مجلـه‌ی علمی پژوهش در علوم رایانه ، شماره ۳ ، پاییز ۱۳۹۵، ص ۵۳-۴۲

ISSN: 2745-3673
http://www.Rcsj.ir

مجله‌ی علمی پژوهش در علوم رایانه (سال دوم)
شماره ۳ / پاییز ۱۳۹۵ / ص ۵۳-۴۲

ارائه رویکردی برای مدیریت دسترسی به فرایندها در برنامه های کاربردی بر اساس مدل AAA

محمود جزایری[۱]، افشین رضاخانی[۲]، لیلا ریخته چی[۳]

[۱] دانشجوی کارشناسی ارشد ، دانشگاه آزاد اسلامی واحد بروجرد

[۲] عضو هیئت علمی ، دانشگاه آیت الله بروجردی

[۳] عضو هیئت علمی، دانشگاه آزاد اسلامی واحد بروجرد

نام و نشانی ایمیل نویسنده مسئول:

محمود جزایری

mah_jazayeri@yahoo.com

چکیده

افزایش تعداد سرورهای شبکه در پی راه اندازی سرویس های مختلف، پایگاه داده های مختلف کاربران و سیاست های متنوع، دسترسی افراد را به منابع مختلف ایجاد خواهد کرد بطوریکه پس از مدتی جهت اضافه کردن کاربر جدید به سیستم، نیاز به تعریف آن در چندین سرور وجود خواهد داشت. این پراکندگی و لزوم اعمال سیاست های متمرکز ،مدیران شبکه را ناچار به اتخاذ تدابیری مؤثرتر می کند لذا تعریف و پیاده سازی AAA سرور یکی از این تدبیرهاست که بر دسترسی کاربران به منابع شبکه ، مدیریت مستقیم و متمرکز نظارت خواهد داشت. AAA سرور یک برنامه نرم افزاری سرور است که امکان دسترسی کاربران را با منابع کامپیوتری شبکه برقرار می کند. این برنامه برای شبکه های اینترپرایز سرویس های احراز هویت ، احراز محوز و حسابداری را فراهم می آورد. در واقع AAA سروربا دسترسی شبکه ، پایگاه داده ها و جدول های اطلاعاتی کاربران در تعامل است.یکی از مسائلی که می توان به عنوان یک چالش پیش رو در مقوله امنیت از آن یاد کرد مدیریت دسترسی در سطح فرایندهای نرم افزاری است. در این پایان نامه رویکردی جدیدی ارائه می گردد تا بتوان مدیریت دسترسی به نرم افزارها را با استفاده از مدل AAA در سطح اپلیکیشن ها انجام داد. به عبارت دیگر در این پایان نامه راهکاری ارائه می گردد که مدیریت دسترسی به اپیکیشن ها بر اساس ماژول طراحی شده بر اساس مدل AAA بیان گردد. فرایندهای مورد استفاده برای کاربرد ها مشخص شده و بر اساس سیاستهای تعریف شده برای کاربران، اجازه دسترسی فرایندها به منابع صادر می گردد.

واژگان کلیدی: احراز هویت - امنیت - سیاست های امنیتی - کنترل دسترسی - AAA

ISSN: 2745-3673
http://www.Rcsj.ir

مقدمه

- یک روش خوب و جامع برای کنترل دسترسی در فرآیندهای کسب و کاری باید حداقل دارای خصیصه‌های زیر باشد:
- سادگی و قابل فهم بودن روش هایی که با کنترل دسترسی ها در ارتباط است
- کارائی بالا
- قابلیت توسعه
- سرعت بالا در دستیابی به سیاست‌ها و داده‌ها
- ایجاد کنترل دسترسی در پایین‌ترین سطوح

در این مقاله به ارائه مدل پیشنهادی جهت فرآیندهای کسب و کار که با کنترل دسترسی ها در ارتباط است می پردازیم. مدل پیشنهادی که بر پایه سیستم های فرآیندگرا می باشد یک روش خوب و جامع برای فرآیندهای کسب و کار است. این مدل به ما معرفی می کند ساختار جدیدی از مدیریت فرآیندها را با استفاده از قابلیت های نرم افزاری که تحت عنوان BPM[1] بیان می شود، در کنترل دسترسی با استفاده از BPM به تولید نرم افزار پرداخته می شود، یعنی فرآیندهای کسب و کار که در گذشته روی کاغذ بصورت دستی مدل می شد با استفاده از نرم افزارهای تولید شده با فرآیندهای کسب و کار در کنترل دسترسی ها، اجازه دسترسی داشتند. همچنین با استفاده از BPM رویکردهای مختلفی را می توان در فرآیندهای سازمانی اجرایی نمود که در حال حاضر، BPM چارچوبی مناسب برای فعالیت های فرآیند محور است و می تواند پیامدهای مثبت قابل توجهی را برای شرکت ها، موسسات و .... به همراه آورد. برای موفق بودن یک طرح از BPM، انتخاب فرآیندهای مناسب بسیار مهم است. از دیدگاه فرآیند کسب و کار، فرآیندگرایی ابزار ارتباطی مورد نیاز کسب و کار در سراسر سازمانها می باشد. در ارزیابی BPM در حدود ۱۰ الی ۱۵ سال قبل سازمانها شروع به یکسان سازی سیستم ها خصوصا در بخش صنایع و طبقه بندی کردن بوسیله یکپارچه سازی و تاسیس فرآیندها از طریق مسیریابی و تبادل داده ها، ردیابی وقایع، خودکارسازی فرآیندها و وفق دادن آنها نمودند. از طریق برنامه ریزی منابع شرکت(ERP)، مدیریت ارتباط با مشتری(CRM)، مدیریت زنجیره ای منابع(SCM)، شرکتهای کوچک توانستند بطور چشمگیری رشد کنند. آنها سیستم های مبادله ای خود را با نرم افزار ERP از طریق خودسازی ارتقاء دادند در حالی که شامل اطلاعاتی از نرم افزار مدیریت ارتباط با مشتری بود .

۱- فرآیندهای کسب و کار

در چند دهه اخیر همواره تاکید بر بحث فرآیندها و تفکر فرآیندگرایی سازمانها بوده است و بحث فرآیندها و مدیریت فرآیندها بحث جدیدی نیست اما صنعت فناوری اطلاعات و ارتباطات تا قبل از ظهور فناوری جدید مدیریت فرآیندهای کسب و کار(که از این پس آن را BPM می خوانیم) از ارائه بستر و راه حلی جامع و شایسته برای تحلیل، تعریف، اجرا، کنترل، بهسازی و فرآیندهای سازمانی ناتوان بوده است. با ظهور BPM که در آگوست سال ۲۰۰۱ برای فرآیند های کسب و کار تشکیل و بوجود آمد، تحقیق عملی بسیاری از دیدگاههای آکادمیک مطرح شده در طی این سالها امکانپذیر شد و فناوری اطلاعات و ارتباطات که در اینجا نیز نقش استراتژیک(بعنوان یک توانمندساز) و نقش ابزاری خود(ابزارهای مدیریت فرآیند کار) را در تحقیق این فناوری BPM به شایستگی نشان داد.اکثر تغییراتی که در حوزه فناوری بوجود آمده اند، باعث ترقی و رشد(تدریجی) در شیوه انجام کارها شده اند. اما این اواخر هر از گاهی با ظهور یک فناوری جدید روبرو بوده ایم که باعث تغییراتی اساسی و بنیادی در حوزه کسب و کار شده است. مانند اینترنت(یا بطور خاص تر فناوری وب و پست الکترونیک) که یکی از اینگونه فناوریها بوده اند. ما بر این باوریم که BPM هم یکی دیگر از این نوع فناوریهاست. پیشرانه های فناوری BPM تکنیکی نیستند، بلکه اقتصادی و مربوط به حوزه کسب و کار می باشند. استراتژی "سیستم های فرآیندگرا" راه حلی مناسب و کارآمد جهت دستیابی به مهارتها و سرمایه مورد نیاز جهت رقابت در بازارهای جدید و جهانی امروز است. برای موفقیت در پیاده سازی این استراتژی، یک بنگاه تجاری باید خود را آماده پذیرش همکاران و تعامل با شرکای تجاری خود نماید. فاکتورهایی همچون موارد ذیل در این بحث مطرح می شوند؛ محصولات، مارکها و قیمت محصولات، بازرهای در دسترس، توان مالی، کارکنان مناسب، دستاوردها و .....فرآیندهای کسب و کاری ترکیبی از مجموعه فعالیت ها و اقدامات مرتبط با همدیگر هستند که یک خروجی بخصوص را ایجاد می نمایند. در مستندات

[1] Business Process Management

ISSN: 2745-3673
http://www.Rcsj.ir

مدیریت فرآیندهای کسب و کاری به عنوان یک اقدام E2E[۲] تعریف می شود که سبب ایجاد ارزش برای مشتریان سازمان می شود. ایجاد ذهنیت و تصویر کلی از عملیات E2E در سازمان امری ضروری است، چرا که فرآیندهای E2E شامل کلیه فعالیت های سازمان می باشند و از میان همه محدودیت های افقی در سازمان عبور می کنند و جهت ارائه خدمات و سرویسهای کامل از دیدگاه سازمان به مشتریان آن ضروری هستند.همچنین در مدیریت فرآیند های کسب و کار که یک روش سازمان یافته و نظام مند هستند که به منظور تعریف، طراحی، ایجاد، مستندسازی، اندازه گیری، پایش و کنترل کلیه فرآیندهای کسب و کار مکانیزه، به منظور دستیابی به نتایج هدف گذاری شده همسو با اهداف استراتژیک سازمان می باشد که بصورت زیر می باشند:

- مدیریت فرآیند کسب و کار یک راهکار مدیریتی و بر مبنای فناوریهای قابل دسترس می باشند.
- مدیریت فرآیند کسب و کار، شامل مدلسازی، تجزیه و تحلیل، طراحی و اندازه گیری فرآیندهای کسب و کار در یک سازمان است.
- مدیریت فرآیندهای کسب و کار یک فناوری است که حاوی ابزارهای لازم برای مدلسازی، شبیه سازی، مکانیزاسیون، یکپارچه سازی و کنترل و پایش فرآیندهای کسب و کار و نیز سیستم های اطلاعاتی می باشد که قادر به پشتیبانی این فرآیندها می باشد.

انواع فرآیندها در محیط کسب و کاری را می توان به سه نوع زیر تقسیم کرد که سه نوع فرآیندکسب وکاروجوددارد :

- فرآیندهای مدیریتی :این فرآیندهافعالیتهای نظام مند مثل: مدیریت راهبردی ونحوه اداره سازمان راحمایت میکنند.
- فرآیندهای عملیاتی(اصلی) :این فرآیندها ارزشی را در راستای کسب وکاراصلی سازمان ایجاد می کنند مثل خرید، تولید، بازاریابی وفروش.
- فرآیندهای پشتیبانی : این فرآیندها،فرآیندهای عملیاتی راپشتیبانی می کنند. مثل حسابداری، استخدام وفناوری اطلاعاتی که فرآیندزمانی کارایی لازم راخواهدداشت که بصورت درست انجام گیرد و زمانی از اثربخشی برخوردارخواهدبودکه بصورت درست انتخاب وطراحی شده باشد .فرآیند، معرفی دسته ای ازفعل وانفعالات است که به منظورتبدیل داده ها(ورودیها) به محصولات(خروجیها) انجام می گیرد.

دریک تعریف خلاصه میتوان گفت که فرآیند، یکسری منطقی ازتراکنشهای مرتبط بایکدیگرمی باشدکه ورودیهارابه نتایج یاهمان خروجیهاتبدیل میکند. که در شکل زیر یک فرآیند منطقی از تراکنش های مرتبط را نشان می دهد.

۱-۱- گامهای پیاده سازی BPM در یک سازمان

۱ - طراحی مدل فرآیند

ایجاد دیاگرام فرآیندها براساس الگوهایی ازقبیلBPMN :

واردکردن فرآیندهای ایجادشده از سایرسیستمهای پشتیبانی کننده XPDL مانند ویزیو۳

- شکست یک فرآیند بزرگ یا پیچیده به چندزیرفرآیند
- ایجاد مستندات کامل براساس فرآیندهای ایجاد شده درقالبهای ورد۴، پی دی اف۵، ویزیو

۲- طراحی مدل داده

- ایجاد موجودیت ها و صفت های مورداستفاده برای نگهداری اطلاعات موردنیاز
- خواندن ونوشتن اطلاعات درسایرپایگاه داده ها با ابزار موجودیت مجازی۶
- نوشتن اطلاعات درسایرپایگاه داده ها۷

۳- طراحی فرمها

- ساخت المانهای
- فرمهاباستفاده ازمؤلفه های تعریف شده درمدل داده

---

[۲] به معنی مبادله به مبادله است، مثلا در تجارت الکترونیکی که در این مدل مبادلات الکترونیکی بطور رسمی برای اهداف مبادله اطلاعات به یکدیگر متصل می شوند.

[3] Visio
[4] Word
[5] PDF
[6] Virtualized Entity
[7] Replicated Entity

ISSN: 2745-3673
http://www.Rcsj.ir

- تعیین ارتباط اجزای فرم بافیلدهای موجودیتهای تعریف شده

۴- تعیین قواعدکسب وکار

- تعیین شروط،محدویتهاوقواعدکاری ازقواعدساده تابسیارپیشرفته برای تعیین مسیریابی فرآیندها

۵- تعیین ایفاکنندگان فعالیتها

- اختصاص هرکدام ازفعالیتهای یک فرآیندبه کاربرانی خاص
- انواع روشهای تخصیص کار:

اول در دسترس[8]: ارسال کاربه اولین شخصی که کارتابلش فعال باشد.

بوسیله بارگذاری:[9] براساس سنجش کارهای موجوددرکارتابلهاواختصاص کاربه شخصی که کارکمتری در کارتابلش موجود می باشد.

- ارسال همزمان کاربه کارتابل گروهی ازپرسنل وحذف آن از کارتابل سایرین درصورت بازشدن توسط یک نفر از آنها
- تعیین نفربعدی انجام دهنده فعالیت برروی کارتعریف شده توسط نفرقبلی
- تخصیص کاربه صورت دستی

۶- یکپارچگی باسایرسیستمهای پایگاههای داده

- اتصال سیستمهای سازمانی به یکدیگربرای بالابردن سطح یکپارچگی باسایرسیستمهای کاربردی سازمان در حین فرآیندبا استاندارد وب سرویس[10]
- امکان درج و فراخوانی اطلاعات بین پایگاه داده های مختلف به شکل دوطرفه
- عدم نیازبه ورود به چند سیستم مختلف
- پرهیز از تعویض سیستمها بابرندهای متفاوت به منظورتامین یکپارچگی بین آنها

۷- اجرای فرآیند

- ورود به سیستم پس از دو روش تایید هویت توسط پایگاه داده یاتایید هویت توسط ویندوز[11]
- ورود به کارتابل جریان کار و مشاهده لیست فرآیندهای ارجاع شده
- انتخاب فرآیند مورد نظر و انجام امور مرتبط

۲- رویکرد پیشنهادی

در این قسمت به بررسی رویکرد پیشنهادی به صورت دقیق می پردازیم. ابتدا کلیات مدل پیشنهادی مورد بررسی قرار می گیرد و سپس اجزای مدل پیشنهادی بصورت دقیق توضیح داده شده و جزئیات آن مشخص می گردد.

۲-۱- کلیات

با مشاهده و بررسی سازمان‌های مختلف که با کسب و کارهای متنوع دیده می‌شود، کمتر توجهی به دادن نقش مدیریتی از طریق فرآیندهای کسب و کاری داده شده است. در این قسمت پیشنهاد می‌گردد مدیریت دسترسی کاربران سازمان به منابع سازمانی(سازمان‌های مبتنی بر فناوری اطلاعات) براساس فرآیندهای تعریف شده در آنها باشد. منابع سازمانی می‌تواند از تجهیزات شبکه مانند روتر و سوئیچ و سرورها گرفته تا برنامه‌های کاربردی و منوهای آن و همچنین جداول و رکوردها و فیلدها در پایگاه داده تعریف گردد. بنابراین پیشنهاد اصلی، ارائه رویکردی برای تدوین چارچوب مدیریت دسترسی به منابع در سازمان ها است که باید براساس فرآیندهای در حال اجرا در سازمان ها ارائه شود. و همانطور که می دانیم شرکت های بزرگ دنیا مانند اوراکل[12]، جاوا[13] ، نت[14] و موسسات تدوین استانداردها مانند گارتنر[15]بر اهمیت فرآیندهای کسب و کاری تاکید دارند. به عنوان مثال در این خصوص جاوا ، تنها برای تمام انواع

[8] First available
[9] By load
[10] Web Service
[11] Windows
[12] Oracle
[13] Java
[14] NET
[15] Garthner

ISSN: 2745-3673
http://www.Rcsj.ir

پروژهایی که مبتنی بر BPM بودند ارائه شد که به عنوان یک محیط یکپارچه توسعه یافته برای انواع مختلف پروژه ها طراحی شد که به این صورت، از طریق کدهای جاوا می توان به فرآیند BPM اجازه داد که جاوای تولید شده را توسط BPM سفارشی کرد و فرآیندهای کسب و کاری را از طریق کنترل دسترسی مدیریت کرد. به همین ترتیب دات نت [16]در ورژن ۲۰۱۳ به بعد BPM.NET را معرفی کرده است. در این ماژول فرآیندهای کسب و کاری را می توان بصورت وضعیت[17]ها و فعالیت ها رصد و مدیریت کرد و مشخص نمود که در هر فرآیند و در هر مرحله از آن چه اقداماتی انجام می گردد. به همین ترتیب گارتنر در مقایسه ای در سال ۲۰۱۵ به بررسی اهمیت فرآیندهای کسب و کاری در سیستم ها پرداخته است. به این صورت که با ارائه این مقاله به بهبود فرآیند کسب و کار کمک کرد که از مزایای کلیدی آن می توان به موارد زیر اشاره کرد:

- ❖ برای مهارت فن آوری های دیجیتال ارزش های جدید در فرآیندهای کسب و کاری ایجاد شده، که رشد و مزیت(فرآیندهای کسب و کاری) آنها را حفظ می کند.

ایجاد یک شالوده مهم بنام BPM که برای بهبود هرچه بهتر نتایج کسب و کار بوجود آمده است.

- ❖ تجربه رویکردهای عملی در جهان واقعی در سازمانها به چالش کشیده شده است.
- ❖ تغییر سازمانی منجر به بهره برداری از فرصت های جدید شده است.

همچنین گارتنر در این مقاله فرآیند کسب و کار را براساس IT بصورت حرفه ای مطرح کرد که برای تحول و نوآوری بوجود آمد. و با توجه به ارائه این مقاله توسط گارتنر مدیریت فرآیند کسب و کاری که شامل تجربه مستقل و تحقیقاتی است به تمامی دستورات فرآیندهای کسب و کاری رسیدگی خواهد شد و آدرس همه دستورات در فرآیندهای کسب و کار به تغییر ناگهانی مدیریت در مورد اینکه فرآیند BPM جدید است یا اینکه به سالها تجربه نیاز دارد دخیل می باشد. بنابراین برای بهبود و عملکرد تحول استراتژیک به پیشبرد و متمرکز شدن در مورد فرآیندهای کسب و کار می توان به موارد زیر اشاره کرد:

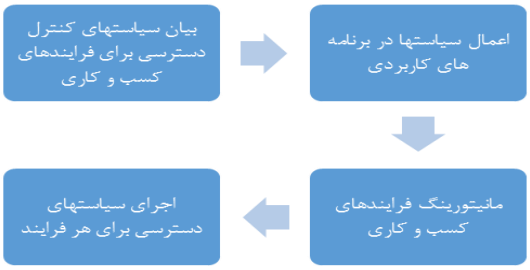
- ❖ افزایش تصویب تغییرات، بهبود و تعامل به همکاری با سازمان ها
- ❖ درخواست مدیریت جهت تصمیم گیری، پیش بینی و تجربه و تحلیل
- ❖ ساخت فرآیند کسب و کاری برای سرمایه گذاری
- ❖ پیاده سازی اطلاعات عملیاتی و فرآیندهای دقیق
- ❖ تاسیس روند موثر

بنابراین با توجه به توضیحات داده شده در این قسمت هدف این است که در سازمان هایی که فرآیندهایش براساس IT هستند(بستر شدن شبکه و کامپیوتر) بتوانیم سرور یا سرورهایی را مستقر بکنیم که بتوانند فرآیندهایی را که در حال انجام هستند در سازمان ها مدیریت و رصد کنند. که با مدیریت و رصد فرآیندها می توانیم دسترسی افراد را به منابع بهتر و کاراتر نموده و بتوانیم فرآیندها را بهبود دهیم. در حقیقت ما یک مدل کنترل و دسترسی ارائه می دهیم که دسترسی افراد را به منابع تجهیزاتی، دیتابیسها، اپلیکیشنها و منوهایی که در آینده خواهیم دید راحت و آسانتر خواهد کرد که آن ها براساس اینکه نقش ها در چه مرحله ای و در چه وضعیتی از سیستم ها قرار دارند و در چه سیستمی از فرآیندهای کاری هستند که در حقیقت هدف این است که بتواند دسترسی ها را ارائه دهد و یا اینکه بتواند آنان را مدیریت کند. در این قسمت به بررسی راهکار پیشنهادی می پردازیم.

هدف اصلی در این پایان نامه ارائه رویکردی است که کنترل دسترسی در برنامه های کاربردی بدرستی و با توجه به نیازمندی های امنیتی سازمان صورت پذیرد. مدیریت دسترسی افراد به برنامه های کاربردی بر اساس فرایندهای کسب و کاری خواهد بود. این بدان معناست که با توجه به اینکه چه فرایند کسب و کاری در حال انجام است ، دسترسی های مجاز به افراد صورت می پذیرد. بنابراین فرایند کلی پیشنهادی بصورت شکل زیر است.

[16] .NET
[17] State

ISSN: 2745-3673
http://www.Rcsj.ir



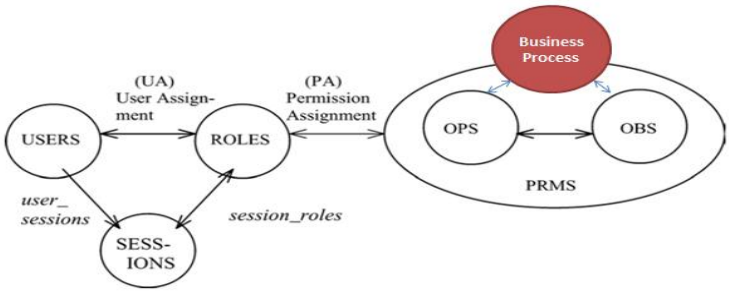
شکل۲-۱- فرایند پیشنهادی

همانطور که در شکل بالا دیده می شود ابتدا باید سیاستهای کنترل دسترسی با تاکید بر فرایندهای کسب و کاری تدوین گردد. پس از آن باید مجوزهای لازم برای هر فرایند مشخص گردد. سپس یک ماژول طراحی می شود که فرایندهای کسب و کاری را مانیتور کرده و به درخواستها بر اساس فرایندها پاسخگو باشد.

۲-۲- بیان سیاستهای کنترل دسترسی بر اساس فرایندها

همانطور که می دانیم در روش کنترل دسترسی مبتنی بر نقش، حق دسترسی ها بستگی به عملیاتی دارد که کاربران در سازمان می توانند انجام دهند. در این مدل مجوز ها به نقش های تعریف شده اختصاص داده می شوند و سپس نقش هر کاربر در سازمان مشخص می گردد. به عنوان مثال کاربر حسابدار یک شرکت، نقش حسابداری به او انتساب داده می شود از این طریق کاربر می تواند از مجوزهای تعیین شده برای نقش حسابدار ، استفاده نماید .بدین ترتیب اگر شرکت دارای چند حسابدار هم باشد، همه آنها دقیقا حق دسترسی های یکسانی خواهند داشت. کنترل کاربران در این مدل به سادگی امکان پذیر است، چرا که می توان به کاربران تنها با انتساب نقش جدید و یا انتقال به نقش دیگر، حق دسترسی های جدید داد. از طرفی با اختصاص دادن یک مجوز جدید به یک نقش و یا گرفتن مجوزی از یک نقش، تمامی کاربرانی که آن نقش به آنها انتساب داده شده است، موقعیت جدیدی در مورد حق دسترسی ها پیدا می کنند.

در مدل پیشنهادی ما، یک خصیصه به کنترل دسترسی نقش مبنا اضافه می گردد. این خصیصه فرایندی است که در حال اجرا است. بعبارت دیگر در بیان سیاستهای کنترل دسترسی علاوه بر نقش ، عامل فرایندکسب و کاری نیز وارد می گردد. بنابراین شکل زیر نشان دهنده جایگاه خصیصه پیشنهادی است که در بلوک پیشنهادی اضافه می گردد.



شکل ۲-۲- اضافه کردن بلوک جدید در مدل RBAC

همانطور که دیده می شود به مجموعه عوامل مدل کنترل دسترسی RBAC ، فرایندهای کسب و کاری نیز اضافه گردیده است. بنابراین هر نوع سیاست کنترل دسترسی باید فرایندها را نیز در خود جای دهد.

برای بیان سیاستهای کنترل دسترسی در مدل پیشنهادی از زبان XACML استفاده می شود. XACML یک زبان مبتنی بر XML برای کنترل دسترسی است که به وسیله کمیته فنی OASIS استاندارد شده است. XACML به عنوان یک روش واگذاری مجوز در جامعه معرفی شده است اگرچه XACML به عنوان یک رشته و به دنبال هم به وسیله OASIS در سال ۲۰۰۳ معرفی شد، اما نبود سازمان هایی که که با آن اقتباس شده است، هنوز وجود دارد.

این زبان که بر اساس زبان XML بوده، برای توصیف خط مشی های امنیتی به کار می رود. این زبان توسط بیش از سی و پنج شرکت بزرگ دنیا مانند IBM، Sun و ... برای توصیف سیاست های سازمانی بکار برده می شود. سناریوی کلی XACMLدر کنترل دسترسی به این صورت است که بررسی می کند آیا درخواست کننده مجاز به دسترسی به منبع خواسته شده است یا خیر. مدلی که این زبان استفاده می کند شامل دو قسمت اصلی محل اجرای خط مشی (PEP)[۱۸] و محل تصمیم گیری خط مشی (PDP)[۱۹] می باشد. برای

[18]Policy Enforcement Point

ISSN: 2745-3673
http://www.Rcsj.ir

انجام فرایند کنترل دسترسی ، محل اجرای خط مشی از محل تصمیم گیری خط مشی سئوال می کند و براساس پاسخی که دریافت می کند تصمیم به اخذ مجوز دسترسی یا عدم اخذ مجوز دسترسی می گیرد. فرایند دقیق انجام کنترل دسترسی در XACML به صورت زیر است:

ابتدا مدیر خط مشی امنیتی (PAP[۲۰]) ، خط مشی امنیتی را نوشته و در PDP قرار می دهد.

۱ -کاربر تقاضای درخواست خود را به PEP می فرستد.

۲ -PEP درخواست دریافت شده را به همان شکل به حامل محتوا[۲۱]ارسال می کند. البته اطلاعات دیگری نیز می تواند به حامل محتوا ارسال شود.

۳ -حامل محتوا یک درخواست XACML ایجاد کرده و آن را به PDP می فرستد.

۴ -PDP از حامل محتوا درخواست دسترسی به خصایای دیگری می کند.

۵ -حامل محتوا برای دسترسی به سایر خصایا یک درخواست به محل اطلاعات خط مشی ها (PIP)[۲۲] می فرستد.

۶ -PIP شروع به جمع آوری اطلاعات خواسته شده از حامل محتوا می کند.

۷ -PIP اطلاعات درخواست شده را به حامل محتوا ارسال می کند.

۸ -حامل محتوا اطلاعات دریافت شده از مرحله قبل را به علاوه سایر اطلاعات مورد نیاز به PDP ارسال می کند.

۹ -PDP بر اساس اطلاعات رسیده خط مشی های امنیتی را ارزیابی کرده و پاسخ محاسبه شده را مجددا به حامل محتوا ارسال می کند.

۱۰ -حامل محتوا نیز اطلاعات دریافت شده از PDP را به فرمت مناسب برای PEP تبدیل و آن را ارسال می کند.

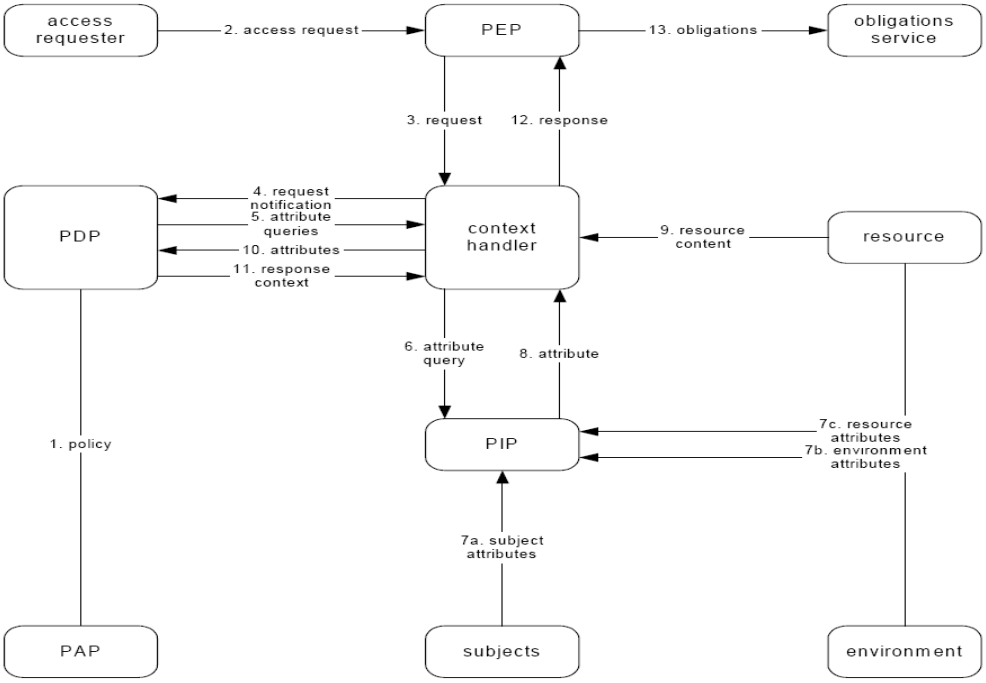
۱۱ -PEP نتیجه را اجرا می کند.

۱۲ -اگر جواب مثبت بود، PEP مجوز دسترسی به منبع درخواست شده را صادر می کند و در غیر این صورت عدم مجوز دسترسی صادر می گردد.

فرایند بالا در شکل زیر نشان داده شده است:

[19]Policy Decision Point
[20]Policy Administrator point
[21] Context Handler
[22]Policy Information Point

ISSN: 2745-3673
http://www.Rcsj.ir



شکل ۲-۳- سناریوی کلی کنترل دسترسی در XACML

۲-۳- اعمال سیاستها در برنامه های کاربردی

تا این قسمت تدابیری اندیشیده شد که سیاستهای کنترل دسترسی بر اساس فرایندهای کسب و کاری بیان گردد. با این کار مشخص خواهد شد که چه نقشهایی در چه فرایندهایی به چه منابعی دسترسی دارند. حال باید بتوان این سیاستها را بگونه ای در برنامه های کاربردی قرار داد که برای آن ها قابل شناسایی باشند. ما برای اینکار بلوکی را بصورت شکل زیر برای برنامه های کاربردی پیشنهاد می کنیم.

جدول ۲-۱- اضافه کردن بلوک جدید

نقش	فرایند	فعالیت	متد	مجوز
R1	P1	A1	M1	Get
R1	P1	A2	M1	Set
. . .				

همانطور که در جدول بالا دیده می شود باید مشخص گردد که چه نقشهایی در چه فرایندهایی ، چه مجوزهایی را دارا هستند. بعنوان مثال نقش r1 در هنگام انجام فرایند p1 ، اگر فعالیت A1 را انجام می دهد به متد M1 مجوز Get دارد. این در صورتی است که همین نقش اگر در فرایند p1 ، در حال انجام فعالیت A2 است ، به این متد (M1) مجوز Set داشته و می توانید مقادیری را تغییر دهد.

۲-۴- مانیتورینگ فرایندهای کسب و کاری

همانطور که دیده شد ، نوآوری مدل پیشنهادی، اضافه کردن بلوک فرایندهای کسب و کاری است. بنابراین باید بتوان فرایندها را مانیتور و رصد کرد تا در هنگام وجود یک درخواست، بتوان فرایندهای جاری در حال

اجرا را رصد کرد. بعنوان مثال فرض کنید از فرایندهای موجود در یک سازمان ، دو فرایند P1 و P2 بصورت زیر موجود باشد.

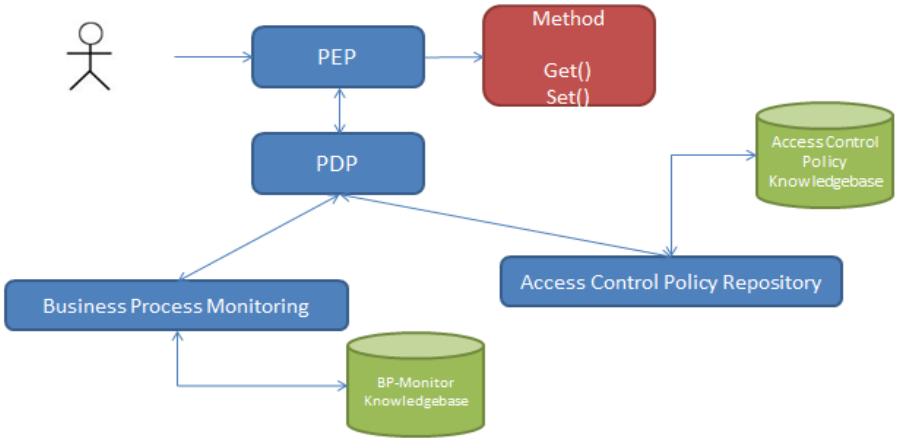
ISSN: 2745-3673
http://www.Rcsj.ir

شکل ۲-۴- فرایندهای نمونه

همانطور که دیده می شود این دو فرایند دارای n و m حالت هستند. حال فرض کنید دو کار در حال حاضر موجود در سیستم وجود دارد. در فرایند P1 ، یک کار در S11 قرار دارد و در فرایند P2 ، یک کار در حال انجام در S23 قرار گرفته اند. بنابراین باید بتوان این حالات و فرایندهای در حال اجرا را مانیتور نمود.

۲-۵- اجرای سیاستهای کنترل دسترسی

حال باید تدابیری اتخاذ گردد که هرگاه کاربری تقاضای منبعی را نمود ، بتوان بر اساس شرایط سیاستهای موجود ، برای آن کاربر ، مجوز / عدم مجوز دسترسی را صادر نمود. این کار بر اساس بهره گیری از جدول مانیتورینگ مطرح شده در بالا صورت می پذیرد. بلوک پیشنهادی این قسمت بصورت شکل زیر است.



شکل ۲-۵- بلوک پیشنهادی

ISSN: 2745-3673
http://www.Rcsj.ir

نتیجه‌گیری

امنیت فضای تبادل اطلاعات مقوله های مهمی هستند ولی به ندرت میزان حفاظت از داده ها و دارایی های اطلاعاتی شهروندان، شرکتها یا حکومت کافی و وافی است. زیرساخت شبکه، مسیریابها، کارگزاران نام و سوئیچهایی که این سیستمها را به هم متصل می کنند، نباید از کار بیفتند و گرنه کامپیوترها نمی توانند دقیق و مطمئن با هم ارتباط برقرار کنند. در اینجا پرسشهای متعددی مطرح می شوند: دقیقاً زیرساخت چیست، در برابر چه تهدیدهایی باید ایمن شود و چگونه می توان حفاظت را با هزینه بهینه فراهم کرد. ولی مبنای همه این پرسشها این است که چگونه سیستم امن را تعریف کنیم.

تفاوتهای میان نیازمندیهای یک دانشگاه و یک سازمان نظامی که کارهای رمزنگاری انجام می دهد را در نظر بگیرید. تفاوت اصلی در نحوه به اشتراک گذاردن اطلاعات است. دانشگاه نتایج پژوهشها (مقاله، گزارش و ...) را در اختیار عموم قرار می دهد. از طرف دیگر سازمان نظامی به محرمانگی اهمیت ویژه ای می دهد. نه تنها سازمان مایل به افشای نحوه شکستن الگوریتمهای رمز نیست، بلکه حتی نمی خواهد دیگران از شکسته شدن الگوریتم رمز آگاه شوند. بنابراین امنیت معنای ثابتی ندارد و این نیاز به تعریف امنیت را گوشزد می کند.

هنگامی که سازمانی بخواهد سیستمهای خود را امن کند باید نخست نیازمندیها را مشخص کند. دانشگاه نیاز به حفاظت از سلامت داده ها و تا حدی محرمانگی آنها- مانند نمرات- دارد. ضمناً ممکن است نیاز به دسترس پذیر بودن سیستم از طریق اینترنت برای دانشجویان و استادان داشته باشد. در مقابل سازمان نظامی به محرمانگی کلیه کارهای خود تأکید دارد. سیستمهای آن نباید از طریق شبکه در دسترس باشند. سلامت داده ها نیز مهم است ولی نه به اندازه محرمانگی آنها، یک سازمان نظامی ترجیح می دهد داده ها از بین بروند تا اینکه افشا شوند.

سیاست امنیتی

نیازمندیهای امنیتی مجاز بودن برخی اعمال (و حالتهای سیستم) را دیکته کرده و بقیه را غیرمجاز می دانند. یک سیاست امنیتی بیان خاصی است از آنچه که مجاز است و آنچه که مجاز نیست. اگر همیشه سیستم در حالتهای مجاز باقی بماند و کاربران تنها اعمالی را که مجاز هستند بتوانند انجام دهند، آنگاه سیستم امن است. اگر سیستم بتواند به یک حالت غیرمجاز وارد شود یا کاربر بتواند عمل غیرمجازی را با موفقیت انجام دهد سیستم ناامن است.

راهکارهای امنیتی

راهکارهای امنیتی سیاست امنیتی را اجرا می کنند: هدف آنها این است که از ورود سیستم به حالتهای غیرمجاز جلوگیری کنند. راهکارها ممکن است فنی یا عملیاتی (یا رویه ای) باشند. به عنوان مثال فرض کنید سازمان نظامی سندهای طبقه بندی نشده و سندهای فوق سری دارند. کاربرانی که حق دسترسی به اسناد فوق سری را ندارند، نمی توانند به آنها دسترسی پیدا کنند.

راهکارهای فنی برای برخی سیاستها مناسب نیستند. برای مثال دانشگاه می خواهد دانشجویان را از داشتن فایلهای موزیک روی کامپیوترشان منع نماید. جهت انجام اینکار راهبران سیستم قادرند کامپیوتر ها را برای یافتن موزیک جستجو نمایند ولی دانشجویان باهوش می توانند فایلهای موزیک را به صورت متنی کدگذاری نمایند. ولی راهکار عملیاتی که دانشجویان را از قراردادن فایل موزیک منع می کند در کنار تنبیه در صورت تخلف، خیلی مناسبتر و مؤثرتر از راهکار فنی می تواند باشد.

این که کل راهکارهای اتخاذ شده به درستی سیاست امنیتی را پیاده سازی می کنند، پرسشی مربوط به اطمینان یا تضمین است. برای مثال فایروالها سیستمهایی هستند که واسطه اتصال سیستم یا شبکه داخلی به اینترنت هستند. فایروال می تواند تلاشهای اتصال به شبکه داخلی از اینترنت را بلوکه کند. با این حال اگر نرم افزار فایروال به درستی نوشته نشده باشد، ممکن است برخی اتصالها که سیاست امنیتی اجازه نداده را بلوکه نکند.

در ادامه دو مثال این مورد را بیشتر توضیح می دهند. اول فرض کنید سیاست سازمان آن است که از شبکه های خارجی نقطه به نقطه استفاده نشود. ساده ترین راه آن است که فایروال به گونه ای پیکربندی شود که پیامهای خارجی درگاه مربوطه را نپذیرد. با این حال اگر فایروال به خوبی پیکربندی نشده باشد، ممکن است پیامی حتّی اگر چه سیاست امنیتی آن را منع کرده باشد، بپذیرد. بنابراین راهکار مورد نظر برای اجرای سیاست امنیتی شکست می خورد.

ISSN: 2745-3673
http://www.Rcsj.ir

دوم فرض کنید دانشگاه یک وبگاه برای اسنادی که قرار است در دسترس پژوهشگران بیرونی باشند، دارد. سیاست امنیتی سیستم آن است که فایلهای موجود در دایرکتوریهای کارگزار وب برای اجرای این سیاست پیکربندی شوند. متأسفانه کارگزار یک خطای نرم افزاری دارد که با فرستادن یک یو آر ال[۲۳] خاص می توان به هر فایل روی سیستم دسترسی پیدا کرد. در این جا راهکار نه به علت پیکربندی نادرست، بلکه به علت خطای نرم افزاری شکست می خورد.

تضمینهای امنیتی

این که چقدر سیاستهای امنیتی نیازمندیها را می پوشانند و راهکارها سیاستها را پیاده سازی می کنند در قلمرو بحث تضمین امنیتی قرار می گیرد. متدولوژیهای مختلفی برای اندازه گیری تضمین یا اطمینان امنیتی وجود دارند. متدولوژی می تواند به عنوان بخشی از فرآیند مهندسی نرم افزار باشد، با این حال هیچ متدولوژی نمی تواند به طور مطلق امن بودن سیستم را تضمین کند، ولی متدولوژیهای مختلف درجه های مختلفی از امنیت را فراهم می کنند. روشهای مختلف ارزیابی میزان تضمین امنیت نه تنها به سیستم، بلکه به محیط ارزیابی و فرآیند تولید سیستم نیز بستگی دارند.

تشکر و قدردانی

با تشکر از جناب آقای دکتر افشین رضاخانی، خانم دکتر لیلا ریخته چی

.

[23] URL

ISSN: 2745-3673
http://www.Rcsj.ir

منابع و مراجع

[1] A. Cau, H. Janicke, B. Moszkowski, “Verification and enforcement of access control policies”, Form Methods Syst Des, De Montfort University, pp. 333-327, May 2013.

[2] M. Koch, L. V. Mancini, F. P. Presicce, “Conflict Detection and Resolutionin Access Control Policy Specifications”, Freie Universit¨at Berlin, Univ. di Roma La Sapienza, George Mason University, LNCS 2303, pp. 223–238, 2002.

[3] M. Sandhu, R.S. Ferraiolo, D.F. and Kuhn, D.R. ‘‘The NIST model for rolebased access control: toward a unified standard’’, In Proceeding of 5th ACM Workshop on Role-Based Access Control, pp. 47–63, Berlin, Germany (2000).

[4] A. P. Maranda, R. Rutkowska, “Implementation of Usage Role-Based Access Control Approach for Logical Security of Information Systems”, Institute of Information Technology, Lodz University of Technology, Poland, 2014.

[5] V. F. Crescini and Y. Zhang .“a system for dynamic access control”, international journal of advertising, Australia, pp, 145-165, November 2005.

[6] R. Gupta, M. Bhide, “A Generic XACML Based Declarative Authorization Scheme for Java”, Verlag Berlin Heidelberg, pp. 44–63, 2005.

[7] Urs Hengartner and Peter Steenkiste, "Access Control to Information in Pervasive Computing Environments", Ninth Workshop on Hot Topics in Operating Systems (HotOS IX), ACM, May 2003, pages 157-162.

[8] M. Kudo, J. Myllymaki, H. Pirahesh and N. Qi, "A Function-Based Access Control Model for XML Databases", CIKM’05 of ACM, page 115-122, November 2005.