فصلنامه سیستم‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند
Intelligent Multimedia Processing and Communication Systems (IMPCS)
انجمن علمی تجارت الکترونیکی ایران
واحد زنجان

ارائۀ یک ساختار امن جهت طراحی و پیاده‌سازی سامانه جامع نشانه‌گذاری جغرافیایی مکان‌های کشور

DOR: 20.1001.1.27832570.1399.1.2.3.9

مقاله پژوهشی

جابر کریم پور[۱]، رسول بابایی*[۲]

۱-دانشکده علوم کامپیوتر، دانشگاه تبریز، تبریز، ایران karimpour@tabrizu.ac.ir

۲- دانشکده مهندسی برق و کامپیوتر، دانشگاه آزاد اسلامی واحد زنجان، زنجان، ایران rasul.babaei@gmail.com

چکیده: در دنیای دیجیتال امروزی داشتن یک آدرس یکتای جغرافیایی برای هر حاکمیتی ضروری است. باتوجه‌به توزیع اطلاعات در سازمان‌های مختلف، نکات مهمی در خصوص محرمانگی، مالکیت و دسترسی به اطلاعات وجود دارد. آدرس یکتای جغرافیایی یک تکاپو و چالش، میان سازمان‌های مختلف حاکمیتی و همچنین مردم و سازمان‌های غیرانتفاعی یک کشور به‌حساب می‌آید. ابعاد مختلفی در این چالش‌ها وجود دارند که چالش‌ها یکپارچه‌سازی اطلاعات موجود در سازمان‌های مختلف و قوانین دسترسی و امنیت اطلاعات محرمانه از اساسی‌ترین چالش‌های این سیستم است. این چالش‌ها زمانی بیشتر و حیاتی‌تر می‌شوند که نیاز باشد این اطلاعات در دسترس سازمان‌های مختلف با قابلیت صلاحیت دسترسی مختلف قرار گیرند. در این تحقیق روشی برای یکپارچه‌سازی مبتنی بر معماری سرویس‌گرا ارائه شده است. برای کنترل، بازرسی و مدیریت، ایجاد و حفظ قوانین دسترسی و محرمانگی، در لایه مسیریابی سرویس‌ها یک سرویس متمرکز امنیتی پیشنهاد شده است. بررسی نشان می‌دهد که روش پیشنهادی چالش‌هایی در خصوص دسترسی، مالکیت، یکپارچه‌سازی، مدیریت متمرکز و بازرسی ارتباطات و سطوح دسترسی را به شکل قابل‌توجهی بهبود بخشیده است.

واژه‌های کلیدی: طرح نشانی استاندارد مکانی ملی، سیستم‌های توزیع شده، معماری یکپارچه‌سازی، معماری سرویس‌گرا، سیستم کنترل دسترسی،

Presentation a secure structure for designing and implementing a comprehensive system of geographical marking of the country's places

Jaber Karimpour[1], Rasul Babaei[2]

1-Department of Computer Science,Uniersity of Tabriz,Tabriz,Iran, karimpour@tabrizu.ac.ir

2- Department of Computer Engineering, Islamic Azad University, Zanjan Branch, Zanjan, Iran, rasul.babaei@gmail.com

Abstract : In today's digital world, having a unique geographical address is essential for any government. With regard to the distribution of information in different organizations, there are important points about confidentiality, ownership and access to information. The unique geographical address is a challenge between different governing organizations as well as the people and non-profit organizations of a country. There are several dimensions to these challenges, the challenges of integrating information in different organizations and the rules of access and security of confidential information are the most fundamental challenges of this system. These challenges become more and more vital when this information needs to be made available to different organizations with different access capabilities. In this research, a method for integration based on service-oriented architecture is presented. A centralized security service has been proposed at the services routing layer to control, inspect and manage, establish and maintain access and privacy rules. The study shows that the proposed method has significantly improved the challenges of access, ownership, integration, centralized management and inspection of communications and access levels.

Keywords : National Spatial Standard Address Design, Distributed Systems, Integration Architecture, Service Oriented Architecture, Access Control System,

تاریخ ارسال مقاله: ۱۳۹۹/۰۷/۳

تاریخ پذیرش مقاله: ۱۳۹۹/۰۹/۲۹

*: نویسنده مسئول

۱-مقدمه

طرح نشانی استاندارد مکانی ملی GNAF[1] پروژه‌ای ملی برای کدگذاری و شناسایی نقاط جغرافیایی کشور است که علاوه بر وجود آدرس‌های ثبت شده افراد در پایگاه‌های اطلاعاتی دستگاه‌های خدمت‌رسان شهری (پست، ثبت اسناد، ثبت احوال، بانک، شهرداری، برق، آب، گاز، مخابرات، نیروی انتظامی و ...)، آدرس منحصربه‌فرد برای هر مکان (ملک) ایجاد می‌گردد که کلید اتصال اطلاعات فوق می‌باشد [۳، ۴] این طرح باتوجه‌به گستردگی اطلاعات در بین سازمان‌های مختلف نیازمند داشتن الگویی اجرایی مناسبی می‌باشد تا هر سازمان بتواند باتوجه‌به مسئولیت خود در این راستا به‌گونه‌ای عمل کند که:

- جامعیت و یکپارچگی سامانه با مشکل روبه‌رو نشود.
- هر سازمان مسئول داده‌های خود باشد.
- هر سازمان بسته به ماهیت خود خدمات موردنیاز را دریافت نماید.
- هر سازمان مسئول به‌روزرسانی داده‌های خود باشد.
- یکپارچگی و اصول امنیتی داده‌ای در هر سازمان رعایت شود.

در کنار موارد بالا، بایستی به سؤالات زیر هم پاسخ مناسب داده شود:

- سازمان باید چه داده‌هایی را در اختیار GNAF قرار دهد؟
- مسئول نگهداری و صحت سنجی داده‌ها کیست؟
- در ساختار اجرایی که هر روز داده‌ها تغییر می‌کند چه زمانی و چگونه این بروز رسانی رخ خواهد داد؟
- دسترسی به اطلاعات و نحوه طبقه‌بندی آنها توسط چه کسی و چگونه کنترل خواهد گردید؟
- ارتباط بین سازمان‌های مختلف برای بروز رسانی و نگهداری و صحت سنجی بر اساس چه الگویی رخ خواهد داد؟

در سال ۱۹۸۳ دولت مرکزی ایالات متحده امریکا با صدور بیانیه‌ای سازمان‌های فدرال را موظف به ایجاد فایل‌های دیجیتال از نقشه‌های موجود بر اساس استانداردهای تعیین شده جهت تسهیل در اشتراک‌گذاری و استفاده آسان و همچنین قابلیت نگهداری بالا از این منابع اطلاعاتی نمود. در سال ۱۹۹۴ فرمان اجرایی ایجاد زیرساخت اطلاعات مکانی ملی (NSDI) را صادر کرد و در کوتاه‌مدت با توسعه NSDI اطلاعاتی مانند نقشه‌های راهبردی، توابع و ساختار داده‌ای برای جستجو و پیداکردن مجموعه داده‌های جغرافیایی، استانداردسازی داده‌ای فعالیت‌ها، ایجاد یک چارچوب مکانی دیجیتال و استراتژی همکاری برای به‌دست‌آوردن داده‌ها را شامل شد. این فعالیت‌ها برای توسعه زیرساخت داده‌های مکانی برای ایالات متحده طراحی شده‌اند که در آن کمیته فدرال اطلاعات جغرافیایی (FGDC) نقش کلیدی را بازی می‌کنند و وظیفه اصلی به‌روزرسانی و توسعه NSDI را دارد. [۲]

پروژه G-NAF در سال ۱۹۹۵ در کشور استرالیا جهت کدگذاری و شناسایی نقاط جغرافیایی کشور استرالیا با همکاری سازمان‌های دولتی این کشور (سازمان نقشه‌برداری و ثبت زمین استرالیا، اداره پست و کمیسیون انتخابات استرالیا) به‌منظور ایجاد و نگهداری یک آدرس ملی برای آدرس‌های در حال استفاده و همچنین آدرس‌های رسمی کشور استرالیا مطرح و تهیه گردید. سازمان PSMA[2] آژانس نقشه‌برداری عمومی استرالیا متصدی توسعه این سامانه، وظیفه بروز رسانی و نگهداری را برعهده دارد. این پروژه با توانمندی‌هایی همچون مدل‌سازی داده‌های یکپارچه، بهینه‌سازی، فرایندهای دست‌کاری داده و همچنین ایجاد یک استاندار کشوری هم‌اکنون در کشور استرالیا در حال استفاده عموم می‌باشد. [۱]

سامانه GNAF برای ارائه خدمات موردنظر خود می‌تواند از داده‌های متفاوتی که در سازمان‌های مختلف (شامل نقشه جغرافیایی، اطلاعات مالکان و صاحبان نقاط مختلف، آدرس پستی استاندارد، نقشه‌های مرتبط با تأسیسات عمومی و شهری و ...) وجود دارد با استفاده از یک معماری خدمات محور و قابلیت تکامل و نگهداری بالا به‌منظور یکپارچه‌سازی خدمات توزیع شده در سازمان‌های مختلف استفاده کند. همچنین وجود یک زیرساخت احراز هویت و کنترل دسترسی برای ایجاد بستر قابل اعتماد در جهت مدیریت صحیح دسترسی به خدمات ارائه شده و داده‌ها توسط هر سازمان، در این سامانه ضروری است.

همه این موارد بیانگر این امر است که پروژه‌ای به این گستردگی با پیچیدگی داده‌ای زیاد و همچنین وجود اطلاعات طبقه‌بندی شده، نیازمند طراحی یک معماری خاص است که بتوان هزینه موارد بیان شده را به حداقل رساند.

در کنار یکپارچه‌سازی دغدغه عمده دیگری برای سازمان‌های همکار در پروژه GNAF وجود دارد که محدودیت‌های شدیدی در نحوه ارائه خدمات آنها ایجاد می‌کند، یکی از این مسائل مهم نحوه اعتبارسنجی و اعطای مجوزهای لازم برای دسترسی به خدمات ارائه شده می‌باشد، این محدودیت عملاً در تمامی پروژه‌های توزیع شده به نحو چشمگیری وجود دارد، بخصوص در سیستم‌هایی که محتوای داده‌ای یک خدمت بر اساس نوع دسترسی آن می‌تواند تغییر کند.

به طور کل می‌توان فارغ از مشکلات عمده‌ای که پروژه GNAF در کشور دارد به دو چالش مهم که از چالش‌های عمده پروژه می‌باشد اشاره کرد.

- نحوه یکپارچه‌سازی خدمات: باتوجه‌به گسستگی اطلاعات لازم در سازمان‌ها مختلف مانند، اداره پست؛ سازمان نقشه‌برداری، قوه قضاییه و ...
- مدیریت محدودیت‌های امنیتی در حوزه دسترسی خدمات و طبقه‌بندی داده‌ای موجود و وجود اطلاعات حساس در نقشه و همچنین زیرساخت‌های کشور

با بررسی مفهومی و اسناد اجرایی GNAF در ایران به نظر می‌رسد که لازم است برای یکپارچه‌سازی این داده‌های توزیع شده در سازمان‌های مختلف یک معماری توزیع شده ارائه گردد تا سازمان‌های خدمت دهنده، بتوانند با نیازهای خدمت گیرنده‌ها به‌آسانی تغییر کنند.

۲ -یکپارچه‌سازی

سیستم‌های توزیع شده به‌تدریج امری عادی می‌شوند. این فراگیر بودن سیستم‌های توزیع شده، عمدتاً به دلیل رشد در سازمان‌ها و استفاده از داده‌ها، نیاز به دسترسی به داده‌ها و منابع شبکه را در مکان‌های گسترده

توزیع شده ایجاد کرده است که هرکدام از آنها هنوز هم باید استقلال خود را حفظ کنند.[۵]

یکپارچه‌سازی[۳]: خواسته یا نخواسته، برنامه‌ها و سیستم‌ها در دهه‌های گذشته به‌صورت مستقل و ناهمگن تولید شده‌اند، و بر اساس نیاز روز این برنامه و سیستم‌ها با یکدیگر به تبادل اطلاعات پرداخته‌اند. در سطوح مختلف، بسته به نوع کنترل‌ها، این تبادل اطلاعات می‌تواند در چندین سطح، پروتکل و فرمت انجام پذیرد. همان گونه که مشخص است، باتوجه‌به تکنولوژی‌های روز، راهکارها و برنامه‌ها در سازمان‌ها در حال تغییر هستند. نه این تغییرات در حال اتمام هستند و نه می‌توان این تغییرات پشت کرد. در عوض ما باید این تغییرات ناهمگن بین سیستم‌ها را مدیریت شود.[۶]

اصطلاحات سیستم توزیع شده[۴] و سیستم مشترک می‌تواند به روش‌های مختلف باتوجه‌به موضوع بحث قابل‌درک باشد. در دیدگاه عمومی سیستم‌های توزیع شده یک کلاس گسترده از سیستم‌های نرم‌افزاری است که در آن، از دیدگاه معماری، اجزای عملکردی در سراسر دستگاه‌ها و یا گره‌های متصل شده به‌وسیله انواع شبکه، گسترش و توزیع شده‌اند[۷]. انواع مختلف زیادی از سیستم‌های توزیع شده برای اهداف مختلف وجود دارد، اعم از روش مبتنی بر نظیر به نظیر[۵]، انتشار/اشتراک[۶] میان‌افزار[۷]انتشار اطلاعات[۸] و سیستم تصویر واحد[۸] برای خوشه‌بندی منابع مدیریتی[۹]. در چنین سیستم‌هایی، دستورات پردازش داده به شکل توزیع شده و فرایندهای هماهنگی نیز توزیع شده است که معمولاً از طریق انتقال نوعی از پیام، مانند فراخوانی از راه دور[۹] و از طریق یک چارچوب میان‌افزار[۱۰] جداگانه انجام می‌شود[۱۰].

۲-۱- EAI

باتوجه‌به موارد بیان شده در زیر، در بسیاری از موارد روش‌های EAI فقط قادر به انجام انتظارات محول شده به آنها از طریق میزان محدودیت‌ها و یا یک روش مطلوب می‌باشند.

- EAI به‌طورکلی داده‌محور است نه فرایند محور.
- راهکارهای EAI مطابق با فرایندهای کسب‌وکار عمل نمی‌کنند. در عوض به طور مستقل تعریف شده‌اند.
- راهکارهای EAI بسیار پیچیده هستند و به دلیل استفاده از فناوری‌های اختصاصی، برای حفاظت طولانی‌مدت، ممکن است امکان استفاده از استانداردهای جدید را ندهند.
- راهکارهای EAI نیاز به دانش محصول خاص دارند که تنها در EAI مربوطه استفاده می‌شوند و در پروژه‌های دیگر امکان استفاده مجدد را ندارند.
- در درازمدت پرهزینه می‌شوند و به سمت معماری اسپاگتی سوق پیدا می‌کنند.

۲-۲-معماری سرویس‌گرا[۱۱] SOA

معماری سرویس‌گرا و معماری سازمانی به‌عنوان چارچوب مفید برای توسعه یک سیستم سازگار، در مقیاس بزرگ است که به طور معمول با استفاده از استانداردهای وب‌سرویس پدید آمده‌اند[۱۱]. SOA معمولاً به سیستمی از سیستم‌های بزرگ که با ترکیب برنامه‌ها به وجود آمده‌اند و به‌وسیله سازماندهی جزء، خدمات سست[۱۲] که در گروه‌های مختلف اجرا می‌شوند و با تبادل پیام ببین هم ارتباط برقرار می‌کنند اشاره می‌کند [۱۲].

خدمات در SOA مزایای بسیاری را فراهم می‌کند، به‌عنوان‌مثال، انتزاع سیستم، استقلال بین منطق کسب‌وکار و منطق کاربرد خاص فناوری، چابکی سازمان و قابلیت استفاده مجدد از مؤلفه‌ها .سه‌لایه انتزاع تعریف شده توسط عبارت‌اند از: لایه خدمات برنامه، لایه خدمات تجاری و لایه خدمات ارکستراسیون .برخی از مطالعات بررسی شده، خدمات متنوعی را درباره تعداد و انواع آنها ارائه می‌دهند[۱۳].

معماری خدمت محور اصطلاحی است برای توصیف یکی از راه‌های اجرای معماری سازمانی که با تجزیه‌وتحلیل کسب‌وکار، به‌منظور شناسایی ساختار و فرایندهای حوزه کسب‌وکار آغاز می‌شود. این رویکرد اجازه تعریف خدمات پیاده‌سازی آنها بر اساس حوزه کسب‌وکار را فراهم می‌آورد[۴].

درحالی‌که توسعه برنامه‌های کاربردی با معماری SOA بسیاری از چالش‌های مهندسی نرم‌افزار را شامل می‌شود، مدیریت این سیستم‌ها چالش‌های بیشتری را دارد [۱۶,۱۵]. SOA از طریق اتصالات سست مابین خدمات خود و سازمان فناوری اطلاعاتی که آنها را مدیریت می‌کند انعطاف‌پذیری را فراهم آورده است. اگرچه این انعطاف‌پذیری ممکن است زمانی که ترکیب برنامه‌های ترکیب شده نیاز به تکامل داشته باشند مشکلات قابل‌توجهی به وجود آورد [۱۶,۱۵,۱۴].

معماری خدمات محور یک معماری در حال تکامل است که اجازه می‌دهد سامانه‌های مختلف توزیع شده بتوانند با رابط‌های تعریف شده معین با پروتکل‌های استاندارد با هم ارتباط برقرار کنند. تفاوت اصلی SOA با سایر معماری‌های یکپارچه‌سازی این است که در SOA کل ارتباطات به‌صورت فرایندی طراحی می‌شوند و هر سازمان ارائه‌دهنده خدمات می‌تواند بر اساس ساختار خود، یک روال داخلی را طی کند.

۱-۲-۲- سیاست‌های کلی حاکمیت معماری خدمات محور[۱۳]

به‌طورکلی واژه حاکمیت، مانند حاکمیت در حکومت سیاسی، مدیریت شرکت و مدیریت فناوری اطلاعات به مدیریت موفق سازمان‌ها یا پروژه‌ها اشاره می‌کند و همچنین اصطلاح سیاست مانند حاکمیت برگرفته از مفهوم آن در حوزه فناوری اطلاعات است و هدف اصلی معرفی و اجرای قوانین (ساختارها، حقوق، دستورالعمل‌ها و استانداردها و ...) کنترل اجرای دقیق آنها در جهت حظ منابع و پیشبرد اهداف کلان می‌باشد.

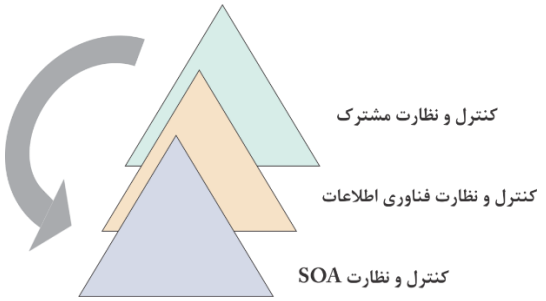
در حوزه معماری سرویس‌گرا باید این قوانین دو خصیصه مهم داشته باشند .

- قوانین یا دستورالعمل و ... که باید تنظیم شوند بخشی از سیستم معماری سرویس‌گرا هستند.
- قوانین واقعی باید از رعایت مقررات کلان سازمان و سیستمی اطمینان حاصل کنند.

به‌طورکلی، حاکمیت سازمانی چارچوب قانونی قوانین و قوانین رهبری و کنترل یک سازمان است. به‌عنوان یک نهاد حاکمیتی وظیفه‌مند بوده و وظیفه تأمین نیازهای را برعهده دارد، لازم است که بتواند همواره کیفیت این خدمات را ارتقا بخشد .برای الزامات عملیات رهبری خوب یک سازمان، می‌توان چهار نقطه عطف عمودی را ارائه داد که به قوانین حاکمیت اعمال می‌شوند.

- مقررات تعیین اهداف تجاری
- مقررات برای ساختارها، زیرساخت‌ها، فرایندها و قوانین دستیابی به آنها
- مقررات ارزیابی دوره‌ای فعالیت‌های رهبری
- مقررات برای اطلاع‌رسانی شرکت‌ها و ذی‌نفعان

به‌طورکلی می‌توان جایگاه حاکمیت در معماری سرویس‌گرا با شکل ۱ توصیف کرد[۱۸]



شکل ۱: ارتباط و جایگاه حاکمیت در معماری سرویس‌گرا

۳-امنیت اطلاعات

امنیت اطلاعات عبارت است از کاهش خطراتی که سیستم‌های اطلاعاتی را در عصر رشد ارتباط متقابل رایانه‌ها، تحت تأثیر قرار داده است. هدف از امنیت اطلاعات ایجاد وضعیتی است که در آن سه معیار برای حفاظت از اطلاعات تعیین شده است:

- محرمانگی[۱۴]: در این زمینه بدین معنی است که فقط کاربران با امتیاز خاص مجاز به دسترسی به اطلاعات حفاظت شده‌اند.
- یکپارچگی[۱۵]: تضمین می‌کند که این اطلاعات فقط توسط کاربرانی که مجوز کافی دارند تغییریافته و یا حذف شوند.
- دسترسی[۱۶]: امکان دسترسی به اطلاعات برای هرکسی که مجاز به دسترسی هست در هر زمانی امکان‌پذیر باشد.

کنترل دسترسی[۱۷] به طور عمده به دو قابلیت اول یعنی محرمانگی و یکپارچگی اشاره می‌کند، اما بر معیار سوم یعنی دسترسی نیز دلالت دارد[۱۹].

در عصر دیجیتال باتوجه‌به در دسترس بودن اطلاعات یکپارچه سازمانی در سیستم‌های اطلاعاتی، بهره‌وری گسترده‌ای در کسب‌وکار حاصل شده است. بااین‌حال، در دسترس بودن اطلاعات مهم در این سیستم شامل خطراتی نیز است، چراکه اکثر حملات از درون خود سازمان انجام شده است[۲۰]

۳-۱-مدل‌های کنترل دسترسی

کنترل دسترسی اختیاری[۱۸]، در اصل"مالکیت شی[۱۹]" بدین معنی که یک یا چند کاربر به‌عنوان مدیر به یک منبع اختصاص داده می‌شود و اعطای مجوز دسترسی به این منبع در اختیار آنها می‌باشد. تصمیم به اعطای دسترسی بر اساس شناسایی یک کاربر و یا گروه اعضا می‌باشد. اصطلاح "اختیاری " بدین معنی است که اعطا مجوز برای عملیات خاص به منابعی مانند فایل‌ها با تأیید مالک تعیین می‌شود. یعنی این‌که هر کاربری قادر به گسترش این حقوق به کاربران دیگر و یا افراد زیرمجموعه خود می‌باشد[۱۹].

کنترل دسترسی اجباری[۲۰] که بر اساس نقاط ضعف کنترل دسترسی اختیاری به وجود آمده و به‌صورت خاص برای مهار این ضعف‌های بالقوه طراحی شده است.[۲۱]

کنترل دسترسی مبتنی بر نقش[۲۱]: در این مدل مجوز برای عملیات بر روی منابع به طور مستقیم به کاربر اختصاص داده نشده است، بلکه یک انتزاعی بین این دو ایجاد شده که به آن نقش گفته می‌شود[۲۲]. معنای این نقش به طور مستقیم با نقش در سازمان قابل‌مقایسه است. افرادی که در یک سیستم وظایف مشابهی انجام می‌دهند، با یک نقش مشابه در سیستم تعریف می‌شوند؛ بنابراین مجوزهای کاملاً متفاوتی موردنیاز است که توسط عملیات لازم برای انجام‌دادن وظایف مختلف محدود شده است و این مجوزها در RBACK به نقش اختصاص داده می‌شود[۱۹]. البته در طول دو دهه گذشته مدل RBACK به‌صورت قابل‌توجه با افزودن قابلیت‌هایی توسعه‌یافته است اما ماهیت کلی آن که اعطای مجوز به نقش بوده تغییری رخ نداده است.

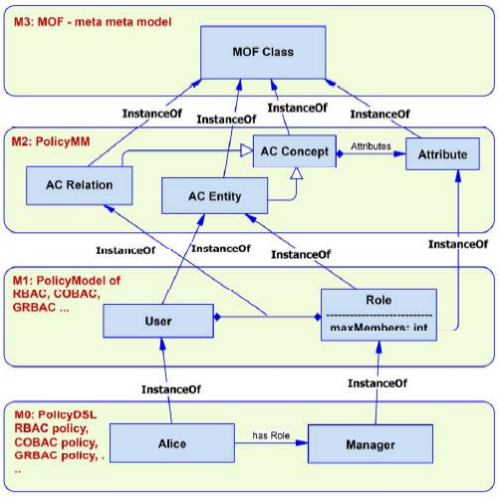
توانایی کنترل دسترسی به اطلاعات حساس بر اساس سیاست، شاید اساسی‌ترین نیاز امنیتی باشد. درحالی‌که بیش از چهار دهه گذشته محققان امنیتی انواع زیادی از سیاست‌ها و مدل‌های سیاست برای رسیدگی به مشکلات امنیتی دنیای واقعی ارائه داده‌اند، تنها بخش کوچکی از این سیاست‌ها از طریق مکانیسم‌های تجاری در دسترس اجرا می‌باشند[۲۳].

هنگام بحث در مورد کنترل دسترسی، ما معمولاً بین مدل و سیاست تمایز قائل می‌شویم، سیاست در مورد بایدونبایدهای دسترسی تصمیم می‌گیرد و مکانیسم پیاده‌سازی و نحوه اجرای خط‌مشی‌های انتخاب شده را مدل مشخص می‌کند[۱۷]

مدل‌های کنترل دسترسی اجازه می‌دهند که قواعد کنترل دسترسی (سیاست‌ها) بیان گردند. این قواعد کنترل مشخص می‌کنند که هر فرد خاص چه دسترسی‌های خاصی به چه اشیای خاصی، به چه منظوری دارند. چندین مدل مجوز وجود دارند که قوانینی برای افراد خاص، اشیا خاص و اقدامات خاص را بیان می‌کنند. کنترل دسترسی نقش محور[۲۲] (RBAC)، معرف مفهوم نقش است که یک انتزاع کلی به بیش از فرد خاص می‌باشد که امتیازات به نقش اختصاص‌داده‌شده است. نقش‌های مختلف پایدار است درحالی‌که افراد مختلف اختصاص‌یافته به آنها ممکن است تغییر یابد. علاوه بر این مفهوم نقش با مفهوم عملکردی همراه است. [۲۴] کنترل دسترسی TRBACK و GTRBACK در مورد زمان

دسترسی و عدم زمان دسترسی قوانین را بیان می‌کند [۲۵]. مدل کنترل دسترسی مبتنی بر سازمان‌ها (ORBAC)اجازه تعیین قوانین مربوطه به موضوعات انتزاعی و اشیا انتزاعی و اقدامات انتزاعی تعیین می‌کند. مدل کنترل دسترسی واقعی انتزاعی(CABAC) یک مدل ترکیبی از موضوعات انتزاعی و واقعی است. محدودیت‌های مختلف در افراد، اقدامات و اشیا تعریف می‌شود، به این صورت که یک موضوع انتزاعی به یک موضوع واقعی اختصاص داده می‌شود و یک عمل انتزاعی به یک عمل واقعی اختصاص‌داده‌شده و یک شی انتزاعی به یک داده واقعی اختصاص می‌یابد[۲۶].

برانیسلاو تنینیچ و همکاران، یک سیستم کنترل دسترسی تحت عنوان PolicyDSL برای مدیریت عمومی مناسب یک مجموعه گسترده‌ای از سیستم‌ها تعریف کردند. بر اساس شکل ۲، یک زیرساخت عمومی سطح ۲M که برای مشخص‌کردن نیازمندی‌های مدل سیاست در سطح Ml مانند RBACK و GTRBAK و ... استفاده می‌شد. برای تعریف مدل سیاست، یک زبان DLS برای تعریف سیاست‌های کنترل دسترسی دارد که به‌صورت پویا تولید می‌شود. یک کارشناس امنیتی قادر به بیان سیاست‌های واقعی کنترل دسترسی سطح ۰M برای مدل‌های کنترل دسترسی با استفاده از DSL تعریف شده، می‌باشد. راه‌حل ارائه شده را می‌توان بدون هیچ تغییری، به تعدادی از سیستم‌هایی که در مدل کنترل دسترسی‌های مختلف هستند اعمال کرد. [۲۷]



شکل ۲: مدل کنترل دسترسی PolicyDSL

ارزیابی ریسک امنیتی یک گام مهم در طراحی سیستم‌های بحرانی است. بااین‌حال، معماران سیستم غالباً فاقد دانش امنیتی لازم برای شناسایی تمام خطرات امنیتی هستند. حتی کارشناسان در آن دسته از خطرات که خود درگذشته تجربه کسب کرده‌اند، تمرکز می‌کنند. بنابراین، آنها می‌توانند خطرات را که برای شان از جذابیت کمتر برخوردار است فراموش کنند. برای کاستن از این موضوع، روش‌های ارزیابی ریسک امنیتی صنعتی و استانداردهایی با کاتالوگ تهدیدها و کنترل امنیت آمده است.[۲۸]

ترکیب ویژگی‌های امنیتی یکی از مهم‌ترین و همچنین یکی از کارهای چالش‌برانگیز در طراحی سیستم‌های توزیع شده است.[۲۹] در طول دهه گذشته محققان و پژوهشگران به این نتیجه رسیده‌اند که اختلاف ویژگی‌های امنیتی باید با استفاده از یک رویکرد سیستماتیک، ترکیب اصول مهندسی نرم‌افزار و مهندسی امنیت حل شود [۳۰].

محققان به‌طورکلی به این نکته اذعان دارند که برای هر استراتژی امنیتی موفق باید آن را طی یک رویکرد جامع به صورتی پایدار و محکم در اصول مهندسی نرم‌افزار بیان کرد که در آن طیف اختلاط امنیتی ویژگی‌هایی از نرم‌افزار در سراسر مراحل آن است و در چرخه توسعه زندگی نرم‌افزار [SDLC] بیان می‌شود[۳۱].

نرم‌افزار امنیتی یک قسمت مهم در توسعه نرم‌افزار است. روزانه آسیب‌پذیری‌های منتشر شده بیشتر و بیشتر می‌شود. ازاین‌رو، طراحان نرم‌افزار و برنامه‌نویسان به طور فزاینده‌ای نیاز به اعمال راه‌حل‌های امنیتی به سیستم‌های نرم‌افزاری دارند. ازاین‌رو الگوهای امنیتی بهترین شیوه رسیدگی به مشکلات امنیتی در محدوده زمانی معین است[۳۲]

طراحی یک زیرساخت احراز هویت[۲۳]، یکی از مهم‌ترین جنبه‌های مهندسی نرم‌افزار یک سیستم امن است. برخلاف انواع سیستم‌های دیگر، سیستم‌های توزیع شده و به‌ویژه سیستم‌های مشارکتی توزیع شده ممکن است نیازمند مدل‌های احراز هویت اختصاصی و دقیق‌تر شده و رویکردهای التزامی باشند که می‌توانند مجموعه‌ای از زیر عناوین معنایی مختلفی را لحاظ نمایند. [۳۳]

به طور سنتی مدل‌های کنترل دسترسی به گروه‌های DAC، MAC، RBAC و اخیراً کنترل دسترسی مبتنی بر ویژگی[۲۴] دسته‌بندی می‌شوند [۳۴، ۳۵، ۳۶].

تولونی و همکاران[۳۷] در بررسی‌های خود از جمع‌بندی مدل‌های مجوز دسترسی، تعدادی از ویژگی‌های این مدل‌ها را بیان کردند که به طور خلاصه می‌توان به موارد زیر اشاره کرد:

مدل مجوز باید عمومی باشد و باید اجازه درست "پیکربندی داشته باشد که بتواند قابلیت پاسخگویی به نیازهای طیف گسترده‌ای از وظایف وابسته به شرکا و مدل‌های شرکت‌ها را داشته باشد".

مدل مجوز باید امکان به اشتراک‌گذاری اشیا از هر نوعی، در هر سطحی از ریز دانگی[۲۵] را داشته باشد.

مدل مجوز باید امکان موردنیاز برای اصلاح قوانین و مشخصات مجوزها را در زمان اجرا بسته به نوع محیط و یا همکاری پویا داشته باشد.

مدل‌هایی با این خصوصیات به طور مستمر در حال خلق شدن برای برآورد الزامات مجوزهای جدید مطرح شده توسط سیستم‌های جدید هستند[۳۸].

۳-۲- راهکار امنیتی

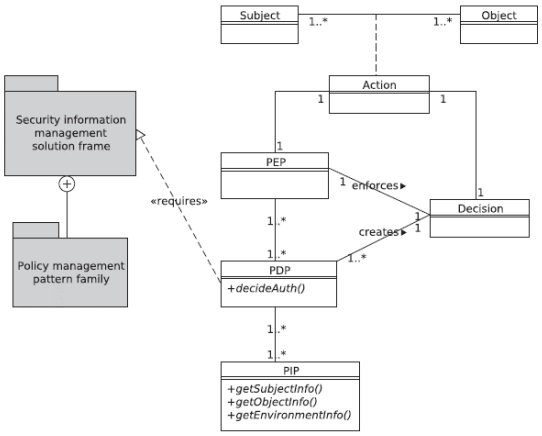
چارچوب راه‌حل‌های امنیتی الهام گرفته از ایده‌های موجود در ساختار الگوی مایکروسافت و الگوی ساختار دلسی و فرناندس است. هر دو به دنبال مدیریت فضای الگوها مطابق با سطوح مختلفی از انتزاع هستند (عمودی)، ساختار مایکروسافت، از دید توسعه (افقی) شامل،

کپسول‌سازی الگوهای مرتبط سطوح مختلف ناشی از انتزاع، بررسی مشکل ریشه مشترک یا سیاست‌ها، محافظت از یک تاکتیک امنیتی خاص می‌باشد. در یک روش مشابه، ساختار راه‌حل‌ها، فضای راه‌حل‌ها را بر اساس ارتباط خانوادگی الگوها به‌صورت افقی (اما مرتبط) و باتوجه‌به سطوح انتزاعی به‌صورت عمودی تقسیم کرده است [۳۹، ۴۰].

معماری انتزاعی مجوز دسترسی (الگوی انتزاعی امنیت)، الگوی امنیت پایه برای اجرای پس‌زمینه مدل مجوز مفهومی، الگوی PBAC می‌باشد [۴۱] . PBAC یک معماری متشکل از چهار جزء اصلی مطابق با اصول کلی سیستم‌های مجوز می‌باشد [۴۲]. این اجزاء عبارت‌اند از:

- خط‌مشی اجرای قوانین[۲۶]: تمام کنترل‌های مجوز را اجرا می‌کند.
- مرحله تصمیم‌گیری سیاست[۲۷]: تمامی تصمیمات مرتبط با مجوز را شامل می‌شود.
- خط‌مشی اطلاعات[۲۸]: تمامی اطلاعات لازم برای تأیید در زمان اجرا را مشخص کرده و جمع‌آوری می‌کند.
- خط‌مشی اجرا[۲۹]: قوانین مجوز را مدیریت و اجرا می‌کند.

مؤلفهٔ خط‌مشی اجرا یک جنبه اساس الگو می‌باشد که سه عنصر اصلی را ایجاد می‌کند، این سه عنصر با هم هسته اصلی الگوی PBAC اصلاح شده به نام معماری انتزاعی مجوز که در شکل ۳ نمایش‌داده‌شده است را تشکیل می‌دهند.



شکل ۳: الگوی انتزاعی مدل امنتی بر اساس PBAK

از دیدگاه انتزاعی اجزا ارائه شده در این الگو به شرح زیر است:

- PEP در مورد اقدامات که توسط یک موضوع دررابطه‌با یک شی آغاز شده مطلع شده است.
- PIP اطلاعاتی از وضعیت کلی سیستم مربوط به موضوع، شی، عمل و محیط اجرایی را جمع‌آوری کرده است.
- PDP شرایط استفاده مجاز برای اعمال داده شده را با استفاده از اطلاعات جمع‌آوری شده توسط PIP تعیین می‌کند و امکان مجاز بودن یا نبودن اقدام موردنظر را ارزیابی و تعیین می‌کند.
- PEP تصمیم را اجرا می‌کند.

یک سامانه چند سکویی (وب– دسکتاپ- موبایل) که برای ارائه خدمت درحوزه آدرس یکتای جغرافیایی در ساختار حاکمیتی کشور ایجاد شود که در این ساختار کاربران حوزه‌های مختلف ستادی، اجرایی و مردمی باتوجه‌به نیازهای مشخص و تعیین شده بتوانند از سیستم استفاده کنند. در این سیستم همکاران و ذی‌نفعان متفاوتی باتوجه‌به حوزه کسب‌وکار مشارکت دارند که این مشارکت به چهار صورت بیان می‌شود.

۴-معماری GNAF بر اساس SOA

بر اساس ساختار موجود در کشور و توجه به مشارکت ارگان‌ها و سازمان‌های مختلف در پروژه GNAF و وجود سامانه‌های مختلف نرم‌افزاری و تخصصی در هر یک از سازمان‌ها و همچنین ایجاد بستر مناسب برای توسعه پذیری، به‌وضوح مشخص است که یک‌یک بستر توزیع شده واقعی برای این پروژه وجود دارد.

در این راستا قبل از ارائه یک مدل معماری به بررسی اجزا این پروژه می‌پردازیم.

۴-۱-سازمان‌های مشارکت‌کننده

سازمان‌های مشارکت‌کننده عبارت‌اند از سازمان‌ها و ارگان‌هایی که به‌نوعی داده‌ها و خدمات موردنیاز در این سامانه را دارند و هر قسمت از داده‌ها و خدمات به‌گونه‌ای تخصصی در سامانه‌های خاص منظوره با مفاهیم تخصصی توزیع شده‌اند و برای واکشی، بازیابی و استفاده از آنها نیاز به شناخت بستر و همچنین تعاریف تخصصی در هر یک از این سامانه‌های نرم‌افزاری وجود دارد.

برای اینکه بتوان به این داده‌ها و خدمات توزیع شده در سامانه‌ها و سازمان‌های مختلف دسترس پیدا کرد روش‌های گوناگونی وجود دارد که هرکدام باتوجه‌به شرایط خاص می‌تواند مفید باشد.

- دسترسی مستقیم به پایگاه داده‌ها
- دسترسی مستقیم به سامانه‌ها
- انتقال داده‌های موردنظر به یک دیتابیس مرکزی
- استفاده از خدمات تولید شده توسط هر سامانه بر اساس پروتکل‌های استاندارد

بر اساس ساختار و ماهیت GNAF و همچنین بستر موجود در کشور و نیز حجم انبوه داده‌های توزیع شده، استفاده از خدمات تولید شده توسط هر سامانه بر اساس پروتکل‌های استاندارد یکی از بهترین گزینه‌های انتخابی برای این پروژه می‌باشد که در آن سامانه GNAF خدمات ارائه شده را جمع‌آوری و خدمات لازم را بر اساس آنها ارائه می‌دهد. آنچه مسلم است وجود پیچیدگی زیاد در بین این خدمات و مدیریت آنها می‌باشد که باتکیه‌بر اصول خدمات محوری می‌توان این مورد را مدیریت نمود.

۴-۲-سازمان‌های استفاده‌کننده

سازمان‌های استفاده‌کننده عبارت است از سازمان‌هایی که خدمات ارائه شده توسط GNAF را استفاده می‌کنند. باتوجه‌به ماهیت GNAF تمامی اقشار جامعه با مسئولیت‌ها و اهداف مختلف از این سامانه استفاده

خواهند کرد. استفاده‌کنندگان این سامانه از مردم عادی جامعه تا سازمان‌های دولتی و خصوصی است. به‌طوری‌که همه باتوجه‌به نیازهای خود از این سامانه استفاده خواهند کرد. این امر باعث می‌شود که نیاز به وجود سیاست‌ها و روش‌هایی جهت مدیریت نمودن دسترسی به داده‌ها بیشتر از سایر سامانه‌ها احساس شود.

یکی از دغدغه‌های مهم در استفاده از خدمات در ساختار توزیع شده بحث طبقه‌بندی داده‌ها و جلوگیری از دسترسی بیش از حد به داده‌ها است و بر اساس یکی از اصول امنیت که می‌گوید: "به هرکسی در حد نیاز و دسترسی باید اطلاعات داده شود"، در این پروژه نیز وجود این اصل بسیار واضح‌تر بیان می‌شود چرا که بسیاری از داده‌های جغرافیایی چیزی جز اطلاعات طبقه‌بندی شده بوده و نیاز به مدیریت دسترسی دارند.

مسلماً پروژه GNAF خود دارای اصولی برای این خواهد بود اما باتوجه‌به ماهیت امنیت نیاز است دفاع در عمق برای این سامانه در نظر گرفته شود، بدین صورت که در چندین لایه مختلف ساختار امنیتی اجرا گردد که در صورت شکسته شدن یک‌لایه، لایه‌های زیرین دیگر جلوی نفوذ و دسترسی غیرمجاز را بگیرد.

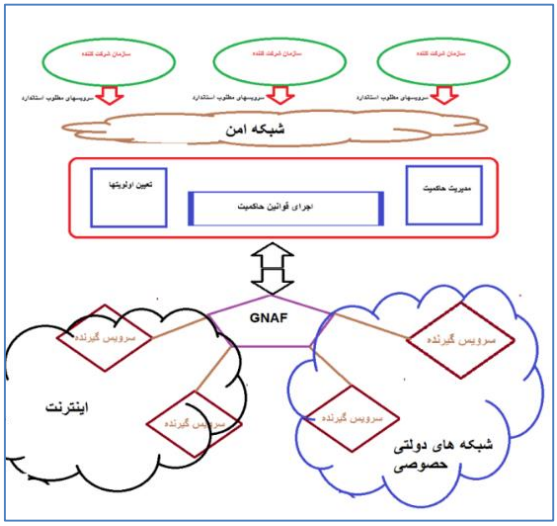
۴-۳- معماری اجرایی

۴-۳-۱- معماری استانی

در شکل ۴ مدل معماری فرض بر این گرفته شده است که هر سامانه فقط به یک استان خدمت خواهد داد و اطلاعات موجود در آن سامانه فقط مربوط به خود استان می‌باشد. این مدل شبیه مدل ایالتی می‌باشد.

موجودیت‌ها استفاده شده برای این مدل عبارت‌اند از

۱. کمیته حاکمیت SOA استانی
۲. سازمان‌های مشارکت‌کننده
۳. سازمان خدمات گیرنده



شکل ۴: معماری GNAF استانی یا منطقه‌ای

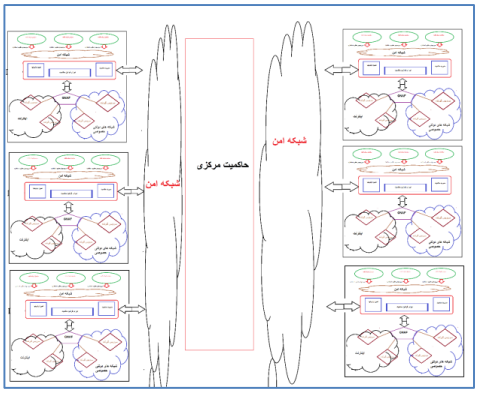
در این معماری سازمان‌های مشارکت‌کننده خدمات خود را بر اساس استانداردهای تبیین شده توسط حاکمیت تولید و در اختیار سازمان حاکمیت قرار می‌دهند. حاکمیت نیز با اجرای فرایندهای متناسب در خصوص امنیت و ترکیب و مدیریت، خدمات را در اختیار GNAF قرار می‌دهد. سپس GNAF به‌عنوان لایه ارائه، این خدمات را در اختیار استفاده‌کننده‌ها قرار می‌دهد که سیاست‌های اجرایی و ساختارهای امنیتی مربوط به خود را نیز رعایت کند.

۴-۳-۲- معماری کشوری ترکیب استانی

در شکل ۵ معماری هر یک از استان‌ها با یک ساختار کاملاً مجزا برای خود یک ساختار GNAF دارند و هر یک از سازمان‌های حاکمیتی نیز به‌عنوان خدمات‌دهنده و خدمات گیرنده خدمات خود را در اختیار سایر استان‌ها قرار می‌دهند. این ارتباط توسط یک حاکمیت مرکزی اتفاق می‌افتد.

موجودیت‌ها استفاده شده برای این مدل عبارت‌اند از

۱. GNAF های استانی
۲. حاکمیت مرکزی



شکل ۵: معماری GNAF کشوری با ترکیب GNAF های استانی

در این مدل هر یک از استان‌ها ساختار خود را دارند و برای ارائه خدمات به سایر استان‌ها و یا استفاده از خدمات سایر استان‌ها به حاکمیت مرکزی متصل شده و نیازهای خود را تأمین می‌کنند.

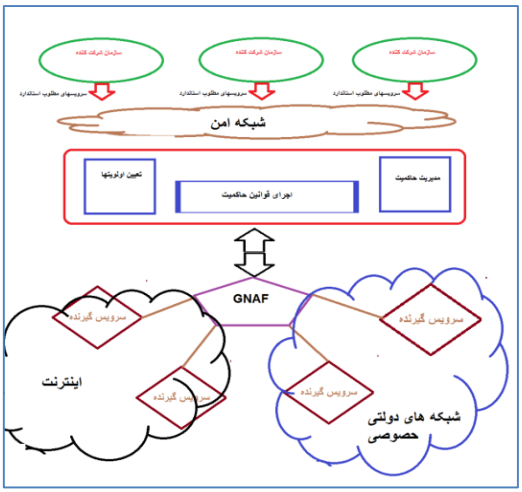
در این ساختار حاکمیت مرکزی با همان اصول حاکمیت استانی تشکیل می‌شود، با این تفاوت که نگرش در این حاکمیت می‌تواند بیشتر مدیریتی باشد تا اجرایی.

۴-۳-۳- معماری کشوری یکپارچه مرکزی

در شکل ۶ ساختار مانند ساختار استانی است و تنها تفاوت گسترش کل ساختار از استان به کشور می‌باشد.

موجودیت‌ها استفاده شده برای این مدل عبارت‌اند از

۱. کمیته حاکمیت SOA
۲. سازمان‌های مشارکت‌کننده
۳. سازمان‌های خدمات گیرنده



شکل ۶ : معماری GNAF کشوری بدون توزیع‌شدگی استانی یا منطقه‌ای

استفاده از این معماری تمرکز را بر روی حاکمیت گذاشته و به‌نوعی مدیریت کل کشور را انجام می‌دهد که در نوع خود می‌تواند مزایا و معایب متعددی نسبت به مدل ۳-۵ داشته باشد.

البته تقسیم‌بندی کشور به فازهای مختلف که از ترکیب‌های متفاوت استفاده می‌کنند نیز امکان‌پذیر است.

باتوجه‌به تنوع سازمان‌ها و داده‌های ارائه شده در این قسمت هر یک از موارد بالا را به‌صورت زیر با مسئولیت‌های بیان شده معرفی می‌کنیم:

۴-۵-موجودیت‌ها و شرح وظایف

بر اساس مصوبه هیئت دولت اعضای مختلفی در این سیستم وجود دارند که به‌طورکلی می‌توان به‌صورت زیر بیان کرد

۴-۵-۱- سازمان‌های ارائه‌دهنده سرویس

سازمان‌های ارائه‌دهنده سرویس به شرح زیر می‌باشند:

اداره پست که وظیفه اختصاص کد پستی و آدرس یکتا به مناطق جغرافیایی بر اساس نقشه مشخص دارد. سازمان نقشه‌برداری مسئول تهیه و نگهداری نقشه‌های دیجیتالی است و هر نوع تغییر در ساختار نقشه‌ها برعهده این سازمان است. سازمان ثبت‌اسناد و احوال که مسئول ثبت و کنترل مالکیت مناطق جغرافیایی را برعهده دارد. در این سیستم، ادارات برق، گاز، مخابرات و انواع اتحادیه‌های اصنافی و ... می‌توانند سرویس‌های لازم را ارائه دهند که باتوجه‌به طراحی انتزاعی و قابلیت گسترش از افزودن آن‌ها اجتناب شده است.

۴-۵-۲- سازمان‌های سرویس‌گیرنده

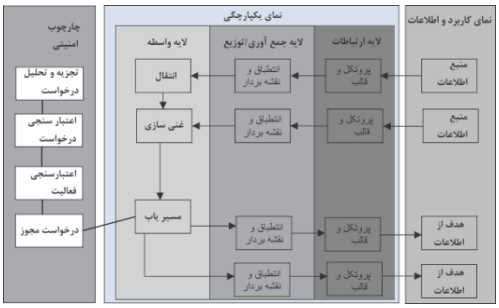
شهرداری‌ها که بر اساس سطوح دسترسی تعیین شده، حق دسترسی به اطلاعات قابل‌دسترسی از سامانه را دارند. سازمان‌های نظارتی و اجرایی که بر اساس قوانین دسترسی حق دسترسی به اطلاعات مالکان و صاحبان را دارند. مالکان که بر اساس قوانین دسترسی فقط حق دسترسی به اطلاعات مربوط به خود را دارند.

۴-۵-۳- سازمان‌های نظارتی

سازمان‌های نظارتی حاکمیتی که می‌تواند باتوجه‌به نوع خدمات و حساسیت آن‌ها با تشخیص حاکمیت وجود داشته باشند؛

۴-۶-معماری سرویس‌گرا

در رول عادی معماری سرویس‌گرا، یک سرویس کنترل دسترسی به لایه مسیریابی اضافه شده است و هر درخواست به‌صورت خودکار و باتوجه‌به سطوح دسترسی تعیین شده، سرویس‌های لازم را باتوجه‌به شکل ۷ فراخوانی و یا منع می‌کند.



شکل ۷ : مدل تکمیلی معماری سرویس‌گرا برای مسیریابی سرویس‌ها باتوجه‌به مدل امنیتی پیشنهادی

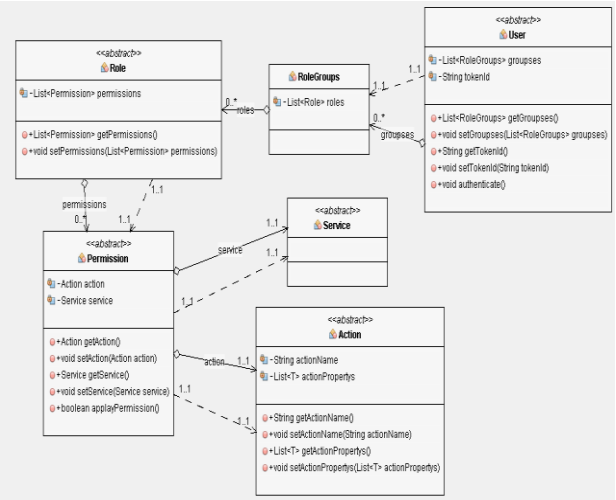
۴-۶-۱- مدل انتزاعی برای مجوز دسترسی

در این مدل انتزاعی یک ساختار بر اساس ترکیب روش‌های RBACK ,PBACK عمل شده است. در خصوص نحوه احراز هویت نیز باتوجه‌به تنوع روش‌های احراز هویتی که می‌تواند برای سازمان در نظر گرفته شود، یک کاربر انتزاعی تعریف شده که می‌تواند در مدل‌های مختلف پیاده‌سازی شود.موجودیت‌های این مدل که به مدل ارائه شده در قالب راه‌حل‌های امنیتی اضافه می‌شوند عبارت‌اند از:

- User: موجودیت انتزاعی کاربر که می‌تواند در مدل‌های مختلف توسعه یابد و در زمان احراز هویت یک توکن به آن اختصاص می‌یابد که این توکن هم باتوجه‌به قوانین حاکمیتی می‌تواند از روش‌های مختلفی تولید و کنترل شود. این توکن ملاک و شناسه اصلی کاربر در زمان اجرای سرویس می‌شود که در زمان اجرا باید وجود داشته باشد.
- roleGrope: لیست نقش‌هایی که یک کاربر می‌تواند.
- Role: موجودیت نقش که به‌صورت پویا در سیستم ایجاد و تغییر می‌کند، مانند نقش‌های سازمانی نیست، این نقش‌ها صرفاً برای ایجاد یک رابطه مفهومی قابل‌درک بین تقسیمات و دسته‌بندی دسترسی به عمل‌های قابل‌اجرا و همچنین سرویس‌های قابل‌دسترسی یک کاربر می‌باشد.
- Permission: مجوزهای هر نقش را مشخص می‌کند که هر نقش چه مجوزهایی را می‌تواند داشته باشد، این مجوزها برای بیان قوانین دسترسی و مجوزهای دسترسی به سرویس و عمل قابل انجام روی آن است که بر اساس قوانین حاکمیت در سیستم ثبت می‌شوند.

- Action: عملی که بر روی سرویس می‌تواند انجام شود و همچنین نیازمندی‌های آن در خصوص ورودی و خروجی‌های هر عمل در اجرای سرویس تشریح می‌کند. در حقیقت آنچه در اجرای سرویس باید باشد و همچنین آنچه به‌عنوان خروجی سرویس باید به کاربر نشان داده شود در این قسمت تعریف می‌شود.
- Service: یک نگاشت بین سرویس اصلی و آنچه سرویس‌گیرنده می‌بیند ایجاد می‌کند.

در شکل ۸ یک مدل انتزاعی از آنچه بیان شد، نمایش داده می‌شود.



شکل ۸ : مدل انتزاعی ساختار داده‌های برای مدل پیشنهادی

۴-۶-۲- طراحی Security Framework GNAF

برای سیستم مذکور یک قاب امنیتی GNAF در نظر گرفته شده است که وظیفه مدیریت دسترسی در خدمات را دارد. باتوجه‌به اینکه مدیریت دسترسی در این‌چنین سامانه‌هایی ترکیبی از چندین خدمت است، در لایه مسیریابی خدمات موردنظر که امکان فراخوانی دارند، فراخوانده شده و پس از واکشی اطلاعات باتوجه‌به قوانین دسترسی اطلاعاتی که قابل نمایش است به سمت درخواست دهنده ارسال شود. یعنی می‌توان این‌گونه بیان کرد که دسترسی در این سطح بر ورودی عملکرد و جزئیات خروجی تمرکز دارد، یعنی یک وضعیت کاملاً انحصاری که با استفاده از چارچوب راه‌حل امنیتی می‌توان آن را ایجاد کرد.

۴-۶-۲-۱ مدل انتزاعی برای Security Framework

مدل ارائه شده به ساختار مدل ارائه شده در security solution frame اضافه می‌شود و باتوجه‌به ساختار آن تغییرات لازم را در نظر می‌گیرد. در این روش باتوجه‌به اینکه ساختار هر درخواست به‌صورت request/response است دو فرایند جدا اجرا می‌شود.

۴-۶-۲-۲- فرایند ارسال سرویس به سرویس دهند

در این مدل ساختار از چندین مبحث اصلی تشکیل می‌شود که باید به ترتیب اجرا گردند، این مراحل عبارت‌اند از:

- تجزیه‌وتحلیل در خواست

هدف این کلاس بررسی درخواست از دید امکان‌سنجی است بدون درنظرگرفتن اینکه چه خدمتی است باید نیازمندی‌های اجرایی آن را بررسی و خدمت درخواستی را بررسی کند تا در صورت عدم وجود خدمت و یا حتی مختل شدن عملکرد آن از اجرای فرایند جلوگیری کند. هدف اصلی از ارائه این خدمت بالابردن سطح کارایی سیستم در مواجه با شرایط نامتعارف است، مانند عدم دسترسی به سرویس و یا ... از اجرای مراحل بعدی که هزینه بیشتری دارند جلوگیری کند. این کلاس باید خدمت و همچنین نوع عمل موردنظر را هم‌زمان بررسی و تجزیه‌وتحلیل نماید.

- ثبت درخواست دهنده RegisterUser

در این مرحله کاربر درخواست دهنده (کاربر/ سیستم/ دستگاه/ارگان) باید احراز هویت شود. در این مرحله باتوجه‌به پیچیدگی‌های مختلف در نحوه احراز هویت موجودیت کاربر به‌صورت انتزاعی در نظر گرفته شده است.

- اعتبارسنجی در خواست RequestValidator

اگر کاربر احراز هویت شود، مرحله اعتبارسنجی خدمت انجام می‌پذیرد که آیا اجرای این درخواست برای این کاربر قابل اعطا است یا نه. در این قسمت صرفاً دسترسی به خود سرویس بررسی و احراز هویت می‌گردد.

- اعتبارسنجی فعالیت activityValidator

در این مرحله نوع اقدامی که در نظر گرفته شده است بررسی و شرایط احراز هویت برای عمل مذکور در خدمت اعلام شده بررسی می‌گردد و همچنین باتوجه‌به این‌که در عمل به یکسری نیازمندی و ورودی نیاز دارد بررسی می‌گردد که این درخواست پیش‌نیازهای لازم را دارد یا نه. مثلاً اگر برای اجرای خدمت خاصی نیاز به ارسال سه پارامتر وجود دارد، آیا این پارامترها به‌درستی مقداردهی شده‌اند یا نه.

- آماده‌سازی سرویس قابل‌اجرا enrichmentService

باتوجه‌به اینکه خدمات ارائه شده توسط GNAF یک مدل نگاشت شده به خدمات اصلی هستند و سرویس‌گیرنده هیچ اطلاعاتی از سرویس اصلی ندارد، باید درخواست خدمت به یک سرویس قابل‌اجرا واقعی تبدیل شده و اجرا گردد. بر همین اساس در این مرحله خدمت اصلی ساخته شده و به مسیریاب جهت اجرا ارسال می‌شود.

۴-۶-۲-۳- مرحله برگشت جواب و ارسال به سرویس‌گیرنده

باتوجه‌به اینکه محدودیت اطلاعات نمایش‌داده‌شده به درخواست‌کننده در خدمات توزیع شده به‌خصوص در سیستم‌های حاکمیتی باتوجه‌به اهمیت اطلاعات بسیار مهم است، از این مرحله برگشت اطلاعات نیز باید ماژول امنیتی یکسری موارد مهم را به ترتیب اجرا کند. این موارد به ترتیب عبارت‌اند از:

۱. اعتبارسنجی جواب برگشتی validateResponse

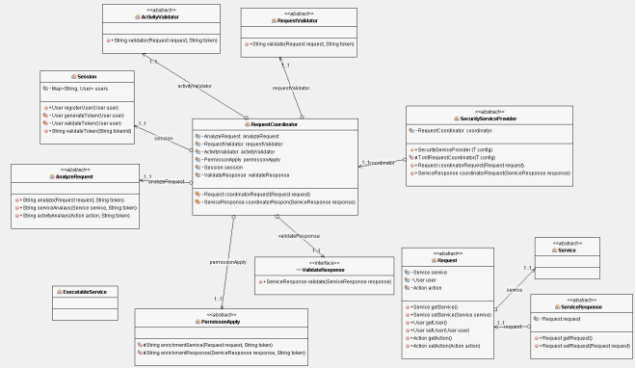
دو هدف در این مرحله پیگیری می‌شود:

- بررسی صحت داده برگشتی باتوجه‌به قوانین تعریف شده در سیستم
- بررسی مجوز دسترسی درخواست‌کننده خدمت به اطلاعات

۲. آماده‌سازی اطلاعات برگشتی enrichmentResponse

پس از اینکه صحت جواب برگشتی و همچنین صحت دسترسی به خدمت برگشتی تأیید شد، در این مرحله باید بر اساس قوانین دسترسی تعریف شده به کاربر اطلاعات برگشتی بررسی و اطلاعات اضافی حذف شوند.

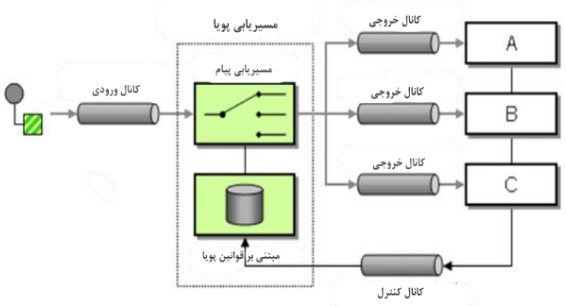
در شکل زیر مدل ارتباطی این رویدادها که به‌صورت انتزاعی بیان شده نشان داده می‌شود.



شکل ۹: مدل انتزاعی رویدادهای کنترل دسترسی پیشنهادی

۴-۶-۳- مدل اجرایی Apache Camel

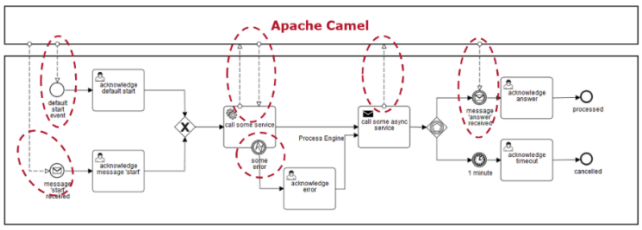
در این تحقیق برای یکپارچه‌سازی خدمات از apache camel استفاده شده است که به‌طورکلی می‌توان معماری مشابه به معماری انتخابی آن را در این تحقیق در شکل ۱۰ نشان داد.



شکل ۱۰ : مدل ارتباطی مسیریابی در مدل پیشنهادی بر اساس قوانین دسترسی

قسمت Dynamic Router قسمتی است که در این تحقیق تغییر خواهد یافت و قوانین و نحوه مدیریت ساختار موردنظر در GNAF به آن اعمال خواهد شد.

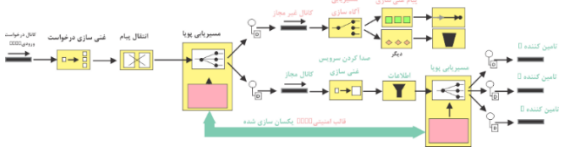
باتوجه‌به اینکه پروژه GNAF داری یک ساختار فرایندی است که بین سازمان‌ها و ارگان‌ها و اشخاص مختلف در حال اجرا است، برای اجرای این فرایند از این معماری که به‌صورت شکل ۱۱ می‌باشد استفاده شده است.



شکل ۱۱: معماری مسیریابی apache camel

۴-۶-۴- مدل معماری تغییریافته با ترکیب مدل security frame و GNAF Apache camel

پس از ترکیب مدل امنیتی پیشنهادی برای GNAF با Appache Camel یک معماری با ساختار شکل ۱۲ به دست می‌آید که قابلیت اجرای موارد بیان شده در صورت‌مسئله را دارد.



شکل ۱۲ : ترکیب مدل انتزاعی امنیتی پیشنهادی برای GNAF بر اساس ساختارهای مسیریابی و قالب امنیتی

۵. جمع‌بندی روش ارائه شده

بررسی‌های انجام شده در خصوص موضوع تحقیق برای پاسخگویی به سؤالات ارائه شده در فصل اول و همچنین موارد مطرح شده در خصوص نیازمند یک مقایسه کامل در خصوص روش‌های موجود می‌باشد.

این بررسی‌ها به‌صورت میدانی و باتوجه‌به موارد مطالعاتی بیان شده در این مقاله انجام شده است و مقایسه رخداده به‌صورت استنتاجی باتوجه‌به ماهیت هر روش بیان می‌شود.

۵-۱-مقایسه و ارزیابی روش ارائه شده

در این قسمت به مقایسه روش‌هایی که می‌تواند برای ارائه GNAF در نظر گرفت را با مدل پیشنهادی در این تحقیق می‌پردازیم.

۵-۱-۱- روش بررسی

روش‌های مختلفی برای پیاده‌سازی GNAF وجود دارد که در اینجا به چند مورد از آن اشاره می‌شود و با روش ارائه شده مقایسه می‌شود.

- روش A2A
- روش B2B
- روش اشتراک‌گذاری داده
- روش EMB

۵-۱-۲- مقایسه از دید کسب‌وکار

در مقوله مقایسه از دید کسب‌وکار که در جدول ۱ نمایش داده شده است بر اساس پارامترهای زیر مطرح می‌شود:

الف) مالکیت اطلاعات

ب) توسعه کسب‌وکار

پ) وابستگی تغییرات

ت) استقلال سرویس‌دهنده و مصرف‌کننده

جدول ۱: مقایسه روش‌ها از دید کسب‌وکار

	الف	ب	پ	ت
روش پیشنهادی	در اختیار مالک	آسان عدم وابستگی کامل	کاملاً مستقل	کاملاً مستقل
A۲A	در اختیار مالک	سخت وابستگی شدید	کاملاً وابسته	کاملاً وابسته
B۲B	در اختیار مالک	سخت وابستگی شدید	کاملاً وابسته	کاملاً وابسته
اشتراک گذار داده‌ها	در اختیار همه	سخت وابستگی به داده‌های اشتراکی	نسبت به تغییر در حوزه داده متغیر	کاملاً مستقل
EMB	قابل مدیریت	سخت وابستگی به داده	نسبت به تغییر در حوزه داده متغیر	کاملاً مستقل

۵-۱-۳- مقایسه از دید فنی

مقایسه معیارهای فنی که در جدول ۲ نشان داده شده است شامل پارامترهای به شرح زیر می‌باشد:

الف) زبان برنامه‌نویسی

ب) پلتفرم

پ) تکنولوژی

ت) توزیع‌پذیری

جدول ۲ : مقایسه از دید فنی

	الف	ب	پ	ت
روش پیشنهادی	مستقل	مستقل	مستقل	بسیار بالا
A۲A	وابسته به نوع ارائه سرویس	وابستگی شدید	مستقل	ندارد
B۲B	بسته به نوع ارائه سرویس (وب‌سرویس مستقل)	وابستگی شدید	مستقل	ندارد
اشتراک گذار داده‌ها	مستقل	مستقل	وابسته به زیرساخت	وابسته به تکنولوژی
EMB	مستقل	مستقل	وابسته به زیرساخت	وابسته به تکنولوژی

۵-۱-۴- مقایسه از دید نگهداری

معیارهای فنی برای مقوله نگهداری سیستم که در جدول ۳ بررسی شده است به شرح زیر می‌باشد:

الف) SLA

ب) وابستگی به محیط

پ) TTM

ت) دامنه برنامه

جدول ۳ : مقایسه از دید نگهداری سیستم

	الف	ب	پ	ت
روش پیشنهادی	بالا	بالا	پایین	بسیار بالا
A۲A	وابسته به تک‌تک خدمت دهنده	وابسته به تکنولوژی	بالا	بسیار پایین
B۲B	وابسته به تک‌تک خدمت دهنده	وابسته به تکنولوژی	بالا	بسیار پایین
اشتراک گذار داده‌ها	بالا	پایین	پایین	بالا
EMB	بالا	وابسته به تکنولوژی	متوسط	بالا

۵-۱-۵- مقایسه از دید کنترل و بازرسی امنیتی

در جدول ۴ مقایسه از دید کنترل و بازرسی امنیتی نشان داده می شود پارامتری اعمال شده به شرح زیر می باشد :

الف) کنترل دسترسی موردی

ب) کنترل دسترسی کامل

پ) مدیریت متمرکز

ت) مدیریت پویا

جدول ۴ مقایسه از دید کنترل بازرسی امنیتی

	الف	ب	پ	ت
روش پیشنهادی	دارد	دارد	دارد	دارد
A۲A	دارد	ندارد	ندارد	ندارد
B۲B	دارد	ندارد	ندارد	ندارد
اشتراک گذار داده‌ها	دارد	ندارد	دارد	ندارد
EMB	دارد	ندارد	دارد	ندارد

۵-۱-۶- مقایسه از دید هزینه و اجرا

از دید اجرا و هزینه، موارد زیر مورد بررسی قرار می‌گیرد:

الف) هزینه زیرساخت

ب) دانش زیرساخت

پ) هزینه نگهداری

ت) هزینه توسعه

این مقایسه در جدول ۵ بیان شده است.

جدول ۵: مقایسه از دیده هزینه اجرا

	الف	ب	پ	ت
روش پیشنهادی	بسیار بالا	بسیار بالا	بسیار بالا	بسیار بالا
A۲A	پایین	پایین	پایین	امکان توسعه ندارد
B۲B	متوسط	پایین	پایین	امکان توسعه کم‌هزینه بالا
اشتراک‌گذاری داده‌ها	بسیار بالا	بالا	بالا	بالا
EMB	بالا	بالا	بالا	بالا

۵-۲-ارزش‌گذاری و جمع‌بندی

پس از بررسی موردی هر قابلیت باتوجه‌به مطالب ارائه شده در این قسمت باارزش گذاری با چهار وضعیت خیلی بد، بد، خوب و خیلی خوب به نتایج مذکور ، جمع بندی در جدول ۶ بیان شده است.

جدول ۶: مقایسه کلی

	روش پیشنهادی	A۲A	B۲B	اشتراک گذار داده‌ها	EMB
مالکیت اطلاعات	بسیار خوب	بسیار خوب	بسیار خوب	بسیار بد	خوب
توسعه کسب‌وکار	بسیار خوب	بسیار بد	بسیار بد	بسیار بد	خوب
وابستگی تغییرات	بسیار خوب	بسیار بد	بسیار بد	بد	بد
استقلال خدمت دهنده و مصرف‌کننده	بسیار خوب	بسیار بد	بسیار بد	بد	بد
زبان برنامه‌نویسی	بسیار خوب	خوب	خوب	بسیار خوب	بسیار خوب
پلتفرم	بسیار خوب	بد	بد	بسیار خوب	بسیار خوب
تکنولوژی	بسیار خوب	بسیار خوب	بسیار خوب	خوب	خوب
توزیع‌پذیری	بسیار خوب	بد	بد	خوب	خوب
SLA	بسیار خوب	بد	بد	خوب	خوب
وابستگی به محیط	بسیار خوب	بد	بد	خوب	خوب
TTM	بسیار خوب	بد	بد	خوب	خوب
دامنه برنامه	بسیار خوب	بسیار بد	بسیار بد	خوب	خوب
کنترل دسترسی موردی	بسیار خوب	بسیار خوب	بسیار خوب	بسیار خوب	بسیار خوب
کنترل دسترسی کامل	بسیار خوب	بسیار بد	بسیار بد	خوب	خوب
مدیریت متمرکز	بسیار خوب	بسیار بد	بسیار بد	خوب	خوب
مدیریت پویا	بسیار خوب	بسیار بد	بسیار بد	بد	بد
هزینه زیرساخت	بسیار بد	بسیار خوب	بسیار خوب	بد	بد
دانش زیرساخت	بسیار بد	بسیار خوب	بسیار خوب	بد	بد
هزینه نگهداری	بسیار بد	بسیار خوب	بسیار خوب	بد	بد
هزینه توسعه	بسیار بد	امکان ندارد	امکان ندارد	بد	بد

باتوجه‌به مقایسه انجام پذیرفته آنچه مشخص است، هزینه تولید و اجرای این روش باتوجه‌به معماری خدمات محور بالا می‌باشد، ولی تا حدودی مشکلات عمده‌ای در ساختار GNAF بر اساس ساختار حاکمیتی در کشور وجود دارد می‌تواند یک گزینه مناسب برای اجرا باشد.

۶. نتیجه‌گیری

داشتن یک آدرس معتبر و دقیق در دسترس برای هر کشور مزایای عمده در حوزه‌های مختلف اقتصادی، خدمت‌رسانی، مدیریت شهری، مدیریت بحران و ... دارد؛ لذا تبدیل و نگهداری آدرس‌های غیراستاندارد موجود به یک آدرس استاندار که مزایای موردنظر را داشته باشد جز نیازهای هر حاکمیتی می‌باشد. در کشور ما نیز از سال ۱۹۹۳ با دستور رئیس‌جمهور پروژه GNAF اجرایی شد. GNAF امکان بررسی و صحت‌سنجی یک نشانی فیزیکی به همراه موقعیت و مختصات جغرافیایی آن را در کشور مقدور می‌سازد .همچنین به‌واسطه ایجاد و راه‌اندازی پایگاه ملی GNAF امکان تعیین موقعیت دقیق نشانی‌های فیزیکی حاصل خواهد شد .هر نشانی که در GNAF ایجاد شده، بین چند نشانی همسان در برابر مجموعه داده مکانی مربوطه مقایسه می‌شود تا بدین ترتیب یک قطعه ملکی، معابر و یا موقعیت مکانی آن نقطه و وجود یا عدم وجود صحت سنجی و راست آزمایی گردد و همچنین کیفیت نشانی آن سنجیده می‌شود. این توانایی‌ها شامل کاربرد روشمند آن برای ایجاد فهرست دقیق و با کیفیت از آدرس‌هایی بود که از چندین منبع مختلف جمع‌آوری می‌شد .در خصوص جمع‌آوری این اطلاعات از منابع مختلف و همچنین ارائه آن به استفاده‌کنندگان در گروه‌های مختلف باعث می‌شود روش‌های مختلفی امکان ارائه این روشمندی را فراهم کنند. باتوجه‌به اینکه معماری سرویس‌گرا ماهیت یکپارچه‌سازی را به شکل فرایند ارائه می‌دهد یک گزینه مناسب برای ایجاد این روشمندی است. در کنار این قابلیت باتوجه‌به حساسیت اطلاعات جغرافیایی در تنوع دسته‌بندی کاربران یک چالش عمده در ساختارهای امنیت اطلاعاتی است. ایجاد یک سرویس احراز هویت و اعطا دسترسی متمرکز به اطلاعات باعث می‌شود که مدیریت امنیت اطلاعات در این سامانه، متمرکز و مبتنی بر قوانین حاکمیت باشد که باعث جلوگیری از دسترسی‌های غیرمجاز کل سیستم شود. باتوجه‌به تنوع پروتکل‌های احراز هویت و همچنین امکان ترکیب این پروتکل‌ها در سطوح مختلف، نیاز به یک مدل امنیتی که بتواند این ترکیب و پیچیدگی ناشی از آن را در سطح قابل قبولی مدیریت کند و باعث کاهش کیفیت سرویس نگردد، وجود دارد. استفاده از قاب امنیتی برای ایجاد سرویس امنیتی باتوجه‌به اینکه تمامی قابلیت‌های سرویس را به همراه توانایی‌های ترکیب‌پذیری ایجاد می‌کند باعث ارائه رویکردی مؤثر می‌گردد.

مراجع

[۱] PSMA Australia Limited is a company owned by state, territory and Australian governments at: www.psma.com.au , 2014.

[۲] The Federal Geographic Data Committee at: www.fgdc.gov,, 2013.

[۳] سرپولکی و محمد، سیستم آدرس‌دهی استرالیا، نشریه علمی مهندسی نقشه‌برداری و اطلاعات مکانی، جلد ۴، شماره ۲، ص ۴۱ تا ۴۸، ۲۰۱۳.

[۴] Schmutz, G., Liebhart, D. and Welkenbach, P., Service-oriented Architecture: An Integration Blueprint: a Real-world SOA Strategy for the Integration of Heterogeneous Enterprise Systems: Successfully Implement Your Own Enterprise Integration Architecture Using the Trivadis Integration Architecture Blueprint, Packt Pub, 2010.

[۵] Ehikioya, S.A. and Olukunle, A.A. A Formal Model of Distributed Security for Electronic Commerce Transactions Systems. International Journal of Networked and Distributed Computing, ۷(۲), pp.۶۸-۸۴, ۲۰۱۹.

[۶] Uzunov, A.V., Fernandez, E.B. and Falkner, K., Security solution frames and security patterns for authorization in distributed, collaborative systems. Computers & Security, Vol. 55, pp. 193-234, 2005.

[۷] Uzunov, A.V., Fernandez, E.B. and Falkner, K., Securing distributed systems using patterns: A survey in Computers & Security, Vol. 31, No. 5, pp. 681-703, 2012.

[۸] Kermarrec, A.M., Triantafillou, P., Xl peer-to-peer pub/sub systems. ACM Computing Surveys (CSUR), Vol. 46, No. ۲, pp.۱-۴۵, ۲۰۱۳.

[۹] Pourzandi, M., Gordon, D., Yurcik, W. and Koenig, G.A, Clusters and security: distributed security for distributed systems in CCGrid, IEEE International Symposium on Cluster Computing and the Grid, Vol. ۱, pp.۹۶-۱۰۴, ۲۰۰۵.

[۱۰] Schmidt, D.C, Design patterns in communications software in Cambridge University Press, Vol. ۱۹, ۲۰۰۱.

[۱۱] Josuttis, N.M., SOA in practice: the art of distributed system design. O'Reilly Media, Inc, ۲۰۰۷.

[۱۲] Lewis, G., Morris, E., Simanta, S. and Smith, D., Service orientation and systems of systems in IEEE software, Vol.۲۸, No.۱, pp.۵۸-۶۳, ۲۰۱۰.

[۱۳] Sukatmi, S. and Afriyanto, A.. IMPLEMENTASI E-GOVERNMENT BERBASIS SERVICE ORIENTED ARCHITECTURE (SOA) PADA KANTOR KECAMATAN NATAR LAMPUNG SELATAN. Jurnal Informasi dan Komputer,۷ (۱) , pp.۷۵-۸۲, ۲۰۱۹.

[۱۴] Gold, N., Mohan, A., Knight, C. and Munro, M., Understanding service-oriented software in IEEE software, Vol.۲۱, No. ۲, pp.۷۱-۷۷, ۲۰۰۴.

[۱۵] Kajko-Mattsson, M., Lewis, G.A. and Smith, D.B., A framework for roles for development, evolution and maintenance of SOA-based systems in International Workshop on Systems Development in SOA Environments. pp. ۷-۷, ۲۰۰۷.

[۱۶] Gold, N. and Bennett, K., Program comprehension for web services in Proceedings۱۲th IEEE International Workshop on Program Comprehension, pp. ۱۵۱-۱۶۰, ۲۰۰۴.

[۱۷] Uzunov, A.V., A survey of security solutions for distributed publish/subscribe systems in Computers & Security, Vol.۶۱, pp.۹۴-۱۲۹, ۲۰۱۶.

[۱۸] Schelp, j., Stutz. M., SOA-Governance.HMD – Praxis derWirtschaftsinformatik, Vol.۲۵۳, No. ۲۵۳, pp.۷۳-۶۶, ۲۰۰۷.

[۱۹] Ferraiolo, D., Kuhn, D.R. and Chandramouli, R., Role-based access control. Artech House, ۲۰۰۳.

[۲۰] Ferraiolo, D.F., Sandhu, R., Gavrila, S., Kuhn, D.R. and Chandramouli, R., ۲۰۰۱, Proposed NIST standard for role-based access control in ACM Transactions on Information and System Security (TISSEC), Vol۴, No.۳, pp.۲۲۴-۲۷۴.

[۲۱] Computer Security Center (US), Computer Security Requirements: Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments in Dod Computer Security Center, ۱۹۸۵.

[۲۲] Ferraiolo, D. and Richard, D. Kuhn. D., Role-based access controls in Proceedings of the ۱۵th NIST-NSA National Computer Security Conference, Baltimore, Maryland., pp. 554-563, 1992.

[۲۳] Ferraiolo, D., Atluri, V. and Gavrila, S., The Policy Machine: A novel architecture and framework for access control policy specification and enforcement. Journal of Systems Architecture, Vol. 57, No. 4, pp. 412-424, 2011.

[۲۴] Ferraiolo, D., Cugini, J. and Kuhn, D.R., Role-based access control (RBAC): Features and motivations In Proceedings of ۱۱th annual computer security application conference, pp. 241-248, 1995.

[۲۵] Joshi, J.B., Bertino, E., Latif, U. and Ghafoor, A., A generalized temporal role-based access control model. IEEE transactions on knowledge and data engineering, Vol. 17, No. 1, pp. 4-23, 2005.

[۲۶] Bouzida, Y., Logrippo, L. and Mankovski, S., Concrete-and abstract-based access control. International journal of information security, Vol. 10, No. 4, pp. 223, 2011.

[۲۷] Trninić, B., Sladić, G., Milosavljević, G., Milosavljević, B. and Konjović, Z., Policydsl: Towards generic access control management based on a policy metamodel In IEEE ۱۲th International Conference on Intelligent Software Methodologies, Tools and Techniques (SoMeT), pp.۲۱۷-۲۲۳, ۲۰۱۳.

[۲۸] de Gramatica, M., Labunets, K., Massacci, F., Paci, F. and Tedeschi, A., The role of catalogues of threats and security controls in security risk assessment: an empirical study with ATM professionals In International Working Conference on Requirements Engineering: Foundation for Software Quality, pp. ۹۸-۱۱۴, ۲۰۱۵.

[۲۹] Belapurkar, A., Chakrabarti, A., Ponnapalli, H., Varadarajan, N., Padmanabhuni, S. and Sundarrajan, S., Distributed systems security: issues, processes and solutions in John Wiley & Sons, ۲۰۰۹.

[۳۰] Davis, N., Humphrey, W., Redwine, S.T., Zibulski, G. and McGraw, G., Processes for producing secure software in IEEE Security & Privacy, Vol.۲, No. ۳, pp.۱۸-۲۵, ۲۰۰۴.

[۳۱] Rosado, D.G., Fernández-Medina, E., López, J. and Piattini, M., Analysis of secure mobile grid systems: a systematic approach. Information and Software Technology, Vol. ۵۲, No. ۵, pp.۵۱۷-۵۳۶, ۲۰۱۰.

[۳۳] Bunke, M., Koschke, R. and Sohr, K., Organizing security patterns related to security and pattern recognition requirements in International Journal on Advances in Security, Vol. ۵, No. ۱, ۲۰۱۲.

[۳۳] Uzunov, A.V., Fernandez, E.B. and Falkner, K., Security solution frames and security patterns for authorization in distributed, collaborative system in Computers & Security, Vol.۵۵, pp.۱۹۳-۲۳۴, ۲۰۱۵.

[۳۴] Bertino, E. and Sandhu, R., Database security-concepts, approaches, and challenges. IEEE Transactions on Dependable and secure computing, Vol.۲, No. ۱, pp.۲-۱۹, ۲۰۰۵.

[۳۵] di Vimercati, S.D.C., Foresti, S. and Samarati, P., Recent advances in access control In Handbook of Database Security in Springer, Boston, MA., pp. 1-26, 2008.

[۳۶] Sandhu, R., The authorization leap from rights to attributes: maturation or chaos? In Proceedings of the ۱۷th ACM symposium on Access Control Models and Technologies, pp. ۶۹-۷۰, ۲۰۱۲.

[۳۷] Tolone, W., Ahn, G.J., Pai, T. and Hong, S.P., Access control in collaborative systems in ACM Computing Surveys (CSUR), Vol. ۳۷, No. ۱, pp.۲۹-۴۱, ۲۰۰۵.
[۳۸] Barker, S., The next ۷۰۰ access control models or a unifying meta-model? In Proceedings of the ۱۴th ACM symposium on Access control models and technologies, pp.۱۸۷-۱۹۶, ۲۰۰۹.
[۳۹] Microsoft , Data patterns, 1st ed. Microsoft Press Pub, 2004.
[۴۰] Delessy, N.A. and Fernandez, E.B., A pattern-driven security process for SOA applications in 2008 Third International Conference on Availability, Reliability and Security, pp. 416-421, 2008.
[۴۱] Delessy, N., Fernandez, E.B., Larrondo-Petrie, M.M. and Wu, J., Patterns for access control in distributed systems in Proceedings of the ۱۴th Conference on Pattern Languages of Programs, pp. 1-11, 2007.

زیرنویس

1. Geocoded National Address File
2. Public Sector Mapping Agencies
3. Integration
4. Distributed Systems
5. Peer-To-Peer-Based
6. Publish/Subscribe
7. Middleware
8. Single-System Image(SSI)
9. Remote Procedure Calls
10. Middleware Frameworks
11. Service Oriented Architecture
12. Loosely
13. SOA Governance
14. Confidentiality
15. Integrity
16. Availability
17. Access control
18. Discretionary Access Control(DAC)
19. Object Ownership
20. Mandatory Access Control(MAC)
21. Role-based Access Control(RBAC)
22. Role Base
23. Authorization
24. Attribute-based access control(ABAC)
25. Granularity
26. Policy Enforcement Point (PEP)
27. Policy Decision Point (PDE)
28. Policy Information Point (PIP)
29. Policy Administration Point (PAP)