ششمین کنفرانس بین المللی انجمن رمز ایران
۱۵ و ۱۶ مهر ماه ۱۳۸۸، دانشگاه اصفهان
انجمن رمز ایران
دانشگاه اصفهان

کاربرد گراف سیاست مقید شده جهت توصیف و تحلیل سیاست‌های کنترل دسترسی در فرآیندهای BPEL

زهرا درخشنده ، بهروز ترک لادانی، ناصر نعمت بخش

دانشکده فنی مهندسی، گروه کامپیوتر، دانشگاه اصفهان

اصفهان، ایران

{derakhshandeh, ladani, nemat}@eng.ui.ac.ir

چکیده

ترکیب وب‌سرویس‌ها از ایده‌های نو در زمینهٔ سیستم‌های مبتنی بر سرویس است. روش‌های ترکیب وب‌سرویس‌ها تنها به توصیف ویژگی‌های عملکردی وب‌سرویس ترکیبی می‌پردازند. به علاوه تحقیقاتی نیز که به وارسی و تحلیل فرآیند ترکیبی پرداخته‌اند، تنها نیازمندی‌های عملکردی ترکیب را مدنظر قرار داده‌اند. کنترل دسترسی به عنوان یکی از ویژگی‌های غیرعملکردی در ترکیب وب‌سرویس‌ها، از نمونه مواردی است که نیاز به توصیف و تحلیل درستی دارد. این امر به‌منظور اطمینان از درستی فرآیند ترکیب، تضمینِ برآوردن سیاست‌های کنترل دسترسی وب‌سرویس‌های شریک و عدم نقض یک سیاست توسط سیاست‌های دیگران الزامی است. در این مقاله با استفاده از مدل کنترل دسترسی گراف سیاست مقید شده (CPG)، طریقهٔ توصیف سیاست‌های کنترل دسترسی وب‌سرویس‌ها و روش استخراج مدل کنترل دسترسی حاصل از ترکیب آنها را بیان می‌کنیم. به علاوه، با استفاده از این مدل امکان وارسی و تحلیل سیاست‌ها به منظور کشف ناسازگاری یا برخورد در میان آنها فراهم می‌آید. در پایان به عنوان نمونه‌ای از کاربرد روش ارائه شده، به مدل کردن سیاست‌های فرآیندهای BPEL به عنوان رایج‌ترین زبان ترکیب وب‌سرویس‌ها می‌پردازیم.

کلمات کلیدی

ترکیب وب‌سرویس‌ها، سیاست کنترل دسترسی،ترکیب سیاست‌ها، وارسی، BPEL.

۱- مقدمه

وب‌سرویس‌ها یکی از تکنولوژی‌های نوین در عرصهٔ سیستم‌های توزیع شده هستند که با ظهور اینترنت و نیاز به انجام تعاملات سازمانی توسط آن شکل گرفته و توسعه یافتند. وب‌سرویس‌ها برنامه‌های کاربردی هستند که مبتنی بر استانداردهای باز و از طریق وب، قابل دسترسی بوده و مجموعه‌ای از عملکردها[1] جهت انجام کسب و کار و یا هرگونه استفادهٔ دیگری را فراهم می‌آورند[۱]. ترکیب وب‌سرویس‌ها به منظور ایجاد وب‌سرویس‌های پیچیده‌تر یکی از روش‌های پاسخ‌گویی به درخواست‌هایی است که با استفاده از وب‌سرویس‌های موجود قابل پاسخ‌گویی نمی‌باشد [۱،۲،۳]. خصوصیت‌های یک وب‌سرویس ترکیبی به دو دستهٔ عملکردی و غیرعملکردی[2] قابل تقسیم است. خصوصیت‌های عملکردی ناظر به بیان مقتضیات روند کاری سیستم حاصل از ترکیب است اما ویژگی‌های غیرعملکردی خصوصیت‌های کیفیتی آن را دربر داشته و درگذر زمان و با تغییر علایق سازمان‌های وابسته، دچار تغییر می‌شوند. امنیت، قابلیت اطمینان و توسعه-پذیری نمونه‌هایی از خصوصیت‌های غیرعملکردی می‌باشند.

[1] Functional

[2] Non-functional

برآوردن نیاز غیرعملکردیِ امنیت، در کنار نیازمندی‌های عملکردی از ضرورت‌های اجتناب‌ناپذیر در امر ترکیب وب‌سرویس‌ها است.

در حال حاضر روش‌های متعددی جهت ترکیب وب‌سرویس‌ها ارائه شده است که عمدتاً توسط سازمان‌ها و موسسات تجاری معرفی شده‌اند و فاقد زیر بنای مبتنی بر مدل‌های صوری می‌باشند. به‌علاوه کلیهٔ این روش‌ها تنها به توصیف و یا تحلیل خصوصیت‌های عملکردی فرآیند ترکیبی پرداخته اند [۴،۵،۶،۷]. به عنوان مثال زبان BPEL، زبان رایج توصیف فرآیند ترکیب وب‌سرویس‌ها است که تنها امکان توصیف بخش عملکردی فرآیند ترکیبی را به ما می‌دهد و در بیان خصوصیات غیرعملکردی فرآیند ترکیبی ناتوان است. این مسئله یکی از موارد ابهام در زمینهٔ به‌کارگیری BPEL است [۴،۵]. حتی تحقیقات زیادی (همچون [۱۱،۸،۹،۱۰]) نیز سعی در تبدیل فرآیند ناشی از آن به مکانیزم‌هایی با شالودهٔ صوری برای ایجاد امکان تحلیل داشته‌اند اما تنها به تبدیل و تحلیل خصوصیت‌های عملکردی پرداخته‌اند. [۱۲] از معدود مواردی است که به مدل‌کردن کنترل دسترسی در ترکیب وب‌سرویس‌ها با استفاده از Event Calculus پرداخته است. روش ما با بهره‌مندی از شمای گرافیکی گراف‌ها میزان فهم بیشتری نسبت به روش‌های منطقی محض دارد. به علاوه به دلیل تعریف طبیعی و جامع‌تری از قیود در روش بکار برده شده، امکان تطابق بیشتر و ساده‌تری با انواع روش‌های ترکیب وب‌سرویس‌ها (مانند BPEL و WSCI و غیره) فراهم می‌آید.

مسئله مهم در زمینهٔ امنیت ترکیب وب‌سرویس‌ها، این است که ممکن است وب‌سرویس‌های شرکت‌کننده در ترکیب از امنیت قابل قبولی برخوردار بوده و سیاست‌های امنیتی مشخصی را دنبال کنند، اما ترکیبی از آنها، تضمین‌کنندهٔ ارضای سیاست‌های تک تک وب‌سرویس‌ها نباشد. چه‌بسا مواردی وجود دارد که وب‌سرویس‌های شریک دارای سیاست‌های کنترل دسترسی متناقضی باشند. از این‌رو نیاز به روشی برای مدل‌کردن سیاست‌های وب‌سرویس‌ها، ترکیب حاصل از آنها و تحلیل چگونگی انتقال حقوق و اطلاعات به چشم می‌خورد.

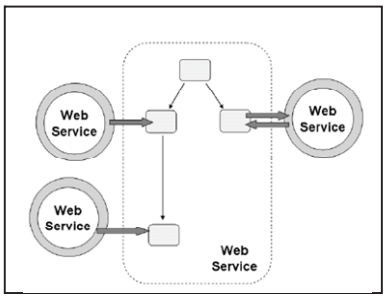
در این مقاله با استفاده از مدل کنترل دسترسی گراف سیاست مقید شده[1] (CPG) به مدلسازی و تحلیل سیاست های وب‌سرویس‌ها و ترکیب آنها می‌پردازیم. CPG یک مدل صوری کنترل دسترسی است که به توصیف سیاست‌های کنترل دسترسی می‌پردازد [۱۸]. با استفاده از این مدل امکان توصیف مقید سیاست‌ها، بیان تو در توی آنها و نیز امکان اعمال انواعی از عملگرهای ترکیب بر آنها به منظور ترکیب مجموعه‌ای از سیاست‌ها وجود دارد. به علاوه در این مدل امکانات لازم برای تحلیل و وارسی سیاست‌های کنترل دسترسی به منظور کشف ناسازگاری یا برخورد در میان سیاست‌های ترکیبی تعبیه شده است. مهم‌تر آنکه با استفاده از مدل CPG و با بهره‌مندی از قوانین انتقال آن علاوه بر مدل‌کردن انتقالات صریح حقوق و اطلاعات، می‌توان انتقالات ضمنی و غیر مستقیم موجود در سیستم که به دلیل ارتباطات نهادهای تشکیل‌دهندهٔ آن صورت می‌پذیرد را کشف و در مدل کنترل دسترسی سیستم مربوطه مدنظر قرار داد.

ترکیب وب‌سرویس‌ها به دو دستهٔ کلی ارکستر وب‌سرویس‌ها و رقص آرایی آنها تقسیم می‌شود. ما در این مقاله روش کلی استخراج مدل CPG ترکیب وب‌سرویس‌ها را بیان می‌نماییم. سپس به عنوان نمونه‌ای از کاربرد روش مطرح شده، به استخراج مدل کنترل دسترسی فرآیند BPEL ، به عنوان رایج‌ترین زبان ارکستر، می‌پردازیم. لازم به ذکر است بدین وسیله امکان مدل‌کردن خصوصیت غیرعملکردی کنترل دسترسی و تحلیل آن را با وجود فقدان زیربنای صوری و عدم توصیف ویژگی‌های غیرعملکردی در BPEL بدست آورده‌ایم.

در ادامهٔ این مقاله، ابتدا در بخش ۲ به مفهوم ترکیب وب‌سرویس‌ها و مشکلات موجود در آن می‌پردازیم. سپس در بخش ۳ مرور مختصری بر مدل کنترل دسترسی گراف سیاست مقید شده خواهیم داشت. روش کلی استخراج مدل CPG از ترکیب وب‌سرویس‌ها را در فصل ۴ مطرح خواهیم نمود. سپس در فصل ۵ به عنوان نمونه‌ای از کاربرد روش استخراج، مدل CPG حاصل از فرآیند BPEL را ارئه خواهیم کرد. در پایان در فصل ۶ به نتیجه‌گیری مقاله و بیان کارهای آتی خود می‌پرازیم.

۲- ترکیب وب‌سرویس‌ها

ترکیب وب‌سرویس‌ها یکی از ایده‌های نو در زمینهٔ سیستم‌های مبتنی بر سرویس است. به‌طورکلی ترکیب وب‌سرویس‌ها به دو دستهٔ ارکست و رقص‌آرایی وب‌سرویس‌ها تقسیم می‌شود [۱۳]. روش ارکستر، تعاملات وب‌سرویس‌ها با یکدیگر در سطح پیام را توضیح می‌دهد که در راستای منطق تجاری سرویس صورت می‌گیرند و امکان دارد کاربردها و سازمان‌ها را در سطح وسیعی به هم پیوند بزنند (شکل ۱). در این روش یک وب‌سرویس به عنوان هماهنگ‌کننده، کل فرآیند را مدیریت می‌کند [۱۳]. BPEL یکی از زبانهای معروف ارکستر وب‌سرویس‌ها می‌باشد.

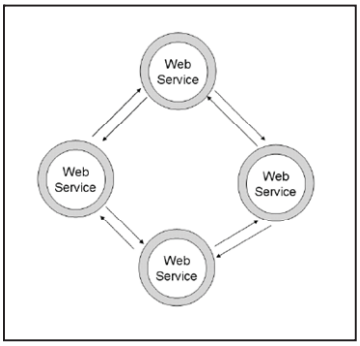


شکل ۱: ارکستر وب سرویس ها

رقص وب‌سرویس‌ها ترتیب پیام‌هایی را دنبال می‌کند که بین چندین شریک رد و بدل می‌شوند(شکل ۲). این روش با پیام‌های

[1] Constrained Policy Graph

عمومی سطح بالای رد و بدل شده بین وب‌سرویس‌ها سروکار دارد تا یک فرآیند کلی در حال اجرا. WSCI از زبانهای رقص آرایی است [۱۴].



شکل۲: رقص آرایی وب‌سرویس‌ها

از جمله زبان‌های ترکیب وب‌سرویس‌ها می‌توان به BPML، WSFL، WSCI، BPEL، XLANG و جبر فرایندها و شبکه‌های پتری اشاره کرد [۷]. از این میان مواردی همچون BPML، WSFL، WSCI، BPEL، XLANG ، فاقد زیربنای صوری و لذا فاقد امکان تحلیل و وارسی هستند و روش‌هایی همچون جبر فرایندها و شبکه‌های پتری از شالودهٔ صوری برخوردارند. اما در هر صورت کلیهٔ این روش‌ها تنها خصوصیت‌های عملکردی فرآیند ترکیبی را بیان می‌کنند [۶]. این در حالی است که تحقیقاتی همچون [۹، ۱۰، ۱۱، ۸] نیز که به تحلیل و وارسی ترکیب وب‌سرویس‌ها پرداخته‌اند، به وارسی و تحلیل خصوصیت‌های عملکردی ترکیب (و نه غیرعملکردی) توجه نموده‌اند.

ما به منظور مدل‌کردن سیاست‌های کنترل دسترسی وب‌سرویس‌ها و
ترکیب آنها و تحلیل سیاست‌های حاصل، از مدل CPG بهره می‌بریم. در بخش بعد به مرور مدل کنترل دسترسی CPG می‌پردازیم.

۳- مدل گراف سیاست مقید شده (CPG)

CPG یک مدل صوری کنترل دسترسی است که به توصیف سیاست های کنترل دسترسی می‌پردازد [۱۸]. با استفاده از این مدل امکان توصیف مقید سیاست‌ها، ترکیب آنها و تحلیل و وارسی سیاست‌ها وجود دارد. در این مدل یک سیاست (مثلاً سیاست یک سیستم یا زیر سیستم) با استفاده از یک گراف محدود مدل می‌شود. در این گراف رأس‌ها نهادهای سیستم می‌باشند و یالها بیانگر شرایطی هستند که در آن شرایط هر رأس مبدأ دارای حق/سیاستی نسبت به رأس مقصد مربوطه می‌باشد. هر رأس مبدأ معرف یک فاعل[1] (○) و هر رأس مقصد بیانگر یک مفعول[2] (●) است. فاعل‌ها می‌توانند کاربران، گروه‌ها، نقش‌ها[3] یا کاربردها و مفعول‌ها می‌توانند فایل‌ها، اسناد، و حتی فاعل‌ها باشند (امکان دارد یک رأس هر دو حالت فاعل- مفعول (⊗) را شامل شود). حقوق اولیه و اصلی تعریف شده در هر سیستمی مجموعه حقوق پایه (R) نام دارند که بسته به نیاز سیستم مربوطه تعیین می‌گردند. در ادامه تعریف رسمی یک CPG عنوان شده است [۱۸]:

۳-۱ تعریف مدل

تعریف۱: گراف سیاست مقید شده (CPG) : اگر S و O به ترتیب مجموعهٔ فاعل‌ها و مفعول‌ها باشند، گراف CPG Ψ یک دوتایی (V, L) است به‌طوری‌که:

- $V \subseteq S \cup O$ مجموعهٔ رأسها، و
- L مجموعهٔ یالهاست که $L \subseteq V \times V \times Label$ و $Label=C:P$ (P به شرط C) برچسب یال ارتباطی است، که در آن:
  - P زیرمجموعه‌ای از حقوق پایه $(P \subseteq R)$ و یا یک گراف CPG است که به‌طور بازگشتی تعریف می‌شود و
  - C قیود لازم برای داشتن حق یا سیاست P توسط رأس مبدأ نسبت به رأس مقصد است. C به صورت یک چهارتایی $(C_s, C_o, C_\alpha, C_\theta)$ تعریف می شود که در آن:
    - C_s بیانگر قید/قیود حاکم بر فاعل است. C_s در حالت پایه یک مسند است که توسط یک پارامتر به فاعل مربوطه اشاره دارد و بطورکلی با استفاده از یک فرمول منطقی (ترکیب منطقی مسندها) تعریف می‌شود.
    - C_o قید/ قیود حاکم بر مفعول که مانند C_s تعریف می‌شود اما پارامتر آن به مفعول مربوطه نگاشت می‌شود.
    - C_α تعیین‌کنندهٔ عملیاتی است که به ازای آن P توسط فاعل نسبت به مفعول معتبر است، و با استفاده از یک مسند با دو پارامتر به فاعل و مفعول مربوطه نگاشت می‌شود. در حالت کلی به وسیلهٔ یک فرمول منطقی تعریف می‌گردد.
    - C_θ بیانگر قیود زمانی می‌باشد. این قید در حالت پایه بیانگر یک بازهٔ زمانی ($[t_s, t_d]$) است و می‌تواند به صورت ترکیبی از بازه‌های زمانی گسترش یابد.

گرامر هرکدام از چهار بخش مجموعهٔ C در رابطهٔ (۱) تعریف می‌شود:

$$C_i = C_i \wedge C_i \mid C_i \vee C_i \mid \neg C_i \mid \beta \mid T \mid F \qquad (۱)$$

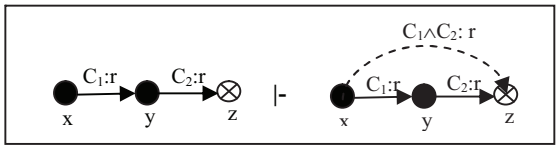
[1] Subject
[2] Object
[3] Roles

که در آن C_i یکی از موارد C_θ, C_α, C_o, C_s می‌باشد. β در حالت‌های C_α, C_o, C_s یک مسند ساده است که بسته به سیستم مربوطه تعریف می‌شود و در حالت $C_i=C_\theta$ یک بازهٔ زمانی به صورت $[t_s,t_d]$ می‌باشد و بدین معنا که حق مورد نظر در فاصلهٔ زمانی بین t_s و t_d معتبر است.

۲-۳ قوانین انتقال حقوق و اطلاعات در CPG

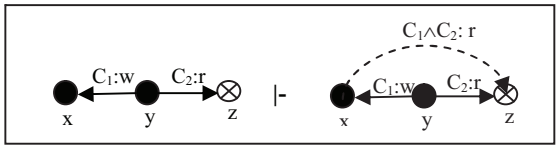
در CPG حالت توسعه‌یافته‌ای از قوانین انتقال مدل Take-Grant [۱۵] تعریف شده و بکار می‌رود. این قوانین به دلیل درنظر گرفتن قیود در مدل کردن سیاست‌ها در CPG توسعه یافته‌اند. از میان قوانین spy, find, pass, post به توضیح دو قانون زیر بسنده می‌کنیم:

- spy : فرض کنید x، y، z سه رأس متمایز در CPG_0 باشند و x و y فاعل درنظر گرفته شوند و یالی از x به y با برچسب C_1:r موجود باشد و یک یال از y به z با برچسب C_2:r وجود داشته باشد، آنگاه قانون spy گراف CPG_0 را با افزودن یک یال ضمنی جدید از x به z با برچسب $C_1 \wedge C_2$: r به گراف CPG_1 تبدیل می‌کند (شکل۳).



شکل ۳: قانون spy

- pass : به همین ترتیب شکل۴ قانونpass را نشان می‌دهد. جزئیات بیشتردر [۱۸] بیان شده است.



شکل ۴: قانون pass

ترکیب سیاست های کنترل دسترسی

گرامر ترکیب سیاست‌ها در CPG به صورت رابطهٔ (۲) می باشد:

$$K= P\cap Q \mid P\cup Q \mid P-Q \mid \neg P \qquad (۲)$$

که در آن K و P و Q سیاست (دیگر گراف‌های CPG) هستند. از این میان حالت اجتماع را به دلیل کاربرد آن در بخش‌های آتی مختصراً توضیح می‌دهیم.

اجتماع $(P\cup Q)$: بدین وسیله دو سیاست در یک سیاست که شامل اجتماعی از هر دو سیاست است ادغام می‌شوند. این عملگر دسترسی‌هایی را که یکی یا هر دو مولفه‌اش اجازه دهند می‌پذیرد.

تعریف ۲: اجتماع$(P\cup Q)$: اگر $P=(V_1, L_1)$ و $Q=(V_2, L_2)$ دو گراف CPG باشند آنگاه گراف $K=(V, L)$ گراف حاصل از اجتماع آنها می‌باشد که در آن:

$$V= V_1 \cup V_2 \ , L= L_1 \cup L_2$$

اگر رأسی در یک گراف فاعل و در گراف دیگر مفعول باشد، در گراف نتیجه به‌صورت $\otimes$ خواهد بود.

۳-۴ تحلیل سیاست‌ها

امکان دارد در زمان ترکیب دو گراف یا در زمان وارسی گراف بدست آمده از یک ترکیب به حالتی برسیم که یک فاعل به‌طور همزمان دو سیاست یا دو حق کاملاً متناقض را نسبت به یک بخش یکسان دارد. در این حالت گوییم سیستم دچار برخورد شده است.

تعریف ۳: برخورد: اگر $Q=(V, L)$ یک CPG باشد که $v_a,v_b\in V$ و $l_1=(v_a, v_b, C_a: P)\in L$ و $l_2=(v_a, v_b, C_b: \neg P)\in L$ و اگر یک تابع یکسان‌ساز θ وجود داشته باشد به‌طوری‌که $\theta(C_a)=\theta(C_b)=C_e$، آنگاه یالهای ارتباطی دو رأس v_a و v_b خواهد بود که نشان‌دهندهٔ برخورد است.

مدل CPG به منظور تحلیل چگونگی انتقال حقوق و اطلاعات از یک گزاره استفاده می‌کند. با استفاده از این گزاره نه تنها وجود یا عدم وجود حقی بین دو رأس مورد نظر پس از اعمال قوانین انتقال بررسی می‌شود، بلکه می‌توان مشخص نمود که حق مورد نظر برای یک فاعل نسبت به مفعول مربوطه، به ازای چه مجموعه شرایطی صادق است. به علاوه می‌توان بررسی کرد که آیا به ازای روی‌دادن یک قید مشخص، انتقال حقوق یا اطلاعاتی در سیستم مربوطه رخ می‌دهد یا خیر؟

تعریف ۴: گزارهٔ $can.obtain(C, \alpha, x, y, CPG_0)$ به ازای روی دادن شرط C و برای حق دسترسی α و رأس‌های x (به عنوان یک فاعل) و y (به عنوان یک مفعول یا فاعل) برقرار است اگر و تنها اگر گراف‌های $CPG_0, CPG_1, \ldots, CPG_n$ و انتقال CPG_0 $\vdash^* CPG_n$ ای موجود باشند به‌طوری‌که با استفاده از CPG_0 و توسط اعمال انتقال به گراف CPG_n دست یابیم و در گراف CPG_n یالی با برچسب $C:\alpha$ از x به y موجود باشد.

اگر مجموعهٔ تمامی قوانین انتقال مورد نظر را مجموعهٔ متناهی A فرض کنیم، انتقال از CPG_0 به CPG_n مبتنی بر اعمال کلیهٔ قوانینِ قابل اعمال بر CPG_i $(0\le i \le n-1)$ با شروع از CPG_0 صورت می‌پذیرد به شرطی‌که پس از بدست آمدن CPG_n امکان اعمال قانون بازنویسی دیگری از مجموعهٔ A، بر آن موجود نباشد. البته این فرآیند می‌تواند زمانی که نتیجهٔ مطلوب مورد نظر رویت شد خاتمه پذیرد (هنگامی که یال مورد نظر با برچسب α از x به y پدیدار شود یا به زبان دیگر سوال مورد نظر پاسخ داده شده باشد) وگرنه تا رسیدن به CPG_n ادامه می‌یابد.

پس از مرور مختصری که بر مفاهیم مدل CPG صورت گرفت، در بخش بعد به نحوهٔ استخراج مدل کنترل دسترسی در ترکیب وب‌سرویس‌ها می‌پردازیم.

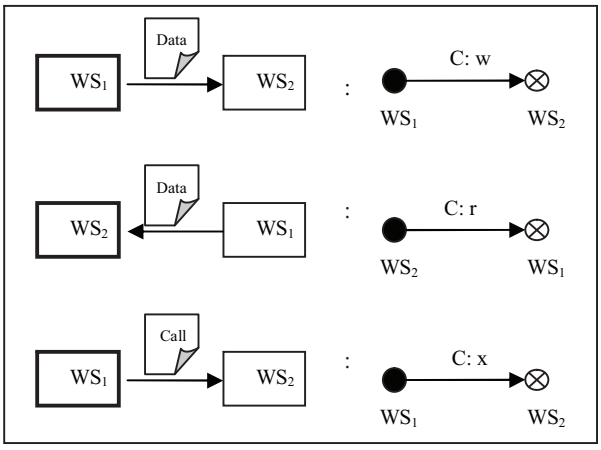
۴- استخراج مدل CPG وب‌سرویس ترکیبی

همان‌طور که دیدیم، از طریق همکاری و ارتباط تعدادی از وب-سرویس‌ها، یک ترکیب حاصل می‌شود. وب‌سرویس‌هایی که به همکاری و ارتباط با یکدیگر پرداخته‌اند ، وب‌سرویس‌های شریک در ترکیب و آنچه از این همکاری نتیجه می‌شود ترکیب وب-سرویس‌ها نام دارد. در بسیاری از موارد یک وب‌سرویس به‌طور مرکزی مدیریت این ارتباطات را بر عهده دارد (ارکستر وب-سرویس‌ها)، و در موارد دیگر بخش متمرکزی وجود ندارد و مجموعه‌ای از تعاملات میان وب‌سرویس‌ها ترکیب مورد نظر را فراهم می‌آورد (رقص آرایی). آنچه در زمینهٔ کنترل دسترسی اهمیت دارد نحوهٔ رد و بدل اطلاعات درمیان بخش‌های شرکت کننده در ترکیب است.

وب‌سرویس‌ها از طریق ارسال و دریافت اطلاعات و یا به‌طور کلی مبتنی بر احضار یکدیگر، با هم در ارتباط قرار می‌گیرند. بسته به هر یک از این موارد جریان متفاوتی از اطلاعات را بین وب-سرویس‌های مذکور خواهیم داشت که در واقع سازندهٔ مدل کنترل دسترسی ناشی از همکاری این وب‌سرویس‌هاست. به وسیلهٔ ارسال و دریافت اطلاعات بین دو وب‌سرویس، به ترتیب امکان نوشتن (w) اطلاعات یکی در دیگری، و امکان خواندن (r) اطلاعات یکی توسط دیگری فراهم می‌آید. از طرفی احضار یک وب‌سرویس توسط وب‌سرویس دیگر، حالت کلی‌تری را شامل می‌شود که آن را حق اجرای[1] وب‌سرویس نامیده و به صورت زیر تعریف می‌کنیم:

تعریف ۵: حق X : به حق اجرای یک مفعول توسط یک فاعل گفته می‌شود. این حق بسته به جریان اطلاعاتی که بین فاعل و مفعول رد و بدل می‌شود، به یکی از حقوق r,w و یا هر دو تبدیل می‌شود.

به عنوان مثال به ازای احضار وب‌سرویس ۱ توسط وب‌سرویس ۲، وب‌سرویس۱ حق اجرای وب‌سرویس ۲ را دارد. شکل ۵ انواع این ارتباطات و نحوهٔ استخراج مدل CPG حاصل از آنها را نشان می-دهد.



شکل ۵: مدل CPG حاصل از انواع رد و بدل داده در ترکیب وب-سرویس‌ها

قید C در این شکل بیانگر شرایطی است که یک وب‌سرویس به ازای برآوردن آنها چنین جریان داده‌ای نسبت به وب‌سرویس دیگر دارد. در حالت بدون شرط[2] این قید مقدار true(T) دارد که به منظور حفظ سادگی از ذکر آن خودداری می‌شود.

اکنون برای بدست آوردن سیاست نهایی ترکیب وب‌سرویس‌ها (با درنظر گرفتن سیاست وب‌سرویس‌های شریک در ترکیب) به‌صورت زیر عمل می‌کنیم:

۱- سیاست هر وب‌سرویس نسبت به نهادهای مربوط به آن (مانند پایگاه دادهٔ وب‌سرویس و یا منابع یا نهادهایی که با آنها در ارتباط است) را با استفاده از یک گراف CPG مدل می-کنیم.

۲- سیاست ترکیب وب‌سرویس‌ها را مبتنی بر آنچه در این فصل عنوان شد بدست می‌آوریم.

۳- اجتماع سیاست‌های وب‌سرویس‌های شریک (مرحلهٔ۱) و سیاست ترکیبی (مرحلهٔ۲) را طبق تعریف ۲ بدست می-آوریم.

با اعمال قوانین انتقال بر گراف نهایی بدست آمده، انتقالات ضمنی اطلاعات که به دلیل ارتباط نهادهای تشکیل دهنده در سیستم پدید آمده‌اند نیز بر آن افزوده می‌شود. از این پس می‌توان (مطابق فصل ۳) به کشف برخورد و وارسی گراف حاصل پرداخت. مثلاً درصورتی‌که در یک سیاست شریک، حق مشخصی برای یک رأس نسبت به دیگری تعریف شده باشد و در گراف ترکیب (مرحلهٔ ۲) نقیض این حق مشاهده شود، در گراف نهایی به برخورد خواهیم رسید. به علاوه ممکن است یک شریک در سیاستش گزارهٔ can.obtain را برای دو نهاد خود و به ازای یک حق مشخص، دارای مقدار نادرست بداند. می‌توانیم با اعمال قوانین انتقال بر گراف نهایی، مقدار گزارهٔ مذکور را در آن بررسی نماییم. در صورت درستی مقدار با تناقض بین سیاست‌ها مواجه شده‌ایم و در غیر این صورت سیاست ترکیبی با سیاست وب‌سرویس مورد نظرمان ناسازگار نیست. به همین ترتیب می‌توانیم به وارسی و تحلیل سیاست‌های مختلف بپردازیم. برای اطلاعات دقیق‌تر از نحوهٔ تحلیل به مثال‌های موردی [۱۸] مراجعه کنید.

به عنوان نمونه‌ای از کاربرد روش ارائه شده در بخش بعد به مدل کردن فرآیند BPEL می‌پردازیم.

۵- کاربرد روش ارائه شده در زبان BPEL

۵-۱ مروری بر زبان BPEL

BPEL به عنوان رایج‌ترین زبان ترکیب (ارکستر) وب-سرویس‌ها[۳،۱۶]، زبانی مبتنی بر XML است که در لایه فوقانی WSDLبنا شده است به‌طوری‌که عملیات‌های ارائه شده توسط یک وب‌سرویس را WSDL مشخص می‌کند و ترتیب

[1] Execute

[2] Unconditionally

فراخوانی عملیات‌ها را BPEL بیان می‌کند. BPEL از سه طریق از WSDL بهره می‌گیرد [۱۳]:

۱- هر فرآیند توصیف شده توسط BPEL خود یک وب‌سرویس است که عملیات‌ها و واسط های خود را از طریق WSDL خود بیان می‌کند.

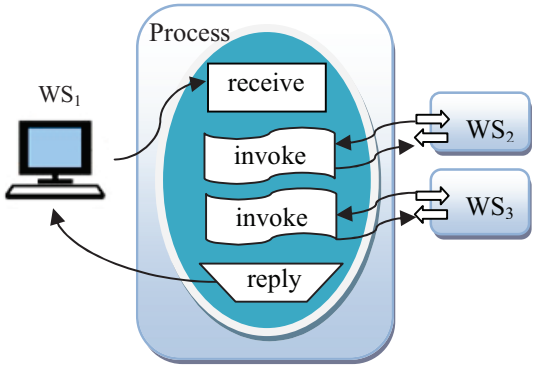
۲- انواع داده‌های موجود در WSDL توسط BPEL برای بیان اطلاعات رد و بدل شده بین درخواست‌ها استفاده می‌شود.

۳- BPEL از WSDL موجود جهت ارجاع به وب‌سرویس‌های خارجی توسط فرآیند ترکیب استفاده می‌کند.

BPEL یک فرآیند کسب و کار را مدل می‌کند که شامل مجموعه‌ای از فعالیت‌ها[1] است که بر اساس جریان کنترل تعریف شده اجرا می‌شوند[۱۶]. BPEL یک زبان توصیف ترکیب است که تنها امکان توصیف بخش عملکردی فرآیند ترکیبی را داشته و امکاناتی را برای بیان خصوصیات امنیتی ترکیب که یک ویژگی غیرعملکردی است فراهم‌نکرده است [۴،۵،۶،۱۲]. این زبان به دلیل فقدان زیربنای صوری امکان تحلیل مستقیم روند صحت را نیز ندارد و برآورده شدن خط مشی‌های امنیتی وب‌سرویس‌های شریک را تضمین نمی‌کند. این در حالی است که هر فرآیند ترکیبی قبل از ایجاد ترکیب، باید از سیاست‌های امنیتی شریکان خود آگاه گشته و در حین ایجاد و اجرای ترکیب ملزم به رعایت آنها باشد. مطالعاتی (همچون [۸،۹،۱۰،۱۱]) نیز که سعی در تبدیل آن به تکنیک‌های صوری برای ایجاد امکان تحلیل داشته‌اند، تنها به تحلیل خصوصیت‌های عملکردی پرداخته‌اند.

۲-۵ استخراج مدل CPG حاصل از فرآیند BPEL

هستهٔ مفهومی فرآیند BPEL، پیامهایی است که بین فرآیند و سرویس‌های شریک در آن رد و بدل می‌شود. سناریوی کلی در BPEL معمولاً به وسیله دریافت یک پیغام توسط فرآیند ترکیب آغاز می‌شود و سپس فرآیند مجموعه‌ای از وب‌سرویس‌های خارجی را فراخوانی می‌کند تا عملیات ترکیبی مورد نظر صورت گیرد و در نهایت پاسخ نهایی را به درخواست‌کننده اعلام می‌کند. در زمینهٔ کنترل دسترسی فعالیت‌هایی که فرآیند BPEL را با محیط خارج از خود درگیر می‌نماید، مورد نظرند؛ چرا که انتقال حقوق و اطلاعات از این طریق میسر می‌گردد. لذا از میان فعالیت‌های جدول (۱) فعالیت‌های احضار وب‌سرویس‌ها (invoke)، دریافت درخواست (receive) و پاسخ‌گویی به درخواست (reply)، پل‌های ارتباطی فرآیند ترکیبی با ارکان خارجی هستند. شکل ۶ فرمت ساده‌ای از فرآیند BPEL را متشکل از سه فرآیند مذکور نشان می‌دهد.



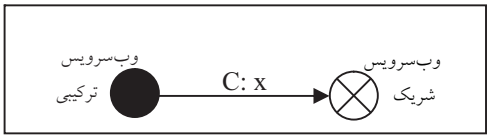
شکل ۶: فرآیند BPEL

هر فعالیت در فرآیند BPEL با یک tag نشان داده می‌شود و دارای صفت‌هایی است از آن میان برخی اجباری و برخی اختیاری می‌باشند. این صفت‌ها به ازای شریک‌های مختلف و بسته به شرایط مقدار مربوط به خود را دارند. به عنوان مثال فرآیند BPEL در سه فعالیت بالا با استفاده از خصوصیت‌هایی همچون partnerLink و portType و partner شریک ارتباطی مورد نظر آن فعالیت را مشخص می‌نماید و از طریق ایجاد ارتباط با اطلاعات مربوطهٔ موجود در فایل WSDL هر شریک، به عملیات مورد نظر (مشخص شده توسط پارامتر operation) اتصال می‌یابد. به عنوان مثال توسط پارامتر partner وب‌سرویس شریک مشخص می‌شود و توسط partnerLink یک پیوند[2] با نام مشخص بین دو شریک در سطح واسط ایجاد می‌شود. توضیح جزئی‌تر این پارامترها نیاز به بررسی جزئی اجزای سند WSDL دارد که مجال آن در اینجا نمی‌باشد. برای توضیحات بیشتر به [۱۷،۱۶] مراجعه کنید.

- invoke : فعالیت invoke عملیات احضار یک وب‌سرویس خارجی است. این فعالیت بر دو گونه یک طرفه و دو طرفه (درخواست –پاسخ) می‌باشد. بدین وسیله وب‌سرویس ترکیبی، عملیات مشخصی از وب‌سرویس شریک را فراخوانی می‌کند. وب‌سرویس ترکیبی به ازای این عملیات، حق اجرای وب‌سرویس شریک را دارد. فرمت کلی این دستور در (3) مشاهده می‌شود.

```
<invoke name=name  operation=Op_name
partner=p_name  partnerLink=PL_name          (3)
portType=PT_name … />
```

شکل (۷) مدل CPG این فعالیت را نشان می‌دهد.



شکل ۷: مدل CPG فعالیت invoke

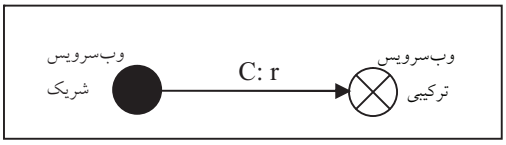
- reply : بدین وسیله وب‌سرویس ترکیبی نتیجهٔ عملیات را به درخواست‌کننده ارسال می‌کند که معادل حق خواندن (r) درخواست‌کننده نسبت به وب‌سرویس ترکیبی می‌باشد (شکل۸). دقت کنید که درخواست‌کننده نیز در حالت کلی

[1] Activities

[2] Link

یکی از وب‌سرویس‌های شریک در ترکیب است. فرمت این فعالیت در (۵) مشاهده می‌شود.

<reply name=name operation=OP_name partner=p_name partnerLink=PL_name portType=PT_name" … /> (5)



شکل ۸: مدل CPG فعالیت reply

- receive : این فعالیت مشخص می‌کند که انتظار دریافت درخواست از کدام شریک را دارد. با استفاده از پارامترهای partner و partnerLink، شریک مورد نظر فرآیند (درخواست کننده) مشخص می‌شود و با استفاده از portType و operation مشخص می‌کند که چه عملیاتی از فرآیند ترکیبی، توسط این درخواست کننده می‌تواند فراخوانی شود. بدین وسیله انجام عملیات درخواستی توسط شریک مشخص شده و ارسال نتیجه به وی توسط دستور reply مربوطه تضمین می‌شود. ترکیب یک فعالیت receive و یک فعالیت reply، یک عملیات درخواست- پاسخ را در portType مربوط به سند WSDL فرآیند ترکیبی نتیجه می‌دهد. فرمت کلی این دستور به صورت (۴) است.

<receive name=name operation=OP_name partner=p_name partnerLink=PL_name portType=PT_name" … /> (4)

لذا R در مدل CPG فرآیند BPEL مجموعهٔ $R=\{r,w, x\}$ می‌باشد که r و w و x به ترتیب حقوق خواندن، نوشتن و اجرا می‌باشند.

قید C در سه فعالیت بالا بسته به نیازمندی‌هایی که فاعل یا مفعول مربوطه باید در هر فعالیت به آنها مقید باشند تعیین می‌شود. به عنوان مثال، حقوق تعیین شده در هر سه فعالیت بالا به ازای انجام عملیات مشخصی از وب‌سرویس مفعول صورت می‌پذیرد. یعنی به ازای عملیات مذکور حق بیان شده بر وب‌سرویس‌ها نسبت به هم صادق است. نام این عملیات توسط پارامتر operation در هر یک از فعالیت‌های invoke، receive و reply مشخص می‌شود و طبق تعریف۱ در بخش ۳ توسط قید C_α بر سیاست مربوط به فعالیت اعمال می‌گردد. به عنوان مثال در فعالیت invoke، به ازای عملیات به نام Op_name ، فرآیند حق اجرای وب‌سرویس شریک را دارد. لذا شرط یال ارتباطی فرآیند و شریک مذکور C=(T, T, Op_name(s,o), T) و به‌طور کلی برچسب این یال x: (T, T, Op_name(s,o), T) خواهد بود. که در آن منظور از s و o (در فعالیت invoke) به ترتیب وب‌سرویس ترکیبی و وب‌سرویس شریک مشخص شده توسط پارامتر partner و partnerLink است.

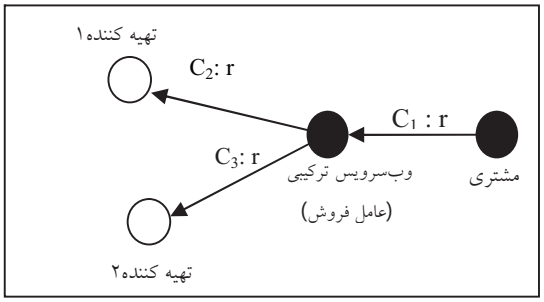
امکان دارد به ازای فرآیندهای مختلف یا به ازای پیوندهای مختلف در یک فرآیند، وب‌سرویس‌ها در همکاری با یکدیگر دارای نقش‌های مختلفی باشند. این نقش‌ها در فایل WSDL، به ازای عملیات‌های مختلف توسط پارامتر role مشخص می شوند و به تبع آن در فرآیند BPEL ، توسط پارامترهای myRole وpartnerRole بیان می‌شوند. پارامتر myRole بیانگر نقش فرآیند BPEL در پیوند بین آن فرآیند و شریک است و پارامتر partnerRole نقش شریک را در پیوند مذکور مشخص می‌کند. به عنوان مثال یک خریدار درخواست خرید خود را به فرآیند ترکیبی می‌فرستد. در این پیوند فرآیند نقش فروشنده را دارد. اما هنگامی که فرآیند ترکیبی درخواست را به وب‌سرویس‌های فروشنده فرستاد، فرآیند نقش خریدار و وب‌سرویس شریک نقش فروشنده را دارد. با اعمال قید عملیات بر فعالیت‌ها و به دلیل ارتباطات تعریف شده در اسناد WSDL هر شریک، این نقش‌ها به‌طور غیرمستقیم بر سیاست مربوطه اعمال می‌شوند. ولی با این وجود و در صورت نیاز مدل CPG به خودی خود انعطاف‌پذیری لازم را برای اعمال نقش‌ها بر سیاست‌ها دارد. نقش یک فاعل با استفاده از قید C_s و قید محدودکنندهٔ یک مفعول با C_o بیان می‌شود.

۵-۳ مثال کاربردی

سناریوی سادهٔ زیر را درنظر بگیرید: یک خریدار نیاز به خرید یک سیستم کامپیوتری (PC) دارد و در عین حال تعدادی از تهیه‌کنندگان وجود دارند که هر کدام بخشی از اجزای یک سیستم کامپیوتری را تولید و ارائه می‌کنند. به جای ارتباط خریدار با هر تهیه‌کننده، خریدار درخواست خود را به یک عامل فروش (وب-سرویس ترکیبی) می‌دهد. عامل فروش با ارتباط با تهیه‌کنندگان مجموعهٔ اجزای مورد نیاز و قیمت آنها را بدست آورده و در اختیار خریدار قرار می‌دهد. قطعه کد زیر نمونهٔ سادهٔ این سناریو را مبتنی بر فرآیند BPEL نشان می‌دهد.

```
<receive name="receive" partnerLink="Buyer"
operation="request" variable="request"
initiate="yes">
</receive>
<invoke name="quote_supplier1"
partnerLink="Supplier1" operation="request_quote"
inputVariable = "part_request"
outputVariable="part_quote">
</invoke>
<invoke name="quote_supplier2"
partnerLink="Supplier2" operation="request_quote"
inputVariable = "part_request"
outputVariable="part_quote">
</invoke>
<!--construct a proposal from the part quotes received
-->
<reply name="reply" partnerLink="Buyer"
operation="send_proposal" variable="proposal">
</reply>
```

به عنوان نمونه مدل حاصل از ارتباط عامل فروش با دو تهیه‌کننده ۱ و ۲ و ارسال نتیجه به خریدار را توسط گراف شکل۹ مدل می‌کنیم:



شکل ۹: مدل CPG حاصل از فرآیند فروش

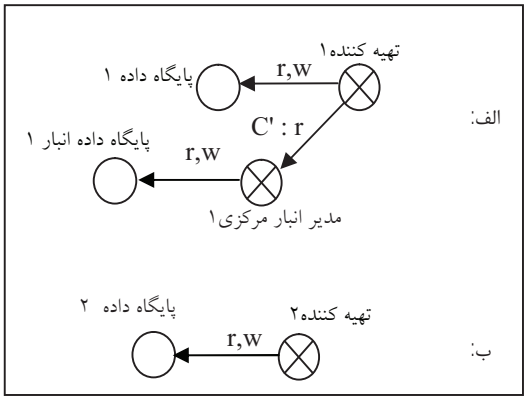
که در آن:

C_1= (T,T, send_proposal(عامل فروش,مشتری),T)

C_2= (T,T, request_quote (عامل فروش, تهیه کننده۱),T)

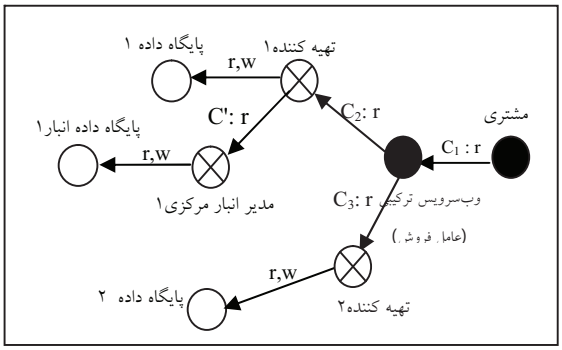
C_3= (T,T, request_quote (عامل فروش, تهیه کننده۲),T)

در عین حال همان‌طور که می‌دانیم هر وب‌سرویس شریک سیاست مربوط به خود را دارد. سیاست تهیه‌کنندگان ۱ و ۲ را به‌صورت شکل (۱۰-الف) وشکل (۱۰-ب) فرض می‌کنیم:



شکل ۱۰: الف) سیاست تهیه‌کننده۱. ب) سیاست تهیه‌کننده۲

اکنون (مطابق مراحل ذکر شده در بخش ۴) اجتماع سیاست وب‌سرویس‌های شریک در ترکیب و سیاست ترکیبی را بدست می‌آوریم (شکل ۱۱).



شکل ۱۱: گراف نهایی فرآیند فروش با درنظر گرفتن سیاست شرکا

با بدست آوردن گراف نهایی ترکیب می‌توان به تحلیل سیاست‌ها پرداخت. روش‌های تحلیل و کشف برخورد و وارسی ناسازگاری در گراف CPG را پیش از این به‌طور کامل توضیح دادیم. به دلیل کمبود جا به تحلیل ساده‌ای بسنده می‌کنیم:

فرض کنیم می‌خواهیم نحوهٔ انتقال اطلاعات را بین مشتری و پایگاه دادهٔ ۱ مورد بررسی قرار دهیم. لذا بررسی می‌کنیم که نتیجهٔ گزارهٔ تعریف شده در بخش ۴-۳ به ازای حق r و برای دو نهاد مذکور چیست و در صورت درست بودن این گزاره ببینیم به ازای چه شرایطی برقرار خواهد بود. پس از دو مرتبه اعمال قانون spy به یال جدید مرتبط مشتری و پایگاه دادهٔ ۱ می‌رسیم. اگر گراف شکل (۱۱) را CPG_0 فرض کنیم آنگاه:

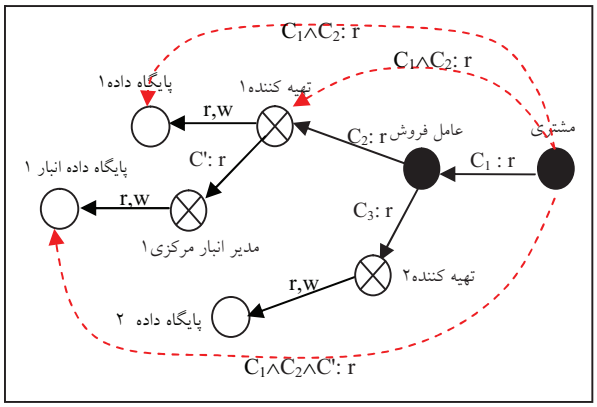
can.obtain(C, r, مشتری, پایگاه داده ۱, CPG_0)= true

و در آن شرط C عبارتست از:

$C=C_1 \wedge C_2$=(T,T,send_proposal (عامل ,مشتری)

∧request_quote (عامل فروش, تهیه کننده۱),T)(فروش

به همین ترتیب چند نمونه اعمال قوانین انتقال بر گراف شکل ۱۱ را در شکل ۱۲ مشاهده می‌کنیم.



شکل ۱۲: گراف نهایی و اعمال قوانین انتقال

۶- نتیجه‌گیری و کارهای آتی

روش‌های ترکیب وب‌سرویس‌ها در هر دو دستهٔ ارکستر و رقص آرایی از فقدان بیان ویژگی‌های عملکردی و عدم امکانات تحلیل به دلیل نداشتن شالوده‌ای صوری رنج می‌برند. ترکیب وب‌سرویس‌ها علی رغم انتظار وب‌سرویس‌های شریک در ترکیب، تضمین کنندهٔ برآوردن سیاست‌های کنترل دسترسی شرکا نمی‌باشد و این امر یکی از معضلات در زمینهٔ ترکیب وب‌سرویس‌هاست. ما در این مقاله روشی برای استخراج سیاست‌های کنترل دسترسی ترکیب وب‌سرویس‌ها و تبدیل آن به مدل CPG ارائه نمودیم. سپس مدل حاصل مورد تحلیل قرار گرفته و هر گونه برخورد یا تناقض بین سیاست‌های شرکا و سیاست حاصل از ترکیب قابل کشف و بررسی است. در این مقاله کاربردی از روش ارائه شده را برای یکی از زبان‌های رایج ارکستر (BPEL) نشان دادیم. ما در کارهای آتی خود به بیان مثال‌های کاربردی جامع در جهت تعمیق مدل و نحوهٔ تحلیل

می‌پردازیم. به‌علاوه کاربرد روش ارائه شده را در زبان‌های دیگر همچون WSCI به عنوان زبان معمول رقص آرایی وب‌سرویس‌ها با مثال‌های کاربردی بیان خواهیم کرد.

مراجع

[1] Srivastava, B. and Koehler, J. (2003).Web service composition, current solutions and open problems, In Proceedings of ICAPS'03 Workshop on Planning for Web Services, Trento, Italy, June 2003.

[2] F.Curbera, R.Khalaf, N.Mukhi, S.Tai, S.Weerawarana, The next step in Web Services, communications of the ACM October 2003/Vol. 46, No.10.

[3] A.Ploskonos, An Introduction into Web Service Composition, Fundamentals of Service-Oriented Engineering, 2005.

[4] A.Charfi, M.Mezini, Middleware Services for Web Service Compositions, Chiba, Japan, ACM .WWW 2005, May, 2005.

[5] A.Charfi, M.Mezini, Using Aspects for Security Engineering of Web Service Compositions, German Research Foundation (DFG) as part of the PhD Program "Enabling Technologies for Electronic Commerce".2005.

[6] Ter Beek, M.H., Bucchiarone, A. and Gnesi, S. (2006). A Survey on Service Composition Approaches: From Industrial Standards to Formal Methods, Technical Report 2006-TR-15, ISTI, Consiglio Nazionale delle Ricerche, 2006.

[7] Yushi, C., Wah, L.E. and Limbu, D.K., Web Services Composition - An Overview of Standards. Synthesis Journal, Fifth issue, ITSC publication, (pp 137-150), 2004.

[8] G. Diaz, Juan-Jos´e Pardo, Mar´ıa-Emilia Cambronero, Verification of Web Services with Timed Automata, Electronic Notes in Theoretical Computer Science 157 (2006) 19–34.

[9] Mariya Koshkina, Franck van Breugel, Verification of Business Processes for Web Services, York University, Department of Computer Science, October 2003.

[10] L.G. Meredith, S. Bjorg. Contracts and Types. Communications of the ACM, 46, No. 10, pp 41-47, October 2003.

[11] H. Schlingloff, A. Martens, K. Schmidt, Modeling and Model Checking Web Services, Electronic Notes in Theoretical Computer Science 126 (2005) 3–26.

[12] M. Rouached, O. Perrin, C. Godart, Securing Web Service Compositions: Formalizing Authorization policies using Event Calculus, 2006.

[13] Chris Peltz, Web service orchestrartion: A review of emerging technologies, tools, and standards, Hewlett-Packard Company (HP), 2003.

a. Assaf et al, Web Service Choreography Interface 1.0, W3C, August 2002.

[14] M. Bishop, Conspiracy and information flow in the Take-Grant Protection Model, Journal of Computer Security, vol 4(4), 1996, pp 331-360.

[15] Alexandre Alves, et al. Web Services Business Process Execution Language, OASIS, 31 January 2007.

[16] Erik Christensen, et al. Web Services Description language, W3C Note, 15 March 2001, http://www.w3.org/TR/wsdl, W3C.

[۱۷] زهرا درخشنده، بهروز ترک لادانی، ناصر نعمت بخش، " گراف سیاست مقید شده (CPG): مدلی برای توصیف و ترکیب سیاست‌های کنترل دسترسی"، چهاردهمین کنفرانس ملی انجمن کامپیوتر ایران، دانشگاه امیر کبیر، اسفند ماه ۱۳۸۷، (CSICC2009).