

Aplicação de modelo de avaliação de confiança com base numa framework TBAC num cenário de Gestão de Saúde

Francisco Nunes, Compta, Portugal

Henrique O'Neill, ISCTE - Instituto Universitário de Lisboa, Portugal, henrique.oneill@iscte-iul.pt

Resumo

Os sistemas distribuídos de âmbito alargado em modo inter-organizacional têm como requisitos base escalabilidade e paradigmas de controlo de acesso dinâmicos de gestão de utilizadores. Neste trabalho abordam-se cenários de gestão de controlo de acesso numa perspectiva da gestão de confiança. Agregam-se e avaliam-se níveis de confiança a partir de dimensões de confiança e é sugerido um esboço de uma framework para controlo de acessos baseados em confiança (TBAC - trust based access control) através de componentes standard.

Palavras-chave: saúde; armazenamento; controlo de acessos, TBAC

1. INTRODUÇÃO

O paradigma dos Ambientes federados emergiu como uma necessidade de endereçar problemas relativos com a partilha de recursos em formato inter-organozacional mas também contribuiu igualmente para a promoção do crescimento exponencial da colaboração inter- organizacional e das relações de negócio entre clientes e fornecedores de serviços externos (ESPs - External Service Providers). No passado o conceito foi aplicado com sucesso em cenários de outsourcing, nas comunidades online, em computação Grid e é por sua vez uma parte essencial nos esforços para consolidar a arquitectura Cloud. Esta nova tecnologia bem como os seus conceitos de gestão geraram uma mudança na forma como a antigamente denominada colaboração estática é conduzida, uma vez que facilita aspectos da dinâmica das relações comerciais entre parceiros a fim de tirar partido dos serviços inter-organizacionais.

Os ambientes federados baseiam-se num sistema de gestão de entidades federadas (FIM - Federated Identity Management), onde os membros cruzam os dados através de um repositório. Quando usam o FIM, as organizações relacionadas têm de delegar as tarefas, como por exemplo, o fluxo de trabalho de autenticação dos utilizadores para as respectivas organizações de origem. Isso permite que os utilizadores utilizem as suas credenciais num único ponto e fazer sign on sem a necessidade de ter user names e passwords para cada serviço novo e, por outro lado, permite às organizações partilhar aplicações sem a necessidade de todas as organizações envolvidas terem de adoptar as mesmas tecnologias de serviços de directório e mecanismos de autenticação.

Contudo, da mesma maneira que estes ambientes proporcionam novas oportunidades, têm estimulado também o interesse na implementação de conceitos de gestão de confiança (TM - Trusting Management) , visto que cada organização envolvida deve confiar nos seus parceiros o que permite que estas atestem os seus utilizadores e serviços, construindo assim um chamado Círculo de Confiança (COT - Circle of Trust). Estes conceitos podem expor os participantes (clientes e serviços prestados) a novos tipos de riscos e com isso levar ao aumento da necessidade da gestão de confiança entre os mesmos.

No entanto, avaliar a confiabilidade dos envolvidos, partindo de uma maneira objectiva, exige - no mínimo - uma definição concisa e formal de confiança e relações de confiança. Esta definição acabou por ser muito difícil de encontrar, principalmente porque a confiança no mundo real é subjectiva e muitas vezes específica para cada cenário.

Como principal contribuição, este trabalho tem em conta várias definições e dimensões de confiança e sugere um modelo formal que pode ser aplicado para gerir e dinamicamente agregar confiança nos ambientes federados. A este respeito, foram identificadas formas como duas entidades podem estar ligadas uma à outra através da noção de confiança. Distingue-se entre (i) confiança directa para as entidades que são conhecidas entre si, por exemplo, por meio da associação ao mesmo domínio de gestão; (ii) confiança indirecta, por exemplo, com base em interacções mutuamente conhecidas através de terceiros.

Enquanto a confiança directa pode ser construída, entre as entidades, sobre a base da confiança adquirida nos contractos de FE e os conceitos clássicos de segurança, como controlo de acesso baseada em políticas com sujeitos exclusivamente identificados, a confiança indirecta endereça o caso cada vez mais importante, das entidades que colaboram em domínios distintos e não têm, à priori, experiências directas entre si. Em vez disso, fizeram experiências baseadas em confiança com um ou mais intermediários, o que permite construir caminhos de confiança ponderados a serem estabelecidos entre estas entidades como input para raciocínio automatizado (Automated Reasoning).

Para investigar uma aplicação prática de uma relação de confiança indirecta, o estudo propõe escalas multi-dimensionais de confiabilidade, tendo em conta experiências passadas tais como a reputação, e mostra a importância de agregar, correlacionando, e refinar a confiança de informação. A fim de delinear a nossa solução para os problemas TM mencionados acima, este trabalho apresenta alguns cenários do mundo real no ponto 2. A abordagem genérica, bem como a aplicação da framework de controlo de acessos baseados em confiança (TBAC – Trusted Based Access Control) estão ilustradas nos pontos 3 e 4. Finalmente, concluímos com uma visão geral sobre os trabalhos relacionados no ponto 5.

2. CENÁRIO: SISTEMA DE SAÚDE FEDERADO

Para ilustrar a necessidade de avaliação de confiança em ambientes federados, apresenta-se um cenário hipotético de sistema de saúde. A colaboração entre agentes de saúde e utentes tem o objectivo de promover um sistema de saúde integrado. Há uma entidade que funciona como intermediário entre os utentes (U), plataformas de saúde (PS), prestadores de serviços médicos consumidores (CCs), bem como prestadores de serviços médicos produtores de conteúdo (CPs). Através de um portal, cada utente que está registado no sistema nacional de saúde e pode escolher a partir de uma lista de serviços médicos disponibilizados que são prestados por CCs e CPs.

Um utente pode solicitar uma consulta de especialidade, por exemplo, de pediatria. Os resultados apresentados pelo portal são classificados e agrupados por critérios oferta dos fornecedores, como por exemplo o consultório médico mais perto da residência ou o que tiver agenda mais disponível. O utente também poderá incluir restrições de Qualidade de Serviço (QoS), por exemplo, a consulta mais próxima honorários cobrados, etc.

Por sua vez é provável que esta consulta vá gerar a necessidade de fazer exames de diagnóstico. Da mesma forma o utente irá agendar os exames auxiliares de saúde pelo mesmo portal. Os resultados desses exames deverão ser registados através do portal pelo CP que irá gerar um apontador para os dados reais. O utente estando ciente que os dados estão disponíveis volta a agendar a consulta no slot que lhe for mais conveniente e voltará à consulta de pediatria. Nessa consulta o CC poderá avaliar a condição de saúde do utente através da interpretação dos resultados dos exames auxiliares de diagnóstico veiculados através do portal de saúde e se for caso disso prescrever a medicação que se imponha através da prescrição electrónica.

Para satisfazer as necessidades do utente, o portal analisa os requisitos, bem como o perfil do utente e se respeita as restrições de QoS com os serviços reais que foram registradas pelos CPs. Assim, um processo de aprendizagem dos caminhos de confiança pode ser criado através de todos os prestadores e que começa com o Portal, e termina no prestador seleccionado.

2.1. Problema de Gestão de Confiança

Uma vez que as relações entre os prestadores de serviços e os utentes apenas podem ser consideradas como transitivas, no caso dos requisitos do utente não terem sido cumpridos como previsto, ou se houve qualquer violação das regras de colaboração por parte de algum dos prestadores, o utente, bem como o próprio portal serão confrontados com problemas de gestão de confiança (TM), pelo que terão de assumir as consequências daí resultantes. A seguir, destacam-se duas questões importantes de Gestão de Confiança (TM):

O portal executa a selecção de prestadores. Está ainda em estudo a possibilidade de melhorar esta selecção e baseá-la na confiabilidade dos prestadores de serviços em relação à sua conformidade com as restrições de QoS e parâmetros anunciados.

Toda a interacção envolve terceiros, sejam os prestadores, o gestor das entidades dos utentes (GEU), que é também responsável pela contabilização relativa ao utente, personalização e tarefas de facturação. Neste caso, o GEU pode e deve estar também ligado através do caminho de confiança e as necessidades do utente, bem como definir a metodologia para escolher e aceitar os prestadores de colaboração do Portal.

2.2. Requisitos

Tendo em conta os conceitos da federação e as relações contratuais entre os prestadores, alguns dos os requisitos para estabelecer a confiança pode ser resumido da seguinte maneira (Latifa Boursas & Hommel, 2009):

- **Informação de confiança:** A interacção entre o utente e o prestador pode ser estabelecida através de múltiplos intermediários. Em tais situações, confiando no prestador produtor, por exemplo, no que respeita à adesão da entrega prazo, ou com relação à conformidade com a anunciada qualidade do serviço, pode depender da experiência de outras entidades com prestador. Queixas de experiências de outros utentes participantes requerem o arquivo dessa informação sobre as interacções anteriores, bem como a recolha de recomendações que possam ser atribuídos a partir de outras partes após cada interacção.
- **Nível de confiança:** Um nível de confiança para prestador precisa de ser quantificado e deve reflectir vários graus de confiança, que ajudam a assegurar que, por exemplo, o prestador pode ser seleccionado somente se atingiu um determinado nível de confiança.
- **Escala de confiança:** É necessário definir uma escala expressiva para codificação da informação em diferentes valores de confiança derivados. No entanto, a forma como esta escala de confiança pode ser expressa depende maioritariamente das interfaces técnicas como bem como os protocolos de comunicação utilizados nos ambientes federados.
- **Contexto de confiança:** O nível de confiança calculado de acordo com a escala de confiança dada pode indicar a confiabilidade do prestador para um determinado contexto. No entanto, este nível de confiança específico obviamente, não pode ser generalizada para qualquer outro contexto de interacções que possam acontecer nas Ambientes federados. Assim, a solução TM tem de suportar uma ampla gama de situações possíveis que a confiança precisa para ser representada como distintamente diferente contexto de confiança.

- Acordos de confiança: A avaliação de confiança recolhida e as necessidades de informação devem ser baseado em acordos de colaboração com os nossos parceiros para avaliar se a prestação de serviços é uma conformidade com o acordado nas regras.

Para ilustrar a necessidade de uma solução de Gestão de Confiança, são investigadas apenas as questões de confiança do ponto de vista de um utilizador num cenário básico. No entanto, é notável que esta solução é destinada a apoiar prestadores para avaliar a confiabilidade dos utilizadores também.

Como conclusão, uma solução de gestão de confiança e de contrato adequada para as Ambientes federados é um requisito essencial. Deve incluir a avaliação e recomendação de informação sobre a reputação dos participantes bem como ferramentas de auditoria para avaliação do cumprimento dos participantes com os acordos que dizem respeito às tarefas colaborativas

3. MODELO DE GESTÃO DE CONFIANÇA E DE CONTRATO

Vamos mostrar então uma abordagem adequada para ultrapassar os problemas de confiança, que poderá passar pela incorporação de uma gestão descentralizada dos acordos ou através de um mecanismo que controla a adesão a esses acordos entre as organizações envolvidas.

3.1. Estabelecimento de acordos de confiança

A ideia por trás dos acordos de confiança inter-organizacionais, serve basicamente para motivar ao estabelecimento de restrições avançadas que permitem às organizações colaboradoras nos ambientes federados expandirem a sua segurança organizacional e as restrições de privacidade com novas políticas inter-organizacionais, tais como regras e deveres que designam os recursos que podem ser partilhados nos ambientes federados, assim como informações sobre estes recursos, tais como os parâmetros de qualidade, de modo a que uma metodologia permita gerar uma avaliação automática destes acordos, e possam ser estabelecidos para testar o comportamento de cada parceiro de acordo com as políticas comuns.

Estes acordos de confiança, como quaisquer outros contractos, têm necessidade de ser criados nos ambientes federados, e dada a sua colocação acessível, torná-los rastreáveis e assegurar que são administrados adequadamente. Além disso, eles, obviamente, precisam de ser estabelecidos de acordo com uma ontologia unificada que permite mapear serviços e recursos para as políticas de qualidade e parametrização. Ao utilizar a mesma ontologia, os fornecedores têm a possibilidade de expressar as suas políticas, e por outro lado, expressarem as suas preferências de forma padronizada.

Em cenários do mundo real estas preferências não são sempre consideradas com o mesmo grau de importância entre as organizações colaboradoras. No entanto, na área de eContracting (Koetsier, Grefen, & Vonk, 2000)(Hoffner, 1999) e na área de Service Level Agreements (SLA) (Ludwig,

Keller, Dan, & King, 2002), foi estudado que os acordos entre as organizações podem ser expandidos, com aspecto na qualidades de serviços (QoS), no nível funcional e Indicador-Chave de Desempenho(KPIs) no nível financeiro, bem como nos níveis técnicos (Parmenter, 2010).

No ponto seguinte, iremos delinear dois métodos para avaliação da razão sobre a confiança no que diz respeito aos acordos de confiança (requisito 1 no ponto 2.2).

3.2. *Confiança a partir de experiências passadas*

Este método visa parceiros de apoio em ambientes federados terem uma espécie de prestação de contas para avaliar o comportamento uns dos outros e, conseqüentemente, a sua confiabilidade.

Como afirmado na secção anterior, a definição de parâmetros de QoS e KPIs ajuda a decidir o que é exactamente considerado uma interacção de confiança.

Além disso, a monitorização desses parâmetros não afecta apenas os acordos de confiança actualmente eficazes, mas também provoca uma adequada e automática resposta à medida se algumas das restrições tiverem sido violadas, em certos casos (requisito nº. 5 da Secção 2.2).

Assim, a nossa solução para avaliar a confiança das experiências passadas pressupõe que os acordos devam considerar dois requisitos:

- O ambiente federado deve definir um quantitativo unificado e uma ontologia de QoS qualitativa, bem como a medição de métodos para avaliar as interacções em comparação com o conjunto de compromissos dos acordos.
- Cada organização parceira deve seguir estas especificações unificadas para descrever o seu compromisso, quanto aos serviços e recursos oferecidos.

Propomos uma descrição detalhada dos recursos partilhados com os parâmetros de qualidade. Esta revisão descrita sugere que as definições de recursos sejam altamente em contexto dependente, a fim de expressar confiança em vários contextos (ver requisito nº 4 da Secção 2.2). Com base nisso, concluímos que o nível de confiança (requisito nº 2 da Secção 2.2) para um parâmetro de qualidade dado um recurso pode ser expresso em percentagem, num determinado ponto t_0 (tempo), de acordo com a seguinte equação

$$T_{\phi}(t_0) = 100\% - \frac{\sum \text{interacções falhadas}_{\phi}(t_0)}{\sum \text{interacções}_{\phi}(t_0)} \quad (1)$$

Onde ϕ representa o triplo (S, Recurso, Parâmetro), referindo-se assim a um cenário S (contexto de confiança).

Uma vez que consideramos principalmente os pedidos falhados da quantidade total de interações e verificações, temos que subtrair a percentagem resultante de 100%, para obter os valores de confiança desejados, na escala de confiança de [0, 1], onde 0 representa desconfiança total e 1 representa completa confiança (cf. requisito nº 3 da Secção 2.2).

Exemplo:

Relembremos o caso de uso de CP da Secção 2 e assim mostramos como as interações podem ser avaliadas concretamente. Como veremos na Secção 4, o resultado da interação dos recursos de um HealthFile será extraídos do arquivo de log da interação entre o utente e a CP. Em seguida, será comparado com valores prometidos, o parâmetro de qualidade visualizationPerformance, no arquivo de acordos. O resultado desta comparação pode ser 1 ou 0, representando respectivamente bem sucedido ou não bem sucedido, dependendo do grau de correspondência entre as duas fontes de informação.

Seguindo a equação 1, a confiabilidade do CP, relacionado a este cenário, pode ser medido pela percentagem de interações falhadas do montante total de interações, com a seguinte equação:

$$T_{\phi}(t_0) = 100\% - \frac{\sum \text{interacções falhadas}_{\phi}(t_0)}{\sum \text{interacções}_{\phi}(t_0)}$$

Em que o parâmetro ϕ , neste caso, pode ser representado da seguinte forma: (S, HealthFile, visualizationPerformance).

T_{ϕ} reflecte a relação de confiança entre o utente e a CP, para um cenário específico S, que é representado em Recurso e em Parâmetro. Por conseguinte, por cada duas interações falhadas de 10 interações, T_{ϕ} diminui a partir do valor inicial 1, para o valor de 0,8.

3.3. Confiança pela reputação

Como mencionado anteriormente, para a realização de ambientes federados, é útil e proveitoso para os parceiros partilharem conhecimento sobre comportamentos, bem como declarações de qualidade de serviço.

Este conhecimento descrito necessita de ser fornecido por outras entidades que já interagiram com ele ou tiveram experiências semelhantes. Na última secção, apresentamos um método para a quantificação de confiança, que se baseia numa avaliação automática das interações anteriores. Nesta secção, apresentamos um método de quantificação subjectivo para um raciocínio sobre a confiança por reputação, sob a forma de troca de avaliações que permitem a criação de feedback através de relatórios sobre as acções de outras entidades.

Foi investigada a criação de uma função para calcular o nível T de confiança, através da integração de aspectos de gestão da reputação (L. Boursas & Danciu, 2008), em que o peso da relação de

confiança entre duas entidades, que não estão relacionadas directamente, é desconhecido, podendo ser calculado através da utilização de metodologias teóricas de grafos, em que as entidades são representadas por nós e as arestas que ligam esses nós representam as relações de confiança entre eles. Note-se que as arestas das relações baseiam-se nos valores de reputação, que por sua vez podem ser atribuídos de acordo com a mesma escala de confiança que foi falada na secção anterior.

3.4. Função de atualização

Como os valores de confiança estão sujeitos a alterações após cada interacção, os níveis de confiança T , podem variar no intervalo $[0, 1]$.

Concluimos que o nível de confiança $T(t)$ em qualquer ponto t (tempo) pode ser sempre calculado em função do estado anterior e da alteração a partir de $(t-1)$ a (t) : $Tl(t) = Tl(t-1) \pm (\text{var})Tl$.

Portanto, definimos uma função de actualização como uma função que trata as potenciais mudanças de ΔT , com objectivo de escalar os três níveis de avaliações na função e a quantidade total de interacções no intervalo $[0, 1]$, como se segue na seguinte função:

$$\Delta Tl \begin{pmatrix} 1 - \frac{1}{2}e^{-\alpha(\sum \text{interacção}(x))} \text{ se } \chi=1 \\ 0 \text{ se } \chi=0 \\ \frac{1}{2}e^{-\alpha(\sum \text{interacção}(x))} \text{ se } \chi=0 \end{pmatrix}$$

Esta diferenciação é devido ao facto de, na maioria dos sistemas de classificação conhecidos, os participantes têm muitas vezes a possibilidade de expressar as suas opiniões de uma forma simples, dando um nível de classificação distinto a cada um. Da mesma forma, neste caso, abordamos a questão de escala das classificações, permitindo aos participantes classificar os outros, de acordo com estes três níveis:

- $\chi = 1$ para uma classificação positiva
- $\chi = 0,5$ para uma classificação neutra
- $\chi = 0$ para uma classificação negativa

O princípio da função exponencial base actualiza a função para incrementar ou decrementar os valores de confiança (acima ou abaixo o valor 0,5) ajudando a gerir a velocidade das alterações requerendo uma quantidade considerável de interacções até que os extremos 0 ou 1 sejam atingidos. Este recurso garante que as interacções positivas sejam suficientes (resp. negativa), para se realizar o alcance do nível de confiança absoluta.

3.5. Agregar a confiança

Nos pontos anteriores, dois métodos lógicos de computação diferentes foram apresentados para estimar o nível de confiança. No entanto, os diferentes níveis de confiança, que podem resultar de

diferentes métodos de cálculo, podem ser desiguais ou até mesmo contraditórios. Devido a este fato, na secção actual apresentamos um algoritmo de agregação que analisa e junta estes valores.

Algoritmo de Agregação(Latifa Boursas & Hommel, 2009): T_{px}

Parâmetros de entrada: Request of principal P_x , Contexto ci , conjunto de níveis de confiança $((T_{px}^{passado}(ci), T_{px}^{reputação}(ci)))$

Parâmetros de saída: Nível de Confiança T_{px}^{Final}

```

1: begin
2:  $ci := evaluateRequest(P_x)$ 
3:  $(T_{px}^{passado}(ci), (T_{px}^{reputação}(ci), (ci))) := ReadContext(ci)$ 
/* O caso onde o nível de confiança está disponível a partir de uma única dimensão */
4: if  $((\exists T_{px}^{passado}(ci), e (\exists (T_{px}^{reputação}(ci))) )$  então
5:  $T_{px}^{final}(ci) = T_{px}^{passado}(ci),$ 
6: end if
7: if  $((\exists T_{px}^{passado}(ci), e (\exists (T_{px}^{reputação}(ci))) )$  então
8:  $T_{px}^{final}(ci) = T_{px}^{reputação}(ci),$ 
9: end if
/* O caso onde o nível de confiança está disponível a partir de mais de uma dimensão */
10: if  $((\bullet ((\exists T_{px}^{passado}(ci), e (\exists (T_{px}^{reputação}(ci))) )$  então
11:  $T_{px}^{final}(ci) = aggregatePastRep(T_{px}^{passado}(ci), T_{px}^{reputação}(ci))$ 
12: end if
13: function  $aggregatePastRep(T_{px}^{passado}(ci), T_{px}^{reputação}(ci))$ 
14:  $T_{px}^{final}(ci) = T_{px}^{passado}(ci) + update(T_{px}^{reputação}(ci))$ 
15: return  $T_{px}^{final}(ci)$ 
16: end

```

Tal como indicado no Algoritmo 1, por meio da função *ReadContent*, o algoritmo verifica a existência de um contexto Ci (i.e. parâmetro de qualidade) se as informações sobre o comportamento anterior e o feedback sobre a reputação solicitada se ambos existirem. No caso de estar disponível apenas um único nível de confiança para o contexto, tal como indicado nas linhas 4 e 7, este valor deve ser considerado como o nível de confiança final, e assim não é necessária a agregação de valor.

No caso oposto, onde o nível de confiança existe a partir de mais do que uma dimensão de confiança, uma regra de agregação é necessária. Assim, a função de agregação *aggregatePastRep* configura $T_{px}^{passado}(ci)$ como valor inicial e incrementa ou decrementa esse valor ($T_{px}^{reputação}((ci))$), de acordo com a função de atualização apresentada no ponto 3.4.

Isto é devido ao facto de que a computação do nível de confiança de uma experiência passada, é realizada automaticamente (depois de cada interacção) através de ferramentas de monitorização, enquanto o nível de confiança de reputação só pode ser avaliado, se pelo menos um parceiro de interacção deixa um nível de classificação no final da interacção.

4. IMPLEMENTAÇÃO E APLICAÇÃO

A realização deste modelo de confiança está previsto dentro de uma relação de "Trust-Based Access Control Framework" (TBAC), que se centra principalmente no desenvolvimento das metodologias e ferramentas de raciocínio automatizadas, mencionadas anteriormente. Segundo a ordem descrita dos fluxos de interacção de trabalho, o Quadro TBAC compreende os seguintes componentes:

"Broker Trust"(corrector de confiança). Representa um importante componente para gerir a implementação e avaliação dos algoritmos, das diferentes avaliações de confiança. Para este objectivo, primeiro recolhe-se a informação relevante sobre o solicitador, em seguida calcula-se o nível de confiança prospectivo por meios de parâmetros de entrada diferentes. Os diferentes cálculos de confiança, bem como os algoritmos de agregação que podem ser aplicados em termos de funções de mapeamento, que são realizadas tal como um conjunto de pacotes distintos.

"Storage System"(Sistema de armazenamento). Este componente está intimamente ligado com o corretor de confiança, porque os aspectos mais desafiadores na avaliação de confiança giram em torno da inicialização, pesquisa, avaliação e actualização das informações de confiança nos ambientes federados.

Para a gestão da informação de confiança, o componente de armazenamento compreende os seguintes sub-componentes:

"Trust agreements repository"(Repositório de acordos de Confiança) : Existem muitas ontologias e idiomas eContract para a implementação deste componente, que deve ser tratada pelos administradores do ambiente federado. A ontologia considerada, bem como a política de QoS propostas por Maximilien et al. em (Maximilien & Singh, 2004) para a selecção dinâmica de serviços web. Ao utilizar a mesma ontologia, os fornecedores têm a possibilidade de expressar as suas políticas e anunciar Parâmetros de QoS, tais como desempenho, custo de transacção e condições críticas das operações.

Um exemplo simplificado da política fornecedora pode ser visualizado na listagem abaixo. Para um serviço 'CP', os detalhes de valor para o parâmetro de qualidade UpdateInfo são indicados pelo elemento <QoS>. Neste exemplo, os valores prometido em no elemento <qValue> são: min, max, e unidade.

```
1 <QoSPolicy ontology='QoSOnt' methods='.' services='CP'>
2   <QoS name='UpdateInfo' promise='bestEffort'>
3     <qValue>
4       <typical>7</typical>
5       <min>5</min>
6       <max>10</max>
7       <unit>day</unit>
8     </qValue>
9   </QoS>
10 </QoSPolicy>
```

Resource description repository" (Repositório de descrição de recursos): Em combinação com o repositório de acordos de confiança, este componente representa os serviços e recursos para a gestão de acesso entre domínios (incluindo a QoS e parâmetros de desempenho).

Realiza-se por meio de Resource Description Framework (RDF , estrutura de descrição de recursos).

“Audit information repositior”(Repositório de Auditoria de informações): Este componente tem como base as informações fornecidas pelos arquivos de logs para avaliar a qualidade das interações entre os parceiros do ambiente federado. Com base nos depósitos anteriores, dois módulos adicionais, que a realizar num conjunto de transformações “eXtensible Stylesheet Language for Transformation “(XSLT) para transformar os documentos XML, podem ser utilizados para controlar o comportamento e registar as interações. O primeiro módulo “AgreementInterceptor“ (interceptor de acordos) percorre o documento do acordo e preparando os parâmetros de desempenho e qualidade na seguinte ordem:

- \$qualityParameter=[[provider;serviceName;
countParam;QoSname; QoSpromise;param:content;
param:content...]]

O segundo módulo “InteractionInterceptor“ (interceptor de interações) juntamente com “AuditingEngine”(Motor de auditoria), avaliam os mesmos parâmetros que são registados nos arquivos de log de cada interação. Em combinação com o módulo anterior, o estado da interação deve ser comparada com os valores em causa no arquivo de acordos. Por fim, o resultado desta comparação pode ser definido como 1 ou 0 dependendo do grau de igualdade entre as duas fontes de informação.

Repositório de identidade: Este repositório gere o armazenamento da informação de identidade da interação parceira e acrescenta-lhe o nível de confiança apropriado, de acordo com o método de avaliação aplicado.

Mecanismo de decisão de acesso (ADE). Representa o componente final da decisão de acesso, com base no grau de confiança, que é necessário para executar uma determinada acção sobre um recurso. O componente ADE é realizado como Policy Decision Point(PDP), usando o eXtensible Access Control Markup Language (XACML).

5. ABORDAGENS RELACIONADAS

Várias abordagens para a gestão de confiança e controle de acesso têm sido exploradas em ambientes de distribuição federados. No entanto, a maioria dos modelos bem conhecidos, inicialmente considerados de confiança em aspectos de delegação, como o Pretty Good Privacy (PGP), bem como a simples infra-estrutura de chave pública (SPKI). A principal questão nestes modelos relaciona-se

com o facto de que, na ausência de entidades autorizadas que possam fazer delegações na forma de afirmações assinadas, não haverá outras alternativas para a questão de confiança de entidades desconhecidas. Há mais modelos de confiança, mas focados num ponto de vista de confiança da gestão da reputação, em diferentes áreas de aplicação, tais como a Web Semântica (Golbeck, 2005) e em sistemas de redes peer-to-peer (Aberer & Despotovic, 2001). No entanto, várias destas abordagens de gestão de reputação acabam por ser falsas ou susceptíveis de fraude, porque os utilizadores podem facilmente obter um novo pseudónimo para tentar superar/alterar avaliações negativas ou injustamente atribuídas. Argumentamos então que as abordagens relacionadas não se devem considerar de confiança a partir de experiências passadas, nem agregando de várias fontes de informação na literatura actual.

6. CONCLUSÃO

A abordagem apresentada neste trabalho mostra uma forma rápida e rentável de complementar a natureza estática de ambientes federados com um conjunto de novos mecanismos de confiança dinâmicos de avaliação, sem afectar terceiros o comprometer a integridade dos ambientes federados. Uma vantagem notável da solução apresentada é a redução do efeito da arbitrariedade dos métodos clássico de avaliação de confiança, que sejam geralmente baseados unicamente na classificação dos indivíduos. Baseia-se na apreciação, actualização e agregação de confiança através da reputação, bem como a partir de experiências anteriores, porque a característica de descrição de recursos com aspectos de qualidade e desempenho em contraste com o que foi acordado, acordos que permitem ter a noção da história reflectindo a confiabilidade da entidade que executou a acção no recurso dado. Embora esta abordagem cumpra os requisitos suscitados, reconhecemos algumas áreas onde possa ser estendida. Uma restrição que deve ser tomada em consideração é a ontologia e linguagem política de QoS que foi usada para expressar a chamada confiança de contextos, porque a expressividade desta ontologia é, obviamente, limitada, uma vez que tem sido desenvolvida para serviços específicos e cenários de usos de recursos. Devido a este facto, mais ontologias genéricas que lidam com QoS e confiabilidade precisam de ser investigadas. Além disso, próximo das abordagens de avaliação de confiança através da reputação e de experiências passadas, futuras pesquisas devem ser orientadas para a identificação, assim como para a agregação de outras fontes de informação de confiança.

REFERÊNCIAS

- Aberer, K., & Despotovic, Z. (2001). Managing trust in a peer-2-peer information system. *Proceedings of the tenth international conference on Information and knowledge management, CIKM '01* (pp. 310–317). New York, NY, USA: ACM. doi:10.1145/502585.502638
- Boursas, L., & Danciu, V. A. (2008). Dynamic inter-organizational cooperation setup in Circle- of-Trust environments. *Network Operations and Management Symposium, 2008. NOMS 2008. IEEE* (pp. 113 –120). doi:10.1109/NOMS.2008.4575124

- Boursas, Latifa, & Hommel, W. (2009). Multidimensional Dynamic Trust Management for Federated Services. Proceedings of the 2009 International Conference on Computational Science and Engineering - Volume 02, CSE '09 (pp. 684–689). Washington, DC, USA: IEEE Computer Society. doi:10.1109/CSE.2009.40
- Golbeck, J. A. (2005). Computing and applying trust in web-based social networks. University of Maryland at College Park, College Park, MD, USA.
- Hoffner, Y. (1999). Supporting contract match-making. Research Issues on Data Engineering: Information Technology for Virtual Enterprises, 1999. RIDE-VE '99. Proceedings., Ninth International Workshop on (pp. 64 –71). doi:10.1109/RIDE.1999.758602
- Koetsier, M., Grefen, P., & Vonk, J. (2000). Contracts for Cross-Organizational Workflow Management. In K. Bauknecht, S. Madria, & G. Pernul (Eds.), Electronic Commerce and Web Technologies, Lecture Notes in Computer Science (Vol. 1875, pp. 110–121). Springer Berlin / Heidelberg. Retrieved from http://dx.doi.org/10.1007/3-540-44463-7_10
- Ludwig, H., Keller, A., Dan, A., & King, R. (2002). A service level agreement language for dynamic electronic services. Advanced Issues of E-Commerce and Web-Based Information Systems, 2002. (WECWIS 2002). Proceedings. Fourth IEEE International Workshop on (pp. 25 – 32). doi:10.1109/WECWIS.2002.1021238
- Maximilien, E. M., & Singh, M. P. (2004). A framework and ontology for dynamic Web services selection. Internet Computing, IEEE, 8(5), 84 – 93. doi:10.1109/MIC.2004.27
- Parmenter, D. (2010). Key Performance Indicators (KPI): Developing, Implementing, and Using Winning KPIs. John Wiley & Sons. Retrieved from http://books.google.fr/books?id=sLP_ipWrfssC