فصلنامه علمی-ترویجی پدافند غیرعامل

سال پنجم، شماره ۴، پاییز ۱۳۹۳، (پیاپی ۱۹): صص ۱-۹

ارائه یک مدل کنترل دسترسی به داده‌های حیاتی سازمان مبتنی بر مذاکره اعتماد با رویکرد پدافند غیرعامل

علی کریمی[۱]، محمود صالح اصفهانی[۲]، محمدرضا حسنی آهنگر[۳]، بهزاد علیزاده[۴]

تاریخ دریافت: ۱۳۹۳/۰۷/۰۵
تاریخ پذیرش: ۱۳۹۳/۰۹/۱۲

چکیده

در محیط‌های گسترده فراسازمانی، برقراری اعتماد در میان سرویس‌های توزیع‌شده، به یک نیاز اساسی تبدیل شده است. کنترل دسترسی و تأمین امنیت داده‌ها، از چالش‌های اساسی در این محیط‌ها محسوب می‌شود. مدل‌های کنترل دسترسی سنتی، با توجه به تعدد سیاست‌های امنیتی در محیط‌های فراسازمانی، به تنهایی پاسخ‌گوی نیازهای امنیتیِ این محیط‌ها نیست. یک رویکرد امیدبخش برای برقراری اعتماد و تعاملاتِ امن بین موجودیت‌ها در چنین محیط‌هایی، رویکرد مذاکره اعتماد است. در این مقاله، برای غلبه بر چالش‌های مذکور، یک مدل کنترل دسترسی جدید با رویکرد پدافند غیرعامل، مبتنی بر سازوکارهای مذاکره اعتماد در بستر معماری استاندارد XACML پیشنهاد شده است. کارآیی و انعطاف‌پذیری مدل پیشنهادی، نشان می‌دهد که کاربردپذیری آن برای توسعه تعاملات الکترونیکی در محیط‌های فراسازمانی بسیار مناسب است.

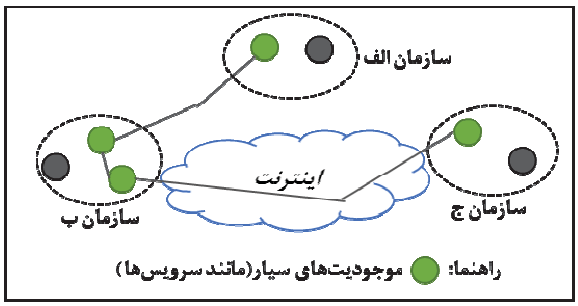
کلیدواژه‌ها: کنترل دسترسی، مذاکره اعتماد، معماری XACML، سیاست‌های امنیتی

۱- دانشجوی دکترای مهندسی نرم‌افزار و عضو هیئت علمی دانشگاه جامع امام حسین(ع) akarimi@ihu.ac.ir – نویسنده مسئول
۲- استادیار و عضو هیئت علمی دانشگاه جامع امام حسین(ع) msaleh@ihu.ac.ir
۳- دانشیار و عضو هیئت علمی دانشگاه جامع امام حسین(ع) mrhassani@iust.ac.ir
۴- دانشجوی کارشناسی ارشد دانشگاه جامع امام حسین(ع)

۱- مقدمه

محیط‌های محاسباتی سرویس‌گرا که عموماً مبتنی بر معماری‌های سرویس‌گرا هستند، یک فضای باز، پویا و توزیع شده است که موجودیت‌های مختلف (از قبیل سرویس‌ها) برای ارائه انواع خدمات تجاری با یکدیگر همکاری می‌کنند. با این حال، در یک محیط همیارانه فراسازمانی پویا، سرویس‌های درگیر در یک فرایند کسب‌وکار اغلب توسط سازمان‌های مختلف تأمین و ارائه می‌شوند (شکل ۱). از این‌رو، عدم پشتیبانی از سازوکارهای امنیتی مشترک در این محیط‌ها کاملاً رایج است. در چنین شرایطی، سرویس‌های مشارکت‌کننده برای دستیابی به اهداف کسب‌وکار سازمان، مجبورند به‌صورت پویا که قبلاً هیچ دانشی نسبت به یکدیگر ندارند، در زمان اجرا با هم همکاری کنند [۱و۲].

با این حال، سیستم‌های سرویس‌گرای مبتنی بر اینترنت، برای برقراری اعتماد بین موجودیت‌ها، با چالش‌های امنیتی فزاینده‌ای مواجه هستند. سیستم‌های کنترل دسترسی سنتی، برای غلبه بر این چالش‌ها کافی نبوده و پاسخ‌گوی نیازهای امنیتی کاربران نیست [۳]. مدل‌های کنترل دسترسی در گذشته، چند مرحله از توسعه خود را گذرانده‌اند و حداقل دارای سه نوع عمده شامل: کنترل دسترسی اختیاری[1] [۴]، کنترل دسترسی اجباری[2] [۵] و کنترل دسترسی مبتنی بر نقش[3] [۶] هستند. همه این مدل‌ها اساساً بر هویت کاربر استوارند، که در آن هر فرد و هر شیء با یک نام منحصربه‌فرد شناسایی می‌شود و کنترل دسترسی، مبتنی بر شناسایی و احراز هویتِ موفقِ یک فرد صورت می‌پذیرد. از آن‌جایی که ماهیت همه آن‌ها مبتنی بر هویت است، بنابراین، مدل‌های DAC، MAC و RBAC عمدتاً در محیط‌های بسته و نسبتاً ثابت، مانند سازمان‌هایی که با مجموعه‌ای از کاربران، منابع و سرویس‌های شناخته‌شده سروکار دارند، مؤثر هستند. مدل‌های کنترل دسترسی سنتی، برای محیط‌های شبکه‌ای باز و پویا مناسب نیستند؛ زیرا در این محیط‌ها اطلاعات کافی در مورد موجودیت‌هایی که با یکدیگر تعامل دارند وجود ندارد، و منابعی که مورد دستیابی قرار می‌گیرند همیشه از قبل شناخته‌شده نیستند. بنابراین، مجوزهای دسترسیِ از پیش‌تعریف‌شده برای یک موجودیت، تقریباً غیرممکن است. از این‌رو، با توجه به تکیه این مدل‌ها بر احرازهویتِ کاربران، و به دلیل فقدان انعطاف‌پذیری و کارآیی آن‌ها، این مدل‌ها برای محیط‌های شبکه‌ای باز و پویا مناسب نیستند. مدل‌های کنترل دسترسی در این محیط‌ها باید قادر باشند، خود را با افزایش و کاهش پویای موجودیت‌ها تطبیق دهند. از این‌رو، به‌عنوان یک راه‌کار اساسی، ترکیب مدل‌های کنترل دسترسی با سازوکارهای مذاکره اعتماد، به منظور تأمین امنیت داده‌های حیاتی سازمان و پدافند در برابر دسترسی‌های غیرمجاز، بسیار ضروری و اساسی است. در این فرایند، مذاکره برای اعتماد، مقدم بر ارزیابی کنترل دسترسی در نظر گرفته می‌شود، زیرا مذاکره امکان می‌دهد جمع‌آوری منابع لازم برای برقراری سطح مورد نیاز از اعتماد انجام شود و موفقیت برای ارزیابی کنترل دسترسی را امکان‌پذیر سازد [۷].



شکل ۱- همکاری فراسازمانی سرویس‌ها در یک محیط محاسباتی سرویس‌گرا [۲]

در این مقاله، مذاکره برای برقراری اعتماد، به منظور پدافند در مقابل ارائه اطلاعات نادرست و نیز مدیریت کنترل دسترسی به منابع، در بستر معماری استاندارد XACML[4] فراهم شده است. مدل پیشنهادی، مذاکره اعتماد خودکار[5] در مرزهای سازمانی، بین موجودیت‌ها از دامنه‌های امنیتی مختلف را امکان‌پذیر می‌سازد. رویکرد مذاکره اعتماد خودکار، توسط وینزبروخ و همکاران پیشنهاد شده است، که هدف آن ایجاد رابطه اعتماد تدریجی بین افراد ناشناس از طریق آشکارسازی تدریجی اعتبارنامه‌ها[6] و سیاست‌های امنیتی است [۸و۹]. در مذاکره اعتماد خودکار، وضعیت مشارکت‌کنندگان 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 قرار می‌دهند. از طرفی، این سازوکار می‌تواند کاربران را جهت آشکار کردن اطلاعات برای ایجاد رابطه اعتماد متقابل به دقت راهنمایی کند. با استفاده از سازوکار مذاکره اعتماد خودکار، طرفین مذاکره قادر خواهند بود با تبادل دوطرفه سیاست‌ها و اعتبارنامه‌ها، مذاکره برای دسترسی به منابع سیستم از قبیل داده‌ها و سرویس‌ها را انجام دهند. این مدل همچنین، آشکارسازی سیاست توسط طرفین مذاکره را بر اساس الزامات مذاکره جاری، ساماندهی می‌کند. این سیاست‌ها تعیین می‌کنند چه ترکیبی از اعتبارنامه‌های یک شخص باید ارائه شود تا دسترسی لازم به یک منبع حفاظت‌شده از سرویس مورد نظر حاصل گردد. با این روش،

1- Discretionary Access Control (DAC)
2- Mandatory Access Control (MAC)
3- Role Based Access Control (RBAC)
4- eXtensible Access Control Markup Language
5- Automatic Trust Negotiation
6- Credentials

امکان تمرکز روی مذاکره و آشکارسازی تدریجی اطلاعات موردنیاز بین طرفین ممکن می‌شود [۱۰]. بدیهی است در این روش، اعتماد به‌صورت تدریجی برقرار می‌شود، و سیاست‌های دربرگیرنده اعتبارنامه‌های حساس، به غریبه‌ها و افراد ناشناس آشکار نمی‌شوند. وقتی اعتماد برقرار شد، اعتبارنامه‌های حساس در صورتی که توسط سیاست اجازه داده شود، آشکار می‌شوند.

این مقاله به‌صورت زیر سازماندهی شده است: در بخش ۲، به بیان مفاهیم اصلی مذاکره و کنترل دسترسی پرداخته می‌شود. در بخش ۳، شرح مختصری از معماری XACML ارائه می‌شود. در بخش ۴، معماری پیشنهادی به تفصیل توضیح داده می‌شود. در نهایت، در بخش ۵، نتیجه‌گیری حاصل از مقاله و کارهای آینده ارائه می‌گردد.

۲- مفاهیم اصلی مذاکره و کنترل دسترسی

معمولاً هر ارائه‌دهنده سرویس، یک سیاست کنترل دسترسی دارد که تعریف می‌کند چه کسی به کدام منبع و برای چه هدفی دسترسی دارد. این سیاست‌ها، مجموعه‌ای از شرایط لازم برای درخواست‌کنندگان منابع را تعریف می‌کند؛ به گونه‌ای که ارائه‌دهنده سرویس می‌تواند در مورد اجازه یا عدم اجازه دسترسی به منبع درخواست‌شده، تصمیم بگیرد. این شرایط، در واقع صفاتی هستند که از اعتبارنامه‌های درخواست‌کنندگان حاصل می‌شوند. اعتبارنامه، بیانیه‌ای است در مورد مالک خود، که توسط یک صادرکننده اعتبارنامه به‌صورت رقمی امضاء و تأیید می‌شود. 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، که توسط ارائه‌کنندگان سرویس (سازمان‌ها) تعریف می‌شوند، مورد استفاده قرار می‌گیرند. اعتبارنامه‌ها همچنین، در سیستم‌های برقراری اعتماد[1] که موجودیت‌ها قصد دارند بر اساس صفات به یکدیگر اعتماد کنند، از اهمیت خاصی برخوردارند [۱۱].

مذاکره، فرایندی است که گروهی از مشارکت‌کنندگان روی برخی موضوعات به توافق متقابل می‌رسند. اساساً در فرایند مذاکره سه مؤلفه وجود دارد [۱۲]:

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

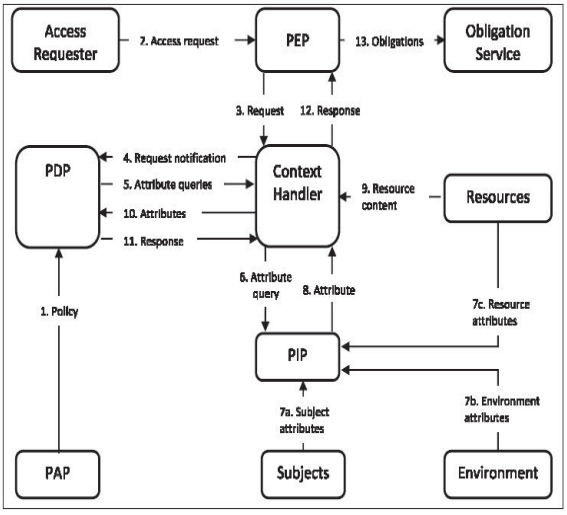
۲- اهداف مذاکره، طیفی از مسائل است که روی آن‌ها باید توافق حاصل شود.

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

براساس آنچه بیان شد، هدف اصلی از مذاکره اعتماد، دسترسی به یک منبع (وب سرویس) است که به‌عنوان یک منبع حفاظت‌شده در نظر گرفته می‌شود. این دسترسی ممکن است شامل مذاکره برای 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 مورد نظر چیست. درخواست‌کننده و ارائه‌دهنده سرویس، هر کدام 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. این سازوکارها، وسیله پدافند در قبال ارائه اطلاعات نادرست یا غیر ضرور توسط طرفین تعامل را فراهم می‌سازد.

۳- معماری کنترل دسترسی XACML

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 از این‌رو فهم و پیاده‌سازی آن، راحت و اتصال آن به ابزارها و فناوری‌های مختلف آسان است.



شکل ۲- جریان سطح بالای معماری XACML [۱۳]

1- Trust Establishment (TE) Systems

شکل (۲)، جریان داده سطح بالای این معماری بر اساس استاندارد OASIS را نشان می‌دهد که شامل رابط‌ها و مؤلفه‌های[1] مختلف برای اتخاذ تصمیمات مجوز دسترسی است. همچنین جدول (۱)، شرح مختصری از هر یک از مؤلفه‌های شکل (۲) را ارائه می‌دهد.

جدول ۱- خلاصه‌ای از شرح مؤلفه‌های جریان داده سطح بالای معماری XACML [۱۳]

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 قابل دسترس 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 براساس 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.

1- components

این معماری براساس 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 مورد استفاده قرار گیرد. زبان درخواست/پاسخ، امکان می‌دهد سئوالی در مورد این‌که آیا عمل مورد نظر روی منبع مورد نظر اجازه داده می‌شود یا خیر، شکل می‌گیرد و نهایتاً پاسخ به این سئوال ارائه می‌شود. پاسخ ارائه‌شده باید شامل یکی از این چهار گزینه باشد: ۱- اجازه دادن[3] (دسترسی مجاز است) ۲- رد کردن[4] (دسترسی غیرمجاز است) ۳- نامعین[5] (خطایی اتفاق افتاده یا برخی مقادیر موردنیاز از دست رفته است، لذا تصمیم‌گیری نمی‌تواند اتخاذ شود) ۴- غیرقابل اجرا[6]، این سرویس هیچ سیاستی برای اِعمال به این درخواست ندارد. بر اساس استاندارد OASIS (شکل ۲)، راه‌اندازی رایج یک درخواست چنین است که کسی یا فرایندی می‌خواهد چندین عمل معین را روی یک منبع انجام دهد. بنابراین، درخواست مورد نظر به مؤلفه‌ای به نام نقطه اجرای سیاست (PEP) که عملاً از آن منبع حراست می‌کند ارسال می‌شود (مرحله ۲). مؤلفه PEP، درخواستی با قالب[7] محلی خود، مبتنی بر «صفات درخواست‌کننده»، «منبع درخواست‌شده»، «عمل موردنظر» 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 هستند (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، ۹) اجرا شده و اطلاعات لازم را به مؤلفه PDP ارسال می‌کند (مرحله ۱۰). در نهایت، مؤلفه PDP سیاست را ارزیابی و پاسخ را در مورد اعطاء یا عدم اعطاء دسترسی برمی‌گرداند (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 صدور مجوز یا عدم اجازه دسترسی به درخواست‌کننده، احتمالاً مجبور به انجام برخی اقدامات (مرحله ۱۳) باشد. فرایند کامل مراحل یادشده، در شکل (۲) نشان داده شده است.

2- Request/ Response
3- Permit
4- Deny
5- Indeterminate
6- Not Applicable
7- Format

۴- مدل پیشنهادی

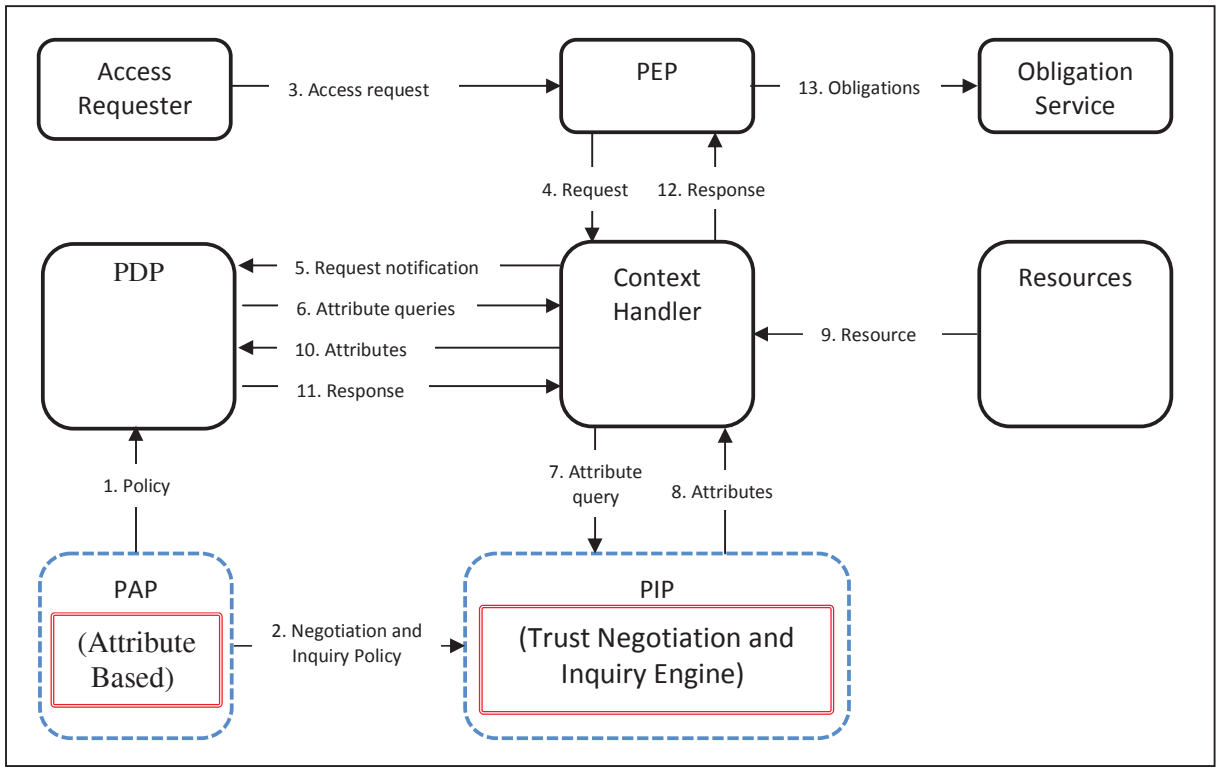
در این بخش، مدل پیشنهادی خود را با عنوان TACM[1] شرح می‌دهیم. این مدل، توسعه‌یافته است و برای تأمین نیازهای کنترل دسترسی، مؤلفه‌های PAP و PIP دست‌خوش اصلاح شده‌اند. در این مقاله، برای کنترل دسترسی موثر به منابع در محیط‌های سرویس‌گرا، به شیوه تعاملات بین درخواست‌کننده و ارائه‌دهنده سرویس جهت برقراری اعتماد و سپس کنترل دسترسی به منبع موردنظر، توجه خاصی معطوف شده است. این مؤلفه‌های توسعه‌یافته، در شکل (۳) با خط‌چین نشان داده شده‌اند.

برای نیل به اهداف مقاله، ساختار سیاست‌های کنترل دسترسی مورد استفاده در مؤلفه PAP توسعه داده شده است. این مؤلفه، متناسب با توسعه قابلیت‌های مدل پیشنهادی، با ساختار کامل بیان شده است و سیاست‌های مبتنی بر صفات را برای مؤلفه PDP تعریف می‌کند (فهرست ۱). این مؤلفه همچنین، علاوه‌بر تعریف سیاست‌های کنترل دسترسی مبتنی بر صفات برای مؤلفه PDP، تعریف «سیاست‌های مذاکره و استعلام»[2] را نیز بر عهده دارد. نمونه‌ای از ساختار NIP (سیاست مذاکره و استعلام) در فهرست شماره (۲) نشان داده شده است. در خط شماره ۳ این فهرست، قسمت «صفات»؛ در خط شماره ۷، قسمت «مراکز مورد اعتماد استعلام صفات» و در خط شماره ۱۸، قسمت «سیاست‌های استعلام صفات» تعریف شده‌اند.

فهرست ۱- نمونه ساختار یک Rule از سیاست کنترل دسترسی موجود در واحد PAP (مدل پیشنهادی)

```
1. <Rule RuleId="2" Effect="Permit">
2. <Target>
3. <Subjects>
4. <Subject>
5. <Attribute AttributeId="subject-id">
6. <AttributeValue>
7. <ALESIdentityAssertion>Professor</ALESIdentityAssertion>
8. </AttributeValue></Attribute>
9. <Attribute AttributeId="National_Code">
10. <AttributeValue>
11. <ALESIdentityAssertion>True</ALESIdentityAssertion>
12. </AttributeValue></Attribute>
13. <Attribute AttributeId="Abuse_History">
14. <AttributeValue>
15. <ALESIdentityAssertion>False</ALESIdentityAssertion>
16. </AttributeValue></Attribute>
17. <Attribute AttributeId="Tax_Pay">
18. <AttributeValue>
19. <ALESIdentityAssertion>True</ALESIdentityAssertion>
20. </AttributeValue></Attribute></Subject>
21. <Subject>
22. <Attribute AttributeId="subject-id">
23. <AttributeValue>
24. <ALESIdentityAssertion>Lecturer</ALESIdentityAssertion>
25. </AttributeValue></Attribute>
26. <Attribute AttributeId="National_Code">
27. <AttributeValue>
28. <ALESIdentityAssertion>True</ALESIdentityAssertion>
29. </AttributeValue></Attribute>
30. <Attribute AttributeId="Tax_Pay">
31. <AttributeValue>
32. <ALESIdentityAssertion>True</ALESIdentityAssertion>
33. </AttributeValue></Attribute>
34. <Attribute AttributeId="High-Risk Driving">
35. <AttributeValue>
36. <ALESIdentityAssertion>False</ALESIdentityAssertion>
37. </AttributeValue></Attribute></Subject></Subjects>
38. <Resources>
39. <Resource> Grades </Resource>
40. <Resource> Records </Resource></Resources>
41. <Actions>
42. <Action> Change </Action>
43. <Action> Read </Action></Actions></Target></Rule>
```

1- Trust Negotiation-Based Access Control Model
2- Negotiation and Inquiry Policy (NIP)



شکل ۳- جریان داده و مؤلفه‌های مدل پیشنهادی

قسمت «صفات»، حاوی مجموعه‌ای از انواع صفات قیدشده در سیاست کنترل دسترسی و نیز انواع صفات مورد سؤال از «مراکز مورد اعتماد استعلام صفات» است که به همراه هر صفت، نوع داده‌ای[1] آن نیز مشخص شده است. قسمت «مراکز مورد اعتماد استعلام صفات»، شامل مجموعه‌ای از مراکز استعلام مورد توافق با سازمان متبوع است که خدماتی جهت استعلام صحت صفات مورد ادعای «درخواست‌کننده» ارائه می‌دهند. در این قسمت به ازای هر مرکز استعلام، خدمات ارائه‌شده آن مرکز به همراه پیش‌نیازهای ارائه هر خدمت نیز مشخص شده است. به‌عنوان مثال، اگر بخواهیم ملّیت و تابعیت یک درخواست‌کننده را از مرکز «ثبت احوال» استعلام کنیم، حداقل پیش‌نیاز ارائه این خدمت، آن است که شناسه ملی به همراه تابعیت مورد ادعای 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 صحت آن صفت مدون شده است. به‌عنوان مثال، در فهرست (۱) نمونه‌ای از ساختار یک Rule در سیاست کنترل دسترسی موجود در مؤلفه PAP نشان داده شده است. این ساختار، در مقایسه با آنچه در [۱۴] آمده است، در راستای اهداف مدل پیشنهادی، توسعه قابل توجهی یافته است.

همان‌طور که قبلاً اشاره شد در مدل پیشنهادی، مؤلفه PIP نیز شاهد تغییرات و اصلاحات شده است و آن نحوه پاسخ‌گویی به «پرس‌وجوی صفات» است. در معماری XACML، این مؤلفه برای انجام وظیفه خود از یک پایگاه داده ثابت و محلی و به‌عنوان تنها منبع مقادیر صفات استفاده می‌کند که عملکرد آن را به شدت 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 معتمَد، سطح اعتماد لازم در فرایند ارزیابی درخواست‌های دسترسی، با انعطاف و اطمینان بیشتری حاصل گردد.

از آنجایی که مدیریت و دسترسی لحظه‌ای به منابع اطلاعاتیِ موردنیاز برای اتخاذ تصمیم، یک مسئله حیاتی است، لذا وابستگی مؤلفه PIP به یک پایگاه داده ثابت و متمرکز، ضمن محدود کردن عملکرد آن، می‌تواند مشکلات و چالش‌های زیادی را به شرح زیر به‌وجود آورد:

1- Data type

2- Trust-Negotiation & Inquiry Engine

۱- عدم انعطاف‌پذیری در دسترسی به نیازهای جدید به دلیل گسترش روزافزون سیاست‌های کنترل دسترسی.
۲- ایجاد نقطه شکست واحد[1] به دلیل تمرکز اطلاعات در یک بانک اطلاعاتی مرکزی.
۳- وابسته بودن پویایی مدل به‌روزرسانی پایگاه داده مرکزی که معمولاً هر لحظه امکان‌پذیر نیست.
۴- ملاحظات و چالش‌های امنیتی خاص برای حفاظت از داده‌های متمرکز.

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

مؤلفه PIP به‌صورت پویا و برخط[2]، و به جای 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 علاوه‌بر بهره‌گیری از نظرات چندین مرکز معتمَد، در صورتی که یکی از این مراکز قابل دسترس نباشد، عملکرد مدل هیچ‌گاه مختل نخواهد شد. همچنین، نیازی به پایگاه داده داخلی برای ذخیره‌سازی و مدیریت صفات مربوط به نهادهای مختلف وجود ندارد و یا اگر بنا به دلایلی نیاز به وجود چنین پایگاه داده‌ای باشد، وابستگی کامل مدل به این پایگاه مرتفع می‌شود.

به این ترتیب، با امکان به‌روزرسانی سیاست‌های کنترل دسترسی از یک سو، 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 «پرس‌وجوی صفت» چگونه استنتاج می‌گردد؟

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

فهرست ۲- ساختار NIP در مدل پیشنهادی

```
<? XML version="1.0" encoding="utf-8"?>
<NegotiationInquiryPolicySet>
<Attributes>
<AttributeInquiryPolicy id="National_Code" dataType="string"/>
<AttributeInquiryPolicy id="Nationality" dataType="string"/>
<AttributeInquiryPolicy id="Absuse_History" dataType="bool"/></Attributes>
<TAICList>
<TAIC id="Judiciary" ServiceUrl="http://localhost:20222/JS.asmx" caption="قوه قضاییه">
<Methods>
<Method id="Has_Absuse_History">
<Parameters>
<Parameter AttributeId=" Absuse_History "/>
<Parameter AttributeId="National_Code"/></Parameters></Method>
<Method id="IsNationality">
<Parameters>
<Parameter AttributeId="National_Code"/>
<Parameter AttributeId="Nationality"/></Parameters></Method></Methods></TAIC></TAICList>
<AttributeInquiryPolicies>
<AttributeInquiryPolicy attributeId="National_Code">
<Step stepId="0">
<statement id="direct">
<condition TAICid="RegistrationOrganization" MethodId="IsTrustedNationalCode"/>
</statement></Step>
<Step stepId="1">
<statement id="each">
<condition TAICid="PoliceForce" MethodId="IsTrustedNationalCode"/>
<condition TAICid="TrafficPolice" MethodId="IsTrustedNationalCode"/>
<condition TAICid="HigherEducationOrganization" MethodId="IsTrustedNationalCode"/>
</statement></Step></AttributeInquiryPolicy>
<AttributeInquiryPolicy attributeId=" Absuse_History ">
<Step stepId="0">
<statement id="each">
<condition TAICid="Judiciary" MethodId="Has_Absuse_History "/>
<condition TAICid="PoliceForce" MethodId="Has_Absuse_History "/>
</statement></Step></AttributeInquiryPolicy></AttributeInquiryPolicies></NegotiationInquiryPolicySet>
```

1- Single Point of Failure 2- Online

با این حال، با توجه به اهداف و عملکرد مدل پیشنهادی و به‌منظور جمع‌بندی و نتیجه‌گیری نهایی، یک ارزیابی تحلیلی برای مقایسه مدل پیشنهادی و مدل استاندارد 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 مقایسه با مدل کنترل دسترسی استاندارد XACML، عملکرد منعطف‌تری از خود نشان می‌دهد. همچنین، باید توجه داشت که توسعه‌پذیری و کارآیی مدل پیشنهادی، در توازنی با اهداف مورد نظر و بهره‌گیری از قابلیت‌های اضافه‌شده، دچار خلل نخواهد شد. لازم به ذکر است در مدل پیشنهادی، برای غلبه بر چالش‌های امنیتی پیش‌رو، و با در نظر گرفتن ویژگی محیط‌هایی که دارای اطلاعات حساس و حیاتی هستند، می‌توان از رویکردهای مختلف فنون نمایندگی[1] مطرح در [۱۵] استفاده نمود.

۵- نتیجه‌گیری و کارهای آینده

در این مقاله، مدل کنترل دسترسی TACM، در بستر معماری XACML با تلفیق ساختار توسعه‌یافته سیاست‌های کنترل دسترسی و سازوکارهای مذاکره اعتماد معرفی گردید. مدل پیشنهادی، برای سیستم‌های پویای فراسازمانی ارائه شده است که در آن، موجودیت‌ها در فرایند دسترسی به منابع متعلق به حوزه‌های امنیتی مختلف درگیر هستند و قبل از انجام تعاملات، نیازمند برقراری اعتماد می‌باشند. در مدل پیشنهادی، مذاکره پویا بر اساس استعلام از چندین مرکز اطلاعاتی قابل اعتماد به‌منظور تایید اعتبارنامه‌های درخواست‌کنندگان سرویس، و نیز مدیریت کنترل دسترسی در چارچوب معماری XACML فراهم شده است. همچنین، برای پوشش کاربردپذیری و حفظ انعطاف‌پذیری مدل پیشنهادی، برخی از مؤلفه‌ها از قبیل PAP و PIP دستخوش تغییرات و اصلاحات اساسی شده‌اند. در مدل پیشنهادی، 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.

با توجه به عدم وجود «نقطه شکست واحد» در مدل پیشنهادی، و ارتباط همزمان با چندین مرکز استعلام، قابلیت دسترسی آن مطلوب و کاربردپذیری آن در محیط‌های واقعی برای توسعه دولت و تجارت الکترونیک بسیار مناسب است. به‌عنوان کار آینده، می‌توان مدل پیشنهادی را پیاده‌سازی و نتایج حاصل را پس از ارزیابی و آزمایش، در محیط‌های عملیاتی جهت بهبود و ارتقای تعاملات الکترونیکی در سطح اینترنت به‌کار گرفت.

جدول ۲- مقایسه ویژگی‌های مدل پیشنهادی و مدل استاندارد XACML

ردیف	ویژگی‌ها	مدل پیشنهادی	مدل استاندارد XACML	توضیح
۱	**انعطاف‌پذیری /مقیاس‌پذیری**	زیاد	کم	با توجه به توسعه عملکرد مؤلفه PIP در مدل پیشنهادی.
۲	**نقطه شکست واحد**	ندارد	دارد	با توجه به عدم وابستگی مدل پیشنهادی به پایگاه داده مرکزی.
۳	**وابستگی به روزآمدسازی اطلاعات صفات**	ندارد	دارد	با توجه به عدم وابستگی مدل پیشنهادی به پایگاه داده مرکزی.
۴	**وابستگی به تأییدیه صفات**	منابع گسترده	منابع محدود	در مدل پیشنهادی بر خلاف مدل استاندارد، اسناد تاییدیه صفات به اطلاعات داخلی و از قبل تعیین‌شده وابسته نیست.
۵	**قابلیت دسترسی**	زیاد	کم	با توجه به عدم وجود «نقطه شکست واحد» در مدل پیشنهادی، و ارتباط همزمان با چندین مرکز استعلام، قابلیت دسترسی آن مطلوب است.
۶	**کاربردپذیری[2]**	زیاد	کم	مدل پیشنهادی، برای محیط‌های واقعی از قبیل دولت الکترونیک بسیار مناسب است.

1- Proxy Techniques
2- Applicable

مراجع

1. Ahmed A. and Zhang N., "Towards the realization of context-risk-aware access control in pervasive computing", Telecommunication Systems Journal, pp. 127-137, (**2009**).
2. Jianxin L., Xudong L., Lu L., Dazhi S. and Bo L., "HiTrust: building cross-organizational trust relationship based on a hybrid negotiation tree", Springer Science +Business Media, (**2011**).
3. He J., Ma S. and Zhao B., "Analysis of Trust-based Access Control Using Game Theory", International Journal of Multimedia & Ubiquitous Engineering, Vol. 8, NO. 4, pp. 15-24, (**2013**).
4. Snyder L., "Formal Models of Capability-Based Protection Systems", IEEE Trans. Computers., Vol. 30, No. 3, pp. 172-181, (**1981**).
5. Bell D. E. and LaPadula L., "Secure Computer Systems: A Mathematical Model", Mitre Corporation, Bedford, MA, (**1973**).
6. Sandhu R. S., Coyne E. J., Feinstein H. L. and Youman C. E., "Role-based Access Control Models", Computers, Vol. 29, No. 2, (**1996**).
7. Haidar D. A., Boulahia N. C., Cuppens F. and Debar H., "XeNA: an access negotiation framework using XACML", Institut TELECOM and Springer-Verlag, (**2008**).
8. Winsborough W. H., and Li N., "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**).
9. Winsborough W. H., Kent E. S. and Vicki E. J., "Automated trust negotiation", In DARPA Information Survivability Conference and Exposition, Hilton Head, SC, Vol. 1, pp. 88-102, (**2000**).
10. Tatyana R., Li Z., Clifford N., Travis L. and Kent E. S., "Adaptive Trust Negotiation and Access Control", SACMAT, (**2005**).
11. Trevor J., "SD3: A Trust Management System with Certified Evaluation", In IEEE Symposium on Security and Privacy, Oakland, CA, (**2001**).
12. Adam J. L., Winslett M. and Kenneth J. P., "TrustBuilder2: A Reconfigurable Framework for Trust Negotiation", IFIP International Federation for Information Processing, (**2009**).
13. Abhinav G., "Extending XACML Access Control Architecture to Decouple Authorization Decisions from Enterprise Applications", Sapient Global Markets, (**2012**).
14. Liu A. X., Chen F., Hwang J. and Xie T., "XEngine: A Fast and Scalable XACML Policy Evaluation Engine", ACM, (**2008**).
15. Kuyoro S. O., Ibikunle F. and Awodele O., "Cloud Computing Security Issues and Challenges", Security, Nigeria, Vol. 9, (**2011**).

TACM: A Trust Negotiation Based Access Control Model to The Organization's Critical Data Using Passive Defense Approach

A. Karimi[1]

M. Saleh Esfahani[2]

M. R. Hasani Ahangar[3]

B. Alizadeh[4]

Abstract

In broad cross-organization environments, establishing trust among distributed services, has become a basic need. Access control and provision of data security, are notable challenges in these environments. Due to different security policies in inter-organizational environment, traditional access control mechanisms are often unable to satisfy users' security requirements. Trust negotiation is a crucial 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 with passive defense approach based on trust negotiation mechanisms with XACML standard architecture to overcome aforementioned challenges is proposed. The model can overcome aforementioned challenges by obtaining necessary level of trust for users before processing their requests to access designated resources. Performance and flexibility of our model show that its applicability is more convenient for development of e-interactions over the internet.

Key Words: *Access Control, Trust Negotiation, XACML Architecture, Security Policies*

1- Instructor and Academic Member of Imam Hussein Comprehensive University (akarimi@ihu.ac.ir) - Writer in Charge
2- Assistant Professor and Academic Member of Imam Hussein Comprehensive University (msaleh@ihu.ac.ir)
3- Associate Professor and Academic Member of Imam Hussein Comprehensive University (mrhassani@iust.ac.ir)
4- MS Candidate of Information Security