Uma Arquitetura de Reputação de Confiança Aplicada ao Ambiente de Computação em Nuvem

Luís Felipe Bilecki, Adriano Fiorese

[1] Departamento de Ciência da Computação (DCC) – Centro de Ciências Tecnológicas
Universidade do Estado de Santa Catarina (UDESC) – 89219-710 – Joinville/SC

luis.bilecki@gmail.com, adriano.fiorese@udesc.br

Abstract. *Cloud computing provides computational resources to users in a scalable and dynamic way. The use of these resources are impacted by issues related to privacy, security and trust. In this sense, this paper presents a trust reputation architecture applied in the cloud computing environment. The reputed trust is based on two data sources: objective and subjective ones. In order to evaluate the proposed architecture, a scenario was developed in a P2P Network Simulator. The evaluation results show the architecture applicability with low overhead.*

Resumo. *De forma dinâmica e escalável a computação em nuvem fornece recursos computacionais para seus usuários. A utilização desses recursos é impactada por problemas relativos a privacidade, segurança e confiança. Nesse sentido, este trabalho pretende apresentar uma arquitetura de reputação de confiança aplicada a computação em nuvem. A reputação dos provedores de nuvem será composta por duas fontes de confiança: objetiva e subjetiva. Um cenário para validar a arquitetura foi desenvolvido utilizando-se um simulador de redes P2P. Os resultados apresentados demonstram a aplicabilidade da arquitetura com um overhead tolerável.*

1. Introdução

A computação em nuvem (CN), de forma dinâmica e escalável, fornece recursos computacionais (processamento, armazenamento, aplicativos) sobre a Internet aos usuários (empresas, entidades governamentais e indivíduos) [Zhang et al. 2010]. Para tanto, *data centers* são utilizados pelos provedores de serviços de nuvem. Com isso, pequenas e médias empresas, estão utilizando os recursos fornecidos pela CN (ex.: armazenamento, banco de dados, entre outros) para construir seus sistemas comerciais e disponibilizar seus próprios serviços [Tang et al. 2016].

A completa adoção de recursos e serviços disponibilizados pela CN é impactada por problemas relativos a privacidade, segurança e a confiança. Os contratos firmados entre o provedor de serviços de nuvem computacional (ou simplesmente provedor de nuvem (PN) para simplificar, como será usado no decorrer do texto) e os usuários, chamados de *Service Level Agreement* (SLA), podem auxiliar no tratamento desses problemas utilizando-se de alguns aspectos monitoráveis (métricas). Contudo, o SLA torna-se insuficiente para o estabelecimento completo da confiança entre os provedores de nuvem e os usuários, uma vez que não leva em consideração aspectos subjetivos da utilização desses serviços por parte do usuário [Noor et al. 2016].

Buscando estabelecer a confiança entre os PNs e os seus usuários, diversas abordagens podem ser utilizadas [Habib et al. 2011]. Muitos pesquisadores citam que os *feedbacks* dos usuários configuram-se como uma boa fonte para avaliar a confiança dos provedores de nuvem [Noor et al. 2016] e outros abordam a combinação desses *feedbacks* com a confiança objetiva (referente ao desempenho - Qualidade de Serviço (QoS)) [Tang et al. 2016]. Porém, tais abordagens não se preocupam em utilizar os valores históricos, relativos a interação entre os usuários e os provedores, bem como não apresentam ou apresentam parcialmente métodos para identificação de ataques ao valor das avaliações do usuário.

No cenário de computação em nuvem, a confiança pode ser entendida como um valor numérico que indica a confiabilidade dos PNs. Desta forma, tal valor pode ser utilizado como um critério para a tomada de decisão relativa a interação com tais provedores [Sabater and Sierra 2005].

O problema da confiança existente pode ser auxiliado pela aplicação de um arquitetura de reputação, que visa calcular, gerenciar e disseminar a reputação dos provedores de nuvem. A reputação é vista como uma medida agregada de um ou mais indicadores históricos a respeito das interações realizadas entre as entidades [Resnick and Zeckhauser 2002].

Desta forma, este trabalho tem por objetivo apresentar uma arquitetura de reputação de confiança, que visa auxiliar seus usuários em processos de tomada de decisão baseados em reputação. Tal arquitetura será responsável por: (i) Compor o valor de reputação baseado em dois indicadores de confiança: objetiva (indicadores de QoS dos PNs) e subjetiva (*feedback* do usuário ao PN); (ii) Fornecer uma abordagem centralizada para disseminar o conhecimento (reputação) e receber requisições dos seus usuários; (iii) Prover uma interface que realize o monitoramento dos indicadores de QoS; (iv) Receber os *feedbacks* fornecidos pelos usuários em relação aos provedores de nuvem, com a finalidade de atualizar a reputação de um PN.

O restante deste trabalho é organizado como se segue. A Seção 2 apresenta os conceitos relacionados a computação em nuvem, confiança e reputação e os trabalhos correlatos ao escopo deste trabalho. Na Seção 3, a arquitetura de reputação é apresentada. A Seção 4 apresenta o cenário dos experimentos e os resultados obtidos. Por fim, a Seção 5 apresenta a conclusão e os trabalhos futuros.

2. Revisão da Literatura

2.1. Computação em Nuvem

A Computação em Nuvem é definida como um conjunto de recursos computacionais disponíveis através da Internet e que podem ser rapidamente fornecidos sem praticamente nenhuma intervenção humana. Tais recursos são provisionados de acordo com a necessidade do usuário. Suas características principais são: acesso aos serviços feito sob-demanda, *pool* de recursos, amplo acesso à rede, elasticidade rápida e serviços mensuráveis [Mell and Grance 2011]. Os serviços são ofertados aos usuários, por meio de três modelos de negócio diferentes: SaaS (*Software* como Serviço), PaaS (Plataforma como Serviço) e IaaS (Infraestrutura como Serviço) [Zhang et al. 2010].

Para avaliar, comparar, classificar e construir um indicador de confiança, o

Cloud Services Measurement Initiative Consortium (CSMIC) desenvolveu um modelo de métricas universalmente aceito, denominado de *Service Measurement Index* (SMI) [Siegel and Perdue 2012]. O SMI é visto como um conjunto de indicadores de desempenho dos PNs, divididos em sete categorias: *accountability, agility, assurance, financial, performance, security, privacy* e *usability* [Garg et al. 2013]. Os indicadores são classificados em duas abordagens, quantitativa que refere-se a valores mensuráveis e qualitativa, baseada na experiência do usuário (*feedback*).

Neste sentido, a reputação dos PNs pode ser medida através de alguns indicadores de qualidade de serviço (QoS), presentes nas categorias mencionadas anteriormente [Tang et al. 2016]. Conforme os autores em [Garg et al. 2013] estes indicadores são definidos como:

- **Disponibilidade**: fração do tempo total em um intervalo padronizado (ex: 30 dias) que o serviço está disponível para atender as requisições;
- **Tempo de Resposta**: diferença de tempo entre a requisição do serviço e o momento que ele está disponível;
- **Segurança**: os PNs apresentam diferentes mecanismos de segurança, como, algoritmos de criptografia e gerenciamento de identidades, segurança dos dados, entre outros [Baranwal and Vidyarthi 2014]. No entanto, neste trabalho este indicador representa o nível de segurança do PN, em uma escala de 1 a 10;
- **Estabilidade**: desvio no desempenho do serviço, por exemplo, em serviços de armazenamento é a variação no tempo médio das operações de leitura e escrita, enquanto em serviços computacionais é o desvio do nível de desempenho especificado no SLA;
- **Preço**: valor cobrado pelo uso dos recursos computacionais.

Estes indicadores são usados pela arquitetura proposta e não são exclusivos de nenhum modelo de serviço. A abrangência da computação em nuvem, por meio dos modelos de serviço, é grande, possibilitando o atendimento das necessidades da grande maioria das entidades envolvidas com tecnologia da informação, por exemplo, as empresas podem utilizar os recursos fornecidos pela computação em nuvem para desenvolver e implantar sistemas comerciais.

A utilização dos serviços disponibilizados pelos provedores de nuvem é, muitas das vezes, dependente da confiança depositada no provedor. Portanto, a confiança representa um elemento chave para provedores de serviço que disponibilizam seus serviços a terceiros através da nuvem. Assim, a Seção 2.2 apresenta os conceitos de confiança, reputação e a relação desses conceitos com a nuvem e seus clientes (provedores de serviço).

2.2. Confiança e Reputação

O conceito de confiança é originário das ciências sociais que estudam o comportamento do ser humano em sociedade. A confiança é objeto de pesquisa nas mais variadas áreas, como por exemplo psicologia, sociologia, economia e computação [Firdhous et al. 2012]. Diversos conceitos de confiança são encontrados na literatura.

Segundo [Rousseau et al. 1998] a confiança é definida como um estado psicológico que compreende a intenção de aceitar a vulnerabilidade, baseada em expectativas positivas das intenções ou comportamento dos outros. Um dos conceitos mais aceitos na

definição de confiança de um modo geral, é o de Gambetta [Gambetta et al. 2000], que define a confiança como um nível particular da probabilidade com a qual um agente avalia outro agente ou grupo de agentes, que irá/irão executar uma ação particular, tanto antes dele poder monitorar tal ação (ou independentemente da sua capacidade de monitorar) e em um contexto no qual isto afeta a sua própria ação.

Não obstante a confiança apresente definições diferentes em diversos contextos, não existe um consenso entre essas definições pois, todas possuem a mesma base conceitual e se inter-relacionam. Por exemplo, em uma implementação computacional, a confiança é definida como um valor numérico que indica quão confiável é um provedor de nuvem, por exemplo [Sabater and Sierra 2005].

No ambiente de computação em nuvem, a reputação pode ser empregada para assegurar a confiança existente entre os consumidores e os provedores de nuvem. A reputação pode ser definida como uma coleção de valores agregada a respeito do comportamento passado dos participantes de uma comunidade [Resnick and Zeckhauser 2002]. Assim, a reputação, de forma geral, pode ser informada ao usuário através de duas abordagens: qualitativa e quantitativa [Mousa et al. 2015]. A qualitativa refere-se a valores categóricos, como, alta, baixa, moderada, entre outros. Na quantitativa, é representada por valores numéricos em um determinado intervalo.

No contexto deste trabalho, a reputação do provedor de nuvem é calculada como um valor referente a dois indicadores históricos de confiança: objetiva (indicadores de QoS) e subjetiva (avaliações dos usuários). Deste modo, um usuário que necessita interagir com um provedor de nuvem, utiliza a reputação como base para a tomada de decisão, com o propósito de utilizar os recursos disponibilizados. Portanto, reputar a confiança, significa disponibilizar através de uma arquitetura de reputação, a reputação dos provedores de nuvem para que os usuários utilizem esse valor para tomada de decisão.

2.3. Trabalhos Relacionados

Alguns trabalhos estabelecem metodologias para a seleção de PNs de acordo com as necessidades do usuário. [Garg et al. 2013] apresentam um *framework* para o ranqueamento e classificação dos PNs através dos indicadores de desempenho e das necessidades dos usuários. Neste *framework* o método multicritério AHP é aplicado no conjunto de dados reais que representa o desempenho dos provedores. Em [Baranwal and Vidyarthi 2014] são apresentadas métricas para avaliar PNs e também um *framework* para a seleção de PNs por meio do método de votação por ranqueamento.

Em outros trabalhos, os indicadores de QoS são aplicados na seleção e identificação de serviços confiáveis. Em [Yau and Yin 2011] são identificados os serviços que apresentam um valor de QoS satisfatório conforme os requerimentos e preferências dos usuários. Em [Tang et al. 2016] é apresentado um *framework* para a seleção de serviços de nuvem, com base na avaliação da confiança destes serviços, considerando o monitoramento de QoS e as avaliações dos usuários. Em [Nguyen et al. 2010] é apresentado um modelo de reputação baseado em redes bayesianas para a avaliação da confiabilidade de *Web Services*. Este modelo integra em um único valor de confiança, as avaliações dos usuários, monitoramento de QoS e a experiência direta do solicitante.

Além das abordagens que consideram o QoS unicamente e a combinação com outra fonte, os autores em [Noor et al. 2016] apresentaram uma plataforma responsável por

buscar serviços de nuvem, coletar avaliações dos usuários e medir a credibilidade dessas avaliações. Dessa forma, uma plataforma de recomendação de serviços de nuvem com base na sua reputação foi apresentada. [Habib et al. 2011] apresentam uma arquitetura de um sistema de gerenciamento de confiança, que avalia a confiança nos provedores de nuvem considerando outras fontes de confiança além do *feedbacks* dos usuários, como por exemplo o QoS, visando auxiliar os consumidores na escolha e identificação de provedores de nuvem confiáveis.

De um modo geral, os trabalhos relacionados utilizam o monitoramento de QoS e as avaliações dos usuários para fornecer meios de selecionar PNs com base na sua confiança, ou consideram somente as avaliações dos usuários como métrica para reputação. A arquitetura proposta calcula a reputação dos provedores de nuvem, usando duas fontes de indicadores de confiança: objetiva (histórico de QoS + QoS monitorado) e subjetiva (avaliações dos usuários com base no QoS). Além deste diferencial em relação aos trabalhos relacionados, a arquitetura de reputação proposta identifica alguns ataques ao valor de reputação e fornece métodos para o tratamento destes.

3. Arquitetura Proposta

A confiança que os usuários estabelecem nos provedores de nuvem (PN), por meio de sua reputação, apresenta-se como um importante fator para a contratação e utilização dos recursos fornecidos pela nuvem. Os sistemas tradicionais de reputação, como, eBay, consideram somente o *feedback* dos usuários para avaliar a reputação. No contexto da computação em nuvem, a reputação dos PNs deve ser baseada em outras fontes de informação [Habib et al. 2011]. Assim, de forma que os usuários possam avaliar a confiança relacionada aos PNs, pretende-se combinar as avaliações dos usuários com indicadores de qualidade de serviço (QoS) para a composição de um valor para reputação dessa confiança.

Em vista disso, a arquitetura de reputação proposta é apresentada na Figura 1. Assim, para determinar o valor de reputação dos provedores de nuvem, as requisições e os dados referentes ao PN serão processados e coletados de forma centralizada. Uma abordagem centralizada fornece um nível maior de privacidade e segurança porém, provê um ponto único de falha, que não é objeto de estudo neste trabalho [Habib et al. 2011]. Através desta arquitetura, pretende-se fornecer um mecanismo às empresas/clientes para tomada de decisão, com base no valor de reputação dos PNs.

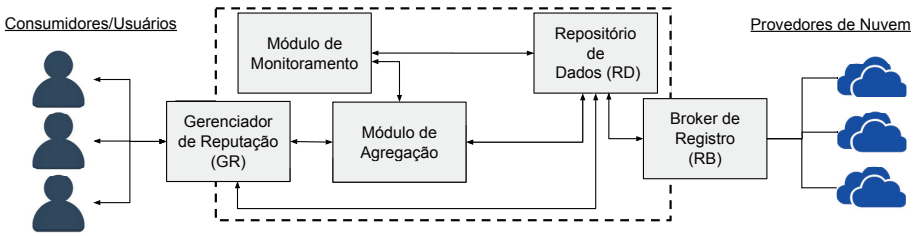


Figura 1. Arquitetura de reputação proposta

A arquitetura de reputação proposta é composta por diversos módulos e elementos, sendo eles:

- **Módulo de Monitoramento**: responsável pelo monitoramento e atualização dos indicadores de QoS do PN. Tal ação pode ser feita por intervalos fixos ou através das solicitações do usuário. O monitoramento dos indicadores de QoS representa um importante papel, pois verifica se a qualidade de serviço prometida no SLA está sendo oferecida;
- **Gerenciador de Reputação (GR)**: interface externa que realiza a comunicação com outros membros, por exemplo, um usuário deseja saber a reputação de um determinado PN ou avaliar subjetivamente um PN;
- **Módulo de Agregação**: responsável pelo cálculo da reputação por meio dos indicadores de QoS e as avaliações dos usuários. Os indicadores de QoS utilizados são: disponibilidade, tempo de resposta, estabilidade, segurança e preço [Baranwal and Vidyarthi 2014]. Este módulo calcula a reputação de serviços similares, embora estes indicadores avaliam qualquer modelo de serviço de nuvem prestado (SaaS, PaaS e IaaS), sendo que não existe um indicador que seja exclusivo para um modelo de serviço. Também, estes indicadores expressam a qualidade de serviço do provedor de nuvem de forma quantitativa.
- **Repositório de Dados (RD)**: armazena os valores históricos e atuais dos indicadores de QoS dos PNs e também as avaliações subjetivas históricas referentes aos *feedbacks* dos usuários aos PNs;
- ***Broker* de Registro (RB)**: para que os PN sejam reputados, eles devem fornecer à arquitetura de reputação as especificações dos serviços bem como os valores dos indicadores de QoS. O RB fornece essa interface.

3.1. Módulo de Agregação

O modulo de agregação utiliza os indicadores históricos de confiança objetiva e subjetiva para calcular a reputação dos provedores de nuvem. Para o cálculo, valores monitorados podem ser considerados juntamente com os valores históricos para verificar a reputação instantânea.

O indicador de confiança objetiva refere-se aos indicadores de QoS, anteriormente mencionados, que refletem no desempenho do provedor de nuvem computacional. Já o indicador de confiança subjetiva é referente às avaliações (*feedbacks*) fornecidas pelos usuários em relação a qualidade do serviço prestado pelos provedores de nuvem.

Dessa forma, a reputação de um provedor de nuvem s, representada na Equação 1, é calculada como a combinação do indicador de confiança objetiva (T_{obj}) com o indicador de confiança subjetiva histórica (T_{sub}) ponderada pelos respectivos pesos de importância (w_{obj} e w_{sub}), definidos de acordo com a preferência do usuário que requisita a reputação.

$$R_s = w_{obj} * T_{obj}(s) + w_{sub} * T_{sub}(s) \tag{1}$$

3.1.1. Indicador de Confiança Objetiva

Este indicador, representado na Equação 2, é calculado através de duas abordagens: analisando a eficiência ($Eff\ (s)$) dos provedores de nuvem baseada no histórico de QoS das interações passadas com usuários e a pontuação ($Esc\,(s)$), que representa a importância relativa desses indicadores (chamada nesse trabalho de confiança multicritério).

$$T_{obj}\,(s)\;=\;Eff\,(s)*Esc\,(s) \tag{2}$$

A eficiência dos provedores de nuvem é útil para verificar o seu histórico de QoS em interações passadas, sendo que quanto maior é a variabilidade no histórico, menor é a eficiência e consequentemente menos confiável será este provedor. Deste modo, a eficiência destes provedores pode ser calculada usando uma abordagem denominada Análise Envoltória de Dados (do inglês *Data Envelopment Analysis* - DEA). A DEA é um método não paramétrico que calcula a eficiência relativa de um conjunto de unidades, em que cada unidade é uma DMU (do inglês *Decision Making Unit*), capaz de converter entradas em saídas [Charnes et al. 1978]. Existem diversos modelos para a DEA, como o CCR (Charnes, Cooper e Rhodes) e BCC (Banker, Charnes e Cooper) [Banker et al. 1984].

Sendo assim, para a aplicação da DEA, as entradas e saídas devem ser modeladas. Neste trabalho as entradas e saídas são compostas pelos indicadores de QoS mencionados. As saídas (O_{kj}) de cada provedor de nuvem (DMU), representadas na Equação 3, são entendidas como a média dos dados históricos de cada indicador de QoS. Os dados históricos compreendem todas as interações já realizadas do PN com os seus usuários. Além disso, ao valor médio é acrescentado o desvio padrão, pois um indicador de QoS do PN, pode apresentar flutuações no conjunto de interações já realizadas.

$$O_{kj} = \overline{H_{kj}}\;+\;\sigma(H_{kj}) \tag{3}$$

As entradas (I_{ki}) são compostas pela média dos valores estimados para cada indicador (i) de QoS do PN (k). Para efetuar a geração dos valores estimados, a regressão linear é usada, através das duas primeiras interações históricas estima-se o valor da terceira, e assim por diante, até a enésima interação passada. Esta abordagem é necessária para verificar o comportamento do PN em futuras interações. A Equação 4 representa a entrada calculada para cada indicador usando o método mencionado.

$$I_{ki} = \overline{X_{ki}}\;-\;\sigma(X_{ki}) \tag{4}$$

Após definidas as entradas e saídas, a eficiência de um provedor de nuvem pode ser calculada. A eficiência é resolvida calculando um modelo da DEA por meio de programação linear. Assim, o modelo BCC da DEA, orientado à saída, é indicado para o contexto, pois os valores de saída (históricos) não dependem das entradas (estimadas).

Além da eficiência calculada pela DEA ($Eff\,(s)$), o indicador de confiança objetivo ($T_{obj}(s)$), contempla um ponderador da eficiência relativa, indicando a importância assimilada pelo provedor de serviço a cada indicador de QoS. Tal ponderador, chamado de confiança multicritério ($Esc\,(s)$), é calculado através da matriz de julgamento do método *Analytical Hierarchy Process* (AHP).

Para a determinação dos pesos de importância de cada indicador, a escala de Saaty [Saaty 1990] é usada, sendo composta por níveis de importância, de 1 a 9, em que

1 representa uma igual importância entre os indicadores e 9 representa uma enorme discrepância entre o significado dos indicadores. Através desta escala, a matriz de julgamento é criada para desempenhar a comparação pareada entre os indicadores de QoS. Desta forma, esse julgamento é realizado através de processos de normalização e cálculo de média, resultando nos pesos de cada indicador ($w1 \ldots w5$). Por fim, a $Esc\,(s)$ representada na Equação 5, é calculada pela multiplicação da média do histórico dos indicadores pelos seus pesos de importância.

$$Esc\,(s) \;=\; (w1 * \overline{D}) \;+\; (w2 * \overline{RT}) \;+\; (w3 * \overline{S}) \;+\; (w4 * \overline{E}) \;+\; (w5 * \overline{P}) \qquad (5)$$

Em que $\overline{D}$, $\overline{RT}$, $\overline{S}$, $\overline{E}$, $\overline{P}$, representam a média dos valores históricos normalizados para os indicadores de disponibilidade, tempo de resposta, segurança, estabilidade e preço, respectivamente, enquanto $w1$ até $w5$ referem-se aos pesos de importância.

3.1.2. Indicador de Confiança Subjetiva

O método usado nesse indicador é baseado nas avaliações dos usuários em relação aos provedores de nuvem, acerca dos indicadores de QoS. Adotou-se a metodologia proposta em [Noor et al. 2016], acrescentando uma abordagem ponderada no cálculo da avaliação subjetiva e o fator de identificação de ataques do tipo avaliação injusta.

Assim, o usuário envia seu *feedback*, na forma de um conjunto de avaliações, a respeito da transação realizada com o PN. O conjunto de avaliações contempla um valor de 0 a 5 para cada indicador de QoS. Portanto, a avaliação subjetiva ($Q_c(c, s)$) de um PN s fornecida pelo usuário c, calculada na Equação 6, é vista como a soma ponderada dos valores atribuídos aos indicadores de QoS na avaliação subjetiva pelos pesos de importância desses indicadores (mesma forma de cálculo adotada na confiança multicritério).

$$Q_c\,(c, s) = (ind_1 * w_1) + (ind_2 * w_2) + \ldots + (ind_n * w_n) \qquad (6)$$

O indicador de confiança subjetiva ($T_{sub}(s)$), representado pela Equação 7, é calculado como a soma ponderada de cada avaliação subjetiva ($Q_c\,(c, s)$) do usuário c ao PN s pelo fator de credibilidade ($C_f\,(c, s)$). Ainda, n representa o total de usuários que avaliaram o PN s e $|V(s)|$ é o total de avaliações subjetivas ao PN s.

$$T_{sub}(s) = \frac{\sum_{c=1}^{n} Q_c\,(c, s) * C_f\,(c, s)}{|V(s)|} \qquad (7)$$

Em qualquer cenário que utiliza o *feedback* dos usuários, o valor da confiança subjetiva está sujeito a ataques. Os ataques buscam desfigurar o comportamento real da entidade que está sendo reputada, que nesse trabalho são os provedores de nuvem. Essa manipulação visa por exemplo, promover entidades com baixa reputação para que sejam selecionados em uma futura utilização/interação. Segundo [Jøsang and Golbeck 2009] são exemplos de alguns ataques:

- Avaliações injustas: ocorre quando um usuário envia um *feedback* de confiança que não reflete a realidade do objeto avaliado, ou seja, quer promover ou prejudicar a reputação de uma determinada entidade;

- Colusão de avaliações: conjunto de múltiplos *feedbacks* (independente do seu valor) que buscam manipular a reputação de uma entidade.

Desta forma, quando os *feedbacks* são enviados à arquitetura de reputação, via GR ao final da interação, eles devem ser analisados, tratados e armazenados no repositório de dados para manutenção do histórico subjetivo. A análise é feita pelo fator de credibilidade ($C_f\,(c,s)$), entendido como a média aritmética dos fatores que identificam alguns ataques que podem ocorrer ao valor total de reputação em função do indicador de confiança subjetiva. Neste trabalho, os fatores são a densidade das avaliações ($D\,(s)$ - ataque de colusão de avaliações) e o ataque de avaliações injustas ($S_{id}(c,s)$).

$$C_f\,(c,s) = \frac{D\,(s) + S_{id}(c,s)}{2} \tag{8}$$

O fator de densidade, representado na Equação 9, modela a situação em que os usuários enviam diversas avaliações em sequência para manipular os resultados do indicador de confiança subjetiva de uma entidade. Este fator consiste na razão entre a quantidade de usuários ($M(s)$) que avaliaram um PN s, e o total de avaliações que o PN s recebeu $|V(s)|$ multiplicado pelo fator de colusão das avaliações subjetivas $L(s)$.

$$D(s) = \frac{M(s)}{|V(s)| * L(s)} \tag{9}$$

O fator de colusão das avaliações subjetivas, representado pela Equação 10, busca reduzir a credibilidade dos usuários que enviam múltiplas avaliações (independente do valor) ao mesmo PN. É calculado como a proporção entre o número de avaliações subjetivas emitidas pelos usuários $|V_c(c,s)|$, que enviaram mais avaliações do que o especificado no limite de colusão $e_v\,(s)$ sobre o total de avaliações ($|V(s)|$) relativas ao PN s.

$$L(s) = 1 + \left(\frac{1}{|V(s)|} \sum_{c=1}^{n} |V_c(c,s)|_{\;[\,|V_c(c,s)|>e_v(s)\,]} \right) \tag{10}$$

Nas avaliações injustas, os usuários com comportamento malicioso enviam várias avaliações para tentar manipular o indicador de confiança subjetiva, buscando aumentá-lo ou diminuí-lo. Este fator, apresentado na Equação 11, compreende a razão entre a quantidade de avaliações fornecidas pelo usuário c ao PN s, que estão acima ou abaixo de um limite k (ex: $k = 4.5$), e a quantidade de avaliações dadas pelo usuário c ao PN s ($|V(c,s)|$).

$$S_{id}(c,s) = 1 - \left(\frac{\sum_{z=1}^{n} |V(c,s)|_{\;[|V(c,s)|\geq k]}}{|V(c,s)|} \right) \tag{11}$$

4. Experimentos e Resultados

Para avaliar a arquitetura de reputação proposta foi construído um cenário no simulador de redes *Peer-to-Peer* (P2P) PeerFactSim.KOM. O cenário, apresentado pela Figura 2, simula a troca de mensagens entre os usuários (provedores de serviço) e a arquitetura proposta. Neste trabalho, os provedores de serviço utilizam os recursos da nuvem de forma colaborativa para fornecer um serviço aos seus clientes. Deste modo, nós de rede apresentando diferentes funcionalidades foram criados e são definidos como:

- **Nó da Arquitetura de Reputação (`ARQ`)**: Este tipo de nó implementa as funcionalidades do Gerenciador de Reputação (GR) e comunica-se com o restante dos módulos da arquitetura;
- **Nó que representa o Provedor de Serviço (`PS`)**: configurados na forma de uma *Service Overlay Network* (SON), estes nós representam os provedores de serviço que utilizam os recursos fornecidos pela nuvem para disponibilizar seus serviços. Assim, este tipo de nó interage com a arquitetura, podendo solicitar a reputação de um PN, enviar avaliações subjetivas referentes a um PN e requisitar informações de monitoramento;
- **Nó que representa um provedor de nuvem (`PN`)**: Este tipo de nó representa um provedor de nuvem computacional;
- **Nó de `Monitoramento`**: Responsável por interagir com o PN e coletar informações de QoS durante a utilização da arquitetura.

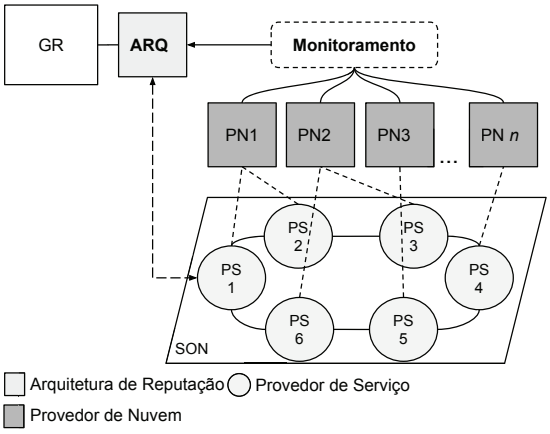


Figura 2. Cenário da Implementação

Na execução dos experimentos alguns parâmetros foram definidos como o tempo de execução da simulação (10080 min), número de PNs (10), número de PS entre 5 e 25 para verificar a escalabilidade da arquitetura e os pesos para cada indicador de QoS, D (0.3830), TR (0.2317), E (0.1861), S (0.1350) e P (0.0642), obtidos através da matriz de julgamento (Seção 3.1.1).

4.1. Avaliação da Reputação

A reputação dos provedores de nuvem é composta de dois indicadores de confiança: objetiva e subjetiva. O indicador objetivo dos PNs teve seu histórico de interações com os PSs composto através de valores aleatórios gerados seguindo uma distribuição de probabilidade linear. Os valores, apresentados na Tabela 1, estão relacionados com a média das interações anteriores de cada indicador de QoS dos PNs, em que D, RT, E, S e P referem-se aos indicadores de disponibilidade, tempo de resposta, estabilidade, segurança e preço.

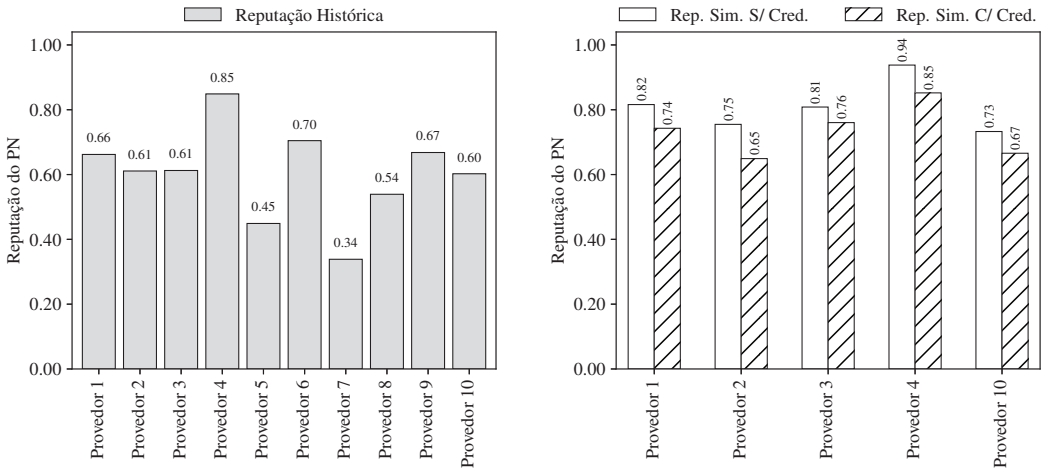
O indicador da confiança subjetiva dos provedores fictícios teve seu histórico composto por meio da base de avaliações reais presente em [Noor et al. 2016]. Essa base contém dez mil avaliações de 113 PNs. Uma etapa de pré-processamento foi realizada para extrair 10 PNs com dez avaliações subjetivas cada um, sendo que cada avaliação

Tabela 1. Valores dos indicadores de QoS

Provedor	$\overline{D}$	$\overline{RT}$	$\overline{E}$	$\overline{S}$	$\overline{P}$
Provedor 1	0,9648	99ms	62	3	$ 0,75
Provedor 2	0,9439	647ms	58	4	$ 0,65
Provedor 3	0,9188	114ms	57	7	$ 0,53
Provedor 4	0,9683	20ms	59	8	$ 0,79
Provedor 5	0,8924	535ms	64	7	$ 0,84
Provedor 6	0,5743	250ms	36	5	$ 0,32
Provedor 7	0,5604	869ms	67	7	$ 0,64
Provedor 8	0,7809	691ms	12	2	$ 0,52
Provedor 9	0,4959	332ms	33	9	$ 0,48
Provedor 10	0,6370	696ms	49	8	$ 0,64

subjetiva é composta por um conjunto de avaliações contendo 5 valores, cada qual para um dos indicadores de QoS utilizados.

Através dos históricos para cada indicador, a reputação dos PNs foi calculada. Para este cálculo, considerou-se o peso de 0.85 para o indicador objetivo e 0.15 para o indicador subjetivo, indicando que o PS atribui maior importância ao indicador objetivo. Os resultados propostos para o cálculo inicial da reputação são ilustrados na Figura 3 (a).



(a) Reputação Inicial (b) Reputação Após a Simulação

Figura 3. Análise da Reputação

Portanto, os provedores de nuvem que apresentam as melhores reputações tem uma melhor qualidade de serviço e tem recebido avaliações positivas em relação ao seu desempenho durante as interações com o usuário. É o caso, por exemplo, dos provedores de nuvem (1, 4, 6 e 9). Contudo, analisando os valores objetivos históricos, é possível notar que esses PNs apresentam melhores valores nos indicadores de QoS mais relevantes (disponibilidade e tempo de resposta), indicando que apresentam uma maior reputação em relação aos demais, ou seja, são capazes de fornecer um serviço confiável, sem muita variação e com melhor qualidade.

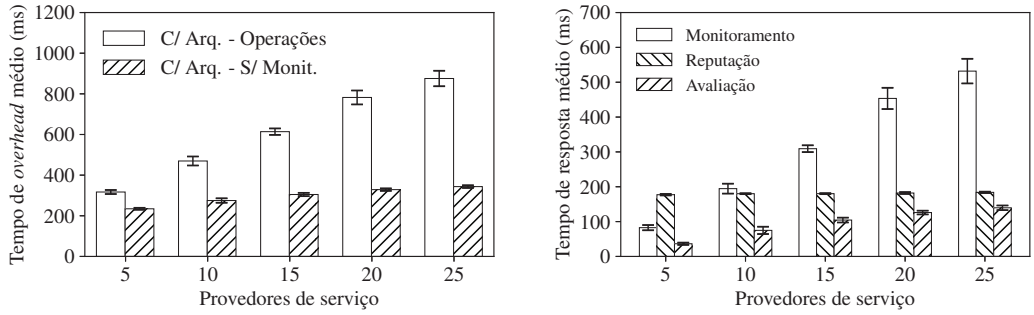
Após a apresentação dos dados históricos e a reputação inicial, uma nova interação entre alguns provedores de nuvem e seus usuários foi simulada. Para isso, construiu-se um ambiente SON com dez provedores de serviço que utilizaram os recursos de cinco

provedores de nuvem (1, 2, 3, 4 e 10). Ao final de cada interação, cada provedor de serviço (usuário) avaliou o provedor de nuvem utilizado, sendo que alguns provedores de serviço enviaram algumas avaliações maliciosas. Desse modo, os resultados são apresentados pela Figura 3 (b), em que apresenta duas opções: (i) Rep. Sim. S/ Cred: reputação atualizada sem considerar o fator de credibilidade do indicador de confiança subjetivo e (ii) Rep. Sim. C/ Cred: reputação atualizada considerando a credibilidade.

Através dos resultados da reputação simulada, pode-se notar que ao desconsiderar a credibilidade no cálculo da reputação, o valor de reputação aumenta desproporcionalmente ao comportamento real, pois um ataque de avaliações maliciosas ocorreu. Desse modo, o fator de credibilidade visa ponderar os valores das avaliações para filtrar quando ocorrem ataques.

4.2. Avaliação da Arquitetura

A avaliação da arquitetura de reputação é composta pelo *overhead* de utilização e o tempo de resposta médio para cada operação. Analisaram-se as operações de requisição de reputação (Reputação), envio de avaliações subjetivas (Avaliação - do PS ao PN) e o monitoramento dos indicadores de QoS (Monitoramento). Os resultados para o *overhead* e tempo médio são apresentados na Figura 4 considerando um intervalo de confiança de 95 %.



(a) *Overhead* de utilização (b) Tempo de resposta médio

Figura 4. Avaliação da arquitetura de reputação proposta

O *overhead* de utilização, ilustrado na Figura 4 (a), foi avaliado por meio de diversas simulações no cenário proposto, sendo que o número de provedores de serviço variou entre 5 e 25 e as requisições à arquitetura de reputação foram uniformemente distribuídas em relação ao tempo de simulação. O *overhead* médio analisado considerou as seguintes opções: (i) *C/ Arq. - Operações*: usando a arquitetura de reputação e considerando todas as operações mencionadas e (ii) *C/ Arq. - S/ Monit.*: usando a arquitetura de reputação e desconsiderando a operação de monitoramento.

Observando a opção *C/ Arq. - Operações*, pode se notar que o tempo de *overhead* aumenta em relação ao número de PSs que estão utilizando a arquitetura. Esse aumento é motivado pelas operações de monitoramento e envio de avaliações subjetivas pois, nesse caso quando o número de PSs aumenta, mais avaliações subjetivas são enviadas a respeito das transações com os PSs. Além do mais, os PNs são mais utilizados, impactando no tempo de resposta da operação de monitoramento simulada dos indicadores de QoS.

A operação de monitoramento foi desconsiderada nos experimentos realizados na opção *C/ Arq. - S/ Monit.*. O monitoramento é uma operação simulada que consiste na

troca de mensagens com dados de indicadores de QoS, entre os nós de monitoramento, PNs e o nó ARQ. Portanto, conclui-se que o monitoramento consome muito tempo.

Outras simulações foram efetuadas usando a opção *C/ Arq. - Operações* para avaliar o tempo médio de resposta de cada operação da arquitetura durante o uso pelos PSs. Os resultados presentes na Figura 4 (b), demonstram que o envio de avaliações subjetivas está fortemente associado com o número de PSs e a operação de monitoramento consome a maior fração do tempo e está relacionada com a quantidade de PSs existentes no ambiente pois, quanto maior o número de PSs maior será o uso dos recursos de nuvem, necessitando assim de mais operações de monitoramento. Ainda, neste caso, o tempo de resposta da operação de monitoramento inclui a troca de mensagens e o tempo de processamento (geração dos valores de QoS e atualização no repositório de dados), na qual a troca de mensagens consome em média 8 ms no cenário proposto.

5. Conclusão

Este trabalho apresentou uma arquitetura de reputação de confiança de provedores de computação em nuvem para auxiliar os processos de tomada de decisão. A arquitetura de reputação proposta é centralizada e composta por diversos elementos, como: módulo de monitoramento, gerenciador de reputação, módulo de agregação, repositório de dados e o *broker* de registro.

Com o propósito de avaliar a arquitetura de reputação proposta, um cenário foi desenvolvido no simulador de redes P2P PeerFactSim.KOM, contemplando os elementos da arquitetura bem como os provedores de nuvem e os usuários, entendidos neste caso, como provedores de serviço que utilizam os recursos da nuvem para disponibilizar seus serviços.

Por meio dos resultados apresentados pode-se notar que arquitetura apresenta meios para tratar ataques que ocorrem com o valor de reputação. Também observa-se que a utilização da arquitetura de reputação no ambiente de computação em nuvem, apresenta um *overhead* aceitável em relação às funcionalidades disponibilizadas e dada a importância da confiança neste contexto. Em um cenário real, o *overhead* pode ser diminuído devido a abordagem de monitoramento ser realizada por ferramentas de hardware e *software*, e não de forma simulada como foi feita na avaliação da arquitetura.

Como trabalhos futuros, pretende-se aplicar esta arquitetura em um cenário real, considerando a replicação do nó de gerenciador de reputação como uma das soluções para resolver o ponto único de falha, e analisar outros aspectos referentes ao desempenho da arquitetura. Além disto, pretende-se introduzir o conceito de bonificação ao cálculo da confiança objetiva de forma a gratificar a reputação dos provedores de nuvem que mantiverem regularidade no conjunto histórico dos indicadores de QoS.

Agradecimentos

Os autores agradecem a UDESC PROMOP pelo suporte financeiro e ao LabP2D.

Referências

Banker, R. D., Charnes, A., and Cooper, W. W. (1984). Some models for estimating technical and scale inefficiencies in data envelopment analysis. *Management Science*, 30(9):1078–1092.

Baranwal, G. and Vidyarthi, D. P. (2014). A framework for selection of best cloud service provider using ranked voting method. In *IACC 2014*, pages 831–837.

Charnes, A., Cooper, W. W., and Rhodes, E. (1978). Measuring the efficiency of decision making units. *European Journal of Operational Research*, 2(6):429–444.

Firdhous, M., Ghazali, O., and Hassan, S. (2012). Trust Management in Cloud Computing: A Critical Review. *ICTer Journal*, 4(2):24–36.

Gambetta, D. et al. (2000). Can we trust trust. *Trust: Making and breaking cooperative relations*, 13:213–237.

Garg, S. K., Versteeg, S., and Buyya, R. (2013). A framework for ranking of cloud computing services. *Future Generation Computer Systems*, 29(4):1012–1023.

Habib, S. M., Ries, S., and Muhlhauser, M. (2011). Towards a trust management system for cloud computing. In *TrustCom*, pages 933–939. IEEE.

Jøsang, A. and Golbeck, J. (2009). Challenges for robust trust and reputation systems. In *SMT 2009, Saint Malo, France*.

Mell, P. M. and Grance, T. (2011). SP 800-145. *The NIST Definition of Cloud Computing, National Institute of Standards & Technology, Gaithersburg, MD*.

Mousa, H., Mokhtar, S. B., Hasan, O., Younes, O., Hadhoud, M., and Brunie, L. (2015). Trust management and reputation systems in mobile participatory sensing applications: A survey. *Computer Networks*, 90:49–73.

Nguyen, H. T., Zhao, W., and Yang, J. (2010). A trust and reputation model based on bayesian network for web services. In *ICWS 2010*, pages 251–258. IEEE.

Noor, T. H., Sheng, Q. Z., Yao, L., Dustdar, S., and Ngu, A. H. (2016). CloudArmor: Supporting reputation-based trust management for cloud services. *IEEE TPDS*, 27(2):367–380.

Resnick, P. and Zeckhauser, R. (2002). Trust among strangers in internet transactions: Empirical analysis of ebay's reputation system. *The Economics of the Internet and E-commerce*, 11(2):23–25.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., and Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of management review*, 23(3):393–404.

Saaty, T. L. (1990). How to make a decision: the analytic hierarchy process. *European Journal of Operational Research*, 48(1):9–26.

Sabater, J. and Sierra, C. (2005). Review on Computational Trust and Reputation Models. *Artificial Intelligence Review*, 24(1):33–60.

Siegel, J. and Perdue, J. (2012). Cloud services measures for global use: the service measurement index (SMI). In *SRII Global Conference (SRII), 2012 Annual*, pages 411–415. IEEE.

Tang, M., Dai, X., Liu, J., and Chen, J. (2016). Towards a trust evaluation middleware for cloud service selection. *Future Generation Computer Systems*.

Yau, S. S. and Yin, Y. (2011). Qos-based service ranking and selection for service-based systems. In *SCC 2011*, pages 56–63. IEEE.

Zhang, Q., Cheng, L., and Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. *Journal of Internet Services and Applications*, 1(1):7–18.