۲-استادیار، دانشگاه جامع امام حسین(ع)

۳- دانشیار، دانشگاه جامع امام حسین(ع)

(دریافت: ۹۳/۰۸/۱۰؛ پذیرش: ۹۴/۰۶/۱۰)

چکیده

ظهور فناوری‌های وب سرویس و سیر تکاملی سامانه‌های توزیع‌شده به سمت معماری‌های سرویس‌گرا، به ارتقای تعاملات هم‌یارانه و اشتراک‌گذاری اطلاعات کمک قابل‌توجهی کرده است. تبادل داده بین سکوهای ناهمگون و تأمین امنیت سرویس‌ها، از چالش‌های اساسی در این معماری محسوب می‌شود که نیازمند توجه ویژه است. سازوکارهای فعلی امنیت اطلاعات و مدل‌های کنترل دسترسی سنتی با توجه به تعدد خط‌مشی‌های امنیتی در معماری‌های سرویس‌گرا، به‌تنهایی پاسخ‌گوی نیازهای امنیتی کاربران نخواهد بود. این مدل‌ها، اغلب ایستا بوده و برای محیط‌های سرویس‌گرا با توجه به ماهیت اقتضایی و پویای آن‌ها، مناسب نیستند. در چنین محیط‌هایی، یک رویکرد امیدبخش برای ایجاد اعتماد و تعاملاتِ امن بین موجودیت‌ها که در آن هیچ دانش و تجربه قبلی نسبت به یکدیگر وجود ندارد، رویکرد مذاکره اعتماد است. در این مقاله، برای غلبه بر چالش‌های مذکور، یک مدل کنترل دسترسی جدید مبتنی بر اعتبارنامه و بر اساس سازوکارهای مذاکره اعتماد پیشنهاد شده است. این مدل، در بستر معماری XACML با تلفیق قابلیت‌های موتور XEngine توسعه یافته است. نتایج حاصل از ارزیابی مدل پیشنهادی؛ کارایی، انعطاف‌پذیری و توانایی آن را در تأمین امنیت سرویس‌ها، و نیز کاربردپذیری آن را در محیط‌های واقعی دولت و تجارت الکترونیکی اثبات می‌کند.

کلمات کلیدی: کنترل دسترسی، مذاکره اعتماد، معماری XACML، موتور ارزیابی XEngine، سیاست امنیتی، اعتبارنامه

۱- مقدمه

محیط‌های محاسباتی سرویس‌گرا، دارای خصوصیات ویژه‌ای هستند که ازجمله می‌توان به پویایی، باز بودن و توزیع‌شدگی آن‌ها اشاره نمود [۱]. در چنین محیط‌های هم‌یارانه فراسازمانی، موجودیت‌های مختلف (از قبیل وب سرویس‌ها) که اغلب توسط سازمان‌های مختلف تأمین و ارائه می‌شوند، برای ارائه خدمات گوناگون باهم همکاری می‌کنند شکل (۱). ازاین‌رو، عدم پشتیبانی از سازوکارهای امنیتی مشترک در این محیط‌ها کاملاً رایج است [۲]. در چنین شرایطی، سرویس‌های مشارکت‌کننده برای دست‌یابی به اهداف کسب‌وکار سازمان، ممکن است مجبور شوند با چندین سرویس دیگر همکاری نمایند که قبلاً هیچ تجربه و دانشی در مورد آن‌ها وجود ندارد [۳].

بااین‌حال، سامانه‌های سرویس‌گرای مبتنی بر اینترنت، در مقایسه با سامانه‌های توزیع‌شده متعارف، پویاتر و دارای اتصال سست‌تر هستند[1] که چالش‌های بیشتری را در برقراری اعتماد بین همتایان در پی دارند. از طرفی، با توجه به تعدد سیاست‌های امنیتی و رشد روزافزون انواع حملات در این محیط‌ها، مدل‌های کنترل دسترسی سنتی پاسخ‌گوی نیازهای امنیتی کاربران نخواهند بود [۵ -۴]. همچنین، اشتراک‌گذاری اطلاعات در این محیط‌ها، چالش‌های امنیتی شدیدتری را در پی‌دارد. از یک‌سو، سامانه‌های هم‌یارانه نیاز دارند دسترس‌پذیری اطلاعات را برای همه‌کسانی که به آن احتیاج دارند امکان‌پذیر سازند، و از طرفی، سازمان‌ها ناچارند از اطلاعات حساس و محرمانه خود حراست کرده و از دسترسی‌های غیرمجاز محافظت نمایند. بدیهی است ایجاد توازن میان دو هدف متناقض روش‌ها و سازوکارهای امنیتی امروزی، بسیار دشوار است [۶].

مدل‌های متعددی برای کنترل دسترسی با رویکرد مذاکره اعتماد، توسط محققان طراحی شده است، اما اکثر این مدل‌ها در تأمین ویژگی‌هایی از قبیل انعطاف‌پذیری، کارایی، محدودیت دسترسی به اعتبارنامه‌ها، تطبیق‌پذیری با محیط‌های عملیاتی واقعی (به‌عنوان مثال؛ پشتیبانی از زیرساخت‌های دولت الکترونیک) و غیره، به‌طور کامل موفق نبوده‌اند. بااین‌وجود، فقدان یک چارچوب و مدل کارآمد و توسعه‌یافته که بتواند کنترل دسترسی به منابع حساس در محیط‌های فراسازمانی را به‌صورت پایدار انجام دهد، احساس می‌شود.

*رایانامه نویسنده پاسخگو: a.karimi@ihu.ac.ir

1- loosely coupled

راهنما: موجودیت‌های سیار (مانند سرویس‌ها)

شکل (۱). همکاری فراسازمانی سرویس‌ها در یک محیط محاسباتی سرویس‌گرا [۳].

ازاین‌رو، مسئله و سؤال اصلی این است که در یک محیط غیر-متمرکز، باز و توزیع‌شده و در شرایط تعدد سیاست‌های امنیتی، چگونه می‌توان به یک درخواست‌کننده سرویس درحالی‌که درگذشته با آن هیچ تراکنشی وجود نداشته است اعتماد کرد و دسترسی او را به اطلاعات کنترل نمود؟ همچنین، مدل پیشنهادی باید دارای چه ویژگی‌ها و قابلیت‌هایی باشد تا بتواند بر مشکلات و نواقص مدل‌های موجود فائق آید؟

مذاکره اعتماد، یک سازوکار مناسبی برای احراز هویت و محیط کنترل دسترسی باز برای چنین محیط‌هایی فراهم می‌کند، اما بااین‌وجود، از حملات بدخواهانه‌ی منجر به ممانعت از سرویس یا نشت اطلاعاتِ حساس رنج می‌برد. ازاین‌رو، ترکیب سازوکارهای کنترل دسترسی و مذاکره اعتماد برای حفاظت از امنیت وب سرویس‌ها و منابع مشترک در حوزه‌های امنیتی مختلف، بسیار تعیین‌کننده و اساسی است [۷].

از آن‌جائی‌که مدل‌های موجود با رویکرد مذاکره اعتماد، از جامعیت و انعطاف‌پذیری لازم برخوردار نیستند، هدف این مقاله آن است که یک مدل جدید با رویکرد تلفیق روش‌های کنترل دسترسی و سازوکارهای مذاکره اعتماد برای تکمیل نواقص مدل‌های موجود ارائه دهد. در مدل پیشنهادی، مذاکره‌ی پویا برای برقراری اعتماد و مدیریت کنترل دسترسی، در یک چارچوب واحد و در بستر معماری استاندارد XACML فراهم شده است. در مذاکره اعتماد، سیاست‌های کنترل دسترسی یک نقش کلیدی برای حفاظت از منابع، در مقابل‌دسترسی‌های غیرمجاز ایفاء می‌کند [۸]. ازاین‌رو، در مدل پیشنهادی، مذاکره برای اعتماد مقدم بر ارزیابی کنترل دسترسی در نظر گرفته شده است. زیرا، مذاکره اجازه می‌دهد منابع لازم برای برقراری اعتماد جمع‌آوری‌شده و ارزیابی کنترل دسترسی با موفقیت انجام گیرد. در مدل پیشنهادی همچنین، از قابلیت موتور ارزیابی XEngine برای بهبود سرعت پردازش درخواست‌ها و کارایی مؤلفه تصمیم‌گیری دسترسی به‌خوبی استفاده شده است.

مقاله به‌صورت زیر سازمان‌دهی شده است: در بخش ۲، به برخی تحقیقات انجام‌شده در زمینه مدل‌های کنترل دسترسی با رویکرد مذاکره اعتماد می‌پردازیم. در بخش ۳، مفاهیم مبنایی مذاکره و کنترل دسترسی را شرح می‌دهیم. در بخش ۴، شرح مختصری از معماری استاندارد کنترل دسترسی XACML ارائه می‌دهیم. در بخش ۵، مدل پیشنهادی به‌تفصیل شرح داده می‌شود. در بخش ۶، پیاده‌سازی نمونه اولیه مدل تشریح می‌شود. در بخش ۷، به ارزیابی عملی مدل پیشنهادی می‌پردازیم و نهایتاً در بخش ۸، بحث و نتیجه‌گیری حاصل از این مقاله ارائه می‌گردد.

۲- پیشینه تحقیق

در محیط‌های محاسباتی سرویس‌گرا، اعتماد، حریم خصوصی و امنیتِ اشتراک‌گذاری منابع فراسازمانی به یک موضوع تحقیقاتی مهم تبدیل شده است [۳]. در حال حاضر، حفاظت از اعتبارنامه‌های حساس بر اساس سیاست‌های کنترل دسترسی و برقراری اعتماد از طریق مذاکره‌ی پویا میان همتایان، تلاش‌های تحقیقاتی زیادی را به خود جلب کرده است. در این بخش، تنها به توضیح تعداد کمی از رویکردهای مرتبط با این حوزه می‌پردازیم.

در [۷]، نویسندگان از چارچوب XACML برای ارائه مدل کنترل دسترسی مبتنی بر نقش استفاده کرده‌اند. آن‌ها از نمایه[1] کنترل دسترسی مبتنی بر نقش برای مدیریت کنترل دسترسی بهره برده‌اند. آن‌ها اعتقاد دارند، این نمایه‌ی توسعه‌یافته، به الزامات کنترل دسترسی پیشرفته پاسخ می‌دهد و بیان چندین مدل کنترل دسترسی در داخل چارچوب XACML را امکان‌پذیر می‌سازد. آن‌ها ، نقش‌های کاربران را که در چارچوب سازمانی قابل‌اتکا است، به صفات نگاشت می‌کنند که همین امر محدودیت‌های این مدل را در پاسخ‌گویی به نیازمندی‌های کنترل دسترسی در محیط‌های فرا- سازمانی مبتنی بر معماری سرویس‌گرا، آشکار می‌سازد.

در [۱۰ –۹]، وینزبروخ و همکاران[2] رویکرد مذاکره اعتماد خودکار[3] را پیشنهاد کرده‌اند، که هدف آن ایجاد رابطه اعتماد تدریجی بین غریبه‌ها از طریق آشکارسازی تدریجی اعتبارنامه‌ها و سیاست‌های امنیتی است. در مذاکره اعتماد خودکار، وضعیت برای ارائه‌دهندگان و درخواست‌کنندگان سرویس یکسان است، لذا هر دو طرف امتیازاتی برای محافظت از اطلاعات آشکارشده خود در طول برقراری اعتماد دارا هستند و یک مدل مذاکره واحد را مورد استفاده

1– profile
2-Winsborough et al.
3- automated trust negotiation (ATN)

قرار می‌دهند. از طرفی، این سازوکار می‌تواند کاربران را جهت آشکار کردن اطلاعات برای ایجاد رابطه اعتماد به‌دقت راهنمایی کند.

بوناتی و ساماراتی[۱] [۱۱]، چارچوبی مبتنی بر زبان سیاست[۲] و یک مدل تعاملی برای تنظیم دسترسی به سرویس‌های شبکه پیشنهاد داده‌اند. این چارچوب برای برقراری اعتماد، از قواعد منطقی برای دسترسی به سرویس‌ها و اجتناب از آشکارسازی اطلاعات حساس غیرضروری استفاده می‌کند. این چارچوب همچنین، محیط‌هایی را مورد هدف قرار می‌دهد که در آن هیچ حوزه امنیتی مرکزی[۳] وجود ندارد. چارچوب آن‌ها، شامل یک زبان سیاست برای مشخصات کنترل دسترسی و یک سازوکار فیلترینگ برای شناسایی سیاست‌های مربوط به مذاکره است. در مدل آن‌ها، یک قاعده دسترسی به سرویس از دو قسمت تشکیل شده است: یک قاعده پیش‌شرط[۴] و یک قاعده شرط لازم[۵]. قواعد پیش‌شرط، شرایطی هستند که یک درخواست‌کننده قبل از دسترسی به سرویس باید آن‌ها را برآورده سازد. قواعد شرط لازم، شرایط کافی برای دسترسی به سرویس را بیان می‌کند، به‌عنوان مثال؛ اگر درخواست‌کننده‌ای یک قاعده شرط لازم را برآورده سازد، مجاز به دسترسی به سرویس خواهد بود. این مدل، برای حفاظت از حریم خصوصی سرویس‌دهنده و مشتری، یک ترتیب خاص بین قواعد پیش‌شرط و شرط لازم اجرا می‌کند. سرویس‌دهنده، قاعده شرط لازم را تا زمانی که درخواست‌کننده یک قاعده پیش‌شرط متناظر را برآورده نکند، آشکار نخواهد کرد. قواعد پیش‌شرط، محدودیت‌ها و قیودی هستند که از دید افراد ناشناس پنهان شده‌اند.

RT [۱۲]، یک زبان مدیریت اعتماد مبتنی بر نقش[۶] و موتور زمان اجرا است که موجودیت‌ها را بر اساس خصوصیات موجود در اعتبارنامه‌های رقمی[۷] آن‌ها، به نقش‌ها نگاشت می‌کند. این سیستم قادر است اعتبارنامه‌هایی که به‌طور محلی قابل‌دسترس نیستند مکان‌یابی و بازیابی نماید. این سیستم همچنین، قادر است از نشت اطلاعات حساس اعتبارنامه‌ها بر اساس رفتار طرفین مذاکره، جلوگیری کند.

SD3 [۱۳]، یک سیستم مدیریت اعتماد است که شامل یک زبان سیاست سطح بالا، یک سازوکار بازیابی گواهینامه و یک کنترل‌کننده پیروی از سیاست‌های محلی[۸] است. موتور ارزیابی این سیستم، پاسخ یک پرس‌وجو را تعیین کرده و نیز پیروی پاسخ از سیاست‌های امنیتی را اثبات می‌کند.

در [۱۴]، ویژگی‌های چارچوب مذاکره اعتماد Trust Builder2 شرح داده شده است. این چارچوب با قابلیت انعطاف‌پذیری، برای پشتیبانی از تحقیقات در حوزه مذاکره اعتماد طراحی شده است و به محققین امکان می‌دهد، نمونه‌سازی و آزمایش رویکردهای مختلف فرایند مذاکره اعتماد را به‌طور سریع انجام دهند. در Trust Builder2، مؤلفه‌های اصلی یک سیستم مذاکره اعتماد با استفاده از رابط‌های انتزاعی[۹] از قبیل Strategy modules، Policy compliance checkers، Query interfaces، Credential chain modules و Audit modules ارائه شده‌اند. این سیستم، حساسیتی نسبت به قالب اعتبارنامه‌ها و سیاست‌های مورداستفاده در حین مذاکره ندارد. پشتیبانی از زبان سیاست جدید و انواع اعتبارنامه‌های جدید و فراهم کردن سازوکارهایی برای بارگذاری این‌نوع اعتبارنامه‌ها توسط مخازن خارجی[۱۰]، از قابلیت‌های آن محسوب می‌شود.

در [۱۵]، سیستم مذاکره اعتماد Trust-*X* شرح داده شده است. این سیستم یک چارچوب فراگیر مبتنی بر XML است که از مذاکره اعتماد در محیط‌های نظیر- به- نظیر پشتیبانی می‌کند. اولین مؤلفه در Trust-*X*، زبان *X*-TNL است که مبتنی بر XML بوده و گواهینامه‌ها و سیاست‌ها را تعیین می‌نماید. اعتقاد بر این است که دسترس‌پذیری یک زبان استاندارد، برای توصیف اطلاعات امنیتی جهت فراهم کردن یک محیط فراگیر برای مذاکره جنبه اساسی دارد. این سیستم، از هیچ قالب اعتبارنامه‌ای به غیر از گواهی‌های *X*-TNL و هیچ سیاست تعریف‌شده‌ای به غیراز زبان *X*-TNL پشتیبانی نمی‌کند. از ویژگی‌های نوآورانه خاص این چارچوب، پشتیبانی از قابلیت *trust tickets* است. بلیت‌های اعتماد درواقع، اعلام وصول‌هایی هستند که گواهی می‌دهند یک کاربر اخیراً مذاکراتی را با طرف مقابل با موفقیت به پایان رسانده است. این بلیت‌ها همچنین، می‌توانند در زمان‌های محدودی ارائه شوند (نوعاً ۲۴ تا ۴۸ ساعت) تا از بخش‌های افزونه مذاکرات بعدی با همان طرف مذاکره صرف‌نظر شود.

یکی از ویژگی‌های بارز مدل پیشنهادی نسبت به سایر

1– Bonatti and Samarati
2– Policy language
3– central security domain
4– prerequisite rule
5- requisite rule
6- role-based trust management language
7- digital credentials
8- local policy compliance checker
9– abstract interfaces
10– external repositories

مدل‌های مشابه این است که این مدل با دید کاملاً کاربردی طراحی و ارائه شده است. برای این‌منظور، ساختار سیاست‌های کنترل دسترسی و نیز ساختار سیاست‌های مذاکره و استعلام از مراکز مورد اعتماد را به‌گونه‌ای طراحی کردیم که قادر باشد شرایط و نیازمندی‌های امنیتی یک سازمان واقعی را برای کنترل دسترسی پوشش دهد. از سوی دیگر، الگوریتم‌های مذاکره و استعلام در مولفه PIP، به‌گونه‌ای طراحی شده‌اند که بر اساس سیاست‌های استعلام اعتبارنامه‌ها، امکان استعلام از چندین مرکز به‌طور همزمان فراهم گردد. این روش از یک سو، اجازه می‌دهد درصورت پاسخ‌گو نبودن برخی از مراکز، امکان استعلام از سایر مراکز فعال و برخط ادامه یابد و عملکرد مدل دچار وقفه و اختلال نگردد و از سوی دیگر، برای نیازهای کنترل دسترسی محیط‌های باز و پویای سرویس‌گرا مناسب باشد. این ویژگی‌ها در بسیاری از مدل‌های ارائه‌شده از جمله، مدل‌های [۷ و ۱۴] فراهم نشده است.

۳- مفاهیم مبنایی مذاکره و کنترل دسترسی

هر ارائه‌دهنده سرویس، معمولاً یک سیاست کنترل دسترسی دارد که تعریف می‌کند چه کسی به کدام منبع و برای چه هدفی دسترسی دارد. عموماً یک وب سرویس به‌عنوان یک منبع، به یک ارائه‌دهنده سرویس تعلق دارد. علاوه بر این، این منبع ممکن است سایر سرویس‌ها یا داده‌های حفاظت‌شده محلی را فراخوانی و مورد دسترسی قرار دهد. این امر، لزوم تعیین و مشخص نمودن تمامی منابع مرتبط با درخواست دسترسی و تعریف سیاست‌های کنترل دسترسی متناظر آن‌ها را روشن می‌کند. این سیاست‌ها مجموعه‌ای از شرایط لازم برای درخواست‌کنندگان منابع را تعریف می‌کند، به‌گونه‌ای که ارائه‌دهنده سرویس می‌تواند در مورد اجازه یا عدم اجازه دسترسی به منبع درخواست شده، تصمیم بگیرد. این شرایط، درواقع صفاتی هستند که از اعتبارنامه‌ها به‌دست می‌آیند. اعتبارنامه، بیانیه‌ای است در مورد مالک خود، که توسط یک صادرکننده اعتبارنامه[1] به‌صورت رقمی امضاء و تائید شده است. یک اعتبارنامه، شامل توصیفی از صفات به‌صورت زوج (نام/ مقدار) است. یک صفت، به‌صورت سن، عضویت، شغل، شماره کارت اعتباری یا هر چیز دیگری که توسط یک فرد تملک می‌شود، تعریف می‌گردد و معمولاً به‌طور مستقیم به هویت او مربوط نمی‌شود. این صفات برای اقناع سیاست‌های کنترل دسترسی یک منبع، مورد استفاده قرار می‌گیرند. آن‌ها همچنین، در سامانه‌های برقراری اعتماد[2] [۱۳]، که موجودیت‌ها قصد دارند بر اساس صفات به یکدیگر اعتماد کنند، از اهمیت خاصی برخوردارند.

از طرفی، سیاست‌های کنترل دسترسی به‌عنوان منابعِ متعلق به ارائه‌دهنده سرویس در نظر گرفته می‌شوند. با این حال، برخی سیاست‌ها ممکن است به‌صورت عمومی قابل‌دسترس نباشند. در چنین شرایطی، لازم نیست صفات موردنیاز برای اقناع آن سیاست‌ها، از قبل توسط درخواست‌کننده منبع شناخته‌شده باشند. این امر، سبب می‌شود اطلاعات موردنیاز هنگام دسترسی به منبع، در اختیار درخواست‌کننده قرار نگیرد.

مذاکره، فرایندی است که گروهی از کاربران روی برخی موضوعات به توافق متقابل می‌رسند. اساساً در فرایند مذاکره سه مؤلفه زیر وجود دارد [۱۴]:

۱- پروتکل‌های مذاکره، مجموعه‌ای از قوانین اداره‌کننده تعاملات هستند.

۲- اهداف مذاکره، طیفی از مسائل که روی آن‌ها باید توافق حاصل شود.

۳- مدل‌های تصمیم‌گیری، وسیله اتخاذ تصمیم هستند که کاربران با استفاده از پروتکل‌های مذاکره برای دست‌یابی به اهداف خود به کار می‌گیرند.

بر اساس آنچه بیان شد، هدف اصلی مذاکره، دسترسی به یک منبع (وب سرویس) است که به‌عنوان یک منبع حفاظت‌شده در نظر گرفته می‌شود. این دسترسی ممکن است شامل مذاکره با سایر موضوعات، مانند دسترسی به برخی اعتبارنامه‌ها یا سیاست‌های حفاظت‌شده نیز باشد. به این معنی که ممکن است سیاست‌ها حساس باشند و هر مشارکت‌کننده‌ای علاقه‌مند نباشد طرف مقابل از نیازمندی‌های کنترل دسترسی او مطلع باشد. می‌پذیریم که برخی سیاست‌های کنترل دسترسی به‌عنوان منابع، موضوعِ مذاکره دسترسی هستند. با این روش، سایر طرفین مذاکره متوجه می‌شوند که الزامات به دست آوردن منبع موردنظر چیست. درخواست‌کننده و ارائه‌دهنده سرویس، هرکدام پروتکل‌های مذاکره خود را پیاده‌سازی می‌کند که چگونگی تبادل اطلاعات برای اقناع سیاست‌های دسترسی متقابل را تعریف می‌کند. مدل تصمیم‌گیری، در سطح هر دو موجودیت، در مورد آنچه از طرف مذاکره‌کننده بر اساس پروتکل مذاکره آشکار و درخواست می‌شود، تصمیم می‌گیرد.

1- credential issuer

2- Trust Establishment (TE) systems

۴- معماری کنترل دسترسی XACML

اغلب برنامه‌های سازمانی، سازوکارهای کنترل و مجوز دسترسی را به روش اختصاصی خود پیاده‌سازی می‌کنند که منجر به تصمیماتِ مجوز دسترسی محدود [1]در داخل برنامه‌ها می‌گردد. در بسیاری از حالات، تصمیمات مجوز دسترسی به‌صورت ضمنی در سطح کل برنامه تعبیه می‌شود. مجوزهای دسترسی تعبیه شده در برنامه‌ها، به کاربران اجازه می‌دهد عمل خاصی را بدون مراجعه به یک سامانه کنترل دسترسی مرکزی انجام دهند. این رویکرد می‌تواند منجر به مشکلات کنترلی جدی ازجمله تضعیف اعتماد در برنامه‌ها و افشای بالقوه داده‌های خیلی حساس به کاربران نهایی شود. معماری XACML برای استانداردسازی دسترسی و اتخاذ تصمیمات مجوز دسترسی در برنامه‌های سازمان، توسعه داده شده است. این فناوری بر پایه زبان XML استوار است و ازاین‌رو فهم و پیاده‌سازی آن راحت و اتصال آن به ابزارها و فناوری‌های مختلف آسان است. در شکل ۲، جریان داده سطح بالای این معماری نشان داده شده است که شامل رابط‌ها و مؤلفه‌های مختلف برای اتخاذ تصمیمات مجوز دسترسی است. جدول (۱)، شرح مختصری از مؤلفه‌های شکل (۲) را ارائه می‌دهد. این معماری بر اساس زبان XML، هر دو زبان سیاست و زبان درخواست/ پاسخ [2] تصمیم‌گیری دسترسی را توصیف می‌کند. زبان سیاست، برای توصیف الزامات عمومی کنترل دسترسی به منابع در سیستم اطلاعاتی مورداستفاده قرار می‌گیرد. زبان درخواست/ پاسخ، امکان می‌دهد سؤالی برای پرسش این‌که آیا عمل موردنظر روی منبع موردنظر اجازه داده می‌شود یا خیر، شکل بگیرد و نهایتاً پاسخ ذی‌ربط برای جواب به این سؤال ارائه می‌گردد. پاسخ ارائه‌شده باید شامل یکی از این چهار گزینه باشد: اجازه دادن [3] (دسترسی مجاز است)، رد کردن [4] (دسترسی غیرمجاز است)، نامعین [5](خطایی اتفاق افتاده یا برخی مقادیر موردنیاز از دست رفته است، لذا تصمیم‌گیری نمی‌تواند اتخاذ شود) یا غیرقابل اجرا [6] (این سرویس هیچ سیاستی برای اِعمال به این درخواست ندارد). بر اساس استاندارد (OASIS) شکل (۲)، راه‌اندازی رایج چنین است که کسی یا فرایندی می‌خواهد چندین عمل معینی را روی یک منبع انجام دهد.

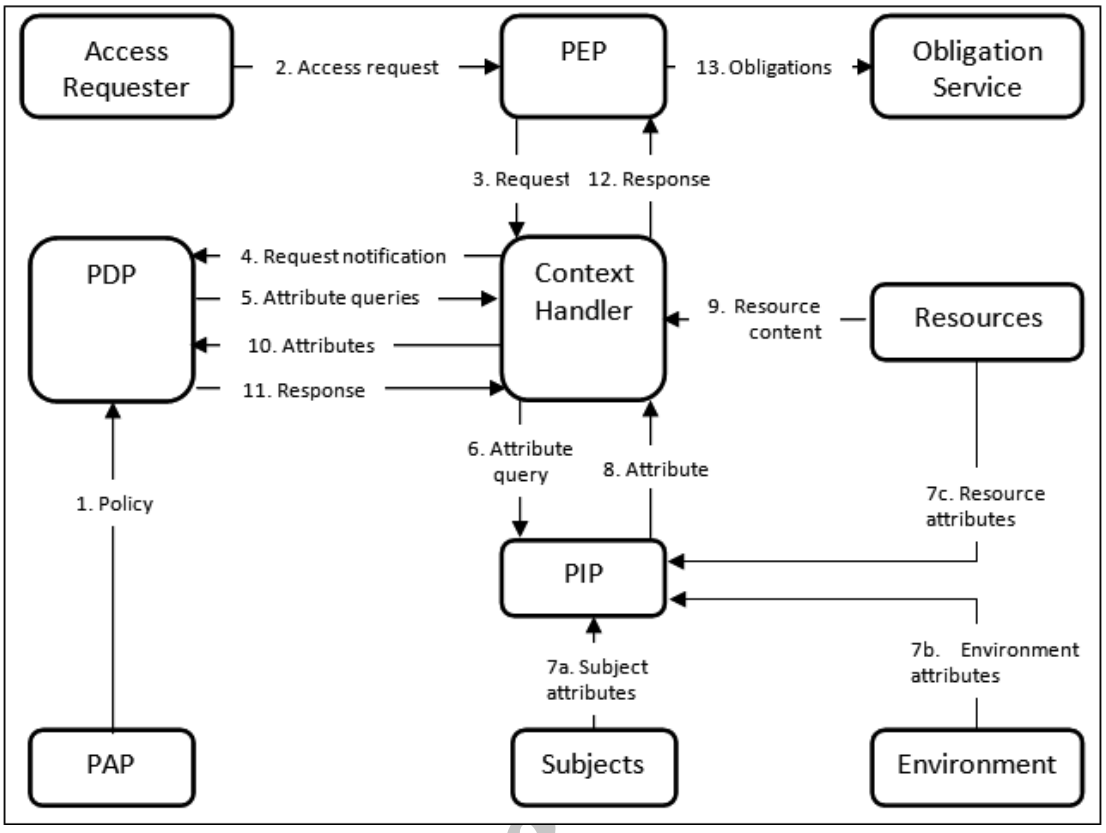
بنابراین، درخواست موردنظر به مؤلفه‌ای به نام نقطه اجرای سیاست (PEP) که عملاً از آن منبع حراست می‌کند ارسال می‌شود (مرحله ۲). مؤلفه‌ی PEP، درخواستی با قالب محلی خود، مبتنی بر

جدول (۱). خلاصه‌ای از شرح مؤلفه‌های جریان داده سطح بالای معماری XACML [۱۷]

ردیف	نام مؤلفه	شرح
۱	Policy	سیاست‌ها، دربرگیرنده قواعدی هستند که مبنایی برای رسیدن به تصمیم مجوز دسترسی را تشکیل می‌دهند. سیاست‌ها در یک سند XML با استفاده از برچسب‌های XACML نوشته می‌شوند.
۲	PAP	نقطه مدیریت سیاست (Policy Administration Point) به‌عنوان مخزن سیاست‌ها عمل می‌کند و آن‌ها را برای مؤلفه PDP قابل‌دسترس می‌نماید.
۳	PEP	نقطه اجرای سیاست (Policy Enforcement Point) به‌عنوان نقطه انتهایی برای درخواست/پاسخ مجوز دسترسی عمل می‌کند.
۴	PDP	نقطه تصمیم سیاست (Policy Decision Point) یک درخواست را برای اتخاذ تصمیم بر اساس سیاست‌های موجود، ارزیابی می‌کند.
۵	PIP	نقطه اطلاعات سیاست (Policy Information Point) به‌عنوان منبع مقادیر صفات عمل می‌کند.
۶	Context Handler (CH)	اداره‌کننده زمینه، به‌عنوان مترجم خدمت می‌کند، یک درخواست را از فرم استاندارد خود به فرم XACML و یک پاسخ XACML را به فرم نمایش استاندارد آن تبدیل می‌کند.
۷	Obligations	سرویس التزام (تعهد)، عملی است مشخص‌شده در سیاست که قبل از ارسال پاسخ به درخواست‌کننده، باید توسط مؤلفه PEP اجرا شود.

«صفات درخواست‌کننده»، «منبع درخواست‌شده»، «عمل مورد نظر» و سایر اطلاعات مربوط به درخواست، ایجاد می‌کند. این درخواست به اداره‌کننده زمینه (مرحله ۳) که یک زمینه درخواست برای مؤلفه PDP (مرحله ۴) می‌سازد، ارسال می‌شود. سیاست‌ها توسط مؤلفه PAP نوشته شده و برای PDP قابل دسترس می‌شوند (مرحله ۱). گاهی اوقات، مؤلفه PDP ممکن است به صفات بیشتری در حین ارزیابی درخواست نیازمند باشد. در این حالت، سؤالات مربوط به صفات به اداره‌کننده زمینه ارسال می‌شوند (مرحله ۵)؛ این مؤلفه صفات را از مؤلفه PIP درخواست می‌کند (مرحله ۶)، سپس مراحل (۷، ۸ و ۹) اجرا شده و اطلاعات لازم را به مؤلفه PDP ارسال می‌کند (مرحله ۱۰). درنهایت، مؤلفه‌ی PDP سیاست را ارزیابی و پاسخ را در مورد اعطاء یا عدم اعطاء دسترسی بر می‌گرداند (مرحله ۱۱). این پاسخ از طریق اداره‌کننده زمینه که آن را به قالب پاسخ محلی PEP تبدیل کرده است (مرحله ۱۲)، به مؤلفه PEP برمی‌گردد. سرانجام، مؤلفه PEP ممکن است قبل از

1– Limited authorization decision
2– Request/response
3– permit
4– deny
5– indeterminate
6– not applicable



شکل (۲). جریان سطح بالای معماری XACML [۱۷]

صدور مجوز یا عدم اجازه دسترسی به درخواست‌کننده، احتمالاً مجبور به انجام برخی تعهدات[1] (مرحله ۱۳) باشد.

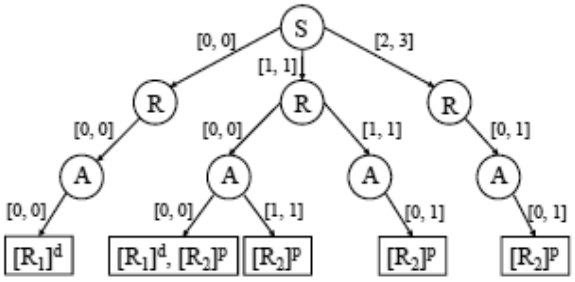
۵- مدل پیشنهادی

در این بخش، مدل پیشنهادی خود را با عنوان TNAC[2] به‌تفصیل شرح می‌دهیم. در این مدلِ توسعه‌یافته، برای تأمین نیازهای کنترل دسترسی و به‌منظور حفظ پویایی و انعطاف‌پذیری مدل، مؤلفه‌های PDP، PAP و PIP دست‌خوش تغییرات اساسی شده‌اند. ویژگی انعطاف‌پذیری، به توانایی یک رویکرد برای کار در شرایط مختلف اشاره می‌کند؛ اگر شرایط تغییر کند، یک روش انعطاف‌پذیر می‌تواند خود را با شرایط جدید وفق دهد. نوآوری ما در این مقاله برای کنترل دسترسی به منابع در محیط‌های سرویس‌گرا، به ساختار مؤلفه‌های یادشده، روش تعاملات و شیوه دست‌یابی به اعتبارنامه کاربران جهت برقراری اعتماد و نیز نحوه ارزیابی درخواست آنان مربوط می‌شود. این مؤلفه‌های توسعه‌یافته در شکل (۵)، با خط‌چین نشان داده شده‌اند.

عملکرد مؤلفه PDP در مدل پیشنهادی، برای ارزیابی یک درخواست بر اساس سیاست‌های موجود، با استفاده از موتور ارزیابی XEngine [۶] به میزان قابل‌توجهی ارتقاء یافته است. با توجه به رشد فزاینده برنامه‌های وب در اینترنت، سیاست‌های کنترل دسترسی نیز به لحاظ اندازه[3] و پیچیدگی[4] به سرعت رشد کرده و منجر به طولانی شدن زمان پردازش درخواست کاربران برای دسترسی به منابع می‌شود. موتور XEngine، یک موتور ارزیابی کارآمد برای سیاست‌های کنترل دسترسی است که زمان پردازش و ارزیابی درخواست‌ها را که یک مسئله حیاتی است به‌شدت کاهش می‌دهد. برای این منظور، موتور XEngine، عملکرد خود را بر روی سیاست‌های تعریف‌شده توسط مؤلفه PAP، اجرا می‌کند. درنهایت، به ازای هر درخواست از یک نهاد[5]، به یک درخت سه لایه مانند شکل (۳) می‌رسد. حال مطابق درخت تصمیم و بر اساس اطلاعات مربوط به نهاد درخواست‌کننده[6]، منبع درخواست‌شده[7] و عمل مورد- نظر[7]، قواعد[8] منتخب برای پاسخ به درخواستِ دسترسی،

1– obligations
2– Trust Negotiation-Based Access Control Model

3– size
4– complexity
5- subject
6- requesting subject
7- requested resource



شکل (۳). درخت تصمیم در موتور XEngine [۶]

عمل موردنظر[1]، قواعد[2] منتخب برای پاسخ به درخواستِ دسترسی، احصاء می‌گردند. بنابراین، در مرحله ۶ از مدل پیشنهادی، صفات مربوط به قواعد قابل‌اجرا[3] توسط XEngine، به‌عنوان (پرس وجوی صفات[4]) استخراج و به اداره‌کننده زمینه ارسال می‌شود و سپس برای دریافت پاسخ به مؤلفه PIP تحویل داده می‌شود (مرحله ۷).

همچنین، ساختار سیاست‌های کنترل دسترسی مورد استفاده در مؤلفه PAP در مقایسه با آنچه در XEngine نشان داده شده است، متفاوت است. این مؤلفه متناسب با توسعه قابلیت‌های مدل پیشنهادی، با ساختار کامل بیان شده است و سیاست‌های مبتنی بر صفات را در قسمت targetها و condition قواعد، برای مؤلفه PDP تعریف می‌کند. شکل (۴)، نمونه‌ای از ساختار یک Rule در سیاست کنترل دسترسی موجود در واحد PAP (مدل پیشنهادی) را نشان می‌دهد. خط ۱۶، شروع تعریف شرایط قاعده بر اساس صفات است. اصالت شناسه ملی (NationalCodeValidity) و عدم سوءپیشینه (Abuse_History)، جزء شرایط تطبیق قاعده با صفات درخواست‌کننده است.

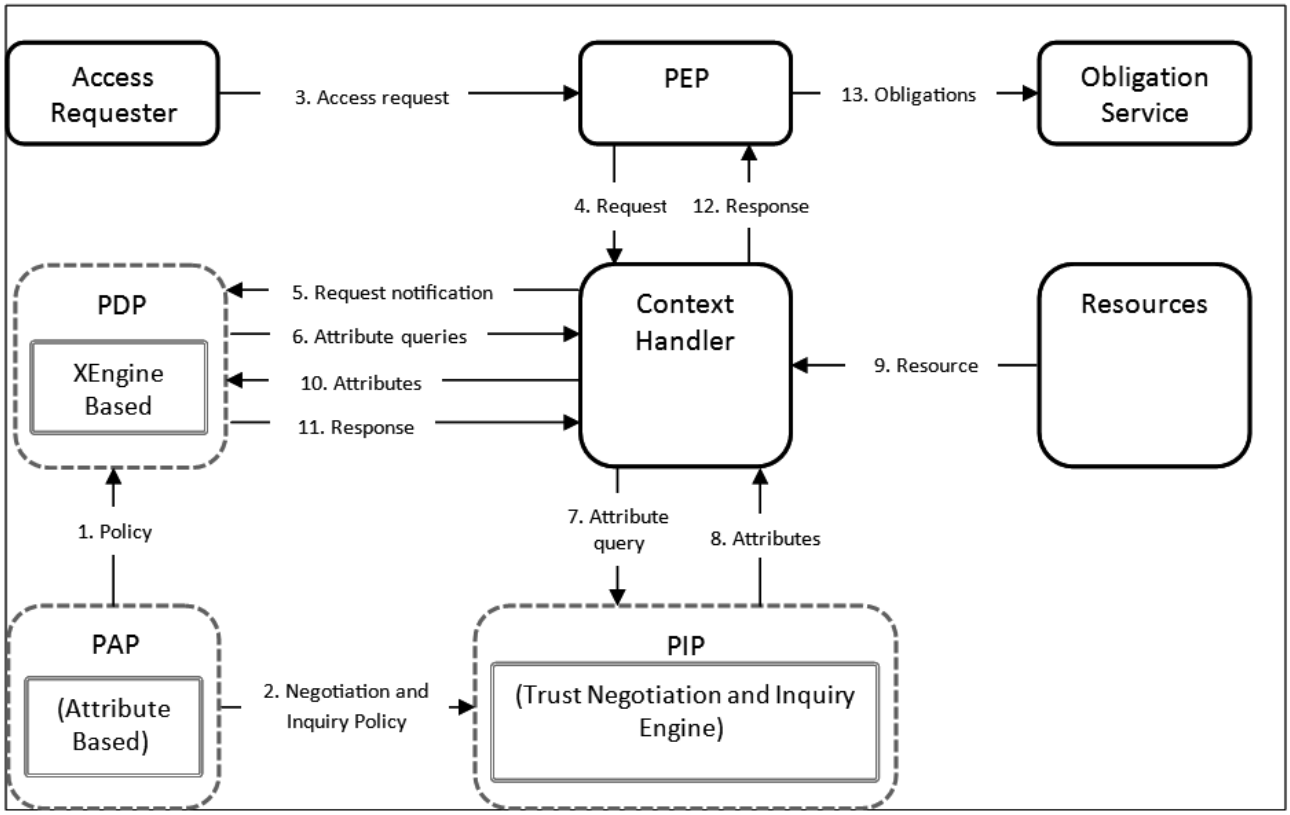
مؤلفه PAP، علاوه‌بر سیاست‌های کنترل دسترسی، تعریف (سیاست‌های مذاکره و استعلام)[5] را نیز بر عهده دارد. این قسمت، به‌نوبه خود شامل اطلاعات مربوط به «مراکز مورد اعتماد استعلام اعتبارنامه»[6] و «سیاست‌های استعلام صفات»[7] از مراکز یادشده است که تعریف ساختار، نحوه پیاده‌سازی و مدیریت آن‌ها، همگی از نوآوری ما محسوب می‌شود.

```
1.    <Rule  RuleId="0" Effect="Permit">
2.    <Target>
3.    <Subjects>
4.    <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
5.    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Professor</AttributeValue>
6.    <SubjectAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string" At-
      tributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"/></SubjectMatch></Subjects>
7.    <Resources>
8.    <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
9.    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Grades</AttributeValue>
10.   <ResourceAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string" At-
      tributeId="urn:oasis:names:tc:xacml:1.0:resource:ResourceId"/></ResourceMatch></Resources>
11.   <Actions>
12.   <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
13.   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Update</AttributeValue>
14.   <ActionAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string" At-
      tributeId="urn:oasis:names:tc:xacml:1.0:action:ActionId"/></ActionMatch></Actions>
15.   </Target>
16.   <Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
17.   <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string_equal">
18.   <ConditionAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string" At-
      tributeId="RegistrationORG:NationalCodeValidity"/>
19.   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Valid</AttributeValue>
20.   </Apply>
21.   <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string_equal">
22.   <ActionAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string" At-
      tributeId="Judiciary:Abuse_History"/>
23.  <AttributeValue DataType=http://www.w3.org/2001/XMLSchema#string>No</AttributeValue>
24.   </Apply></Condition></Rule>
```

شکل (۴). نمونه ساختار یک Rule از سیاست کنترل دسترسی موجود در واحد PAP (مدل پیشنهادی)

1– action
2– rules
3– executable rules
4– attribute queries

5– Negotiation and Inquiry Policy (NIP)
6– Trusted Credential Inquiry Centers (TCICs)
7– Attribute Inquiry Policies



شکل (۵). جریان داده و مؤلفه‌های اصلی مدل پیشنهادی

قسمت «مراکز مورد اعتماد استعلام اعتبارنامه»، شامل مجموعه‌ای از مراکز استعلام موردتوافق با سازمان متبوع است که خدماتی جهت استعلام اعتبار صفات مورد ادعای «درخواست‌کننده» ارائه می‌دهد. در این قسمت به ازای هر مرکز استعلام، خدمات ارائه‌شده آن مرکز به همراه پیش‌نیازهای ارائه هر خدمت مشخص شده است. به‌عنوان مثال، اگر به خواهیم ملیت و تابعیت یک درخواست‌کننده را از مرکز «ثبت‌احوال» استعلام کنیم، حداقل پیش‌نیاز ارائه این خدمت آن است که شناسه ملی به همراه تابعیت موردادعای او را به مرکز یادشده ارسال نماییم. در قسمت «سیاست‌های استعلام صفات»، به ازای هر صفت فهرستی از مراکز استعلام به همراه سیاست‌های استعلام، یعنی نحوه احراز اعتبار آن صفت مدون شده است. ساختار و روش مدیریت موارد یادشده در بخش ۶ به‌تفصیل توضیح داده می‌شود.

همان‌طور که قبلاً اشاره شد در مدل پیشنهادی، مؤلفه PIP نیز شاهد تغییرات اساسی است و آن نحوه پاسخ‌گویی به «پرس وجوی صفات[1]» است. در معماری XACML، این مؤلفه برای انجام وظیفه خود از یک پایگاه داده ثابت و محلی استفاده می‌کند که عملکرد آن را به مقدار زیادی محدود می‌کند. برای جبران این نقیصه و به‌منظور افزایش پویایی و انعطاف‌پذیری مدل، در این مؤلفه از یک «موتور استعلام و مذاکره اعتماد[2]» برای جمع‌آوری مقادیر صفات مربوط به یک درخواست مجاز استفاده شده است. این مؤلفه، امکانی فراهم می‌کند تا با اجرای مجموعه‌ای از پرسش و پاسخ (مذاکره) و استعلام از چندین مرکز مورد اعتماد، سطح اعتماد لازم در فرایند ارزیابی درخواست‌های دسترسی، با انعطاف و اطمینان بیشتری مؤلفه‌ی PIP به‌عنوان تنها منبع مقادیر صفات عمل می‌کند و و درواقع یک پایگاه داده مرکزی[3] است که اطلاعات و مقادیر صفات مربوط به نهادها، منابع و شرایط محیطی را نگهداری و مدیریت می‌کند. ازآنجایی که مدیریت و دسترسی لحظه‌ای به منابع اطلاعاتیِ موردنیاز برای اتخاذ تصمیم یک مسئله حیاتی است، لذا وابستگی مؤلفه‌ی PIP به یک پایگاه داده ثابت و متمرکز، ضمن محدود کردن عملکرد آن، می‌تواند مشکلات و چالش‌های زیادی را به شرح زیر به وجود آورد:

۱- عدم انعطاف‌پذیری در دسترسی به نیازهای اطلاعاتی جدید به‌دلیل گسترش روزافزون سیاست‌های کنترل دسترسی.

1- Attribute Query

2- Trust-Negotiation & Inquiry Engine

3– central database

۲- ایجاد نقطه شکست واحد[1] به‌دلیل تمرکز اطلاعات در یک بانک اطلاعاتی مرکزی.

۳- وابسته بودن پویایی مدل به‌روز رسانی پایگاه داده مرکزی که هرلحظه امکان‌پذیر نیست.

۴- کاهش کارایی تدریجی مدل در ارزیابی درخواست‌ها به‌دلیل افزایش حجم اطلاعات پایگاه داده مرکزی

۵- محدود شدن اسناد و مدارک تأییدیه صفات، به اطلاعات داخلی و از قبل تعیین‌شده.

۶- ملاحظات و چالش‌های امنیتی خاص برای حفاظت از داده‌های متمرکز.

در مدل پیشنهادی، تمهیدات لازم برای غلبه بر مشکلات و چالش های یادشده در مؤلفه PIP، از طریق اضافه نمودن «موتور استعلام و مذاکره اعتماد» پیش‌بینی شده است. این مؤلفه درواقع، مسئول مذاکره برای کنترل دسترسی با جمع‌آوری اعتبارنامه‌ها و آشکارسازی سیاست‌ها است.

مؤلفه PIP به‌صورت پویا و برخط[2]، و به‌جای ارجاع به یک پایگاه داده ثابت، پس از بررسی سیاست‌های مذاکره تعریف‌شده در مؤلفه PAP، مذاکره برای کسب اطلاعات موردنیاز را جهت متقاعد کردن سیاست‌های کنترل دسترسی آغاز می‌کند. از مزایای مؤلفه PIP توسعه‌یافته، آن است که علاوه بر بهره‌گیری از نظرات چندین مرکز مورداعتماد، درصورتی‌که یکی از این مراکز قابل‌دسترس نباشد، عملکرد مدل هیچ‌گاه مختل نخواهد شد. همچنین، نیازی به پایگاه داده داخلی برای ذخیره‌سازی و مدیریت صفات مربوط به نهادها وجود ندارد و یا اگر هم بنا به دلایلی نیاز به وجود چنین پایگاه داده‌ای باشد، وابستگی کامل مدل به این پایگاه مرتفع می‌شود. به‌این‌ترتیب، با امکان به‌روزرسانی سیاست‌های کنترل دسترسی از یک‌سو، و قابلیت به‌روزرسانی «مراکز استعلام صفات» از سوی دیگر، مؤلفه PIP قادر است پاسخ‌گویی پویا، مطمئن و منعطفی را از خود به نمایش بگذارد. بدیهی است برای تضمین پویایی در استنتاج از پاسخ‌های به‌دست‌آمده توسط مؤلفه PIP، نیاز به تعیین سیاست‌هایی است که ما این سیاست‌ها را، «سیاست‌های مذاکره» می‌نامیم. حال باید روشن شود که نحوه تعامل با این «مراکز استعلام» چگونه خواهد بود؟ و پاسخ به‌دست‌آمده برای یک «پرس وجوی صفت» چگونه استنتاج می‌گردد؟

در مدل پیشنهادی، اداره‌کننده زمینه پس از دریافت پاسخ از مؤلفه PIP توسعه‌یافته (مرحله ۸)، و اطلاعات منابع درخواست شده (مرحله ۹)، آن‌ها را به مؤلفه PDP تحویل می‌دهد (مرحله ۱۰). در مؤلفه PDP، ارزیابی درخواست با سرعت مطلوب توسط موتور XEngine انجام شده و نتیجه ارزیابی (مجاز یا رد) از طریق مؤلفه PDP به مؤلفه اداره‌کننده زمینه ارسال می‌شود (مرحله ۱۱). درنهایت، مؤلفه اداره‌کننده زمینه پاسخ را به مؤلفه PEP (مرحله ۱۲) برمی‌گرداند تا تصمیم اتخاذشده را عملی سازد.

۶- پیاده‌سازی مدل پیشنهادی

پیاده‌سازی مدل پیشنهادی، در محیط NET Framework.، زبان برنامه‌نویسی C#، به روش شیءگرا و با استفاده از قابلیت‌های وب سرویس انجام گرفته است. این چارچوب روی سخت‌افزاری با CUP 3.4 GHZ و RAM 4 GB اجرا می‌شود. اهم فعالیت‌های انجام‌شده در پیاده‌سازی مدل پیشنهادی به‌قرار زیر است:

- استفاده از سیاست‌های کنترل دسترسی با ساختار کامل‌تر شامل، افزودن بخش «صفات» در قسمت condition از قواعد. در این راستا، ساختار XML سیاست های موردنیاز برای تصمیم‌گیری در مؤلفه PDP. مطابق شکل (۴)، استفاده شده است.
- استفاده از ساختار Attribute Query مربوط به مراحل ۶ و ۷.
- استفاده از ساختار Attributes مربوط به مراحل ۸ و ۱۰.
- تهیه ساختار XML برای ارائه سیاست‌های مذاکره و استعلام.
- تبیین نحوه پاسخ‌گویی مؤلفه PIP به Attribute Query، با استفاده از NIP و بر اساس مذاکره با درخواست‌کننده و استعلام از «مراکز استعلام اعتبارنامه».
- نحوه تصمیم‌گیری مؤلفه PDP برای انتخاب Rule نهایی از میان Ruleهای منتخب، بر اساس صفات تائید شده توسط مؤلفه PIP.

۶-۱- ساختار NIP (سیاست مذاکره و استعلام)

نمونه‌ای از ساختار (سیاست مذاکره و استعلام) در شکل (۶) نشان داده شده است. این ساختار با (مجموعه سیاست‌های مذاکره و استعلام[3]) آغاز می‌شود (خط شماره ۲) که شامل دو بخش عمده «فهرست مراکز استعلام مورد اعتماد اعتبارنامه ها[4]» و «سیاست‌های استعلام صفات[5]» (خط شماره ۱۸) است. در خط شماره ۴، مرکز استعلام قوه قضاییه تعریف شده است. این مرکز از طریق متد مربوطه (خط شماره ۶)، با دریافت پارامتر شناسه ملی

1- single point of failure
2– online

3-NegotiationInquiryPolicySet
4-Trusted Credential Inquiry Centers (TCICs)
5-AttributInquiryPolicies

(خط شماره ۸)، امکان استعلام سوءپیشینه درخواست کننده دسترسی به داده‌ها را فراهم می‌کند. در خط شماره ۸، دو ویژگی نوع داده[1] و شناسه صفت[2] به‌عنوان «معرف صفت[3]» این پارامتر، تعیین شده است. در خط شماره ۹، سازمان ثبت‌احوال به‌عنوان یک مرکز استعلام دیگر تعریف شده است. متد خط شماره ۱۱، با دریافت پارامترهای خطوط ۱۳ تا ۱۷، امکان استعلام اعتبار شناسه ملی درخواست‌کننده را فراهم می‌نماید.

بخش تعریف «سیاست‌های استعلام صفات» از خط شماره ۱۸ آغاز می‌شود. در خط شماره ۱۹، شروع تعیین سیاست استعلام اعتبارِ صفتِ «شناسه ملی» است. در خط شماره ۲۰، اولین عبارت تعیین اولویت استعلام تعریف شده است. نوع این عبارت، مرکب[4] است یعنی. شامل مجموعه‌ای از عبارات دیگر که نتیجه نهایی، ترکیبی از نتایج عبارات زیرمجموعه آن است. شناسه تابع عبارات مرکب[5]، شامل همه (All)، هر (Each) و مستقیم (Direct) است. این شناسه تعیین‌کننده نحوه ترکیب نتایج عبارات زیرمجموعه است. All، به معنی آن است که اعتبار عبارت مرکب، وابسته به اعتبار همه عبارات زیرمجموعه است و نامعتبر بودن یکی از عبارات زیرمجموعه، عدم اعتبار عبارت مرکب را تعیین می‌کند. Each، به معنی آن است که معتبر بودن یکی از عبارات زیرمجموعه، جهت معتبر بودن عبارت مرکب، کافی است. Direct، به معنی آن است که اعتبار عبارت مرکب، به‌طور مستقیم وابسته به اعتبار اولین عبارت زیرمجموعه است. خطوط شماره ۲۱ و ۲۴، دو عبارت زیرمجموعه عبارت مرکب خط شماره ۲۰ هستند. خط ۲۲، عبارت ساده‌ای به‌عنوان زیرمجموعه‌ای از عبارت مرکب خط شماره ۲۱ تعریف می‌کند. در عبارات ساده، دو ویژگی مرکز استعلام اعتبارنامه و متد مربوطه، تعیین‌کننده نحوه مذاکره با درخواست‌کننده و نحوه استعلام است. در خط ۲۲، مرکز استعلام (سازمان ثبت‌احوال) و متد آن «تعیین اعتبار کد ملی[6]» تعریف شده است.

در ادامه، برای اجرایی شدن مدل پیشنهادی، کلاس‌های برنامه کاربردی در سه دسته زیر طراحی و پیاده‌سازی شده‌اند.

- مجموعه کلاس‌های سیاست‌های کنترل دسترسی (XACMLPolicy).

این کلاس‌ها، برای بارگذاری، تفسیر و اداره ساختار XML سیاست‌های کنترل دسترسی طراحی شده‌اند.

- مجموعه کلاس‌های XEngine.

این کلاس‌ها، جهت اجرای عملیات XEngine شامل گام‌های عددی سازی، نرمال‌سازی و ایجاد ساختار درختی و به‌منظور افزایش سرعت پردازش تصمیمات دسترسی، بر روی سیاست‌های کنترل دسترسی طراحی شده‌اند.

- مجموعه کلاس‌های Negotiation and Inquiry Policies

این مجموعه، شامل کلاس‌هایی هستند که عملیات مذاکره و استعلام را پشتیبانی می‌کنند. این کلاس‌ها ساختار سیاست‌های مذاکره و استعلام را پیاده‌سازی و سازوکارهای مذاکره و استعلام را فراهم می‌کنند. در این مجموعه از کلاس‌ها، می‌توان مجموعه‌ای از انواع شرایط و نیازمندی‌های امنیتی مربوط به دسترسی به خدمات ارایه‌دهندگان سرویس را پشتیبانی کرد. بدیهی است، تعریف و مدیریت نیازمندی‌های امنیتی دسترسی به خدماتِ خاص ارایه‌دهندگان سرویس، سازوکار خاص خود را می‌طلبد. به‌عنوان مثال، یک ارایه‌دهنده سرویس ممکن است برای دسترسی به سرویس A، شرایط زیر را اعلام نماید: $[(C_1 \vee (C_2 \wedge C_3)) \wedge C_4]$ مفهوم این عبارت آن است که درخواست‌کننده برای دسترسی به سرویس A، باید گواهی‌های C_1 یا هر دو گواهی C_2 و C_3 به‌طور همزمان و گواهی C_4 را از مراکز صدور گواهی مربوطه ارایه نماید. به‌منظور تامین شرایط اعلام‌شده توسط ارایه‌کننده سرویس، به کمک کلاس های یادشده و ساختار «سیاست مذاکره و استعلام» (شکل ۶) ساختار شرایط استعلام به‌صورت زیر ارایه می‌شود.

۷- ارزیابی عملی

در این بخش، برای اثبات کارایی مدل پیشنهادی، آزمایش‌هایی طراحی می‌کنیم تا عملکرد آن را از ابعاد مختلف مورد بررسی قرار دهیم. همان‌طور که قبلاً اشاره شد، جهت افزایش سرعت عملکرد مؤلفه PDP، از موتور XEngine استفاده کرده‌ایم. با توجه به توسعه ساختار سیاست در مدل پیشنهادی، موتور XEngine می‌باید بر اساس سیاست‌های کنترل دسترسی مبتنی بر صفات، عمل کند. صفات افزوده‌شده به ساختار سیاست در بخش Codition قواعد (شکل ۴)، تأثیری در عملکرد سه‌گام XEngine ندارد.

از این‌رو، عملکرد XEngine را در مورد «زمان تولید پرس‌وجوی صفات» و «زمان تصمیم‌گیری دسترسی»، بر اساس سیاست‌های کنترل دسترسی مبتنی بر صفات و فاقد صفات، مورد بررسی و آزمایش قرار می‌دهیم. آزمایش‌های انجام‌شده نشان می‌دهد که افزودن صفات به ساختار سیاست‌های کنترلی، در عملکرد XEngine

1- DataType
2- AttributeId
3- Attribute Designator
4- compound
5- FunctionId
6- NationalCodeValidity

```
1. <?xml version="1.0" encoding="UTF-8"?>
 2. <NegotiationInquiryPolicySet>// مجموعه سیاست‌های مذاکره و استعلام
 3. <TCICList> // فهرست مراکز استعلام مورد اعتماد اعتبارنامه‌ا
 4. <TCIC id="Judiciary" ServiceUrl="http://localhost:20222/JS.asmx" caption="قوه قضاییه">
 5. <Methods>
 6. <Method id="Has_Abuse_History">//متدی برای استعلام سوءسابقه مشتری از قوه قضائیه
 7. <Parameters>
 8. <Parameter DataType="http://www.IRIDTSD.org/2015/XMLSchema#string"
AttributeId="RegistrationORG:National_Code"/></Parameters></Method></Methods></TCIC>
 9. <TCIC id="RegistrationORG" ServiceUrl="http://localhost:20222/JS.asmx"
caption="سازمان‌ثبت‌احوال">
10. <Methods>
11. <Method id="NationalCodeValidity">
12. <Parameters>
13. <Parameter DataType="http://www.IRIDTSD.org/2015/XMLSchema#string"
AttributeId="RegistrationORG:National_Code"/>
14. <Parameter DataType="http://www.IRIDTSD.org/2015/XMLSchema#string"
AttributeId="RegistrationORG:FirstName"/>
15. <Parameter DataType="http://www.IRIDTSD.org/2015/XMLSchema#string"
AttributeId="RegistrationORG:LastName"/>
16. <Parameter DataType="http://www.IRIDTSD.org/2015/XMLSchema#string"
AttributeId="RegistrationORG:FatherName"/>
17. <Parameter DataType="http://www.IRIDTSD.org/2015/XMLSchema#string"
AttributeId="RegistrationORG:BirthDate"/></Parameters></Method></Methods></TCIC></TCICList>
18. <AttributeInquiryPolicies>//سیاست‌های استعلام صفات
19. <AttributeInquiryPolicy DataType="http://www.IRIDTSD.org/2015/XMLSchema#string"
AttributeId="RegistrationORG:National_Code"> // صفت موردنظر
20. <statement type="Compound" FunctionId="Each"> // سیاست‌های استعلام صفت کد ملی
21. <statement type="Compound" FunctionId="Direct">
22. <statement type="Simple" TCICid="RegistrationORG" MethodId="NationalCodeValidity"/>
23. </statement>
24. <statement type="Compound" FunctionId="All">
25. <statement type="Simple" TCICid="PoliceForce" MethodId="NationalCodeValidity"/>
26. <statement type="Simple" TCICid="TrafficPolice" MethodId="NationalCodeValidity"/>
27. </statement></statement></AttributeInquiryPolicy>
28. <AttributeInquiryPolicy DataType="http://www.IRIDTSD.org/2015/XMLSchema#string"
AttributeId="Judiciary:Abuse_History">
29. <statement type="Compound" FunctionId="Direct">
30. <statement type="Simple" TCICid="Judiciary" MethodId="Has_Abuse_History "/>
31. </statement></AttributeInquiryPolicy></AttributeInquiryPolicies>
32. </NegotiationInquiryPolicySet>
```

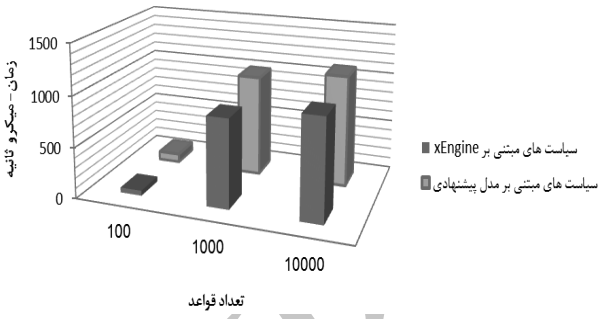
شکل (۶). ساختار NIP در مدل پیشنهادی

تاثیر قابل‌توجهی نداشته است و کماکان گزینه مناسبی برای افزایش سرعت عملکرد مدل پیشنهادی محسوب می‌شود. در این آزمایش، حجم‌های مختلفی از سیاست‌های کنترل دسترسی، هم مبتنی بر XEngine و هم مبتنی بر مدل پیشنهادی تولید می‌کنیم. تفاوت این سیاست‌ها، در صفات افزوده شده به بخش Subject است. درخواست مشخصی را تعیین می‌کنیم که در مجموعه قواعد موجود در سیاست‌ها، بر اساس قاعده آخر قابل پاسخ‌دهی باشد. این درخواست، با همه شرایط ذکر شده و به تعداد ۱۰ مرتبه اجرا می‌شود. در ادامه، نتایج حاصل از اجرای مدل‌های XEngine و TNAC برای محاسبه

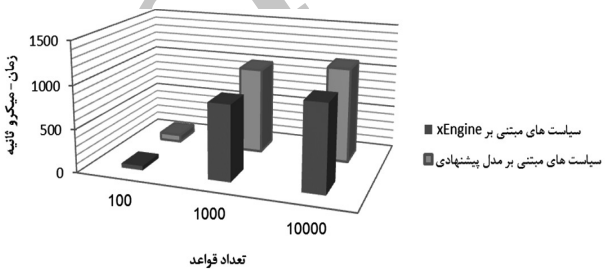
```
1.  Statement1 type="Compound" FunctionId="All"
2.    Statement2 type="Compound" FunctionId="Each"
3.      Statement3 type="Compound" FunctionId="Direct"
4.        Statement type="Simple" C1
5.      Statement3
6.      Statement4 type="Compound" FunctionId="All"
7.        Statement type="Simple" C2
8.          Statement type="Simple" C3
9.      Statement4
10.   Statement2
11.   Statement type="Simple" C4
12. Statement1
```

شکل (۷). شرایط استعلام دسترسی به سرویس A

زمان تولید «پرس‌وجوی صفات» و زمان «تصمیم‌گیری دسترسی» نشان داده شده است (شکل ۹ - ۸).



شکل (۸). مقایسه «زمان تولید پرس وجوی صفات» در ساختار سیاست‌های مبتنی بر مدل TNAC و .XEngine



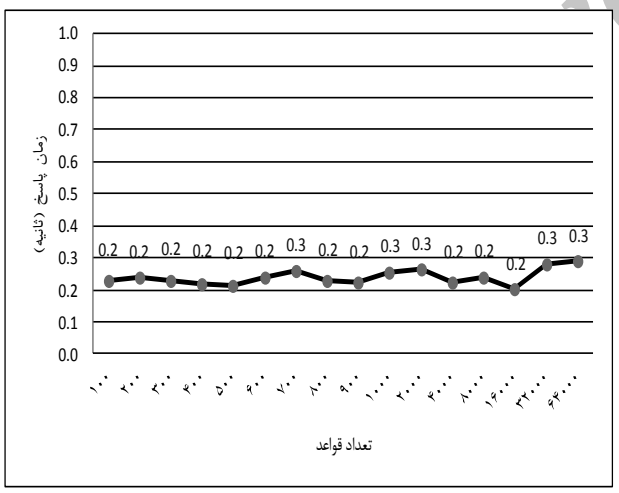
شکل (۹). مقایسه «زمان تصمیم‌گیری دسترسی» در مدل TNAC و .XEngine

همان‌طور که در شکل (۸) مشاهده می‌شود، سیاست‌های کنترل دسترسی در سه مقیاس ۱۰۰، ۱۰۰۰ و ۱۰۰۰۰ قاعده (Rule) تولید شده‌اند. در این آزمایش، مقایسه زمان تولید «پرس‌وجوی صفات» بین دو مدل، نشان از اختلاف زمانی بسیار ناچیز دارد و این اختلاف، با افزایش حجم سیاست‌ها به دلیل تاثیر نامحسوس وجود صفات در «زمان تولید پرس‌وجوی صفات»، نسبت مستقیم نخواهد داشت. در ادامه، نتیجه حاصل از اجرای دو مدل برای ارزیابی «زمان تصمیم‌گیری دسترسی» نشان داده شده است. شرایط این آزمایش، همانند آزمایش اول پیش‌بینی شده و نتیجه آن در شکل (۹) نشان داده شده است

همان‌طور که در شکل (۹) مشاهده می‌شود، باز هم اختلاف «زمان تصمیم‌گیری دسترسی» با دو مدل مورد نظر، ناچیز بوده و با افزایش حجم سیاست‌ها، زمان تصمیم‌گیری، بدلیل تاثیر محدود صفات در مقایسه صفات استعلام شده بخش PIP و صفات قوانین نامزد پاسخ‌دهی، افزایش چندانی نخواهد یافت.

حال به‌منظور اطمینان از زمان پاسخ مطلوب مدل پیشنهادی، عملکرد XEngine را در این راستا مورد ارزیابی قرار می‌دهیم. زمان پاسخ، از ارسال درخواست کاربر شروع و تا پایان دریافت پاسخ محاسبه می‌شود. این زمان شامل: ۱- عملکرد XEngine برای تهیه «پرس‌وجوی صفات»، ۲- عملکرد PIP برای مدیریت مذاکره با درخواست‌کننده و استعلام صفات از TCIC و ۳- عملکرد XEngine جهت پردازش تطبیق نتیجه «پرس‌وجوی صفات» دریافت‌شده از PIP با شرایط قواعد منتخب و تهیه پاسخ نهایی است. لازم به ذکر است که این زمان بدون در نظر گرفتن سربار بستر ارتباطی (زمان انتظار برای ارسال و دریافت پاسخ از درخواست‌کننده و TCICs)، محاسبه می‌شود.

در این آزمایش، حجم‌های مختلفی از سیاست‌های کنترل دسترسی، بر اساس تعداد قواعد، تولید می‌گردد. به ازای هر تعداد از قواعد، تعداد ۱۰۰ درخواست همزمان به‌صورت تصادفی تولید و ارسال می‌گردد. برای حصول نتیجه بهتر، این فرایند حداقل به تعداد ۱۰ مرتبه تکرار می‌شود. کمینه زمان پاسخ مدل پیشنهادی به‌عنوان زمان پاسخ مدل برای آن تعداد از قواعد ثبت می‌شود. تعداد قواعد را از ۱۰۰ آغاز نموده و با افزایش ۱۰۰ قاعده به ۱۰۰۰ قاعده می‌رسانیم. با توجه تغییرات ناچیز زمان پاسخ، آهنگ تغییرات تعداد قواعد را به‌صورت نمایی تا ۶۴۰۰۰ قاعده افزایش داده و نتایج آزمایش را به‌صورت شکل شماره ۱۰ به‌دست می‌آوریم.



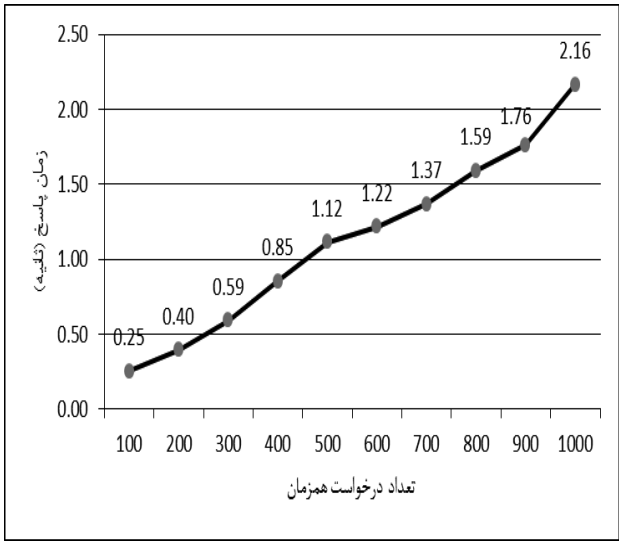
شکل (۱۰). زمان پاسخ صد درخواست هم‌زمان متناسب با افزایش تعداد قواعد در مدل پیشنهادی

همان‌طور که در شکل (۱۰) مشاهده می‌شود افزایش تعداد قواعد، تأثیر قابل‌توجهی در زمان پاسخ مدل پیشنهادی ندارند. این مسئله با توجه به روش تهیه «پرس‌وجوی صفات» و روش تطابق نتیجه آن‌ها با قواعد منتخب توسط XEngine، منطقی و قابل توجیه بوده و بیانگر کارایی و عملکرد مطلوب مدل پیشنهادی است. در مدل

پیشنهادی از رویکرد Forwarding Table موتور XEngine استفاده شده است و XEngine در هر پردازش، تنها سه جدول (به تعداد لایه‌های درخت تصمیم‌گیری شکل (۳)) را بررسی می کند. ازآنجایی‌که سه جدول فوق، در حافظه اصلی، بارگذاری و مورد پردازش قرار می‌گیرد، لذا سرعت پردازش و رسیدن به نتیجه نهایی فارغ از تعداد قواعد موجود در هر لایه از درخت XEngine قابل‌توجه است.

در آزمایش دوم، با تعداد ۱۰۰۰ قاعده ثابت، تعداد درخواست‌های همزمان را افزایش می‌دهیم. هدف از این آزمایش، بررسی مقیاس‌پذیری مدل پیشنهادی است. همان‌طور که در شکل ۱۱ ملاحظه می‌شود، تعداد درخواست‌های همزمان از ۱۰۰ تا ۱۰۰۰ درخواست افزایش یافته است و با افزایش تعداد درخواست‌های همزمان، زمان پاسخ به‌صورت خطی افزایش می‌یابد. از موارد فوق به این نتیجه می‌رسیم که، یکی از معیارهای اصلی تحلیل عملکرد و ارزیابی کارایی مدل، یعنی مقیاس‌پذیری آن به‌طور کامل محقق شده است.

از طرفی، با توجه به اهداف و عملکرد مدل پیشنهادی و به منظور جمع‌بندی و نتیجه‌گیری نهایی، علاوه بر ارزیابی عددی، یک ارزیابی توصیفی و مفهومی نیز برای مقایسه مدل پیشنهادی و معماری XACML انجام گرفته است که نتایج آن در جدول (۲) نشان داده شده است. از مجموع ارزیابی‌های انجام‌گرفته، می‌توان ادعا کرد مدلی که در این مقاله ارائه شده است در دنیای واقعی و در



شکل (۱۱). زمان پاسخ درخواست‌های هم‌زمان در مدل پیشنهادی

جدول (۲). مقایسه ویژگی‌های مدل پیشنهادی و مدل استاندارد XACML.

ردیف	ویژگی‌ها	مدل پیشنهادی TNAC	مدل استاندارد XACML	توضیح
۱	انعطاف‌پذیری	زیاد	کم	با توجه به توسعه عملکرد مؤلفه PIP در مدل پیشنهادی، توانایی آن در پشتیبانی از نیازمندی‌های امنیتی سازمان‌ها و نیز توانایی کار در شرایط مختلف تضمین شده است.
۲	نقطه شکست واحد	ندارد	دارد	با توجه به عدم وابستگی مدل پیشنهادی به پایگاه داده مرکزی و قابلیت استعلام اعتبارنامه‌ها از مراکز مورداعتماد.
۳	وابستگی به به‌روزرسانی اطلاعات صفات	ندارد	دارد	با توجه به عدم وابستگی مدل پیشنهادی به پایگاه داده مرکزی.
۴	بهبود کارایی	مطلوب	دارد	با توجه به بهبود کارایی مولفه PDP در مدل پیشنهادی، کارایی آن بر اساس آزمایش‌های انجام‌شده مطلوب است.
۵	وابستگی تأییدیه صفات	منابع گسترده	منابع محدود	در مدل پیشنهادی، اسناد تأییدیه اعتبارنامه‌ها صرفاً وابسته به اطلاعات پایگاه داخلی و از قبل تعیین‌شده نیست و لذا پایداری آن مطلوب است.
۶	ملاحظات و چالش‌های امنیتی	چالش‌های امنیتی محیط‌های سرویس‌گرا	چالش‌های امنیتی محیط‌های متمرکز	در مدل پیشنهادی، از فن نمایندگی[1] برای فائق آمدن بر چالش‌های امنیتی استفاده شده است.
۷	ضریب اعتماد به پاسخ «پرس‌وجوی صفات»	زیاد	زیاد	در مدل پیشنهادی نیز، به‌دلیل استفاده از رویکرد مذاکره اعتماد و بهره‌گیری از چندین مرکز استعلام قابل‌اعتماد، ضریب اعتماد عملکرد PIP افزایش یافته است.
۸	قابلیت دسترسی	زیاد	کم	با توجه به عدم وجود «نقطه شکست واحد» در مدل پیشنهادی و ارتباط همزمان با چندین مرکز استعلام، قابلیت دسترسی به آن بسیار مطلوب است.
۹	سرعت پاسخ‌گویی	نسبتاً کم	زیاد	نسبت به توسعه قابلیت‌ها و انعطاف‌پذیری مدل پیشنهادی، سرعت پاسخ‌گویی آن قابل‌قبول است.
۱۰	کاربردپذیری[2]	زیاد	کم	مدل پیشنهادی، با توجه به توسعه مولفه‌های PDP، PIP و PAP، برای محیط‌های واقعی دولت الکترونیک بسیار مناسب و کاربردی است.

1-proxy technique
2-applicability

مقایسه با معماری XACML، عملکرد منعطف‌تری از خود نشان می‌دهد. همچنین، باید توجه داشت که کارآیی مدل پیشنهادی، در توازنی با اهداف مورد نظر و بهره‌گیری از قابلیت‌های اضافه شده، دچار خلل نخواهد شد.

همان‌طور که قبلاً نیز اشاره شد، یکی از چالش‌ها و دغدغه‌های مهم در محیط‌های همکاری فراسازمانی با توجه به تعدد سیاست‌های کنترلی، مربوط به چالش‌های امنیتی است. در مدل پیشنهادی، برای غلبه بر چالش‌های امنیتی پیشرو، از فنون نمایندگی استفاده شده است. با توجه به راهبردهای مختلف به‌کارگیری نمایندگی، چندین رویکرد مطرح است [۱۶]. ما در این مدل، با درنظر گرفتن ویژگی محیط‌هایی که دارای اطلاعات حساس و حیاتی هستند، از راهبرد «نماینده سازمان- میزبان[1]» بهره برده‌ایم.

۸- نتیجه‌گیری و کارهای آینده

در این مقاله، مدل کنترل دسترسی TNAC، مبتنی بر معماری XACML با تلفیق قابلیت‌های موتور ارزیابی XEngine و سازوکارهای مذاکره اعتماد معرفی گردید. مدل پیشنهادی، برای سامانه‌های پویای فراسازمانی ارائه شده است، که در آن نهادهای درگیر در فرایند دسترسی به منابع متعلق به حوزه‌های امنیتی مختلف هستند و قبل از انجام تعاملات، نیازمند برقراری اعتماد می‌باشند. در مدل پیشنهادی، مذاکره‌ی پویا بر اساس استعلام از چندین مرکز اطلاعاتی قابل‌اعتماد به‌منظور تائید اعتبارنامه‌های درخواست‌کنندگان سرویس، و نیز مدیریت کنترل دسترسی در چارچوب معماری XACML فراهم شده است. همچنین، برای پوشش کاربردپذیری و حفظ انعطاف‌پذیری مدل TNAC، برخی از مؤلفه‌ها از قبیل PDP، PAP و PIP دستخوش تغییرات اساسی شده‌اند. استفاده از قابلیت موتور ارزیابی XEngine برای افزایش سرعت ارزیابی درخواست‌های دسترسی و حفظ کارایی، ویژگی دیگری است که در مدل پیشنهادی به آن توجه شده است. در مدل TNAC، ابتدا مذاکره بین درخواست‌کننده و ارائه‌دهنده سرویس انجام می‌گیرد تا همه صفاتی که برای برقراری اعتماد و ارزیابی موفقیت‌آمیز یک درخواست دسترسی لازم است، جمع‌آوری شوند. برای تأمین نیازمندی‌های امنیتی مدل، از فن نمایندگی و راهبرد «نماینده سازمان میزبان» استفاده کرده‌ایم.

درنهایت، نمونه اولیه مدل پیشنهادی را پیاده‌سازی کرده و آزمایش‌های متعددی به‌منظور ارزیابی کارایی آن انجام گرفت. نتایج حاصل از پیاده‌سازی و آزمایش این مدل، شواهد محکمی است که کارایی، مقیاس‌پذیری و کاربردپذیری آن را اثبات می‌کند. به‌عنوان کار آینده، می‌توان از قابلیت WSDL 2.0 برای حفظ محرمانگی اعتبارنامه‌های کاربران و جلوگیری از افشای اطلاعات حساس طرفین مذاکره در حین تبادل اطلاعات استفاده نمود و همچنین به‌منظور توسعه بیشتر قابلیت‌های مدل، می‌توان مدیریت شرایط محیطی و صفات منابع را نیز به‌طور کامل مدنظر قرار داد.

1- organization-hosted proxy

۹- مراجع

[1] A. Karimi, M. S. Esfahani, and M. R. Hassani Ahangar, "MCDTWS: A Novel Multiple Criteria Decision-Based Trust Management Model in Web Services," J. of Passive Defense Science and Technology, vol. 3, no. 3, pp. 181-192, 2013 (In Persian).

[2] A. Ahmed and N. Zhang, "Towards the realization of context-risk-aware access control in pervasive computing," Telecommunication Systems Journal, 2009.

[3] J. Li, X. Liu, L. Liu, D. Sun, and B. Li, "HiTrust: building cross-organizational trust relationship based on a hybrid negotiation tree," Springer Science Business Media, 2011.

[4] J. He, S. Ma, and B. Zhao, "Analysis of Trust-based Access Control Using Game Theory," International Journal of Multimedia & Ubiquitous Engineering, vol. 8, no. 4, pp. 15-24, 2013.

[5] T. Ryutov, L. Zhou, C. Neuman, T. Leithead, and K. E. Seamons, "Adaptive Trust Negotiation and Access Control", in Proc. of the 10th ACM Symposium on Access Control Models and Technologies, Stockholm, Sweden, 2005.

[6] A. X. Liu, F. Chen, J. Hwang, and T. Xie, "XEngine: A Fast and Scalable XACML Policy Evaluation Engine," ACM, 2008.

[7] D. A. Haidar, N. uppens-Boulahia, F. Cuppens, and H. Debar, "XeNA: an access negotiation framework using XACML," Institut Telecom and Springer-Verlag, 2008.

[8] T. Yu and M. Winslett, "A unified scheme for resource protection in automated trust negotiation," in Proc. of SP'03, 2003.

[9] W. H. Winsborough and N. Li, "Towards practical automated trust negotiation," In Proceedings of the 3rd international workshop on policies for distributed systems and networks (POLICY' 02) Monterey, CA, USA, 2002.

[10] W. H. Winsborough, K. E. Seamons, and V. E. Jones, "Automated trust negotiation," In DARPA Information Survivability Conference and Exposition, vol. I, pp. 88-102, Hilton Head, SC, January 2000.

[11] JP. Bonatti and P. Samarati, "A Unified Framework for Regulating Access and Information Release on the Web," In Journal of Computer Security, vol. 10, no. 3, pp. 241-271, 2002.

[12] N. Li, J. Mitchell, and W. H. Winsborough, "RT: A role-based trust-management framework," In Proceedings

of The Third DARPA Information Survivability Conference and Exposition (DISCEX III), April 2003.

[13] JJ. Trevor, "SD3: A Trust Management System with Certified Evaluation," In IEEE Symposium on Security and Privacy, Oakland, CA, 2001.

[14] A. J. Lee, M. Winslett, and K. J. Perano, "TrustBuilder2: A Reconfigurable Framework for Trust Negotiation," in Trust Management III."Springer Berlin Heidelberg," pp. 176-195, 2009.

[15] E. Bertino, E. Ferrari, and A. C. Squicciarini, "Trust-X: A peer-to-peer framework for trust establishment," IEEE Transactions on Knowledge and Data Engineering vol. 16, no. 7, pp. 827–842, 2004.

[16] M. Singhal, S. Chandrasekhar, T. Ge, R. Sandhu, R. Krishnan, G. J. Ahn, and E. Bertino, "Collaboration in Multicloud Computing Environments: Framework and Security Isues," IEEE omputer Society, vol. 46, no. 2, pp. 76-84, 2013.

[17] "eXtensible Access Control Markup Language (XACML) Version 2 standard OASIS, February," 2005.

TNAC: A Novel Trust Negotiation Based Access Control Model Using XACML Architecture

A. Karimi*, M. Saleh Esfahani, M. R. Hasani Ahangar

* Imam Hossein University

(Received: 01/11/2014, Accepted: 01/09/2015)

ABSTRACT

the emergence of Web services technologies and the evolution of distributed systems toward Service Oriented Architectures (SOA) have helped significantly promote collaboration and information sharing. Data exchange among heterogeneous platforms and provision of service security are two notable challenges in SOA architecture that require due consideration. Due to different security policies in inter-organizational environment, current information security mechanisms and traditional access control models are often unable to satisfy users' security requirements. Trust negotiation is a cruicial and promising approach in trust establishment and secure interactions between entities for which there is no pre-existing knowledge or experience. In this paper, a new access control model based on attributes and trust negotioation techniques to overcome these challenges is proposed. This model is developed within XACML standard architecture together with Xengine evaluation engine features. Numerical results and performance evaluation of our model show that the proposed model has more flexibilility and performance than existing models. Moreover, the model is able to provide service security and also, proves it's applicability in real e-government and e-commerce environments.

Keywords: Access Control, Trust Negotiation, XACML Architecture, Security Policy, Credential.

* Corresponding Author Email: a.karimi@ihu.ac.ir