As Organizações Virtuais (OVs) representam uma proeminente e flexível forma de colaboração na qual um conjunto de entidades (empresas) compartilham competências e riscos para atender um objetivo de negócio. Suas interações são apoiadas pela Internet e podem utilizar recursos de nuvem computacional. Nesse sentido, a integração entre OV e nuvem apresenta vários benefícios. No entanto alguns problemas relacionados a privacidade, segurança e confiança surgem. Um dos principais problemas é a confiança na qualidade de serviço ofertada pelos provedores de nuvem. Desse modo, essa dissertação apresenta uma arquitetura de reputação de confiança aplicada às OVs baseadas na nuvem, para apoiar os processos de tomada de decisão.

Orientador: Dr. Adriano Fiorese

Coorientador: Dr. Omir Correia Alves Junior

Joinville, 2017

ANO
2017

LUÍS FELIPE BILECKI | UMA ARQUITETURA DE REPUTAÇÃO DE CONFIANÇA NO CONTEXTO DA INTEGRAÇÃO ENTRE ORGANIZAÇÕES VIRTUAIS E COMPUTAÇÃO EM NUVEM

UNIVERSIDADE DO ESTADO DE SANTA CATARINA – UDESC
CENTRO DE CIÊNCIAS TECNOLÓGICAS – CCT
PROGRAMA DE PÓS GRADUAÇÃO EM COMPUTAÇÃO APLICADA

DISSERTAÇÃO DE MESTRADO

UMA ARQUITETURA DE REPUTAÇÃO DE CONFIANÇA NO CONTEXTO DA INTEGRAÇÃO ENTRE ORGANIZAÇÕES VIRTUAIS E COMPUTAÇÃO EM NUVEM

LUÍS FELIPE BILECKI

JOINVILLE, 2017

LUÍS FELIPE BILECKI

UMA ARQUITETURA DE REPUTAÇÃO DE CONFIANÇA NO CONTEXTO DA INTEGRAÇÃO ENTRE ORGANIZAÇÕES VIRTUAIS E COMPUTAÇÃO EM NUVEM

Dissertação submetida ao Programa de Pós-Graduação em Computação Aplicada do Centro de Ciências Tecnológicas da Universidade do Estado de Santa Catarina, para a obtenção do grau de Mestre em Computação Aplicada.

Orientador: Dr. Adriano Fiorese
Coorientador: Dr. Omir Correia Alves Junior

JOINVILLE

2017

Ficha catalográfica elaborada pelo(a) autor(a), com
auxílio do programa de geração automática da
Biblioteca Setorial do CCT/UDESC

Bilecki, Luís Felipe
Uma Arquitetura de Reputação de Confiança no Contexto da Integração entre Organizações Virtuais e Computação em Nuvem / Luís Felipe Bilecki. - Joinville , 2017.
138 p.

Orientador: Adriano Fiorese
Coorientador: Omir Correia Alves Junior
Dissertação (Mestrado) - Universidade do Estado de Santa Catarina, Centro de Ciências Tecnológicas, Programa de Pós-Graduação em Computação Aplicada, Joinville, 2017.

1. Arquitetura de Reputação. 2. Organizações Virtuais. 3. Computação em Nuvem. I. Fiorese, Adriano. II. Alves Junior, Omir Correia. , .III. Universidade do Estado de Santa Catarina, Centro de Ciências Tecnológicas, Programa de Pós-Graduação em Computação Aplicada. IV. Título.

Uma Arquitetura de Reputação de Confiança no Contexto da Integração entre Organizações Virtuais e Computação em Nuvem

por

Luís Felipe Bilecki

Esta dissertação foi julgada adequada para obtenção do título de

Mestre em Computação Aplicada

Área de concentração em "Ciência da Computação,
e aprovada em sua forma final pelo

CURSO Mestrado Acadêmico em Computação Aplicada
CENTRO DE CIÊNCIAS TECNOLÓGICAS DA
UNIVERSIDADE DO ESTADO DE SANTA CATARINA.

Banca Examinadora:

Prof. Dr. Omir Correia Alves Junior
CCT/UDESC (Coorientador/Presidente)

Prof. Dr. Charles Christian Miers
CCT/UDESC

Prof. Dr. Luiz Fernando Bittencourt
UNICAMP por videoconferência

Joinville,SC, 23 de agosto de 2017.

AGRADECIMENTOS

Inicialmente agradeço a minha família que sempre me apoiou e me incentivou em cada escolha que eu fizesse.

Ao meu orientador, Prof. Dr. Adriano Fiorese, pela orientação, dedicação, paciência e pelos comentários e discussões que possibilitaram a realização deste trabalho.

Aos membros que participaram da banca de qualificação e dissertação, Prof. Dr. Omir Correia Alves Junior, Prof. Dr. Charles Christian Miers e Prof. Dr. Luiz Fernando Bittencourt, pelos comentários e avaliações que contribuíram para o enriquecimento deste trabalho.

A Universidade do Estado de Santa Catarina, pelo apoio financeiro através do programa de bolsas de monitoria de pós-graduação (PROMOP).

Aos meus amigos Andrei Carniel, Paulo Roberto Vieira Junior, Pedro Henrique Narloch, Ana Carolina Tomé Klock, Jonatas Marques, Tathiana Duarte, Emanoeli Madalosso, Anderson Marcondes por terem me ajudado, incentivado e pelos momentos de descontração.

E por fim, gostaria de agradecer a Deus, que sem ele nada seria possível.

A persistência é o menor caminho do êxito.

Charles Chaplin

RESUMO

As Organizações Virtuais (OVs) configuram-se como uma proeminente e flexível forma de colaboração na qual um conjunto de entidades compartilham recursos, habilidades, competências e riscos no atendimento de um objetivo em comum. Além disto, seu processo de comunicação e as interações são suportadas por uma infraestrutura computacional baseada na Internet, por exemplo, Computação em Nuvem (CN) ou Computação em Grade. Desse modo, a integração entre OV e CN, ou seja, o uso de recursos de nuvem pela OV, pode contribuir para a redução de custos com manutenção e infraestrutura computacional. Contudo, algumas barreiras relativas a privacidade, confiança e segurança acabam surgindo e podem ser impeditivos para realizar o atendimento da oportunidade de colaboração. Um dos problemas observados na integração entre OV e CN é a confiança na qualidade de serviço ofertado pelos provedores de nuvem (PN), uma vez que os parceiros de negócio da OV (empresas) utilizam estes recursos para disponibilizar seus serviços e realizar atividades de colaboração. Uma das alternativas para a solução deste problema de confiança é por meio da aplicação de arquiteturas de reputação. As arquiteturas de reputação recebem as avaliações dos usuários, monitoram e processam outros indicadores de confiança com o propósito de fornecer a reputação de uma determinada entidade e auxiliam no estabelecimento e gerenciamento de um relacionamento de confiança. O presente trabalho apresenta uma arquitetura de reputação de confiança que auxilia nos processos de tomada de decisão existentes nas OVs baseadas na nuvem computacional. A arquitetura calcula a reputação dos provedores de nuvem através de dois indicadores de confiança: objetiva (desempenho do PN em relação a alguns indicadores de QoS) e subjetiva (avaliações dos parceiros de negócio). De forma a avaliar a arquitetura de reputação, desenvolveu-se um cenário de avaliação no simulador de redes *Peer-to-Peer* (P2P) PeerFactSim.KOM. O cenário simula uma OV que usa os recursos da nuvem e também realiza requisições à arquitetura de reputação. Os resultados da simulação no cenário proposto indicam: (i) efetividade da avaliação e identificação de ataques ao indicador de confiança subjetiva; (ii) efetividade na penalização e recompensa no indicador de confiança objetiva em históricos de QoS com maiores oscilações (iii) baixo *overhead* da arquitetura proposta em relação as funcionalidades propostas durante a fase de operação da OV; e (iv) escalabilidade em relação ao número de parceiros de negócio na OV.

Palavras-chave: Organizações Virtuais, Computação em Nuvem e Reputação.

ABSTRACT

Virtual Organizations (VOs) represent a prominent and flexible collaboration initiative, in which a set of entities share resources, skills, competences, and risks to attend a common goal. Moreover, their communication process and interactions can be supported on an Internet basis, using Cloud Computing (CC) or Grid Computing. Thereby, the VO and CC integration, that is the use of cloud resources by VOs, can promote the reduction of infrastructure costs and maintenance, interoperability, among others. However, some issues related to privacy, trust, and security arise and can impact the attendance of the collaboration opportunity. One of the observed issues, in the VO and CC integration, is how much trust VO's members put in the cloud provider, particularly in a scenario where business partners (VO's members) use the cloud provided resources to make available their services and in order to interact with other entities. One of the alternatives to cope with the trust issue is the utilization of reputation architectures. A reputation architecture receives the users feedback, monitors, and processes other information sources in order to assess the reputation to an entity, and help establish and manage a trust relationship. This work presents a trust reputation architecture to assist in the several decision-making processes existing in a cloud computing based VO. The proposed architecture assess the cloud providers reputation by means of two trust indicators: objective (perfomance of a service related to some QoS indicators) and subjective (feedback from business partners to cloud providers). A scenario was developed in the PeerFactSim.KOM Peer-to-Peer (P2P) network simulator, with the purpose of simulate a VO that uses cloud resources and makes requests to the reputation architecture. The simulation results in the proposed scenario indicate: (i) effective identification and evaluation of subjective trust attacks; (ii) effective application of penalty and reward factors on the objective trust indicator, comprising unstable cloud provider's historical QoS data; (iii) low overhead related to the proposed architecture operations, and (iv) scalability regarding the amount of VO's business partners.

Keywords: Virtual Organization, Cloud Computing, and Reputation.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

AHP *Analytic Hierarchy Process*

BRS *Beta Reputation System*

CSMIC *Cloud Services Measurement Initiative Consortium*

DEA *Data Envelopment Analysis*

EN *Enterprise Network*

IaaS *Infrastructure as a Service*

KPI *Key Performance Indicator*

NIST National Institute of Standards and Technology

OC Oportunidade de Colaboração

OV Organização Virtual

P2P *Peer-to-Peer*

PN Provedor de Nuvem

PaaS *Platform as a Service*

QoS *Quality of Service*

RBS *Reputation Broker Service*

SaaS *Software as a Service*

SLA *Service Level Agreement*

SMI *Service Measurement Index*

SOA Arquitetura Orientada a Serviço

STORE *Stocasthic Reputation Service for Virtual Organizations*

TIC Tecnologias de Infraestrutura e Comunicação

UML *Unified Modeling Language*

SUMÁRIO

1 INTRODUÇÃO E JUSTIFICATIVA

Diversos desafios sócio-econômicos, como por exemplo a globalização e a competitividade, motivaram as pequenas e médias empresas a adotar metodologias de trabalho colaborativo com o propósito de reduzir o tempo e custos envolvidos no processo produtivo (ESPOSITO; EVANGELISTA, 2014). Uma dessas metodologias de trabalho colaborativo é a rede de colaboração, que configura-se dentre várias formas, como por exemplo, uma organização virtual (CAMARINHA-MATOS; AFSARMANESH, 2005).

Uma Organização Virtual (OV) pode ser vista como uma aliança temporária na qual um conjunto de entidades (geralmente empresas) legalmente independentes, heterogêneas e geograficamente distribuídas compartilham recursos, informações, custos, habilidades e riscos a fim de alcançar objetivos específicos de negócio (atender a uma oportunidade de colaboração) (CAMARINHA-MATOS et al., 2009).

As OVs podem usufruir das tecnologias de infraestrutura e comunicação (TIC) (ex: computação em nuvem (CN), computação em grade, entre outras) como ferramenta de suporte aos negócios e transações entre pessoas e empresas (ZAMANIAN; MOHSENZADEH; NASSIRI, 2014).

A existência de uma OV é guiada pelo seu ciclo de vida, apresentado inicialmente em Camarinha-Matos e Afsarmanesh (1999), o qual contempla quatro fases: criação, operação, evolução e dissolução. Em outro estudo, realizado em Camarinha-Matos et al. (2009), a fase de metamorfose foi acrescentada, sendo referente a maiores mudanças nos princípios, objetivos e filiações, motivando a criação de uma nova OV.

Desse modo, no momento em que a OV está em operação, cada parceiro de negócio (entidade - empresa) da OV troca informações e compartilha recursos através de dois cenários de infraestrutura de comunicação: tradicional e na nuvem (ZAMANIAN; MOHSENZADEH; NASSIRI, 2014). O cenário tradicional utiliza somente a Internet para a troca e compartilhamento de informações entre os parceiros de negócio da OV (RUARO; RABELO, 2016a). Por sua vez, no cenário na nuvem, a troca de informações, hospedagem e execução de aplicações ocorre através dos recursos e serviços (ex: armazenamento, infraestrutura, *softwares*) disponibilizados pelos provedores de nuvem externos (ZAMANIAN; MOHSENZADEH; NASSIRI, 2014; RUARO; RABELO, 2016a).

A integração entre OV e CN (cenário na nuvem) fornece vários benefícios para a rede de colaboração, tais como: redução de custos e de manutenção com infraestru-

tura, provisionamento de recursos computacionais sob demanda e independência de tempo e lugar para realizar a colaboração (ZAMANIAN; MOHSENZADEH; NASSIRI, 2014).

Contudo, com o crescente aumento do número de provedores de nuvem com características semelhantes entre os serviços fornecidos (GARG; VERSTEEG; BUYYA, 2013), os parceiros de negócio e o gestor da OV são confrontados com problemas relacionados à segurança, privacidade e confiança. Assim, a busca e seleção de provedores de nuvem mais adequados a questão da confiabilidade torna-se um fator crítico de sucesso para que a operação da OV atenda os requisitos esperados (ALHAMAD; DILLON; CHANG, 2010). Ou seja, os parceiros de negócio da OV necessitam confiar nos recursos que são disponibilizados pelos provedores de nuvem.

Nesse sentido, um dos meios de auxílio na resolução desses problemas, é através dos contratos que são firmados entre os clientes (gestor da OV ou parceiro de negócio) e os provedores de nuvem. Os contratos, chamados de *Service Level Agreement* (SLA), podem auxiliar no gerenciamento da operação da OV, fornecendo indicadores que devem ser medidos e controlados conforme os valores estabelecidos previamente.

No entanto, o gerenciamento do SLA torna-se insuficiente para o estabelecimento de um relacionamento de confiança entre os provedores de nuvem e os parceiros de negócio da OV, pois não leva em conta alguns aspectos subjetivos, como *feedbacks* (avaliações), da utilização desses serviços por parte do usuário (NOOR et al., 2016b).

Dessa forma, um dos principais problemas observados durante a existência da OV é a falta de uma arquitetura ou sistema que realize o gerenciamento e avaliação da confiança e auxilie nos processos de tomada de decisão existentes, seja entre os parceiros de negócio no processo de colaboração ou do parceiro de negócio ao provedor de nuvem que disponibiliza os seus recursos para a OV (NEATA; URZICA; FLOREA, 2011; ARASTEH; AMINI; JALILI, 2012). Além disso, um dos principais problemas observados na integração da OV com a computação em nuvem, é a confiança depositada pelos parceiros de negócio ao provedores, seja na formação da OV e/ou na operação da OV. Assim, entende-se que a questão da confiança desempenha um papel crítico durante a existência da OV (ARENAS; AZIZ; SILAGHI, 2010), pois os parceiros de negócio da OV transferem seus serviços e informações para os provedores de nuvem externos.

A confiança e seu gerenciamento são tópicos de pesquisa discutidos em várias áreas e aplicações (YU et al., 2010; FIRDHOUS; GHAZALI; HASSAN, 2012), e de uma forma geral, tal conceito define-se como um grau de crença subjetiva a respeito dos

comportamentos de uma entidade/objeto em particular (CHO; SWAMI; CHEN, 2011). Ainda, a confiança refere-se ao relacionamento de duas entidades, em que uma confia nas ações ou interações que são desempenhadas por outra entidade (BARBOSA; MORAIS, 2016). Por exemplo, em um ambiente de OVs, a confiança pode assumir valores numéricos que indica o quão confiável é uma entidade ou provedor de nuvem (GRANATYR et al., 2015), isto é, valores dentro de um determinado intervalo (ex: [0,1]) (SABATER; SIERRA, 2005).

Uma das formas de auxiliar a solução do problema de confiança na OV como um todo, ou seja auxiliar no estabelecimento de um relacionamento de confiança, é através da aplicação de arquiteturas de reputação (VOSS; WIESEMANN, 2005; KERSCHBAUM et al., 2006; HALLER, 2008b; MASHAYEKHY; GROSU, 2012). Uma arquitetura de reputação tem como objetivo principal determinar e disseminar a confiança em ambientes através da reputação (RUAN; MARTIN, 2011), ou seja, realiza o cálculo, gerenciamento, manutenção e distribuição (disseminação) da confiança. Desse modo cada entidade da OV, por exemplo um provedor de nuvem, tem um valor de reputação definido. Por sua vez, a reputação nesse contexto, é vista como um valor calculado por meio da agregação de um ou mais indicadores de confiança (ex: avaliações (opiniões), qualidade de serviço, indicadores de desempenho, entre outros) que representam o desempenho passado e atual desse provedor de nuvem em OVs (RESNICK; ZECKHAUSER, 2002; ACAMPORA; CASTIGLIONE; VITIELLO, 2014).

Uma arquitetura de reputação também disponibiliza meios para auxiliar os processos de tomada de decisão desempenhados pelos membros da OV. Um dos exemplos de tomada de decisão é o processo de busca e seleção de parceiros de negócio e/ou recursos de nuvem que pode ser apoiado pela reputação. Dessa forma, a aplicação de uma arquitetura de reputação em OVs, visa reduzir os riscos existentes na fase de operação da OV, devido ao fato que o processo de colaboração ocorre com entidades/provedores reconhecidos, pois o processo de busca e seleção foi apoiado pela reputação calculada para essas entidades.

Além de fornecer suporte ao estabelecimento de um relacionamento de confiança, tal arquitetura deve apresentar métodos ou técnicas que efetuem o tratamento de ataques ao valor de reputação, especificamente aos valores dos *feedbacks* (avaliações) fornecidos, quando os parceiros de negócio agem de forma maliciosa para promover ou prejudicar a reputação de um provedor de nuvem (JØSANG; GOLBECK, 2009).

Desse modo, esse trabalho propõe uma arquitetura de reputação de confiança que visa auxiliar a tomada de decisão em OVs que são baseadas na nuvem, ou seja, OVs que utilizam a nuvem computacional como infraestrutura de comunicação. A arquitetura proposta é desenvolvida de forma centralizada e fornece apoio às fases de

criação, operação e dissolução de uma OV. Nessas fases, a arquitetura pode ser aplicada do seguinte modo:

- **Fase de criação da OV**: auxilia a busca e seleção dos provedores de nuvem computacional fornecendo a reputação dos provedores de nuvem para apoiar a tomada de decisão, auxiliando o gestor da OV a selecionar provedores de nuvem;
- **Fase de operação da OV**: verifica e monitora o desempenho do provedor de nuvem e fornece a reputação atualizada do mesmo durante o processo de atendimento da oportunidade de colaboração; e
- **Fase de dissolução da OV**: atualiza a participação de um provedor de nuvem em uma OV, ou seja, cada parceiro de negócio da OV fornece para a arquitetura de reputação seu *feedback* de avaliação em relação ao provedor de nuvem que disponibilizou seus serviços/recursos.

1.1 OBJETIVOS

O objetivo geral do presente trabalho é propor uma arquitetura de reputação de confiança aplicada ao contexto da integração entre organizações virtuais e computação em nuvem visando auxiliar os processos de tomada de decisão, relativos à confiança, presentes no ciclo de vida da OV.

Este trabalho tem como objetivos específicos:

- Revisar os conceitos básicos relacionados à redes de colaboração, reputação e computação em nuvem;
- Realizar a revisão bibliográfica para identificar o estado da arte no que tange aos sistemas de reputação aplicados em OVs e áreas correlatas;
- Especificar o modelo conceitual da arquitetura de reputação, apresentando o sistema de reputação proposto, e seus respectivos módulos;
- Implementar os módulos da arquitetura que tratem do cálculo e disseminação da reputação;
- Especificar e implementar um módulo de monitoramento do desempenho dos provedores de nuvem para verificar a reputação de um provedor de nuvem em um determinado momento, durante a fase de operação da OV;
- Disponibilizar um módulo que realize o armazenamento dos dados que são utilizados no cálculo da reputação, ou seja, dados relativos ao desempenho do provedor de nuvem bem como as avaliações fornecidas pelos parceiros de negócio,

para atualizar a reputação de um provedor de nuvem após algumas participações em OVs;

- Especificar e desenvolver o ambiente de testes da arquitetura de reputação proposta; e
- Realizar a avaliação de forma simulada da arquitetura de reputação proposta no contexto da integração entre organizações virtuais e computação em nuvem.

1.2 METODOLOGIA DA PESQUISA

Para a classificação desta pesquisa, foram consideradas as propostas apresentadas em Eden (2007), Gil (2008), Gerhardt e Silveira (2009) e Wazlawick (2014). Desse modo, classificou-se essa pesquisa quanto ao método, natureza, abordagem, objetivos, método científico e nível de maturidade.

Em relação ao método ou procedimento de pesquisa, esta pesquisa é classificada como pesquisa bibliográfica, devido à sua elaboração ser realizada a partir de materiais disponíveis na literatura especializada, e experimental, pois esta pesquisa sugere a identificação de um problema, formulação da questão de pesquisa e uma proposta de solução a ser comprovada por meio da aplicação e análise de algum experimento. Para analisar a arquitetura de reputação proposta, um ambiente de integração foi desenvolvido em um simulador de redes P2P, com o propósito de avaliar de forma simulada a arquitetura de reputação em relação ao seu uso na OV, conforme pode ser visto no capítulo 5.

Quanto à natureza, esta pesquisa é categorizada como aplicada, pois utiliza-se de um conjunto de fundamentações teóricas específicas para aplicar-se ao problema da confiança existente na integração das OVs com computação em nuvem.

Em relação à abordagem, esta pesquisa é categorizada como quantitativa, pois os resultados gerados podem ser analisados estatisticamente e por meio dos experimentos computacionais realizados verifica-se a viabilidade da arquitetura proposta. Por fim, a reputação é construída essencialmente de forma quantitativa.

Em relação aos objetivos ou finalidade, pode-se dizer que esta pesquisa é classificada como exploratória pois, através de um levantamento bibliográfico, visa realizar um levantamento preliminar da área de estudo, identificando oportunidades de pesquisa e também esboça algumas interpretações e soluções acerca do objeto de pesquisa.

Quanto ao método científico, nesta pesquisa é adotado o método indutivo, pois o processo de raciocínio parte do conhecimento de fenômenos específicos do objeto de pesquisa para a formulação da teoria, ou seja, parte do particular para o geral.

Por fim, em relação à maturidade de pesquisa, conforme a escala proposta em Wazlawick (2014), pode-se classificar esta pesquisa como nível 2, ou seja, ocorre a apresentação de algo diferente, com paradigma tecnocrático predominante. Este trabalho foi classificado neste nível de maturidade devido ao fato de que não existe um *benchmark* universal para a comparação de arquiteturas de reputação, os testes são conduzidos pelo próprio autor com seu próprio conjunto de dados em um ambiente controlado e é realizada uma comparação com um método de cálculo de reputação presente em um sistema de reputação da literatura.

1.3 ORGANIZAÇÃO DO DOCUMENTO

O restante deste documento está organizado como se segue. O capítulo 2 apresenta a revisão bibliográfica dos conceitos relacionados para o desenvolvimento do trabalho, abrangendo: organizações virtuais, confiança, reputação e computação em nuvem.

No capítulo 3 os trabalhos relacionados a esta pesquisa são apresentados, verificando sistemas de reputação e modelos de confiança que são aplicados a OVs e em algumas áreas correlatas. Por fim, o capítulo 3 apresenta, ao final, um quadro comparativo dos trabalhos revisados.

O capítulo 4 apresenta a arquitetura de reputação proposta. A arquitetura de reputação proposta é implementada de forma centralizada e apresenta alguns módulos que são responsáveis por armazenar os dados referentes às transações, calcular a reputação dos provedores de nuvem, receber e enviar requisições e realizar ações de monitoramento.

No capítulo 5 é apresentado o ambiente de integração construído no simulador de redes P2P PeerFactSim.KOM (STINGL et al., 2011) para a avaliação da arquitetura. Esse ambiente simula a interação e troca de mensagens entre a OV, os provedores de nuvem e a arquitetura de reputação proposta. Além disso, os resultados provenientes da avaliação são apresentados neste capítulo. Por fim, o capítulo 6 apresenta as considerações finais e sugestões de possíveis trabalhos futuros.

Ainda, o apêndice A, subsidia a compreensão do trabalho apresentando a modelagem conceitual da arquitetura proposta, envolvendo os principais diagramas de caso de uso e diagramas de sequência de sua operação.

2 FUNDAMENTAÇÃO TEÓRICA

O objetivo deste capítulo é apresentar os conceitos necessários para o desenvolvimento e compreensão da arquitetura de reputação proposta. Nesse capítulo são apresentados os conceitos relacionados a organizações virtuais, bem como os conceitos de confiança, reputação e as características de uma arquitetura de reputação. Além disso, apresenta algumas questões relativas à computação em nuvem, como os indicadores de desempenho, que são utilizados na arquitetura de reputação proposta.

2.1 ORGANIZAÇÕES VIRTUAIS

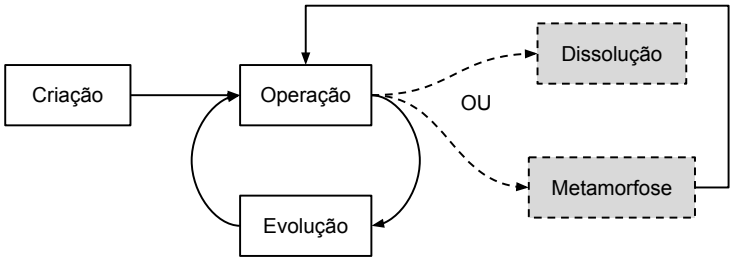
Devido à dinamicidade e competitividade do ambiente corporativo, as empresas têm percebido a necessidade de colaborarem umas com as outras e operarem com maior agilidade e flexibilidade (ESPOSITO; EVANGELISTA, 2014). Através disso, as empresas unem-se em redes colaborativas e compartilham competências distintas para alcançar metas comuns, por exemplo, um objetivo de negócio (ALAWAMLEH; POPPLEWELL, 2010).

As redes colaborativas são configuradas a partir de várias formas, como por exemplo: uma cadeia de suprimentos que é caracterizada pela estabilidade e excelente definição de papéis, em que proporciona o mínimo possível em coordenação e troca de informações; e uma organização virtual (OV), vista como uma rede dinâmica e orientada a objetivo, criada para atender um projeto específico ou oportunidade de colaboração (oportunidade de negócio) (CAMARINHA-MATOS et al., 2009).

Uma organização virtual, uma rede de colaboração, é definida como uma aliança temporária de um conjunto de entidades (geralmente empresas) legalmente independentes, heterogêneas e geograficamente dispersas que compartilham suas competências, habilidades, riscos e custos para alcançar determinados objetivos específicos de negócio, por exemplo, atender uma oportunidade de colaboração (CAMARINHA-MATOS et al., 2009).

Dada à dinamicidade do ambiente da OV é interessante compreender o seu ciclo de vida e as suas etapas. Inicialmente o ciclo de vida foi proposto por Camarinha-Matos e Afsarmanesh (1999), compreendo quatro fases ou estágios: criação, operação, evolução e dissolução. No entanto, em Camarinha-Matos et al. (2009) foi realizada uma adição ao ciclo de vida básico propondo a etapa de metamorfose. Desse modo, o ciclo de vida de uma OV é representado pela Figura 1.

Figura 1 – Ciclo de vida de uma organização virtual

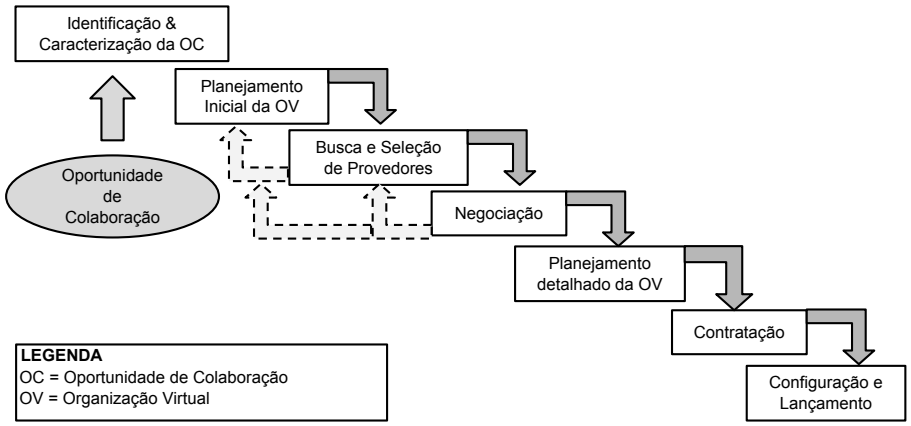


Fonte: Adaptado de Camarinha-Matos et al. (2009).

Assim, conforme apresentado em Camarinha-Matos et al. (2009), o ciclo de vida de uma OV é subdividido como se segue:

- **Criação**: Fase de início da OV em que ocorre as atividades de criação, definição de objetivos, seleção de entidades, entre outras subfases ilustradas na Figura 2;

Figura 2 – Etapas da fase de criação da OV



Fonte: Adaptado de Camarinha-Matos et al. (2009).

- **Operação**: Nesta fase ocorre o atendimento da oportunidade de colaboração, ou seja, os parceiros de negócio colaboram e trocam informações para atender o(s) objetivo(s) específico(s) de negócio;

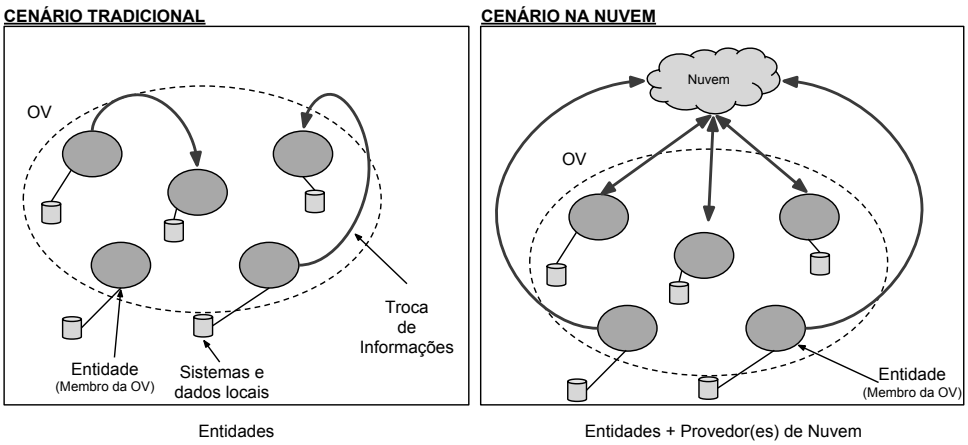
- **Evolução**: Essa fase é motivada por pequenas mudanças ocasionadas pelo aumento de tarefas ou incapacidade de algum membro em atender o objetivo de

negócio. Para isso, torna-se necessário reconfigurar a OV, efetuando a troca de membros da OV ou a adição de novos membros;

- **Dissolução:** Fase em que ocorre o término das atividades da OV. É motivada principalmente por duas situações: o atendimento bem-sucedido dos objetivos específicos de negócio ou pela decisão dos membros em interromper as atividades. Além disso, nessa fase ocorre a avaliação da colaboração dos parceiros e provedores de serviço, coleta de informações das avaliações, redefinição das responsabilidades e papéis de cada membro da OV, entre outras; e
- **Metamorfose:** Mudança ocasionada por alterações no mercado ou na demanda. A metamorfose afeta a rede de colaboração como um todo, criando uma nova forma de organização, quando inicialmente a rede de colaboração não atinge de forma apropriada os objetivos definidos inicialmente na fase de criação da OV.

No momento em que a OV está em operação dois cenários em termos de infraestrutura de comunicação entre os parceiros de negócio podem existir. Um cenário tradicional que utilize somente a Internet como meio de auxílio no atendimento da oportunidade de colaboração, e outro cenário na nuvem em que os recursos tecnológicos fornecidos pela computação em nuvem são utilizados (ZAMANIAN; MOHSENZADEH; NASSIRI, 2014; RUARO; RABELO, 2016a). Os cenários mencionados são apresentados pela Figura 3.

Figura 3 – Comparativo entre OVs nos cenários tradicional e em nuvem computacional



Fonte: Produção do próprio autor.

No cenário tradicional da OV, a troca de informações e compartilhamento de recursos é feita diretamente entre os parceiros de negócio (entidades), com o apoio

de uma infraestrutura de comunicação, por exemplo, a Internet. Nesse cenário, os parceiros de negócio com o apoio dos sistemas e dados armazenados localmente colaboram para atender uma oportunidade de colaboração e comunicam-se diretamente uns com os outros (RUARO; RABELO, 2016a).

Diferentemente do cenário tradicional, o cenário na nuvem utiliza os recursos fornecidos pelos provedores de nuvem externos (terceiros), como por exemplo, armazenamento, infraestrutura e *softwares*, disponíveis através dos modelos de serviço como: *Software as a Service* (SaaS), *Platform as a Service* (PaaS) e *Infrastructure as a Service* (IaaS) (MELL; GRANCE, 2011). Conforme Ruaro e Rabelo (2016b), nesse cenário, a troca de informações, hospedagem e execução de aplicações se realiza através da nuvem computacional.

Desse modo, em ambos os cenários, as entidades que formam uma OV desempenham diferentes papéis durante o seu ciclo de vida (CAMARINHA-MATOS; AFSARMANESH, 2001). Assim, cada entidade pode atuar como gestor/gerente da OV, parceiro de negócio da OV, *broker* da OV, entre outros. Conforme apresentado em Camarinha-Matos e Afsarmanesh (1999) estes papéis são definidos como:

- **Gestor/Gerente da OV**: é definido como o componente regulador das atividades relacionadas à OV. Este papel pode ser exercido por um nó especializado em atividades de gestão (nó externo à OV) ou pode ser desempenhado por um membro da OV. É responsável por manter informações sobre os parceiros de negócio da OV, reconfigurar a OV (caso necessário), supervisionar e gerenciar as atividades, entre outras responsabilidades;

- **Parceiro de Negócio da OV**: são as empresas que participam da OV no atendimento da oportunidade de colaboração. Suas principais atividades são definidas como compartilhamento e troca de informações e a colaboração com outras empresas;

- ***Broker* da OV**: tem como principal atividade criar ou iniciar uma OV. A partir da identificação e caracterização da oportunidade de colaboração OC, o *broker* reconhece as competências e habilidades necessárias para atender à OC e assim realiza a busca e seleção de parceiros de negócio para compor a OV. Na fase de operação da OV, ele atua como um moderador resolvendo conflitos entre os parceiros, quando houver; e

- **Outros papéis**: além dos papéis mencionados, pode-se considerar alguns outros, como por exemplo: gerente de projeto, auditor, técnico da rede, provedor de dados, provedores de nuvem, provedores de serviço, entre ou-

tros (CAMARINHA-MATOS; AFSARMANESH, 1999; CAMARINHA-MATOS; AFSARMANESH, 2001).

No decorrer do ciclo da OV as entidades (empresas, atores e diferentes sistemas computacionais) precisam desempenhar diversas funções, como compartilhamento e integração de informações, coordenação de atividades, planejamento, supervisão de execução de atividades, entre outras. Uma das dificuldades para a execução dessas funções e para a colaboração no ambiente das OVs é o estabelecimento e o gerenciamento da confiança das partes envolvidas (empresas ou parceiros de negócio) nos provedores de nuvem, representando um fator crítico para o sucesso no atendimento da oportunidade de colaboração e na execução das demais atividades (MSANJILA; AFSARMANESH, 2008; SQUICCIARINI; PACI; BERTINO, 2011).

Desta forma, o estabelecimento da confiança representa um importante papel para o ciclo de vida da OV, seja entre os parceiros de negócio ou dos parceiros de negócio aos provedores de nuvem.

2.2 CONFIANÇA

O avanço da tecnologia nas últimas décadas colaborou para o surgimento de um cenário em que vários usuários (pessoas, aplicações e empresas) interagem, compartilham e trocam informações nos mais variados tipos de serviço. Essa interação na maioria das vezes ocorre de forma anônima, na qual a outra parte assume o risco de interagir com uma entidade desconhecida. Dessa forma, para reduzir os riscos nesse ambiente, os conceitos de confiança e reputação podem ser empregados.

A confiança enquanto conceito é bastante estudada pelas ciências sociais em função do estudo do comportamento humano em sociedade. Entretanto, a confiança também é objeto de pesquisa em várias áreas, como por exemplo: psicologia, economia e computação (CHO; SWAMI; CHEN, 2011). Na área da computação está relacionada com questões relativas à segurança, privacidade dos dados e reputação (uma das formas de estabelecer um relacionamento de confiança) (MSANJILA; AFSARMANESH, 2008; RUAN; MARTIN, 2011).

Em Petri et al. (2012) é mencionado que a confiança é definida de acordo com a sua área de aplicação. No entanto, a literatura apresenta diversas definições de confiança de uma forma geral, sendo que algumas são dominantes e utilizadas para a construção de uma definição adequada ao contexto (MSANJILA; AFSARMANESH, 2008).

Conforme apresentado em Rousseau et al. (1998), a confiança é vista como um comportamento psicológico que está relacionado com a intenção de aceitar ou

não a vulnerabilidade durante a interação com alguém ou alguma coisa. Já, Gambetta et al. (2000) definem confiança como um nível particular da probabilidade em que um agente avalia outro agente ou um grupo de agentes em relação a sua capacidade de executar uma ação ou atividade em um determinado ambiente/contexto.

No ambiente das OVs, a confiança é vista como uma percepção que um parceiro de negócio tem em relação a outro, no sentido de realizar e completar as tarefas impostas, podendo tal percepção habilitar a colaboração (MSANJILA; AFSARMANESH, 2008). Mais especificamente, em um ambiente de integração entre OVs e computação em nuvem, a confiança é definida como a percepção de um parceiro de negócio em relação ao provedor de nuvem, o qual disponibiliza serviços e recursos ao ambiente da OV (KO et al., 2011).

Nesse trabalho, adota-se a definição de confiança em um ambiente computacional apresentada em Sabater e Sierra (2005). Nesse caso, a confiança é vista como um indicador caracterizado por um valor numérico (ex: de 0 até 1) que representa o quão confiável alguma entidade é, seja provedor de nuvem, serviço, usuário, entre outros (SABATER; SIERRA, 2005).

Não obstante as diferentes definições de confiança em vários contextos, Firdhous, Ghazali e Hassan (2012) identificaram alguns elementos comuns para qualquer definição de confiança, sendo: auxilia ambientes incertos e de alto risco; é usada como base na tomada de decisão; apresenta caráter subjetivo ou objetivo; sensível ao contexto e é dinâmica em relação ao tempo e novas observações. Além disso, outros requisitos específicos de confiança em OVs foram identificados em Winkler et al. (2007), sendo: a confiança é um relacionamento bidirecional e é comparável entre os diferentes participantes.

A confiança aparece como um fator de extrema importância ao atendimento da oportunidade de colaboração (ARENAS; AZIZ; SILAGHI, 2010; PAN; LI; YU, 2013), tanto no cenário tradicional quanto no cenário na nuvem. De forma específica, nas OVs baseadas na nuvem, os parceiros de negócio utilizam os recursos e serviços fornecidos pelos provedores de nuvem externos. Desse modo, torna-se necessário definir um meio para auxiliar o estabelecimento de uma relação de confiança nesse contexto.

Uma das formas de auxiliar no estabelecimento de uma relação de confiança é através da aplicação de uma arquitetura de reputação (VOSS; WIESEMANN, 2005; RUAN; MARTIN, 2011). A arquitetura de reputação tem como objetivo calcular, gerenciar, atualizar e disseminar a reputação de alguma entidade no ambiente das OVs, por exemplo. Além disso, tal arquitetura disponibiliza meios para auxiliar o processo de tomada de decisão na OV. Por fim, os conceitos de reputação de forma geral, mo-

delos de rede, bem como as características necessárias para a implementação são apresentadas na seção 2.3.

2.3 REPUTAÇÃO

A reputação, conceito conhecido e aplicado em diversas áreas, desempenha um importante papel auxiliando o estabelecimento e gerenciamento da confiança em vários ambientes (ANDRULIS et al., 2009). Além disso, fornece meios para auxiliar o processo de tomada de decisão quando é necessário compartilhar, integrar e combinar informações com entidades anônimas (VAVILIS; PETKOVIĆ; ZANNONE, 2014).

De forma geral, a reputação busca auxiliar as pessoas na escolha de parceiros confiáveis no mundo virtual (ex: *e-commerce*), que são honestos no mundo real (FOUSS; ACHBANY; SAERENS, 2010). Por exemplo, um gestor da OV que deseja interagir com um provedor de nuvem, leva em consideração a reputação do serviço disponibilizado pelo provedor para assim analisar se irá interagir com ele ou não. Desse modo, esse processo de tomada de decisão, sendo realizado através da reputação, visa reduzir os riscos durante o atendimento da oportunidade de colaboração, ou seja na operação da OV. Assim, a colaboração passa a ocorrer com entidades/provedores reconhecidos, devido ao seu comportamento anterior em outras OVs (reputação) (KERSCHBAUM et al., 2006; ANDRULIS et al., 2009).

De uma forma básica, segundo Resnick e Zeckhauser (2002), a reputação é vista como um valor gerado através de um processo de agregação de uma coleção de *feedbacks*/opiniões ou valores referentes ao comportamento passado dos participantes de uma comunidade. Conforme apresentado em Dharmaadi et al. (2014), a reputação pode ser entendida como a estimativa da qualidade de alguém mediante as avaliações daqueles que o conhecem ou com o qual interagiram. Por exemplo, a reputação no eBay®, é vista como um conjunto de avaliações e comentários que um vendedor recebeu mediante as transações realizadas com os consumidores.

Diferentemente, no ambiente das OVs, o conceito de reputação pode ser definido através de várias formas. Por exemplo, em Javaid, Majeed e Afzal (2013), a reputação dos parceiros de negócio é calculada por meio de um conjunto de indicadores de desempenho que representam questões financeiras, organizacionais, tecnológicas e operacionais. No STORE (ANDRULIS et al., 2009) a reputação das empresas/parceiros de negócio é composta pela agregação de vários indicadores de confiança baseados em aspectos financeiros, organizacionais, externos, entre outros e que estão relacionados ao desempenho dos parceiros. Por fim, no PathTrust (KERSCHBAUM et al., 2006) a reputação é composta através de um indicador de confiança subjetiva, ou seja, é calculada através das avaliações (ex: notas de 0 a 1) fornecidas pelos parceiros

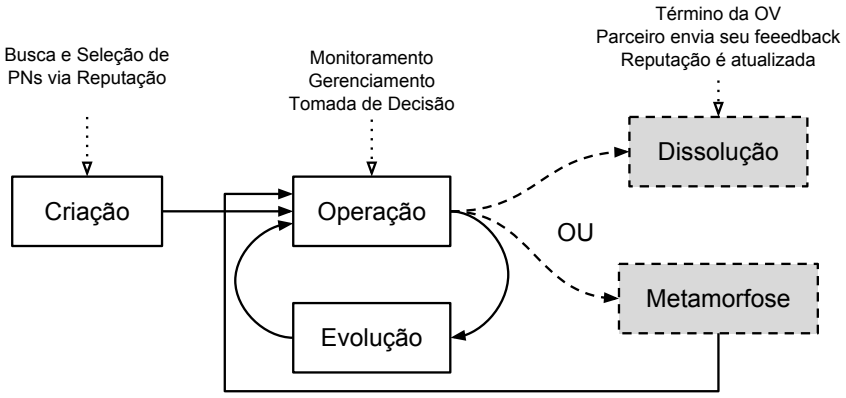
durante a colaboração nas OVs passadas.

No entanto em uma OV baseada na nuvem computacional, a reputação dos provedores de nuvem, por exemplo, deve considerar outros elementos e indicadores de confiança além dos *feedbacks* ou avaliações dos consumidores. Conforme apresentado em Habib, Ries e Muhlhauser (2011), pode-se considerar o SLA, indicadores de qualidade de serviço (QoS), certificados, auditorias, entre outros.

Assim, nesse trabalho, adota-se a definição de reputação aplicada às OVs, em que a reputação é definida como um processo de agregação de um ou mais indicadores de confiança relacionados com o comportamento passado e atual das entidades presentes nas OVs (KERSCHBAUM et al., 2006; ANDRULIS et al., 2009). Desse modo, o valor de reputação dos provedores de nuvem, nesse trabalho, é baseado em dois indicadores de confiança objetiva e subjetiva. O indicador de confiança objetiva está relacionado com o desempenho passado e atual de um provedor de nuvem qualquer em OVs, sendo calculado através de alguns indicadores de QoS. Enquanto o indicador de confiança subjetiva é obtido através das avaliações fornecidas pelos parceiros de negócio da OV em relação aos serviços prestados pelos provedores de nuvem.

Além das definições apresentados o conceito de reputação está ligado com o ciclo de vida da OV. Dessa forma, o relacionamento existente entre a reputação e a OV é ilustrado pela Figura 4.

Figura 4 – Relacionamento entre a reputação e o ciclo de vida da OV



Fonte: Adaptado de Voss e Wiesemann (2005).

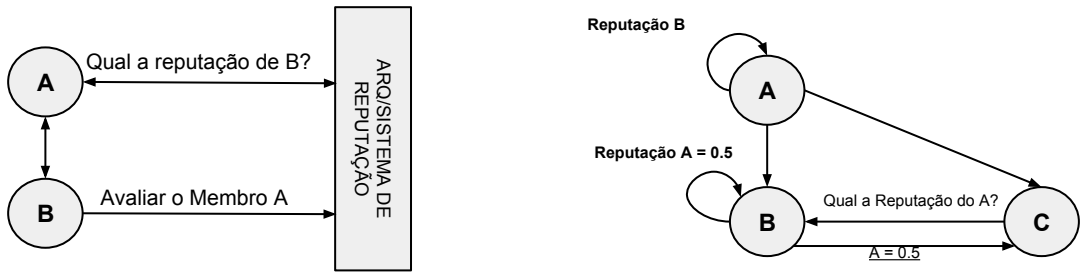
A reputação apresenta utilização mais relevante na fase de criação/formação da OV, pois é necessário buscar e selecionar provedores de nuvem, sendo que essa

etapa pode ser auxiliada através da reputação. Nas outras fases a reputação é gerenciada e atualizada, sendo que na etapa de operação, o desempenho objetivo é monitorado, enquanto na fase de dissolução, a arquitetura de reputação recebe novas avaliações subjetivas e o valor de reputação de um provedor qualquer é atualizado.

Conforme mencionado na seção 2.2, em um ambiente computacional, a reputação é gerenciada através da aplicação de uma arquitetura de reputação. Tal arquitetura é responsável por receber as avaliações subjetivas dos usuários, monitorar e processar outros indicadores de confiança (ex: objetivo - desempenho) para fornecer a reputação de uma determinada entidade a algo/alguém. Desse modo, as funcionalidades relativas à reputação, como cálculo, disseminação e coleta de informações, podem ser implementadas através de dois modelos de rede: centralizado e distribuído (MOUSA et al., 2015).

Os modelos de rede determinam a forma como a arquitetura de reputação é implementada, ou seja, de que modo atende as requisições solicitadas pelos usuários. Dessa forma, a Figura 5 apresenta os dois modelos de rede principais, sendo: centralizado e distribuído. O modelo centralizado é mais comum em cenários que exigem o papel de uma autoridade central, como ambientes de *e-commerce*. Por sua vez, o modelo distribuído é comumente aplicado em redes P2P.

Figura 5 – Modelos de rede para uma arquitetura de reputação



(a) Centralizado

(b) Distribuído

Fonte: Produção do próprio autor.

No modelo centralizado, apresentado na Figura 5 (a), existe um elemento central responsável pelo recebimento das avaliações dos membros que tiveram interações diretas com outros membros e de outros valores usados nos indicadores de confiança, como por exemplo, valores resultantes do monitoramento do QoS (ARENAS; AZIZ; SILAGHI, 2010). Esse modelo também disponibiliza a reputação ou informações de todos os membros para os solicitantes de forma pública e fornece maior segurança,

privacidade e um melhor desempenho (HABIB; RIES; MUHLHAUSER, 2010). Um dos exemplos de aplicação deste modelo de rede é o sistema utilizado no eBay®[1].

No modelo distribuído, apresentado na Figura 5 (b), cada membro armazena a opinião ou *feedback* referente a interação com outros membros da mesma rede e quando questionado sobre a reputação de algum membro, pode fornecê-la (VAVILIS; PETKOVIĆ; ZANNONE, 2014). Esse modelo de rede utiliza outros tipos de informação além dos *feedbacks* fornecidos pelos membros, considerando também a comunidade, rede ou contexto em que o membro está inserido.

As interações no modelo de rede distribuído são descritas como se segue. Um membro `C` deseja interagir com `A`, porém ainda não se relacionaram diretamente. O membro `C` questiona a comunidade sobre a reputação de `A`. Então, o membro `B` responde a reputação de `A` ao membro `C`.

O modelo de rede distribuído é amplamente aplicado a sistemas multi-agentes, rede *ad-hoc* móvel, redes *Peer-to-Peer* (P2P) (CHO; SWAMI; CHEN, 2011). Nas redes P2P, um dos exemplos é o PeerTrust (XIONG; LIU, 2004), que utiliza cinco parâmetros para o desenvolvimento de uma métrica geral de reputação: (1) *feedback* obtido através de outros membros, (2) total de transações que um membro teve com outro membro, (3) credibilidade da fonte do *feedback*, (4) fator de contexto da transação e (5) fator de contexto da comunidade.

Os modelos de rede apresentados estão relacionados à forma como a arquitetura de reputação disponibiliza as informações e atende as requisições. Além disso, tal arquitetura deve apresentar outros elementos referentes às informações usadas na reputação, por exemplo, como o cálculo da reputação é feito, como o valor de reputação é informado ao usuário, entre outros. Por fim, esses elementos são apresentados pela seção 2.3.1.

2.3.1 Elementos Comuns em uma Arquitetura de Reputação

A implementação de uma arquitetura de reputação deve apresentar alguns elementos comuns identificados em alguns trabalhos de revisão definidos na literatura, como por exemplo, Hoffman, Zage e Nita-Rotaru (2009) e Mousa et al. (2015). De acordo com Mousa et al. (2015), esses elementos são definidos como: coleta de informações, agregação, disseminação e a tomada de decisão.

A coleta de informações refere-se ao procedimento de coleta das informações dos participantes de um determinado ambiente, sendo esta informação utilizada na etapa de agregação para o cálculo da reputação de um participante. Essas informações incluem os valores usados para calcular alguns indicadores de confiança, como,

[1] http://www.ebay.com/

os *feedbacks* do parceiro de negócio da OV. Por exemplo, um parceiro de negócio disponibiliza seu *feedback* em relação ao serviço prestado pelo provedor de nuvem. Além disso, o conjunto de informações também pode contemplar o histórico de valores referente ao indicador de confiança objetiva (desempenho) desses provedores, armazenado no repositório de dados (WINKLER et al., 2007).

A agregação é o elemento que realiza o cálculo da reputação baseado nos valores obtidos através da coleta de informações (HOFFMAN; ZAGE; NITA-ROTARU, 2009; TAVAKOLIFARD; ALMEROTH, 2012). Alguns métodos podem ser utilizados nesta etapa e são definidos como:

- **Soma ou média**: comumente encontrado em ambientes de comércio eletrônico, este método soma o número de transações positivas e negativas, para calcular a reputação de um vendedor ou comprador;
- **Modelos *Fuzzy***: os valores de reputação podem ser representados através de variáveis *fuzzy*, as quais a partir das funções de pertinência (*membership functions*) descrevem o nível de reputação de um participante. Através da aplicação de regras *fuzzy*, inferência e defuzzificação, o valor é calculado (LIN; LI; HUANG, 2011);
- **Modelos probabilísticos**: o valor da reputação é calculado através de funções de densidade de probabilidade, na qual o escore atualizado é calculado por meio da combinação dos valores históricos e a nova avaliação (HALLER, 2008a);
- **Modelos estocásticos**: Os eventos são modelados usando a cadeia de Markov (TAVAKOLIFARD; ALMEROTH, 2012) e a reputação pode ser calculada, por exemplo, através do teorema de bayes (HALLER, 2008b); e
- **Customizado**: modelos personalizados desenvolvidos para um contexto e que podem ser adaptados a outros cenários;

A disseminação é referente ao envio da reputação para os solicitantes, por exemplo, um parceiro de negócio. É relacionada com os modelos de rede apresentados na seção 2.3, podendo ser feita de forma centralizada ou distribuída. Além desses modelos, a disseminação pode ocorrer periodicamente através de intervalos fixos de tempo ou de acordo com funções, eventos ou uma mensagem de requisição e resposta (KALIDINDI et al., 2011).

A tomada de decisão refere-se a forma como o valor de reputação é informado pela arquitetura de reputação, podendo estar presente na forma de valores quantitativos e qualitativos (TAVAKOLIFARD; ALMEROTH, 2012). Os valores quantitativos

são entendidos como números inteiros ou frações presentes em um determinado intervalo. Os valores qualitativos referem-se a uma grandeza categórica que expressa a reputação, por exemplo, baixa, moderada, alta, muito alta, entre outras formas.

Por fim, nota-se que esses elementos devem ser adotados na implementação de uma arquitetura de reputação. Pois, tal arquitetura deve apresentar uma forma de informar, calcular e atualizar a reputação das entidades atendidas para fornecer suporte aos processos de tomada de decisão existentes.

2.4 COMPUTAÇÃO EM NUVEM

A computação em nuvem é definida como um conjunto de recursos computacionais (processamento, armazenamento, conectividade, plataformas, aplicações ou serviços) que são disponibilizados via rede (Internet) e que podem ser rapidamente liberados e fornecidos sem qualquer intervenção humana, ou seja, com o mínimo de interações com o provedor de serviço, considerando que os recursos são provisionados de acordo com a necessidade do usuário (MELL; GRANCE, 2011).

Conforme apresentado em Noor et al. (2013), os recursos disponibilizados através da nuvem computacional apresentam cinco características essenciais, como: autoatendimento sob demanda, amplo acesso à rede, agrupamento de recursos, elasticidade rápida e serviço mensurável.

No ambiente de computação em nuvem, diferentes membros participam de diferentes processos. O National Institute of Standards and Technology (NIST) (MELL; GRANCE, 2011) define a arquitetura de referência de alto nível para computação em nuvem que contempla atores, entendidos como uma pessoa ou organização, que desempenham papéis nas transações, processos ou tarefas. Segundo o NIST (2014) estes papéis são definidos como:

- **Consumidor**: mantém uma relação de negócios com o provedor de nuvem e usa os serviços fornecidos através dos modelos de negócio (SaaS, PaaS e IaaS). Neste trabalho, o consumidor é entendido como o parceiro de negócio da OV;

- **Fornecedor**: entidade responsável por disponibilizar um ou mais serviços para as partes interessadas (consumidores). Nesse trabalho, o fornecedor é visto como o provedor de nuvem, o qual disponibiliza os seus serviços para os parceiros de negócio da OV;

- **Portador**: atua como um intermediário, fornecendo conectividade e transporte de serviços de nuvem entre os consumidores e os fornecedores;

- **Auditor**: um auditor avalia os serviços disponibilizados pelos provedores de nuvem nos requisitos de controle de segurança, privacidade e desempenho; e

- **Corretor (*Broker*)**: segundo Grivas, Kumar e Wache (2010), o corretor ou *broker* é responsável por intermediar o relacionamento entre o consumidor e o provedor de nuvem, fornecendo recomendações de uso e entrega de serviços. Neste trabalho esse papel pode ser auxiliado pela arquitetura de reputação, na qual o *broker* forneceria, além dos dados básicos e informações do serviço a ser contratado, a reputação para que o consumidor escolhesse o serviço de acordo com as suas necessidades.

A nuvem computacional, segundo o modelo de referência do NIST, pode apresentar quatro modelos de implantação que apresentam vantagens e desvantagens de aplicação para os usuários (ZHANG; CHENG; BOUTABA, 2010). Conforme Mell e Grance (2011) e Arockiam, Monikandan e Parthasarathy (2011), os modelos de implantação são definidos brevemente como: (i) **nuvem pública**: infraestrutura computacional é mantida e adquirida pelo próprio provedor de nuvem (ii) **nuvem privada**: a infraestrutura computacional é adquirida e mantida pela organização que implementa e mantém a nuvem, por exemplo, empresas; (iii) **nuvem híbrida**: combinação de dois ou mais modelos de nuvem (pública, privada ou comunitária) e (iv) **nuvem comunitária**: compartilhamento da infraestrutura computacional entre as organizações de uma comunidade.

O ambiente de computação em nuvem fornece os serviços por meio de três modelos de negócios diferentes, entendidos como modelo SPI (**S***oftware*, **P***latform* e **I***nfrastructure*). Conforme apresentado em Noor et al. (2013), os modelos definem-se como: (i) ***Software as a Service* (SaaS)**: permite aos clientes executar *softwares* na nuvem através da Internet; (ii) ***Platform as a Service* (PaaS)**: uma camada de *software* programável para o desenvolvimento e instalação de serviços dos consumidores ou adquiridos por terceiros, utilizando linguagens de programação e ferramentas suportadas pela nuvem computacional; e (iii) ***Infrastructure as a Service* (IaaS)**: disponibiliza recursos de *hardware* (processamento, armazenamento, rede, entre outros) sob demanda para que os usuários possam hospedar seus próprios serviços.

Com o propósito de avaliar os diferentes serviços disponibilizados pela computação em nuvem, o *Cloud Services Measurement Initiative Consortium* (CSMIC) foi desenvolvido, o qual fornece um conjunto de métricas universalmente aceitas que podem ser utilizadas para realizar tal avaliação e também para monitorar o desempenho dos serviços disponibilizados pelos provedores de nuvem. Dessa forma, a seção 2.4.1 apresenta o CSMIC e o conjunto de indicadores de desempenho usado para avaliar serviços de nuvem e também os indicadores que podem ser usados para compor a

reputação dos provedores de nuvem.

2.4.1 Indicadores de Desempenho

Com o intuito de padronizar a medição e especificação de indicadores de desempenho para a avaliação e comparação de provedores de nuvem computacional, foi desenvolvido o *Cloud Services Measurement Initiative Consortium* (CSMIC). O CSMIC fornece métricas universalmente aceitas para atender uma necessidade dos clientes ou consumidores, para realizar a avaliação de benefícios e cálculo de risco dos serviços fornecidos pelos provedores de nuvem computacional (SIEGEL; PERDUE, 2012).

O *Service Measurement Index* (SMI), proposto pelo CSMIC, é entendido como um conjunto de indicadores de desempenho chave (do inglês *Key Performance Indicators* (KPIs)) que mensuram o desempenho do serviço fornecido pelo provedor e são utilizados para comparar diferentes serviços (GARG; VERSTEEG; BUYYA, 2011). Hierarquicamente, o SMI divide-se em sete categorias: Responsabilidade (*Accountability*), Agilidade (*Agility*), Garantia de Serviço (*Assurance*), Financeiro (*Financial*), Desempenho (*Performance*), Segurança (*Security*), Privacidade (*Privacy*) e Usabilidade (*Usability*). Cada categoria contém um conjunto de atributos, em que cada atributo tem sua definição e forma de coleta (obtenção do valor) (SIEGEL; PERDUE, 2012). Por exemplo, a categoria agilidade, é composta dos atributos de capacidade (memória, processamento e disco) e elasticidade dos serviços/recursos.

Os indicadores de desempenho podem ser divididos em duas categorias: qualitativos e quantitativos. Os qualitativos estão diretamente relacionados com a experiência do usuário em relação ao serviço prestado (BARANWAL; VIDYARTHI, 2014). Por sua vez, os quantitativos, por exemplo tempo de resposta e disponibilidade, podem ser mensurados através de ferramentas de *hardware* e *software* que realizam o monitoramento (GARG; VERSTEEG; BUYYA, 2013).

Desse modo, considerando o objetivo desse trabalho, a reputação dos provedores de nuvem adota em sua composição um indicador de confiança objetiva. O indicador de confiança objetiva é baseado no desempenho do provedor de nuvem e é calculado através de alguns indicadores que representam o QoS, e que estão presentes nas categorias disponíveis do SMI. Desse modo, nesse trabalho adotou-se alguns indicadores de QoS e que de acordo com Garg, Versteeg e Buyya (2013) são definidos como:

- **Tempo de Resposta**: Representa a diferença de tempo existente entre a requisição de um serviço e o tempo em que ele está disponível. O principal objetivo dos provedores de nuvem é fornecer um serviço/recurso minimizando o tempo de

resposta. Por fim, esse indicador tem o tempo representado através da unidade de medida de milissegundo (ms);

- **Disponibilidade**: Representa a fração do tempo total avaliado em um intervalo de tempo padronizado que o serviço está disponível para atender as requisições. É representado através de porcentagem, por exemplo, 99.9999% (0.999999) de disponibilidade;

- **Estabilidade**: É definido como a variação no desempenho do serviço. Em serviços de armazenamento de dados é a variação no tempo médio das operações de leitura e escrita nos dispositivos de armazenamento. Nos serviços de disponibilização de recursos computacionais, é o desvio do nível de desempenho especificado no SLA, sendo representado pela Equação 2.1.

$$E = \sum \frac{\frac{\alpha_{avg.i} - \alpha_{sla.i}}{T}}{n} \tag{2.1}$$

  Em que α refere-se a um recurso computacional (processamento, rede, entre outros), $avg.i$ é o desempenho médio observado pelo usuário que requisitou o serviço, $sla.i$ são os valores de desempenho acordados no SLA, T é o tempo de serviço e n é o total de usuários (GARG; VERSTEEG; BUYYA, 2011). Nesse sentido, o indicador de estabilidade é representado através de um valor numérico. Para isso, nesse trabalho, adota-se o intervalo de valores apresentado em Garg, Versteeg e Buyya (2013) em que a estabilidade é dada em um nível de 0 até 100.

- **Segurança**: O estabelecimento da segurança é uma das maiores preocupações para a proteção de dados, garantia de privacidade e também para assegurar a confiança. Os provedores de nuvem podem utilizar diferentes formas de segurança, como por exemplo, algoritmos de criptografia, gerenciamento de identidade e suporte de segurança física, rede e dos dados (HABIB; RIES; MUHLHAUSER, 2010). De uma forma geral, este indicador representa as medidas de segurança que um provedor de nuvem oferece em seus serviços. Entretanto, para a composição da reputação (especificamente o indicador de confiança objetiva) de um provedor de nuvem, considerou-se que o indicador de segurança representa um valor quantitativo em um dado intervalo de valores. O intervalo é de 0 até 10 e foi definido de acordo com Garg, Versteeg e Buyya (2013). Dessa forma, esse intervalo indica que um serviço de um provedor de nuvem pode apresentar até dez níveis de segurança, sendo que 0 significa que não é adotada nenhuma medida de segurança, enquanto 10 seria o maior valor, ou seja, todas as medidas de segurança são adotadas nos serviços disponibilizados; e

- **Preço**: Em serviços IaaS, este indicador é definido como o valor cobrado por uso de um recurso. Por exemplo, valor cobrado por hora de uso de uma máquina virtual ou valor cobrado pelo armazenamento em Gigabytes (GB) por mês (KHURANA; BAWA, 2016). Em outros modelos de serviço, por exemplo SaaS, o preço pode ser o valor cobrado pelo uso da aplicação, podendo ser mensal, semanal, entre outras formas de precificação.

Desse modo, esses indicadores de QoS apresentados são utilizados pela arquitetura proposta porque não são exclusivos de nenhum modelo de serviço (SaaS, PaaS, IaaS) e são quantitativos e mensuráveis, diferentemente de outros indicadores de QoS, como por exemplo, técnicas de virtualização, sistemas operacionais suportados, plataformas suportadas, tipos de suporte aos usuários, entre outros (GARG; VERSTEEG; BUYYA, 2013). Por fim, na seção 2.4.2 é apresentado o relacionamento existente entre os conceitos relativos a computação em nuvem e organizações virtuais.

2.4.2 Organizações Virtuais e Computação em Nuvem

A operação de uma OV está integrada às tecnologias de informação e comunicação para facilitar a cooperação entre os parceiros de negócio e responder de forma eficiente à OC. O surgimento de novas tecnologias, como por exemplo, a computação em nuvem e computação em grade, favoreceram a OV para o aumento da eficiência e flexibilidade no processo de colaboração, possibilitando uma rápida resposta no atendimento da OC, reduzindo custos com infraestrutura computacional, entre outros fatores (ZAMANIAN; MOHSENZADEH; NASSIRI, 2014).

Um *framework* para a criação de OVs utilizando a nuvem computacional como infraestrutura de comunicação é apresentado em Zamanian, Mohsenzadeh e Nassiri (2014). Este *framework* é dividido em três camadas: a camada de negócios responsável pelos processos de colaboração, regras e comunicações entre as organizações; a camada de serviços que é responsável pelo gerenciamento e contratação dos serviços dos provedores de nuvem e a camada de componentes que gerencia os serviços de nuvem para os parceiros de negócio da OV (ZAMANIAN; MOHSENZADEH; NASSIRI, 2014).

No *framework* proposto, os parceiros de negócio através das atividades da camada de serviço utilizam os recursos fornecidos pelos provedores de nuvem através dos seus modelos de serviço (PaaS, SaaS, IaaS) para desenvolver seus aplicativos ou fornecer seus serviços no ambiente da OV. Conforme Zamanian, Mohsenzadeh e Nassiri (2014) a OV pode usar alguns recursos computacionais fornecidos pelo modelo IaaS (armazenamento, processamento e rede) e também os parceiros de negó-

cio podem utilizar *softwares* de gestão de negócio e de projetos que estão disponíveis através do modelo SaaS.

Outros autores como Ruaro e Rabelo (2016a) apresentam uma avaliação de requisitos e ferramentas de computação em nuvem para a aplicação nas redes de colaboração, como por exemplo, uma OV. Dessa forma, a OV pode utilizar os serviços provenientes do modelo SaaS para criação e compartilhamento de documentos em diferentes formatos, como contratos, planilhas e projetos. As ferramentas PaaS também são utilizadas para hospedagem de aplicações web desenvolvidas nas linguagens de programação suportadas pelo provedor, alguns exemplos de uso do PaaS inclui a criação e execução de pequenos aplicativos para gerenciamento de projetos (RUARO; RABELO, 2016a). Por fim, o modelo IaaS pode disponibilizar máquinas virtuais para instanciar servidores web (hospedagem de aplicações) e outros tipos de serviços (RUARO; RABELO, 2016b).

Algumas características e requisitos foram apresentados na taxonomia de integração entre OV e Computação em Nuvem por Moraes et al. (2015). Nessa taxonomia evidenciaram-se características comuns entre os dois paradigmas, como: independência geográfica, flexibilidade, adaptabilidade, disponibilidade, entre outras, e também foi verificada a aplicabilidade dessa forma de integração, caracterizada por finalidade e necessidade.

Outras formas de integração entre OV e computação em nuvem, são discutidas nos trabalhos presentes em Li et al. (2010), Lee e Desai (2014), Lee (2014) e Garcia, Castillo e Puel (2013). Em Li et al. (2010), a integração é discutida no aspecto de construção de políticas de segurança e gerenciamento de confiança para uma OV baseada na nuvem. Em Lee e Desai (2014) e Lee (2014) são discutidos modelos para a implementação de OVs na plataforma OpenStack e alguns problemas que decorrem desta aplicação, como por exemplo, autenticação e segurança em ambientes dinâmicos. Por fim, em Garcia, Castillo e Puel (2013) é apresentado um serviço de filiação de membros da OV para prover federação de identidades em ambientes compostos por múltiplos provedores de nuvem.

Assim, a computação em nuvem na integração com a OV apresenta-se como uma eficiente ferramenta para auxiliar o processo de colaboração através do fornecimento de recursos de forma distribuída. No entanto, nessa integração alguns problemas podem surgir, como, privacidade, segurança e confiança. Um dos principais problemas observados é falta de um sistema que realize o gerenciamento de confiança neste ambiente e suporte os processos de tomada de decisão. Uma das formas de auxiliar na solução do problema de confiança em OVs é através da aplicação de uma arquitetura de reputação de confiança que é responsável principalmente por apoiar os processos de tomada de decisão, fornecendo a reputação dos provedores de nuvem.

Nesse sentido, a arquitetura de reputação presente nesse trabalho pode ser aplicada a qualquer OV que utilize algum recurso disponibilizado sob a forma de SaaS, PaaS e IaaS por meio dos provedores de nuvem que implementam o modelo de nuvem pública.

2.5 CONSIDERAÇÕES PARCIAIS

O capítulo apresentou os principais aspectos referentes à OV e a utilização de nuvem computacional para sua implementação, bem como os conceitos referentes à confiança e reputação associados aos parceiros de negócio da OV e provedores de nuvem.

Uma OV é uma rede de colaboração na qual um conjunto de entidades se une para compartilhar competências, recursos, riscos e habilidades a fim de alcançar objetivos específicos de negócio. Sendo que tal interação é suportada por uma infraestrutura de comunicação baseada na Internet. Assim, a utilização de uma nuvem computacional por parte dos parceiros de negócio componentes da OV faz todo o sentido.

Uma das principais preocupações para a execução de funções e colaboração nas OVs é o estabelecimento e gerenciamento da confiança entre os elementos envolvidos, sendo, neste caso, os parceiros de negócio e provedores de nuvem. Dessa forma, a confiança configura-se como um elemento crítico para o sucesso no atendimento da oportunidade de colaboração por parte da OV. Nesse sentido esse capítulo também abordou os conceitos de confiança e sua relação com OV bem como a reputação e seus principais elementos.

Por fim, o capítulo abordou os conceitos relacionados a computação em nuvem. A computação em nuvem é basicamente definida como um conjunto de recursos computacionais disponibilizados via rede (Internet) e que podem ser rapidamente provisionados e disponibilizados aos parceiros de negócio de acordo com as suas necessidades. Nesse sentido, a OV faz uso desses recursos disponibilizados pelos provedores de nuvem para realizar a troca de informações, aplicações e hospedagem de serviços.

3 TRABALHOS RELACIONADOS

Os temas de confiança e reputação são objetos de estudo em diversas áreas e tópicos da computação. A utilização/aplicação de reputação é vista, por exemplo, nas redes *Peer-to-Peer* (P2P), ambientes de *e-commerce*, redes colaborativas, computação em nuvem, entre outras.

Nas redes P2P, a dinamicidade e o comportamento anônimo dos pares da rede motivam a necessidade da construção de um ambiente confiável, para o qual, os sistemas de reputação são empregados de forma a distinguir pares honestos, maliciosos e desonestos (KURDI, 2015). Alguns exemplos em redes P2P incluem o PeerTrust (XIONG; LIU, 2004), um modelo de confiança composto por cinco fatores usado para avaliar a reputação de um par da rede e o EigenTrust (KAMVAR; SCHLOSSER; GARCIA-MOLINA, 2003), um algoritmo de reputação utilizado em uma rede P2P para reduzir a possibilidade de arquivos corrompidos.

Em ambientes de *e-commerce*, a aplicação da reputação auxilia no estabelecimento de um relacionamento de confiança entre entidades desconhecidas (XIE; ZHONG; DENG, 2014). Nesse caso, os sistemas de reputação, por exemplo, Beta (JØSANG; ISMAIL, 2002) e ReGreT (SABATER; SIERRA, 2001), são utilizados para auxiliar os processos de tomada de decisão existentes entre as transações realizadas pelo consumidor.

Nas redes colaborativas, um dos obstáculos para o processo de colaboração é o estabelecimento e o gerenciamento da confiança. Uma das questões que emergem é como realizar a gestão de provedores de nuvem confiáveis ou parceiros de negócio confiáveis no ambiente das OVs. Nesse sentido, alguns trabalhos estão sendo desenvolvidos para fornecer suporte aos processos de tomada de decisão existentes na OV e auxiliar no estabelecimento de uma relação de confiança, por exemplo, em Kerschbaum et al. (2006), Haller (2008b), Arenas, Aziz e Silaghi (2010) e Mashayekhy e Grosu (2012).

Na computação em nuvem, os problemas relativos à privacidade, segurança e confiança nos serviços fornecidos dificultam a adoção desses serviços por parte dos usuários. Devido à dinamicidade do ambiente de computação em nuvem, o estabelecimento da confiança é uma tarefa inevitável (MUCHAHARI; SINHA, 2012; MACHHI; JETHAVA, 2016; NOOR et al., 2016a). Para isso, alguns trabalhos relacionados à arquiteturas de reputação e modelos de confiança são desenvolvidos para, por exemplo, fornecer suporte à tomada de decisão por parte do usuário dos serviços da nuvem.

Dessa forma, o restante desse capítulo é dividido como se segue. Na seção 3.1

os trabalhos relacionadas à confiança e reputação aplicadas em OVs são apresentadas. As abordagens envolvendo confiança e reputação somente na computação em nuvem são apresentadas pela seção 3.2. Por fim, na seção 3.3 é apresentado um quadro comparativo dos trabalhos relacionados.

3.1 ABORDAGENS APLICADAS A OVs

O PathTrust (KERSCHBAUM et al., 2006) é um sistema de reputação aplicado à etapa de seleção de membros (nesse caso, empresas) durante a formação de uma OV. Para participar do processo de formação da OV, um membro deve se registrar em uma *Enterprise Network* (EN), que fornece um sistema de reputação centralizado. Ao final, na fase de Dissolução da OV, cada membro fornece seu *feedback* (positivo ou negativo) ao sistema em relação a transação efetuada com outros. Na EN, a reputação de um membro é medida de acordo com as avaliações realizadas por outros membros da OV. Por fim, Kerschbaum et al. (2006), relatam que a aplicação de um sistema de reputação em OVs traz benefícios que não podem ser quantificados monetariamente. No entanto, tal aplicação garante um aumento no número de transações positivas, menor risco quando se utiliza um provedor com reputação alta e fornece meios para que a OV forneça um serviço melhor, utilizando a reputação no processo de busca e seleção de membros.

Arenas, Aziz e Silaghi (2010) apresentam um sistema de reputação aplicado a uma organização virtual criada utilizando computação em grade. Nesse sistema é avaliada a reputação do usuários e também dos provedores de grade computacional. A reputação dos usuários é calculada de acordo com a utilização dos recursos e serviços, por exemplo, se o usuário tenta executar uma ação não permitida, o seu nível de reputação sofre alterações, ou seja, recebe uma qualificação baixa proveniente do serviço. Ainda, a reputação dos provedores de serviço é calculada através dos indicadores de QoS. Por fim, além das questões relacionadas com reputação, através desse sistema é possível que o gestor da OV crie e finalize uma OV e o monitoramento e controle dos recursos computacionais seja realizado.

Pan, Li e Yu (2013) apresentam um algoritmo de reputação que fornece suporte para a criação da OV utilizando recursos de nuvem e que considera a reputação de cada provedor, minimizando assim os problemas ao lidar com entidades desconhecidas. Neste trabalho relacionado, a reputação é baseada no histórico de colaboração (participações passadas em OVs) de cada provedor de serviço, ou seja, avaliações fornecidos pelos parceiros de negócio aos provedores. O algoritmo funciona da seguinte forma: ao iniciar uma OV, é estabelecido que dois serviços são necessários, o serviço A e B. O provedor X é selecionado pois é o único fornecedor de A. A partir disto, um serviço B deve ser escolhido, sendo que para isso existem dois candidatos, os pro-

vedores Y e Z. Dessa forma, o provedor a ser escolhido será o que apresentar maior confiança, ou seja, se X confia mais na colaboração com Y, esse será selecionado.

O *Stocasthic Reputation Service for Virtual Organizations* (STORE) (HALLER, 2008b) é um sistema de reputação que auxilia a tomada de decisão na seleção de parceiros de negócio, que é desempenhada pelo gestor da OV, ou através de outra organização. Para a reputação no STORE, um indicador de confiança proposto em Winkler et al. (2007) foi utilizado. Este indicador de confiança representa uma agregação de vários indicadores baseados em aspectos financeiros, operacionais, organizacionais, externos e terceiros (certificados, auditorias, informações de empresas externas, etc) que refletem o desempenho da organização.

Em Javaid, Majeed e Afzal (2013) é apresentado um sistema de reputação aplicado no processo de seleção eficiente de parceiros para a composição de OVs em ambientes de recuperação de desastres e emergências. Nesse cenário, em virtude da sua dinamicidade, os métodos comuns de busca e seleção (por exemplo, métodos de tomada de decisão multicritério) não são aplicáveis. O sistema de reputação é apresentado como Arquitetura Orientada a Serviço (SOA), composta pelos componentes responsáveis pela coleta, compilação e agregação dos fatores e critérios e outro elemento responsável pelo cálculo da reputação em situações de emergência.

Mashayekhy e Grosu (2012) apresentam um *framework* para a formação de OVs utilizando recursos da computação em grade, considerando a reputação de cada provedor de serviços de *Grid*. A reputação é formada com base nas interações passadas, para avaliar como é o fornecimento dos recursos requisitados. Na integração entre computação em grade e OV, um elemento-chave na formação da OV é a confiança existente nos provedores de serviços de *Grid* na entrega dos recursos prometidos. Em alguns casos, o provedor participa de uma OV, contudo falha na entrega dos recursos, afetando o atendimento da oportunidade de colaboração. Por fim, os resultados da análise do *framework* mostram que uma OV estável não só garante uma alta reputação entre os participantes, mas maximiza o retorno individual de cada participante.

Arasteh, Amini e Jalili (2012) apresentam um modelo de controle de acesso de recursos aplicado à organizações virtuais. O modelo desenvolvido pelos autores engloba três fatores: uso dos *feedbacks* para calcular a confiança e reputação; política única de controle de acesso para recursos compartilhados em OVs e é utilizada uma ontologia para fornecer uma percepção comum acerca das organizações. Além disso, os autores apresentaram uma comparação do trabalho desenvolvido em relação aos modelos tradicionais de controle de acesso, como *Role-based Access Control* (RBAC) e *Dynamic Access Control* (DAC).

Kerschbaum (2009) apresenta um sistema de reputação centralizado utilizado

na fase de formação da OV. O sistema de reputação desenvolvido contempla algumas funcionalidades relativas à segurança das avaliações fornecidas pelos provedores de serviço, por exemplo, toda a comunicação entre o sistema e o avaliador, ocorre em canais seguros e autenticados, utilizando protocolos de criptografia, entre outros.

Em Papaioannou e Stamoulis (2010) um sistema de reputação para uma OV baseada em computação em grade é apresentado. Este sistema utiliza a reputação para apoiar o processo de atribuição de tarefas, via *grid service broker*, sendo que a reputação é baseada no desempenho individual de cada agente presente na OV.

Em outros trabalhos, são apresentados modelos de confiança aplicados a OVs, como por exemplo em Neata, Urzica e Florea (2011) e Mun, Shin e Jung (2011). Em Neata, Urzica e Florea (2011) um modelo de confiança para uma OV baseada em agentes é definido. A confiança, nesse contexto, é vista como um valor gerado através da agregação dos valores passados de desempenho de cada agente e suas características. Além disso, esse modelo de confiança é utilizado para suportar a tomada de decisão, ou seja, auxilia na decisão de quando ou não interagir com certo agente.

Mun, Shin e Jung (2011) apresentam um modelo de confiança orientado a objetivos aplicado ao processo de criação da OV, contemplando a teoria da lógica difusa nessa fase, especificamente na seleção de parceiros de negócio em uma OV baseada em projetos/objetivos. Nesse modelo, a confiança configura-se como a probabilidade de que um elemento confiável (membro participante do projeto) satisfaça os objetivos (metas) enquanto completa as tarefas que lhe foram atribuídas.

3.2 ABORDAGENS APLICADAS A COMPUTAÇÃO EM NUVEM

Conforme mencionado em Pearson e Benameur (2010), a confiança nos provedores de nuvem é vista como um problema na adoção de recursos ou serviços da nuvem. Desse modo, alguns trabalhos na literatura abordam modelos de confiança, arquiteturas de reputação e confiança e métodos de seleção de serviços, a fim de apresentar soluções ao problema da confiança bem como auxiliar na tomada de decisão por parte do usuário durante a seleção de serviços de nuvem.

Alguns autores apresentam modelos de confiança para a computação em nuvem de forma a estabelecer um meio para sua mensuração. Em Chakraborty e Roy (2012) e Tan et al. (2016) são apresentados modelos de confiança quantitativos baseados no *Service Level Agreement* (SLA). Nesses modelos, as métricas obtidas através do SLA são usadas para estimar a confiança do serviço disponibilizado pelo provedor de nuvem. Muchahari e Sinha (2012) apresentam como contribuição principal uma arquitetura de gerenciamento da confiança em ambientes de nuvem, sendo composta por um modelo de confiança baseado nos *feedbacks* dos usuários da nuvem.

Outros trabalhos apresentam arquiteturas e sistemas que são destinadas ao gerenciamento da confiança no ambiente da computação em nuvem. Habib, Ries e Muhlhauser (2011) apresentam uma arquitetura de gerenciamento de confiança para o ambiente de computação em nuvem, com o propósito de identificar serviços confiáveis através de diferentes atributos, como: *feedbacks*, SLA, certificados, auditorias, entre outros. Em Noor et al. (2016b) uma plataforma de recomendação de serviços de nuvem através da reputação é apresentada. A reputação é baseada nos *feedbacks* recebidos a cada interação dos usuários com os provedores de nuvem. Ainda, Tang et al. (2017) apresentam um sistema para auxiliar a seleção de serviços de nuvem com base na confiança, considerando o monitoramento do QoS e das avaliações dos usuários.

Sharma e Banati (2016) apresentam um *framework* para a implementação de confiança em nuvens IaaS. A confiança é calculada através da lógica *fuzzy* usando os fatores de desempenho e agilidade que são avaliados pelos usuários. Além disso, os autores comentam que outros fatores podem ser adicionados a métrica de confiança. Em Machhi e Jethava (2016) é apresentado um *framework* de gerenciamento da confiança para o ambiente de nuvem. Nesse *framework*, a confiança é calculada com base nos *feedbacks* fornecidos pelos usuários. Ainda, através de alguns parâmetros relacionados com o comportamento dos usuários, o *framework* realiza o filtro dos *feedbacks* duvidosos, ou seja, aqueles *feedbacks* que tem como objetivo promover ou prejudicar o valor de confiança de um provedor qualquer.

Outros trabalhos relacionam a questão do gerenciamento de confiança com a análise de risco, por exemplo Theoharidou, Tsalis e Gritzalis (2013) e Xie et al. (2012). Theoharidou, Tsalis e Gritzalis (2013) apresentam um estudo de revisão relacionado a análise de risco em ambientes de nuvem computacional e apresentam os requerimentos para a disponibilização da análise de risco como serviço (*Risk-as-a-Service*). Além disso, mencionam que o nível de confiança observado em um serviço ou provedor de nuvem está relacionado com o risco associado em futuras interações. Em Xie et al. (2012) é apresentado um *framework* para gerenciamento de risco em ambientes de computação em nuvem. Esse *framework* tem como objetivo auxiliar no estabelecimento de um relacionamento de confiança entre os usuários e os provedores de nuvem.

Por fim, alguns trabalhos apresentam métodos para facilitar a seleção de serviços de nuvem computacional, por exemplo Garg, Versteeg e Buyya (2013) e Baranwal e Vidyarthi (2014). Garg, Versteeg e Buyya (2013) utilizam os indicadores de desempenho e as necessidades do usuário em um *framework* para realizar o ranqueamento e classificação dos provedores de nuvem. O *framework* é baseado no método multicritério *Analytic Hierarchy Process* (AHP). Baranwal e Vidyarthi (2014) apresentam

métricas de avaliação dos provedores de nuvem e disponibilizam um *framework*, baseado no método de votação por ranqueamento, usado para a busca e seleção de serviços de nuvem.

3.3 QUADRO COMPARATIVO

Os trabalhos relacionados com reputação e confiança no ambiente das OVs e de forma geral na computação em nuvem são sumarizados e classificados de acordo com algumas características no Quadro 1, sendo elas:

- **Usado em**: a contribuição do trabalho relacionado pode ser aplicada somente na computação em nuvem (CN) ou na organização virtual (OV);
- **Tipo**: classifica-se como sistema de reputação (SR), algoritmo de reputação (AR), modelo de confiança (MC), *framework* de confiança (FC), seleção de serviços de nuvem (SS), análise de risco (R) e controle de acesso (CA);
- **Objetivo (Obj.)**: utilização de indicadores objetivos que podem estar relacionados com o QoS, desempenho, entre outros para o cálculo da confiança, reputação ou seleção de serviços;
- **Subjetivo (Subj.)**: utiliza as avaliações dos usuários no método de cálculo;
- **CN e OV**: integra computação em nuvem com OV;
- **BP e OV**: aplica o trabalho relacionado ao nível dos parceiros de negócio (BP) da OV; e
- **Ciclo da OV**: indica se o trabalho relacionado atende a todas as fases do ciclo de vida da OV, desde sua criação até a dissolução.

Quadro 1 – Comparação entre os trabalhos relacionados

(continua)

Trabalho	Usado em	Tipo	Obj.	Subj.	CN e OV	BP e OV	Ciclo da OV
Habib, Ries e Muhlhauser (2011)	CN	SR	X	X			
Chakraborty e Roy (2012)	CN	MC	X				
Muchahari e Sinha (2012)	CN	MC		X			
Xie et al. (2012)	CN	R	X	X			

Fonte: Produção do próprio autor.

Quadro 1– Comparação entre os trabalhos relacionados

(conclusão)

Trabalho	Usado em	Tipo	Obj.	Subj.	CN e OV	BP e OV	Ciclo da OV
Theoharidou, Tsalis e Gritzalis (2013)	CN	R					
Garg, Versteeg e Buyya (2013)	CN	SS	X				
Baranwal e Vidyarthi (2014)	CN	SS	X				
Tan et al. (2016)	CN	MC	X				
Noor et al. (2016b)	CN	SR		X			
Sharma e Banati (2016)	CN	FC		X			
Machhi e Jethava (2016)	CN	FC		X			
Tang et al. (2017)	CN	SS	X	X			
Kerschbaum et al. (2006)	OV	SR		X		X	
Haller (2008b)	OV	SR	X			X	
Kerschbaum (2009)	OV	SR		X		X	
Papaioannou e Stamoulis (2010)	OV	SR	X			X	
Arenas, Aziz e Silaghi (2010)	OV	SR	X	X		X	
Neata, Urzica e Florea (2011)	OV	MC	X			X	
Mun, Shin e Jung (2011)	OV	MC		X		X	
Mashayekhy e Grosu (2012)	OV	SR		X			
Arasteh, Amini e Jalili (2012)	OV	CA		X		X	
Pan, Li e Yu (2013)	OV	AR		X	X		
Javaid, Majeed e Afzal (2013)	OV	SR	X	X		X	
Arquitetura Proposta	OV	SR	X	X	X		X

Fonte: Produção do próprio autor.

Nos trabalhos relacionados aplicados somente na computação em nuvem, nota-se que poucos trabalham com a combinação de dois indicadores de confiança, ou seja, indicador objetivo (QoS e SLA) e subjetivo (*feedbacks*) (HABIB; RIES; MUHLHAUSER, 2011; XIE et al., 2012; TAN et al., 2016). No entanto, a maioria dos que utilizam avaliações dos usuários em suas contribuições, não consideram técnicas para

o tratamento de ataques ao valor dessas avaliações, com exceção do trabalho apresentado em Machhi e Jethava (2016), o qual considera um filtro para a identificação de *feedbacks* duvidosos provenientes de ataques. Ainda em relação aos trabalhos aplicados na computação em nuvem, nota-se que alguns utilizam o risco para auxiliar no estabelecimento de uma relação de confiança, por exemplo em Xie et al. (2012), o risco é mensurado através de diversas características objetivas (medidas de segurança e outros requisitos) e subjetivas (avaliações).

Nas abordagens aplicadas em OVs, percebe-se que poucos trabalhos abordam a questão da integração de organizações virtuais e computação em nuvem. Essa lacuna indica que a adoção dos recursos de nuvem nas OVs é uma tendência crescente e uma nova área de aplicação, pois a primeira contribuição envolvendo a integração é de 2013 (PAN; LI; YU, 2013). Além disso, nota-se que estudos futuros são necessários em OVs baseadas na nuvem endereçando tópicos como confiança, reputação e a sua aplicação.

Conforme a comparação apresentada, não foi possível identificar dentre os trabalhos revisados, algum que atenda a todas as etapas do ciclo de vida da OV, desde a fase de criação da OV até a fase de dissolução da OV. Alguns trabalhos aplicados nas OV são utilizados somente na etapa de busca e seleção de parceiros de negócio, por exemplo Kerschbaum et al. (2006), Haller (2008b), Kerschbaum (2009).

Outros trabalhos em OVs consideram a interação com os provedores de *grid* computacional, como Arenas, Aziz e Silaghi (2010), Papaioannou e Stamoulis (2010) e Mashayekhy e Grosu (2012). Dessa forma, a reputação é utilizada para apoiar o processo de formação de uma OV que utiliza os recursos da computação em grade, bem como auxiliar na alocação e distribuição de tarefas e recursos.

O restante dos trabalhos apresentados auxiliam na solução do problema da confiança existente entre os parceiros de negócio da OV através da reputação. Porém, não consideram a utilização de recursos provenientes da computação em nuvem. Nesse contexto, a reputação dos parceiros de negócio é calculada por meio das avaliações recebidas durante as participações em OVs passadas. Diferentemente dos trabalhos apresentados, a aplicação de uma arquitetura de reputação no ambiente da nuvem exige que o valor de reputação seja calculado com outros indicadores de confiança, além dos *feedbacks* (avaliações dos usuários) (HABIB; RIES; MUHLHAUSER, 2011). Dessa forma, em uma OV baseada na nuvem, a reputação de cada provedor de nuvem deve considerar mais de um indicador de confiança. Assim, a reputação de um provedor é baseada nos *feedbacks* fornecidos pelos parceiros de negócio, bem como pelo seu desempenho em relação à alguns dos indicadores de QoS mencionados anteriormente na seção 2.4.1.

Desse modo, tendo realizada a comparação entre os trabalhos relacionados, este trabalho propõe uma arquitetura de reputação de confiança, que calcula, coleta, gerencia e dissemina a reputação dos provedores de nuvem através de uma abordagem centralizada. Conforme mencionado em Habib, Ries e Muhlhauser (2011), o uso de uma abordagem centralizada visa desempenho e menor consumo de largura de banda com trocas de informações entre os membros. Além disso, tal abordagem fornece um nível maior de privacidade e segurança das informações gerenciadas pela arquitetura.

Assim, o valor de reputação de cada provedor de nuvem é calculado através da agregação de dois indicadores de confiança objetiva e subjetiva. O indicador de confiança objetiva está relacionado ao desempenho histórico e atual do provedor de nuvem, o qual é construído através de alguns indicadores de QoS. E o indicador de confiança subjetiva refere-se aos *feedbacks*, ou seja avaliações (notas), que são fornecidos pelos parceiros de negócio da OV em relação aos provedores de nuvem. Além disso, através da arquitetura proposta, a reputação dos provedores de nuvem é atualizada e gerenciada durante a fase de operação da OV, por meio do módulo de monitoramento, a ser especificado na seção 4.2.

Em relação às abordagens aplicadas na computação em nuvem, a arquitetura proposta compartilha algumas características, como a reputação ser baseada em dois indicadores de confiança: objetiva e subjetiva, pois Habib, Ries e Muhlhauser (2011) identificaram que a reputação em um contexto que utiliza os recursos da nuvem, deve ser composta por outros indicadores de confiança além dos *feedbacks* de seus usuários.

Diferentemente das abordagens relacionadas as OVs, usadas para tomada de decisão em relação aos parceiros de negócio e também em OVs que usam recursos de computação em grade, a arquitetura de reputação proposta neste trabalho é aplicável a uma OV baseada na nuvem e auxilia os processos de tomada de decisão desempenhados pelo gestor da OV e o parceiro de negócio da OV, como por exemplo, busca e seleção de provedores de nuvem apoiada pela reputação, substituição de um provedor de nuvem em função de sua reputação atual durante a fase de operação da OV, entre outros.

3.4 CONSIDERAÇÕES PARCIAIS

O capítulo apresentou os principais trabalhos relacionados ao objetivo deste trabalho. Inicialmente foram apresentados os trabalhos relacionados à aplicação do conceito de confiança e reputação em OV, através de modelos de confiança e sistemas de reputação.

Nas abordagens aplicadas em OVs notou-se que a maioria concentra-se em auxiliar a tomada de decisão no nível dos parceiros de negócio, ou seja, através da reputação fornece meios para auxiliar o processo de busca e seleção de parceiros de negócio. Outras abordagens consideram a interação entre os provedores de computação em grade, porém, não foi identificada nenhuma arquitetura de reputação que auxiliasse uma OV baseada na nuvem computacional.

Em relação às abordagens especificamente aplicadas em computação em nuvem, percebeu-se que são apresentados principalmente *frameworks*, modelos de confiança e sistemas que auxiliam a tomada de decisão nesse ambiente. Dessa forma, a arquitetura proposta compartilha algumas características desses trabalhos, como indicador de confiança objetiva, subjetiva e o uso da reputação como apoio ao processo de tomada de decisão.

Por fim, um quadro comparativo resumo das contribuições, bem como das características dos trabalhos relacionados foi apresentado, auxiliando na identificação da lacuna existente relativa à aplicação de uma arquitetura de reputação para OV baseada na nuvem computacional.

4 ARQUITETURA DE REPUTAÇÃO

A OV representa um conjunto de entidades (empresas) que colaboram entre si para atender um objetivo específico de negócio (CAMARINHA-MATOS et al., 2009). Desse modo, durante os processos de colaboração, um dos problemas observados é o estabelecimento e o gerenciamento da confiança entre as partes envolvidas, ou seja, entre os parceiros de negócio ou dos parceiros de negócio aos provedores de nuvem (SQUICCIARINI; PACI; BERTINO, 2011).

Uma das formas de suportar o estabelecimento da confiança entre as partes envolvidas na OV é através da aplicação de arquiteturas de reputação (VOSS; WIESEMANN, 2005; HALLER, 2008b). Nesse sentido, esse capítulo apresenta a arquitetura de reputação de confiança proposta, a qual busca auxiliar os processos de tomada de decisão existentes no ciclo de vida da OV. Esses processos incluem, por exemplo, a busca e seleção de provedores de nuvem guiada pela reputação.

A arquitetura de reputação é responsável por coletar, calcular, gerenciar e disseminar as informações pertinentes à reputação dos provedores de nuvem no ambiente das OVs baseadas na nuvem, ou seja, OVs que utilizam os recursos dos provedores de nuvem. Nesse sentido, para a adequada implementação e implantação da arquitetura proposta, torna-se necessária a análise de seus requisitos fundamentais.

Sendo assim, os requisitos funcionais da arquitetura proposta são definidos como:

1. Gerar um indicador de confiança objetiva referente ao desempenho histórico relacionado a qualidade de serviço do provedor de nuvem;

2. Gerar um indicador de confiança subjetiva referente ao histórico de *feedbacks* fornecidos ao provedor de nuvem pelos membros da OV, na ocasião da dissolução da OV;

3. Utilizar dois indicadores de confiança (objetiva e subjetiva) para calcular a reputação dos provedores de nuvem, através do módulo de agregação;

4. Disponibilizar através de um modelo de rede uma forma de atender requisições e fornecer retorno referente às operações disponibilizadas pela arquitetura;

5. Prover um módulo para o monitoramento dos indicadores de QoS durante a fase da operação da OV;

6. Receber os *feedbacks* fornecidos pelos parceiros de negócio da OV aos provedores de nuvem, com a finalidade de atualizar o histórico de participações em uma OV e consequentemente a reputação;

7. Fornecer apoio à tomada de decisão por parte do gestor da OV durante o ciclo de vida da OV. Por exemplo, fornecer a reputação dos provedores de nuvem para auxiliar o processo de busca e seleção na fase de criação/formação.

Esses requisitos funcionais estão relacionados com algumas decisões de implementação motivadas pela literatura, como por exemplo, o cálculo da reputação, modelos de rede, e os outros elementos que são mencionados na seção 2.3.1. No ambiente de OV na nuvem, deve-se definir que informações são usadas no cálculo da reputação. Nesse caso, conforme Habib, Ries e Muhlhauser (2011), a reputação dos provedores de nuvem é calculada através de dois indicadores de confiança objetiva e subjetiva.

Além disso, o modelo de rede de reputação deve ser definido, de forma a especificar um meio de atender e disseminar informações relacionadas a reputação. Nesse trabalho é adotado o modelo de rede centralizado. Conforme apresentado em Habib, Ries e Muhlhauser (2010), esse modelo garante um melhor desempenho e um menor consumo de largura de banda com troca de informações. Também fornece um nível maior de privacidade e segurança das informações relacionadas à reputação, que são gerenciadas pela arquitetura. No entanto, o modelo de rede centralizado representa um ponto único de falha (*Single Point of Failure (SPOF)*), o que exige replicação e redundância como atenuantes.

Assim, tendo em vista as demais características necessárias para a correta implantação e utilização, os requisitos não funcionais da arquitetura são definidos como:

1. Utilizar um banco de dados para armazenar os valores que compõem os indicadores de confiança objetiva e subjetiva referentes aos provedores de nuvem e outras informações;

2. Disponibilização das informações de QoS dos serviços fornecidos pelos provedores de nuvem à arquitetura de reputação;

3. Disposição dos parceiros de negócio em avaliar os provedores de nuvem quando da dissolução da OV.

Nota-se que tais requisitos não funcionais estão ligados a restrições da arquitetura de reputação, ou seja, para fornecer a reputação dos provedores de nuvem é necessário que os provedores de nuvem disponibilizem as informações referentes aos

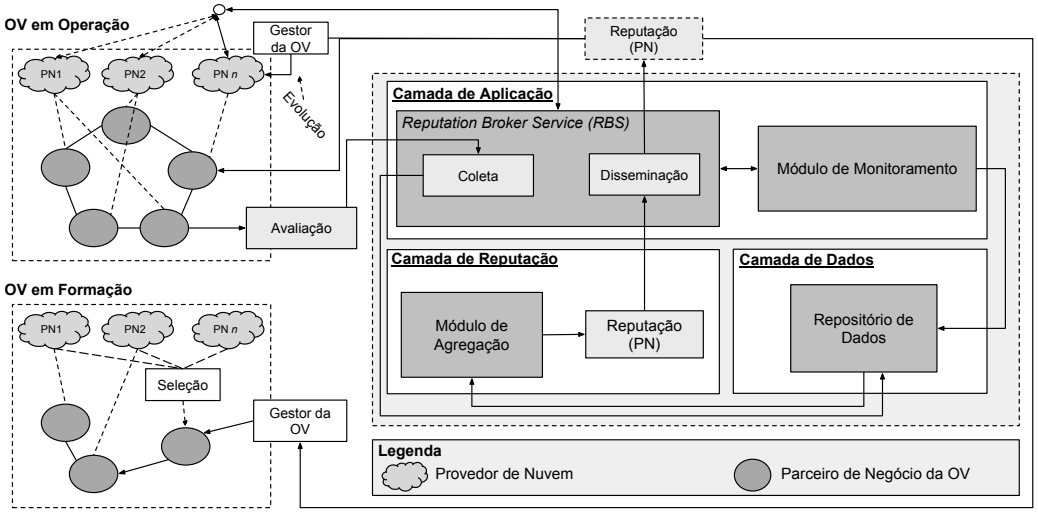
seus serviços bem como o QoS e que os parceiros de negócio avaliem os provedores na dissolução da OV.

Por fim, tendo levantado os requisitos, a arquitetura proposta e seus módulos são especificados e apresentados nas próximas seções.

4.1 PROPOSTA DA ARQUITETURA

A arquitetura proposta é representada pela Figura 6 e é composta por várias camadas e módulos que realizam as funcionalidades relacionadas com a reputação. Na implementação utilizou-se o modelo de rede centralizado, na qual as requisições e informações são recebidas e atendidas por uma entidade centralizada, nesse caso, o *Reputation Broker Service* (RBS).

Figura 6 – Arquitetura de reputação de confiança



Fonte: Produção do próprio autor.

A arquitetura de reputação apresenta três camadas: aplicação, reputação e dados. A camada de aplicação contém o módulo RBS e o módulo de monitoramento. A camada de reputação é composta pelo módulo de agregação que realiza o cálculo do valor da reputação. Por fim, a camada de dados apresenta o repositório de dados que armazena os valores usados para calcular os indicadores de confiança objetiva e subjetiva, provedores entre outros.

Cada camada da arquitetura proposta apresenta alguns módulos e esses módulos são entendidos como:

- **Módulo de Monitoramento**: realiza o monitoramento e atualização de alguns indicadores de QoS (ex: tempo de resposta, estabilidade e disponibilidade) de

cada provedor de nuvem durante a fase de operação em alguma participação em OVs;

- **Módulo de Agregação**: realiza o cálculo do valor da reputação do provedor de nuvem baseado nos indicadores de confiança objetiva e subjetiva. O indicador de confiança objetiva é proveniente do desempenho do provedor de nuvem através de alguns indicadores de QoS mencionados na seção 2.4.1, sendo, disponibilidade, tempo de resposta, estabilidade, segurança e preço. O indicador de confiança subjetiva é proveniente dos valores dos *feedbacks* pelos parceiros de negócio em relação aos provedores de nuvem;
- **Repositório de Dados**: é responsável por armazenar os valores provenientes do módulo de monitoramento e também os valores usados nos indicadores de confiança objetiva (indicadores de QoS mencionados do provedor de nuvem) e subjetiva (*feedbacks* (avaliações - notas) fornecidos pelos parceiros de negócio da OV para os provedores de nuvem); e
- **Reputation Broker Service (RBS)**: É o responsável pela interação com o parceiro de negócio da OV e/ou gestor da OV, ou seja, disponibiliza acesso às operações da arquitetura para esses elementos. Por exemplo, um parceiro de negócio da OV pode fornecer seu *feedback* referente a um provedor de nuvem ao RBS, o qual coleta esse *feedback* e armazena-o no repositório de dados para atualizar o histórico de participações desse provedor em OVs. Ainda, o gestor da OV pode solicitar a reputação de um provedor de nuvem em um dado momento, comunicando-se com o RBS.

A arquitetura proposta está relacionada com o ciclo de vida da OV, sendo particularmente útil durante a fase de criação/formação. Contudo, desempenha outros papéis de gerenciamento e manutenção no restante do ciclo de vida da OV. Desse modo, pode-se definir as interações entre as entidades, fases da OV e a arquitetura, como se segue:

- **Criação/Formação da OV**: o gestor da OV comunica-se com a arquitetura via RBS para obter o valor de reputação de um determinado provedor de nuvem (PN) e assim utilizar essa informação para a tomada de decisão no processo de busca e seleção de PNs, associar tal PN ao parceiro de negócio e continuar a formação da OV ou configurar a OV para a fase de operação;
- **Operação da OV**: um parceiro de negócio da OV pode solicitar a reputação de um determinado provedor de nuvem e também requisitar operações de monitoramento, para que seja possível verificar a reputação do provedor de nuvem em um determinado momento (durante a participação na OV);

- **Evolução da OV**: caso venha a ocorrer uma queda no valor de reputação do provedor de nuvem, motivada por um desvio nos valores de QoS prometido, o gestor da OV deve analisar se efetua a troca deste recurso do provedor de nuvem. Para tanto, o gestor da OV solicita o valor de reputação de outros provedores de nuvem, disponíveis no repositório de dados, à arquitetura de reputação (RBS) para efetuar o processo de tomada de decisão; e

- **Dissolução da OV**: cada parceiro de negócio da OV envia para a arquitetura um ou mais *feedbacks* referentes ao PN que forneceu os serviços ou recursos. Deste modo, a participação histórica dos provedores de nuvem em OVs é atualizada e consequentemente, também, sua reputação.

Além dos requisitos e modelo da arquitetura apresentados, no apêndice A é apresentada a modelagem conceitual da arquitetura, através de alguns dos diagramas da *Unified Modeling Language* (UML), como o diagrama de casos de uso e sequência. Por fim, as próximas seções apresentam cada módulo disponibilizado pela arquitetura de reputação.

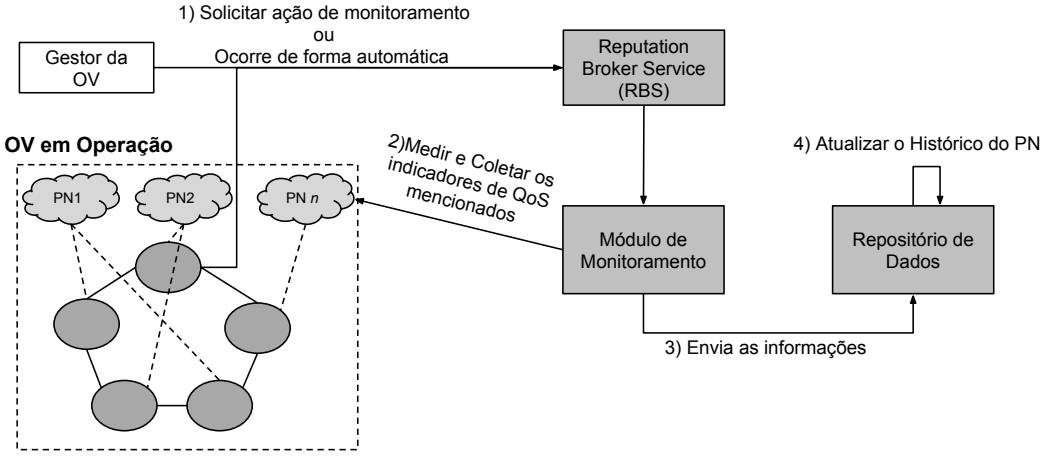
4.2 MÓDULO DE MONITORAMENTO

O Módulo de Monitoramento tem como objetivo monitorar o desempenho do provedor de nuvem. Assim, realiza-se o monitoramento de alguns indicadores de QoS, como disponibilidade, tempo de resposta e estabilidade, mencionados na seção 2.4.1. O monitoramento é realizado durante a fase de operação da OV e é uma tarefa de suma importância tanto para o parceiro de negócio quanto para o provedor de nuvem. No lado do parceiro de negócio em relação ao provedores de nuvem, o monitoramento desempenha a função de verificação dos valores de QoS atuais. O funcionamento desse módulo é apresentado na Figura 7.

A operação de monitoramento é projetada para ocorrer através de duas formas: requisições automáticas ou manuais. As requisições automáticas são disparadas durante a fase de operação da OV em um intervalo de tempo definido pelo gestor da OV. Em contrapartida, a requisição manual de monitoramento é solicitada pelo parceiro de negócio e/ou gestor da OV ao RBS.

Após uma requisição de monitoramento, o módulo de monitoramento, através de ferramentas de *hardware* e *software* (GARG; VERSTEEG; BUYYA, 2013), como, por exemplo, *CloudWatch*, *Nimsoft*, *Monitis*, *Nagios*, entre outras (ACETO et al., 2013), realiza a medição e coleta dos indicadores de QoS mencionados (ex: disponibilidade, tempo de resposta, estabilidade) dos provedores de nuvem. Após isso, as informa-

Figura 7 – Modelo do módulo de monitoramento



Fonte: Produção do próprio autor.

ções, ou seja os valores, são enviadas ao repositório de dados para atualizar o histórico objetivo (desempenho) do provedor de nuvem.

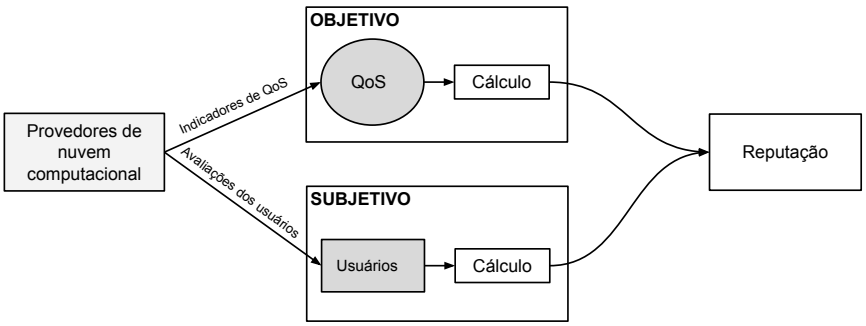
Dessa forma, através das informações monitoradas (QoS) obtidas pelo módulo de monitoramento, pode-se calcular a reputação atual dos provedores de nuvem. Para isso, a reputação de um provedor de nuvem, quando solicitada na fase de operação da OV, é calculada utilizando as informações monitoradas e históricas de QoS disponíveis no repositório de dados.

4.3 MÓDULO DE AGREGAÇÃO

O Módulo de Agregação é utilizado para efetuar o cálculo da reputação dos provedores de nuvem. A reputação dos provedores de nuvem é calculada através da agregação de dois indicadores de confiança: objetivo e subjetivo (HABIB; RIES; MUHLHAUSER, 2011). Este módulo tem seu funcionamento ilustrado na Figura 8.

O indicador de confiança objetiva é proveniente do desempenho do provedor de nuvem, que deriva do conjunto de alguns indicadores de QoS mencionados e especificados na seção 2.4.1, ou seja, disponibilidade, tempo de resposta, segurança, estabilidade e preço (BARANWAL; VIDYARTHI, 2014). Esses indicadores selecionados para representar o desempenho do provedor de nuvem podem ser aplicados a qualquer modelo de serviço de nuvem (SaaS, PaaS e IaaS). Além disso, são quantitativos e mensuráveis, diferentemente de outros indicadores que também representam o QoS, como técnicas de virtualização, sistemas operacionais suportados, plataformas suportadas, tipos de suporte ao usuário, entre outros (GARG; VERSTEEG; BUYYA, 2013).

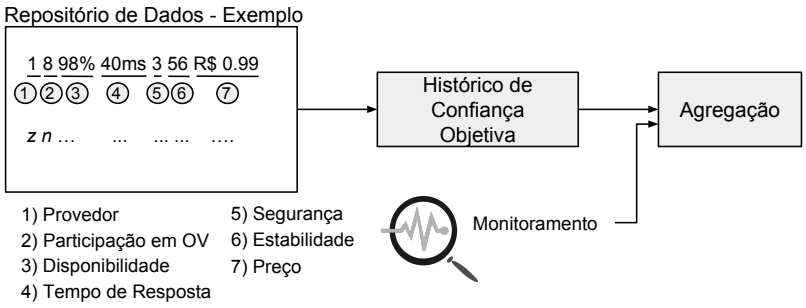
Figura 8 – Modelo do módulo de agregação



Fonte: Produção do próprio autor.

Um exemplo das informações usadas no cálculo de indicador de confiança objetiva é apresentado na Figura 9. Além disso, é apresentado a forma como o histórico referente aos indicadores de QoS é armazenado no repositório de dados da arquitetura. Os números de 1 até 7, presentes na Figura, representam os atributos que são armazenados no repositório de dados, desde o identificador do provedor (1), número de sua participação em OVs (2), e os valores dos indicadores de QoS mencionados (3 até 7).

Figura 9 – Exemplo de informações referentes ao indicador de confiança objetiva



Fonte: Produção do próprio autor.

Conforme o exemplo exposto na Figura 9, percebe-se que o repositório de dados permite armazenar informações de QoS de z provedores com n participações passadas em OVs. Além disso, o repositório de dados também é responsável por armazenar as informações referentes aos *feedbacks* (indicador de confiança subjetiva) fornecidos pelos parceiros de negócio.

A partir da busca no repositório de dados, o indicador de confiança objetiva

de um provedor de nuvem qualquer pode ser calculado. Esse indicador é baseado nas informações históricas dos valores de QoS mencionados e tem seu valor obtido através de um método de cálculo a ser especificado na seção 4.3.1. Após o cálculo do indicador, o valor é enviado ao módulo de agregação o qual calcula o valor de reputação de um provedor de nuvem. Por fim, durante a fase de operação da OV, os valores monitorados são utilizados em conjunto com os valores históricos, para calcular o valor de reputação dos provedores de nuvem, naquele instante de tempo.

O indicador de confiança subjetiva, utilizado para a agregação/geração do valor de reputação, é composto pelos *feedbacks* fornecidos pelos parceiros de negócio em relação aos provedores de nuvem. O provedor de nuvem é avaliado subjetivamente pelo parceiro de negócio da OV durante a fase de dissolução da OV. Deste modo, o parceiro de negócio da OV fornece seu *feedback* em relação a qualidade do serviço prestado pelo provedor de nuvem durante a participação em uma OV.

Dessa forma, a reputação (R) dos provedores de nuvem é dada pela combinação de dois indicadores históricos de confiança: objetivo (histórico de qualidade de serviço e monitoramento atual de QoS - quando solicitado) e subjetivo (*feedback* dos parceiros), conforme apresentado na Equação 4.1.

$$R_s = \omega_{obj} * T_{obj}(s) + \omega_{sub} * T_{sub}(s) \tag{4.1}$$

De acordo com a definição adotada para a reputação, T_{obj} é o indicador de confiança objetiva histórica e atual (quando houver) para o provedor de nuvem s, T_{sub} é o indicador de confiança subjetiva histórica e ω_{obj} e ω_{sub} são os pesos definidos para os respectivos indicadores de acordo com a preferência do gestor da OV. Os pesos definem qual indicador de confiança tem mais importância durante o cálculo. Por fim, as subseções 4.3.1 e 4.3.2, detalham a forma de cálculo para cada indicador de confiança, respectivamente, objetivo e subjetivo.

4.3.1 Indicador de Confiança Objetiva (T_{obj})

O indicador de confiança objetiva tem como meta avaliar os provedores de nuvem com base no seu desempenho expresso pelos indicadores que representam a qualidade de serviço (QoS) especificados na seção 2.4.1. Esse indicador é objetivo, pois utiliza valores históricos de QoS que por sua natureza são valores discretizáveis e monitoráveis, e que não são dependentes de uma interpretação subjetiva (TANG et al., 2017).

O método usado para calcular este indicador objetivo, no contexto da integração entre OV e computação em nuvem, é composto por dois elementos: a eficiência relativa e a importância relativa. A eficiência relativa refere-se a eficiência de um provedor

de nuvem em relação ao seu desempenho em participações passadas nas OVs, ou seja, com base na análise histórica do QoS (ALVES JUNIOR, 2011) é verificada a eficiência considerando que um histórico com mais variabilidade ocasiona um valor menor de eficiência. Assim, entende-se que menos confiável será o provedor de nuvem durante o fornecimento dos recursos/serviços durante o atendimento da oportunidade de colaboração da OV.

A importância relativa é calculada como um escore de ponderação (nesse trabalho, chamado de confiança multicritério) para a eficiência relativa. Esse escore é um valor associado com a importância atribuída pelo gestor da OV a cada indicador de QoS. Para a geração desse escore, uma técnica de avaliação pareada de dados pode ser utilizada com grande proveito. Tal técnica, nesse caso, é extraída do método de avaliação de dados multicritério, *Analytic Hierarchy Process* (AHP), e refere-se a matriz de julgamento.

A Equação 4.2 representa o indicador de confiança objetiva T_{obj} do provedor de nuvem s. Assim, o indicador é composto pela eficiência relativa $Eff\,(s)$ e pelo escore de ponderação $Esc\,(s)$ (confiança multicritério).

$$T_{obj}\,(s) \;=\; Eff\,(s) * Esc\,(s) \tag{4.2}$$

O cálculo da eficiência relativa $Eff\,(s)$ é apresentado em detalhes na seção 4.3.1.1 enquanto o cálculo da confiança multicritério $Esc\,(s)$ pode ser visto na seção 4.3.1.2.

4.3.1.1 Eficiência Relativa ($Eff\,(s)$)

A eficiência relativa dos provedores de nuvem (PN) é calculada através do método de Análise Envoltória de Dados (do inglês *Data Envelopment Analysis* (DEA)). O DEA, um método não paramétrico, tem como objetivo realizar a medição e avaliação da eficiência relativa de um conjunto de unidades (CHARNES; COOPER; RHODES, 1978). Tais unidades, chamadas de DMUs (do inglês *Decision Making Units*), apresentam as mesmas variáveis de entrada e saída e representam entidades que são analisadas conforme sua capacidade de transformar entradas em saídas (COOPER; SEIFORD; ZHU, 2011). Em um cenário real, as unidades podem representar países, empresas, universidades, provedores de nuvem, entre outros (COOPER; SEIFORD; TONE, 2006). Neste trabalho, para efeito de cálculo da eficiência relativa, o provedor de nuvem é tratado como uma DMU, e o conceito de eficiência está relacionado ao seu histórico de participações anteriores em OVs.

Através do método do DEA pode-se calcular a eficiência de uma DMU e também identificar se uma DMU é mais eficiente em relação a outra (COOPER; SEI-

FORD; ZHU, 2011). Essas operações são realizadas sem que o usuário ou gestor da OV estabeleça pesos ou determine uma relação funcional que retorne o valor da eficiência (COOPER; SEIFORD; TONE, 2006). No DEA, a eficiência de uma DMU é dada como relativa, pois conforme Cooper, Seiford e Tone (2006) é calculada através da comparação dos valores de suas entradas em relação aos valores das entradas e saídas das DMUs que são mais produtivas, isto é, em termos comparativos, 100% eficientes.

Para a aplicação do DEA existem diversos modelos, como por exemplo CCR e BCC (MARTIĆ; NOVAKOVIĆ; BAGGIA, 2009). O modelo CCR, abreviatura do sobrenome de seus criadores, Charnes, Cooper e Rhodes (CHARNES; COOPER; RHODES, 1978), é adequado para ser aplicado em cenários em que uma alteração nos valores de entrada ocasiona uma variação proporcional nos valores de saída. Outro modelo, chamado de BCC de Banker, Charnes e Cooper (BANKER; CHARNES; COOPER, 1984), é projetado para trabalhar com entidades que apresentam retornos variáveis de escala, isto é, modela algumas situações em que uma ou mais alterações nos valores de entrada podem causar um acréscimo ou decréscimo não necessariamente proporcional no valor de suas saídas.

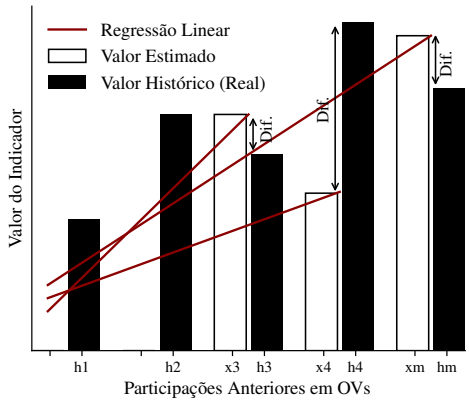
Após a definição dos modelos de aplicação da DEA, torna-se necessário especificar como foi realizada a modelagem das variáveis de entrada e saída e quais indicadores representam essas variáveis para as DMUs (provedores de nuvem). Para isso, nesse trabalho tais variáveis são modeladas através da análise histórica (participações passadas em OVs) dos indicadores de QoS, especificados na seção 2.4.1, dos provedores de nuvem. Esses indicadores tem seus valores normalizados em uma escala de 0 a 1 para a aplicação na DEA. Desse modo, a modelagem das entradas e saídas é detalhada a seguir.

Conforme mencionado em Vose (2008) e Lemos et al. (2014), a variabilidade nos dados é vista como um dos principais fatores que afetam a capacidade humana de predizer eventos futuros. Assim, a variabilidade no histórico de qualidade de serviço de um provedor de nuvem pode representar um impacto no comportamento desse provedor de nuvem nas suas futuras participações em OVs. Logo, quanto maior é a variabilidade no histórico de um PN, menor será sua eficiência, devido a imprevisibilidade de predizer seu comportamento em futuras participações nas OVs (LEMOS et al., 2014).

A previsibilidade é útil para analisar o comportamento futuro do provedor de nuvem em uma OVs levando em conta o histórico de participações em OVs. Desse modo, a previsibilidade é vista como variável de entrada (valores estimados) e é calculada através de várias regressões lineares para cada indicador de QoS, conforme exposto na Figura 10 (LEMOS et al., 2014). Ou seja, para cada provedor de nuvem

os valores previstos (estimados) para cada um dos indicadores de QoS, são utilizados como entradas para os efeitos de cálculo utilizando DEA.

Figura 10 – Geração dos valores estimados de cada indicador de QoS usando análise histórica



Fonte: Adaptado de Lemos et al. (2014)

Assim, cada variável de entrada correspondente a um indicador i de QoS (disponibilidade, tempo de resposta, segurança, estabilidade e preço) de um provedor de nuvem k, tem seu valor calculado através da Equação 4.3.

$$I_{ki} = \overline{X_{ki}} + \sigma(X_{ki}) \tag{4.3}$$

O valor de uma variável de entrada é composto pela média aritmética dos valores estimados ($\overline{X_{ki}}$) e o desvio padrão dos valores estimados. Os valores estimados para um indicador de QoS i, são obtidos através de um processo de regressão linear, ilustrado na Figura 10. O processo é realizado como se segue: através dos valores históricos das duas primeiras participações em OVs, a terceira participação é estimada, em sequência com os três primeiros valores, estima-se a quarta participação e assim sucessivamente até alcançar o enésimo valor histórico (h_m), na qual a última participação em OVs é estimada (LEMOS et al., 2014).

As variáveis de saída também são referentes aos indicadores de QoS. Contudo, essas variáveis são o valor médio ($\overline{H_{kj}}$) obtido através dos valores presentes no histórico de participações passadas em OVs. Desse modo, a Equação 4.4, representa a saída calculada para um indicador j de QoS de um provedor de nuvem k (LEMOS et al., 2014).

$$O_{kj} = \overline{H_{kj}} - \sigma(H_{kj}) \tag{4.4}$$

Logo, para cada indicador de QoS haverá um valor de entrada representado pela média dos valores estimados (previsibilidade), enquanto o valor de saída é representado pela média dos valores históricos reais. Assim, um provedor de nuvem que apresentar uma menor diferença entre os valores estimados e reais pode ser considerado como o mais eficiente, dado ao fato que apresenta uma menor variabilidade nos dados históricos (LEMOS et al., 2014).

Assim, por meio das definições das entradas e saídas utilizadas no DEA, a eficiência relativa dos provedores de nuvem pode ser calculada. De acordo com o DEA, a eficiência relativa de um PN$_s$ é dada como a razão entre as suas saídas e entradas, sendo representada pela Equação 4.5.

$$Eff\,(s) = \frac{\sum_{j=1}^{s} u_j y_{jo}}{\sum_{i=1}^{r} v_i x_{io} + v_o} \tag{4.5}$$

Em que x_{io} e y_{jo} representam a entrada i e saída j da DMU o (provedor de nuvem), v_o é o fator de escala usado no modelo BCC do DEA, v_i e u_j são os pesos definidos pelo DEA e r e s referem-se a quantidade de indicadores de entrada e saída, respectivamente.

Essa razão pode ser modelada por meio de um problema de programação linear através de um dos modelos já mencionados do DEA. No contexto desse trabalho, o modelo BCC orientado a saídas é o mais indicado, pois não existe uma relação proporcional entre os valores das saídas (reais) e as entradas (estimados). Isso é motivado pelo fato que as participações históricas de um PN não necessariamente influenciam as participações futuras desse provedor, ou seja, o desempenho futuro (qualidade de serviço) de um PN pode assumir qualquer valor, sem estabelecer uma relação funcional com os valores presentes no histórico de participações anteriores em OVs. Além disso, foi utilizado a orientação a saída, pois a eficiência de um PN está relacionada com o seu desempenho real (histórico). Por fim, a formulação do problema de programação linear é entendida como:

$$min\, z_0 \;=\; \sum_{i=1}^{r} v_i x_{io} + v_o \tag{4.6}$$

Sujeito à:

$$\sum_{j=1}^{s} u_j y_{jo} \;=\; 1 \tag{4.7}$$

$$\sum_{i=1}^{r} v_i x_{ik} \;-\; \sum_{j=1}^{s} u_j y_{jk} \;+ v_o \leq 0 \,\forall\, k \tag{4.8}$$

$$v_i,\; u_j \geq 0, v_o \in \mathbb{R}\, k \;=\; 1, 2, 3, \ldots, n \tag{4.9}$$

Como o modelo DEA utilizado nesta arquitetura é orientado a saída, a restrição 4.7 garante que a soma das saídas ponderadas pelos pesos calculados pelo DEA seja igual a 1, pois a eficiência de um provedor s é vista como uma razão $\frac{1}{z_o}$. As outras restrições referem-se ao valor da eficiência gerado, garantindo que a solução não apresente valor de eficiência maior que 100% e que os valores das entradas, saídas e pesos sejam não negativos. Além disso, o valor do fator de escala v_o pode assumir qualquer valor (positivo, negativo ou zero) (COOPER; SEIFORD; TONE, 2006). Por fim, nas restrições, o n representa a quantidade de provedores que estão envolvidos no cálculo da eficiência relativa.

A solução desse problema de programação linear fornece o valor da eficiência relativa (Eff) necessário para o cálculo do indicador de confiança objetiva de um determinado provedor de nuvem, conforme a Equação 4.2. Ainda, o indicador de confiança objetiva utiliza um escore de ponderação da eficiência relativa, conforme descrito na seção 4.3.1.2.

4.3.1.2 Confiança Multicritério ($Esc(s)$)

A confiança multicritério é vista como um escore de ponderação para a eficiência relativa. Esse escore é calculado como um valor único que representa a importância atribuída pelo gestor da OV a cada indicador de QoS. Para gerar esse escore, uma técnica de avaliação pareada de dados pode ser usada. Neste trabalho, tal técnica é extraída do método de avaliação de dados multicritério *Analytic Hierarchy Process* (AHP).

O método de avaliação de dados multicritério AHP faz uma análise quantitativa e qualitativa de um conjunto de indicadores, ou seja, a partir dos critérios (indicadores) é possível associar uma ordem de importância (peso) para cada um deles (MA; HU, 2015). Nesse sentido, a matriz de julgamento presente no método AHP é usada.

O escore de ponderação ou confiança multicritério é calculado pela Equação 4.10. O escore é composto pela soma dos valores de cada contribuição multicritério ($CMInd$) do indicador de QoS, em que D, RT, S, E, P, representam os indicadores de disponibilidade, tempo de resposta, segurança, estabilidade e preço, respectivamente. Esses indicadores foram especificados na seção 2.4.1.

$$Esc(s) = CMInd^s_D + CMInd^s_{RT} + CMInd^s_S + CMInd^s_E + CMInd^s_P \tag{4.10}$$

A contribuição multicritério, representada na Equação 4.11, é vista como um valor calculado para cada indicador k de QoS do provedor de nuvem s. Dessa forma, é composta pelos elementos: média histórica normalizada de cada indicador ($\overline{X^s_k}$) (de

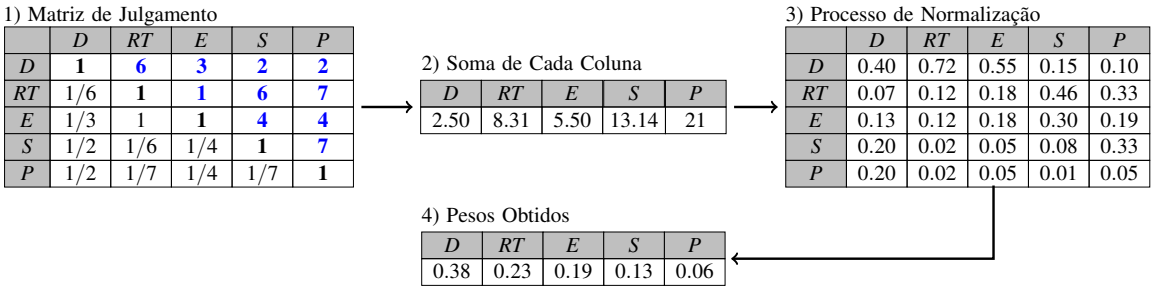
0 a 1), peso de importância (w_k), fator de penalização histórico ($FPen_k^s$) e fator de recompensa histórico ($FRec_k^s$).

$$CMInd_k^s = w_k \times \overline{X_k^s} - FPen_k^s + FRec_k^s \tag{4.11}$$

Os pesos de importância para cada indicador de QoS (critérios no AHP) são gerados através da manipulação da matriz de julgamento do método AHP. A matriz de julgamento é uma matriz quadrada que realiza a comparação dos critérios de forma pareada, utilizando uma tabela de graus de preferência, proposta em Saaty (1990). Essa tabela apresenta os graus variando de 1 a 9, em que o nível 1 representa que os indicadores possuem a mesma importância e o nível mais alto, 9, representa a maior discrepância possível entre o significado dos indicadores.

A matriz de julgamento ($n \times n$) é composta por linhas e colunas que são referentes aos critérios avaliados. O valor a_{ij} representa a importância do critério da linha i face o critério da coluna j. Como esta matriz é recíproca, apenas os valores da metade triangular superior (elementos à direita e acima da diagonal principal) necessitam ser avaliados, já que a outra metade deriva desta, na forma $a_{ji} = \frac{1}{a_{ij}}$. A diagonal principal é preenchida com valores iguais a 1, pois critérios iguais apresentam a mesma importância. O preenchimento dessa matriz é de responsabilidade do gestor da OV e é apresentado no passo 1 da Figura 11. Nela foram utilizados valores empíricos adequados a escala de Saaty (SAATY, 1990) para a comparação de cada um dos indicadores de QoS utilizados pela arquitetura de reputação proposta.

Figura 11 – Matriz de julgamento



	D	RT	E	S	P
D	**1**	**6**	**3**	**2**	**2**
RT	1/6	**1**	**1**	**6**	**7**
E	1/3	1	**1**	**4**	**4**
S	1/2	1/6	1/4	**1**	**7**
P	1/2	1/7	1/4	1/7	**1**

D	RT	E	S	P
2.50	8.31	5.50	13.14	21

	D	RT	E	S	P
D	0.40	0.72	0.55	0.15	0.10
RT	0.07	0.12	0.18	0.46	0.33
E	0.13	0.12	0.18	0.30	0.19
S	0.20	0.02	0.05	0.08	0.33
P	0.20	0.02	0.05	0.01	0.05

D	RT	E	S	P
0.38	0.23	0.19	0.13	0.06

Fonte: Produção do próprio autor.

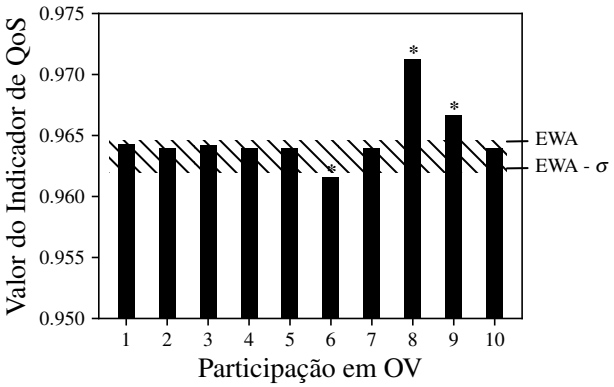
A normalização da matriz é realizada após seu preenchimento. Para isto, é calculada a soma de cada coluna e cada elemento da matriz é dividido pela soma da coluna a qual pertence. Por fim, após o processo de normalização, a média aritmética

de cada linha da matriz é calculada. Essa sequência de cálculos é representada pelos passos 2, 3 e 4 da Figura 11, os quais resultam nos valores dos pesos de importância para cada indicador de QoS.

Na Equação 4.11, relativa à contribuição multicritério, dois fatores são considerados: penalização e recompensa. A penalização é usada para punir os provedores de nuvem que apresentam um histórico de participações em OVs com mais oscilações. Em contrapartida, a recompensa visa gratificar os provedores de nuvem que apresentam um histórico com um desempenho constante, ou seja, o mínimo possível de variações (SCEKIC; TRUONG; DUSTDAR, 2012).

Os valores referentes aos fatores de penalização e recompensa são calculados por meio do histórico de participações de um provedor de nuvem. Dessa forma, a Figura 12 apresenta um exemplo ilustrativo, com os valores históricos de um indicador qualquer para um provedor de nuvem qualquer e a margem aceitável (região hachurada) para esse indicador.

Figura 12 – Valores de um indicador nas participações passadas em OVs para um PN qualquer



Fonte: Produção do próprio autor.

A margem aceitável, utilizada nos cálculos dos fatores de penalização e recompensa, representa o intervalo de valores desejável para um indicador com base no seu histórico de participações. Dessa forma, a margem é definida como a região compreendida entre o limite superior, que é calculado através da média exponencialmente ponderada (EWA), e o limite inferior, entendido como a diferença entre o valor da EWA e o desvio padrão, do conjunto de valores históricos de um indicador de QoS. Cada indicador de QoS, de cada provedor de nuvem, tem sua margem aceitável no contexto da contribuição multicritério. Assim, através do exemplo proposto na Figura 12, nota-se que alguns valores estão fora da margem aceitável, como os valores da participações em OVs 6, 8 e 9, de forma que essa quantidade de valores entra no cálculo do fator de

penalização e o restante, ou seja, a quantidade de valores que está dentro da margem aceitável é considerada no cálculo do fator de recompensa.

A Média Exponencialmente Ponderada (do inglês *Exponentially Weighted Average* (EWA)) é uma medida de tendência central bastante utilizada devido à sua eficiência e simplicidade computacional (MONTGOMERY; RUNGER, 2002). Nesse trabalho, a EWA calcula o valor aceitável de um indicador de QoS a partir de um histórico de participações em OVs para um provedor de nuvem s. A Equação 4.12 apresenta o cálculo da EWA.

$$\overline{EWA}_k^s = \frac{\sum_{i=1}^{n} w_i k_i}{\sum_{i=1}^{n} w_i} \tag{4.12}$$

Em que $k = \{k_1, k_2, k_3, ..., k_n\}$ é o conjunto de valores históricos de um provedor de nuvem s para um indicador k em n participações passadas em OVs e w representa um fator de decaimento normalizado (peso), definido pelo gestor da OV.

Para estabelecer a margem aceitável, além do valor médio calculado pela EWA, deve-se considerar uma métrica de variabilidade. Sendo assim, optou-se por utilizar o desvio padrão (σ) das participações históricas como forma de atenuar pequenas oscilações no histórico. Assim, a margem aceitável para o exemplo presente na Figura 12, é compreendida pela região entre o limite superior (EWA = 0.9658) e limite inferior, calculado através da diferença entre a EWA e o desvio padrão, sendo igual à 0.9624.

Dessa forma, o fator de penalização, representado na Equação 4.13, é calculado como a diferença entre a média aritmética do histórico do indicador e o limite inferior da margem aceitável, ponderada pela razão entre a quantidade de valores do indicador que estão fora da margem aceitável e a quantidade que representa o tamanho do histórico desse indicador. Nesse caso, $\overline{K}$ representa a média aritmética do histórico do indicador k, EWA_k^s é o valor calculado pela EWA para o histórico do indicador k, Δ_k^s é a diferença entre a EWA e o desvio padrão para o indicador k (limite inferior da margem aceitável) e n é o total de participações em OVs (tamanho do histórico).

$$FPen_k^s = (\overline{K} - \Delta_k^s) \times \frac{\sum_{i=1}^{n} 1_{\,[\,k_i > EWA_k^s\,] \vee [\,k_i < \Delta_k^s\,]}}{n} \tag{4.13}$$

O fator de recompensa, representado pela Equação 4.14, é calculado pela diferença entre a média aritmética do histórico do indicador e o limite inferior da margem aceitável, ponderada pela razão entre a quantidade de participações em que o valor do indicador k se encontra presente na margem aceitável e o tamanho do histórico (n).

$$FRec_k^s = (\overline{K} - \Delta_k^s) \times \frac{\sum_{i=1}^{n} 1_{\,[\,\Delta_k^s \leq k_i \leq \mathrm{EWA}_k^s\,]}}{n} \tag{4.14}$$

De forma a exemplificar os cálculos dos fatores mencionados considere a Figura 12. Alguns dados podem ser observados, como: 3 valores (destacados com asterisco) fora da margem aceitável e 7 valores presentes na margem aceitável. Nesse exemplo temos: EWA (0.9658), desvio padrão (0.0026), $\triangle_k^s$ (0.9624) e média histórica do indicador (0.9648).

Desse modo, para os dados apresentados, o fator de penalização tem o valor 0.00072 e o fator de recompensa 0.00168 em relação ao indicador analisado. Através disto, pode-se notar que devido a uma maior quantidade de valores presentes na margem aceitável, para esse indicador, esse provedor será mais recompensado do que penalizado em relação ao seu histórico de participações em OVs.

4.3.2 Indicador de Confiança Subjetiva (T_{sub})

O indicador de confiança subjetiva (T_{sub}) representa as avaliações (*feedbacks*) fornecidas pelo parceiro de negócio da OV ao provedor de nuvem e seu cálculo foi adaptado da formulação proposta em Noor et al. (2016b).

Neste trabalho os *feedbacks* são coletados e armazenados no repositório de dados através da arquitetura de reputação proposta. Este indicador de confiança é dito subjetivo pois é proveniente das avaliações dos parceiros de negócio da OV, as quais são baseadas na experiência ou percepção que o parceiro de negócio obteve durante as interações com tal provedor de nuvem.

Durante a fase de dissolução da OV, preferencialmente, cada parceiro de negócio da OV envia seu *feedback* à respeito da transação realizada com o provedor de nuvem. O *feedback* é representado através de um conjunto de avaliações apresentado pela Tabela 1. O conjunto contempla um valor de 0 a 5, entendido como uma avaliação (nota), atribuída pelo parceiro de negócio da OV para cada indicador de QoS (disponibilidade (D), tempo de resposta (RT), segurança (S), estabilidade (E) e preço (P)).

Tabela 1 – Conjunto de avaliações, representando o *feedback* de um membro da OV

D	RT	S	E	P
4.25	4.0	3.0	4.0	4.5

Fonte: Produção do próprio autor.

Quando *feedbacks* são enviados à arquitetura proposta, a mesma realiza a coleta e armazena tais *feedbacks*, ou seja, os valores que os compõem (conjunto de avaliações). Assim, permite que esses *feedbacks* sejam utilizados em cenários que

apresentam diferentes pesos de importância.

Por meio do conjunto de avaliações de um *feedback* calcula-se o valor agregado subjetivo. O valor agregado subjetivo é referente ao *feedback* (avaliações subjetivas) emitido por um parceiro de negócio (membro da OV) em uma interação com um provedor de nuvem. Esse valor, calculado pela Equação 4.15, é a soma ponderada do valor de cada indicador do conjunto de avaliações mencionado anteriormente. Desse modo, $Q_c\,(c, s, z)$ representa o valor agregado subjetivo do parceiro de negócio c em relação ao provedor de nuvem s durante uma interação ou transação z realizada, k_x refere-se à nota (avaliação) atribuída pelo parceiro de negócio da OV ao indicador x de QoS e w_x é o peso de importância (calculado de acordo com a confiança multicritério ($Esc\,(s)$) na seção 4.3.1).

$$Q_c\,(c, s, z) = \sum_{x=1}^{5}(k_x * w_x) \tag{4.15}$$

Como forma de exemplo para o cálculo do valor agregado subjetivo considere os seguintes dados: valores do conjunto de avaliações (Tabela 1) e os pesos definidos na matriz de julgamento apresentada na seção 4.3.1. Assim o valor agregado subjetivo ($Q_c\,(c, s, z)$) de um membro da OV em relação a um provedor de nuvem em questão, é calculada como:

$$\begin{aligned} Q_c\,(c, s, z) = (4.25\ *0.383) + (4.0\ *0.2317) + (3.0\ *0.1861) + (4.0\ *0.135) \\ +(4.5\ *0.0642) \\ Q_c\,(c, s, z) = 3.94 \end{aligned}$$

Desse modo, o indicador de confiança subjetiva de um provedor de nuvem s é definido pela Equação 4.16. Esse indicador é calculado através da razão entre o somatório da média aritmética de m *feedbacks* fornecidos por n parceiros de negócio, em que cada *feedback* é representado pelo seu valor agregado subjetivo ($Q_c\,(c, s, z)$) ponderado pelo fator de credibilidade das avaliações ($C_f\,(c, s)$) e a quantidade de parceiros de negócio (n).

$$T_{sub}\,(s) \;=\; \frac{\displaystyle\sum_{c=1}^{n} \frac{\sum_{z=1}^{m} Q_c(c, s, z) \times C_f\,(c, s)}{m}}{n} \tag{4.16}$$

Através da abordagem adotada no cálculo é possível utilizar tanto os *feedbacks* históricos, ou seja, participações passadas do provedor s em OVs, juntamente com os *feedbacks* coletados na fase de dissolução da OV. Além disso, isso modela a pos-

sibilidade de um membro da OV utilizar mais de um serviço do mesmo provedor de nuvem.

Conforme observado em Noor et al. (2016b) os *feedbacks*, representados pelos seus valores agregados subjetivos, são úteis para compor a reputação dos provedores de nuvem. No entanto, esses *feedbacks* são alvos de manipulação através de algumas formas de ataque, ou seja, os parceiros de negócio da OV podem tentar enviar avaliações maliciosas com o propósito de promover ou prejudicar o indicador de confiança subjetiva de um provedor de nuvem e consequentemente a reputação desse provedor.

De forma a resolver esse problema Noor et al. (2016b) propõem a análise da credibilidade dos *feedbacks* fornecidos pelos usuários. Assim, essa análise é realizada através do fator de credibilidade que é especificado na seção 4.3.2.1.

4.3.2.1 Fator de Credibilidade ($C_f\,(c,s)$)

O fator de credibilidade tem como principal objetivo efetuar o tratamento de alguns ataques, os quais podem manipular o valor do indicador de confiança subjetiva de um determinado provedor de nuvem. De uma forma geral, no ambiente da OV na nuvem, os ataques realizados nos *feedbacks* podem ocorrer através de duas formas: colusão de avaliações e ataque de avaliações injustas (JØSANG; GOLBECK, 2009).

O ataque de colusão de avaliações ocorre quando um parceiro de negócio da OV envia *feedbacks* (com qualquer valor) em exagero (vários *feedbacks*) para manipular os resultados do indicador de confiança subjetiva (NOOR et al., 2016b).

O ataque de avaliações injustas é realizado por parceiros de negócio da OV que apresentam comportamento malicioso durante o envio de *feedbacks* (JØSANG; GOLBECK, 2009). Esse comportamento malicioso refere-se à vários *feedbacks* injustos que são enviados, ou seja, esses *feedbacks* apresentam um conjunto de avaliações com os mais altos valores (entre 4 e 5) ou os valores mais baixos (entre 0 e 1), os quais não refletem o real desempenho desse provedor de nuvem durante as interações. Desse modo, os usuários tentam promover ou prejudicar o indicador de confiança subjetiva de um provedor de nuvem.

Nesse sentido, o fator de credibilidade ($C_f\,(c,s)$) é utilizado para efetuar o tratamento das formas de ataques mencionadas. Esse fator é calculado através da Equação 4.17 e é composto por dois subfatores, sendo que $D\,(s)$ representa o subfator de densidade das avaliações, usado na identificação do ataque de colusão de avaliações, e $U\,(c,s)$ é o subfator de avaliações injustas. Cada subfator é ponderado pelo seu peso de importância na formação do fator de credibilidade. Os pesos de cada

subfator, representados por ρ e Ω, podem ser definidos pelo gestor da OV.

$$C_f\left(c,s\right) = \frac{\left(\rho * D\left(s\right)\right) + \left(\Omega * U(c,s)\right)}{2} \tag{4.17}$$

Em relação ao ataque de colusão de avaliações, Noor et al. (2011, 2013, 2016b), sugerem que a quantidade de *feedbacks* fornecidos durante uma interação é relevante para a análise dessa forma de ataque. Desse modo, através do cálculo da densidade das avaliações é possível identificar os ataques de colusão (NOOR et al., 2016b). Assim, a Equação 4.18 apresenta a fórmula do cálculo para a densidade, que é composta pela quantidade de parceiros de negócio da OV ($M(s)$) que avaliaram o provedor de nuvem s, $|V(s)|$ corresponde à quantidade total de *feedbacks* relativos ao provedor de nuvem s e $L(s)$ representa o subfator de colusão:

$$D(s) = \frac{M(s)}{|V(s)| * L(s)} \tag{4.18}$$

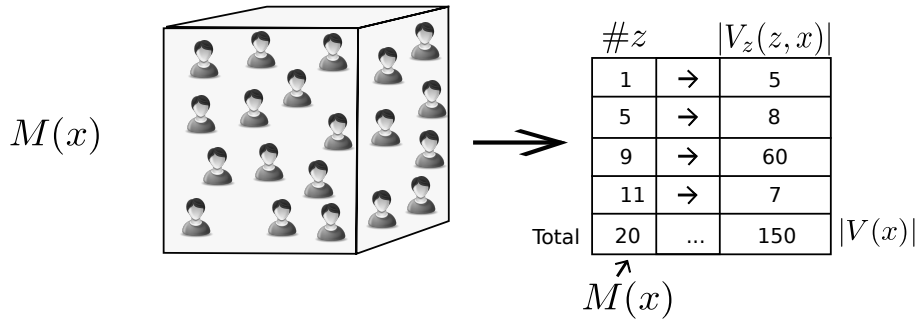
O subfator de colusão ($L(s)$), segundo Noor et al. (2016b), tem como propósito reduzir o valor da credibilidade do parceiro de negócio da OV, quando este envia múltiplos *feedbacks* (independente do valor agregado subjetivo) ao mesmo provedor de nuvem em uma participação em OV, ou seja, envia mais *feedbacks* do que o tolerável/aceitável. O subfator de colusão, ilustrado na Equação 4.19, é calculado como uma razão entre a quantidade de *feedbacks* dos parceiros de negócio da OV ($|V_c(c,s)|$) que enviaram mais *feedbacks* do que o estabelecido no limite de colusão $e_v\left(s\right)$ (tal condição é expressa entre colchetes no somatório (GRAHAM; KNUTH; PATASHNIK, 1994, p. 24) da Equação 4.19), e a quantidade total de *feedbacks* recebidos ($|V(s)|$) pelo provedor de nuvem s. Ainda, n refere-se a quantidade de parceiros de negócio que avaliaram o provedor de nuvem s.

$$L(s) = 1 + \left(\frac{1}{|V(s)|}\sum_{c=1}^{n} |V_c(c,s)|_{\ [|V_c(c,s)|>e_v(s)]}\right) \tag{4.19}$$

A Figura 13 traz alguns dados e ilustra a composição dos parâmetros para o cálculo dos subfatores usados na densidade das avaliações. Assim, é possível notar que 20 parceiros de negócio da OV avaliaram o provedor de nuvem x ($M(x) = 20$), totalizando 150 *feedbacks* a este provedor ($|V(s)| = 150$) sendo que o parceiro 9 da OV forneceu 60 avaliações ao provedor x ($|V_9(9,x)| = 60$). Por fim, supõe-se que o limite de colusão de avaliações esteja estabelecido em 10 ($e_v(s) = 10$).

Dessa forma, o subfator de colusão $L(s)$ para o exemplo apresentado na Figura 13, tem o valor igual à 1.40. De acordo com a Equação 4.18, a densidade das avaliações para o caso analisado é igual à 0.09523. Importante notar que quanto maior

Figura 13 – Exemplo para a densidade das avaliações



Fonte: Adaptado de Noor et al. (2016b).

for a densidade, mais credíveis são as avaliações, ou seja, são provenientes de parceiros de negócio que apresentaram um comportamento normal durante o envio de *feedbacks*, isto é, a quantidade de *feedbacks* fornecidos apresenta-se próximo ao limite aceitável ($e_v(s)$).

Em outra forma de ataque, o de avaliações injustas, os parceiros de negócio da OV apresentam comportamento malicioso e enviam vários *feedbacks* injustos. Esses *feedbacks* são compostos por conjuntos de avaliações com valores altos (entre 4 e 5) ou baixos (entre 0 e 1), que são usados para manipular os resultados do indicador de confiança subjetiva, ou seja, promover ou prejudicar um provedor de nuvem. Assim, torna-se necessário estabelecer um fator que reduza a credibilidade desses membros que apresentam esse tipo de comportamento.

Algumas abordagens são adotadas na literatura para identificar o ataque de avaliações injustas. Essas abordagens verificam o desvio das avaliações em relação a opinião da maioria que avaliou a mesma entidade. Desse modo, nota-se que algumas técnicas são usadas, como a estatística para filtragem de *feedbacks* (WHITBY; JØSANG; INDULSKA, 2004), métodos de filtragem e descontos de *feedbacks* (ZHANG et al., 2012), lógica fuzzy (LIU et al., 2013), entre outras.

As abordagens mencionadas desconsideram as avaliações que não estão de acordo com a opinião da maioria para amenizar os efeitos dos ataques realizados. No entanto, neste trabalho, as avaliações que diferem da opinião da maioria não serão simplesmente desconsideradas, mas utilizadas na avaliação de um fator de credibilidade, que poderá reduzir a importância das demais avaliações fornecidas por esses membros.

Conforme exposto em Malik e Bouguettaya (2009) para a identificação e tratamento do ataque de avaliações injustas, um algoritmo de agrupamento de da-

dos é usado com grande proveito. Nesse trabalho é usado o algoritmo *K-Means* (k-médias) (MACQUEEN, 1967) para identificar a opinião (*feedback*) da maioria dos avaliadores em relação ao provedor de nuvem.

O algoritmo *K-Means* é aplicado para todos os *feedbacks* de um provedor de nuvem s, ou seja, todos os valores agregados subjetivos que estão presentes no repositório de dados. Após as interações desse algoritmo, obtém-se os centroides, entendidos como grupos de valores. Nesse sentido, a Equação 4.20, obtém o centroide com maior filiação, ou seja, o que contém a maior quantidade de observações (*feedbacks*) agrupadas por similaridade.

$$M = centroide(max(\mathbb{R}_f)) \quad \forall\, f \tag{4.20}$$

Em que, M é o centroide com maior filiação, f é a quantidade total de grupos (*clusters*), $max(\mathbb{R}_f)$ retorna o grupo $\mathbb{R}$ com maior filiação, e $centroide(x)$ fornece o centroide de um grupo x (MALIK; BOUGUETTAYA, 2009).

A obtenção do centroide com maior filiação possibilita a realização do cálculo do subfator de avaliações injustas. Desse modo, a Equação 4.21 é responsável por calcular o subfator de avaliações injustas para um determinado parceiro de negócio c da OV em relação aos *feedbacks* fornecidos para um provedor de nuvem s (MALIK; BOUGUETTAYA, 2009). O subfator considera a distância euclidiana entre o centroide com maior filiação (M) e os valores agregados subjetivos (A) dos *feedbacks* fornecidos pelo membro c da OV ao provedor s.

Na Equação 4.21, A_i refere-se ao valor agregado subjetivo fornecido pelo parceiro de negócio da OV durante a interação i. O conjunto A representa j valores agregados subjetivos, ou seja, pode ser composto por um ou mais *feedbacks* referentes a uma ou mais interações em OVs. Também, A pode conter diversos *feedbacks* que são provenientes de usuários com comportamento malicioso. Esses usuários apresentam o objetivo de promover ou prejudicar o indicador de confiança subjetiva de um provedor de nuvem.

Além disso, a Equação 4.21, considera o desvio padrão (σ) dos valores agregados subjetivos dos *feedbacks*. Assim, o cálculo da distância euclidiana retorna um valor maior que 1, e o desvio padrão é usado como forma de normalização dessa distância em um intervalo de 0 a 1 (MALIK; BOUGUETTAYA, 2009).

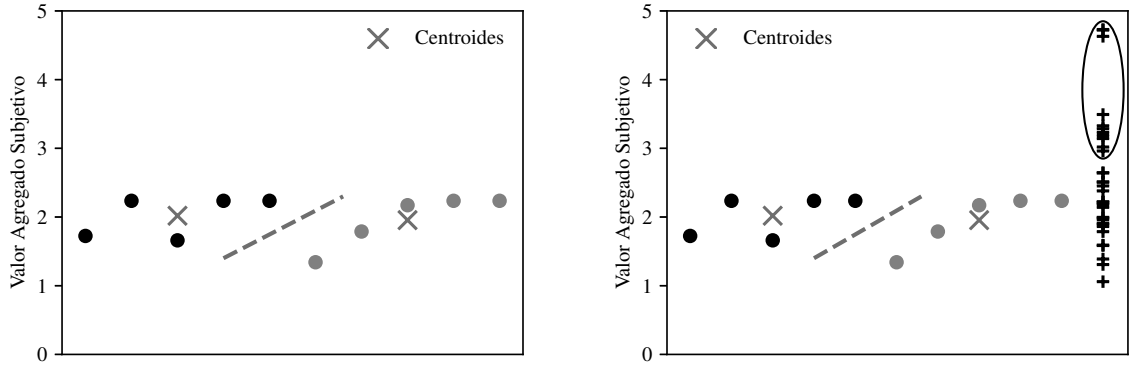
$$U(c,s) = \begin{cases} 1 - \dfrac{\sqrt{\sum_{i=1}^{j}(M-A_i)^2}}{\sigma}, & \text{se } \sqrt{\sum_{i=1}^{j}(M-A_i)^2} < \sigma \\ 1 - \dfrac{\sigma}{\sqrt{\sum_{i=1}^{j}(M-A_i)^2}}, & \text{senão} \end{cases} \tag{4.21}$$

Desse modo, o subfator de avaliações injustas é representado no intervalo de 0 a 1. De forma básica esse subfator realiza a análise dos *feedbacks* fornecidos, com os valores agregados subjetivos presentes em A, por um membro da OV que interagiu com um determinado provedor de nuvem. Essa análise tem como objetivo verificar o quão próximo os valores agregados subjetivos, gerados pelos *feedbacks*, estão do centroide com maior filiação, ou seja, o qual reflete a opinião da maioria em relação ao serviço prestado pelo provedor de nuvem.

De forma a exemplificar o cálculo do subfator de avaliações injustas considere os dados presentes na Figura 14 que são referentes a um provedor de nuvem qualquer. Os dados apresentados na Figura 14a são referentes ao valores agregados subjetivos históricos, ou seja, obtidos em participações passadas nas OVs. Já na Figura 14b, além do histórico, são apresentados os valores agregados subjetivos ($Q_c(c, s, z)$) obtidos na dissolução de uma OV qualquer que são representados pelo marcador +. Os valores representados pelo marcador + foram gerados a partir de *feedbacks* provenientes de ataques, isto é, alguns apresentam conteúdo malicioso.

Inicialmente, para o cálculo do subfator de avaliações injustas, o algoritmo K-Means é aplicado nos valores agregados subjetivos presentes no repositório de dados. Isso é visto nas Figuras 14a e 14b que apresentam cada *cluster* e seu centroide (X), em que os círculos pretos são os valores subjetivos agregados presentes no *cluster* 1 enquanto os círculos cinzas referem-se ao *cluster* 2, por exemplo. Após isso, obtém-se o centroide com maior filiação (M), ou seja, o qual contém a maior quantidade de observações agrupadas. Nesse caso, como os dois *clusters* apresentam a mesma quantidade, o último *cluster* é escolhido (*cluster* 2).

Figura 14 – Exemplo de aplicação do fator de avaliação injusta



(a) *Feedbacks* do histórico

(b) *Feedbacks* do histórico e novos *feedbacks*

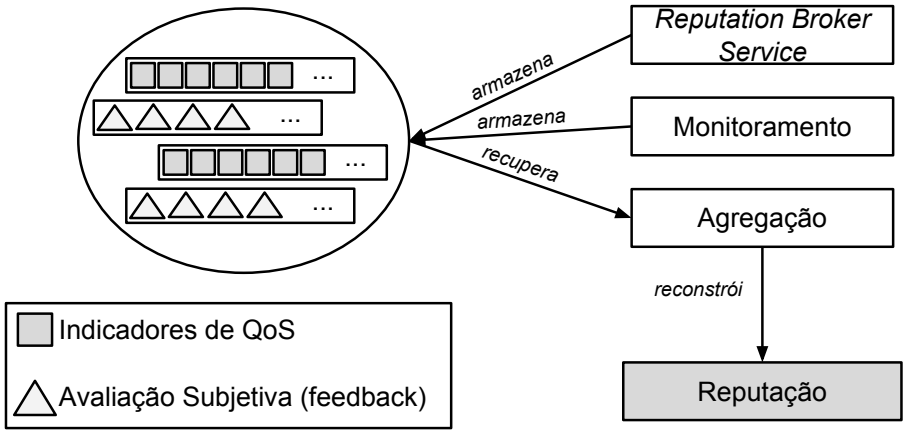
Fonte: Produção do próprio autor.

Após a definição do centroide com maior filiação, o subfator de avaliações injustas ($U(c, s)$) pode ser calculado. Desse modo, aplicando os valores agregados subjetivos (marcador +) representados pela Figura 14b à Equação 4.21, temos que o subfator de avaliações injustas é calculado como 0.8554. O valor desse subfator estando próximo de 1, indica que o membro c da OV forneceu *feedbacks* condizentes com a opinião da maioria. Em contrapartida, quanto mais distante de 1, a credibilidade desse membro é diminuída proporcionalmente em relação aos valores agregados subjetivos dos *feedbacks* fornecidos.

4.4 REPOSITÓRIO DE DADOS

O repositório de dados tem suas interações com os outros módulos da arquitetura apresentadas na Figura 15. Esse módulo tem como principal objetivo armazenar os valores históricos de QoS, bem como os valores históricos dos *feedbacks* (notas presentes no conjunto de avaliações) fornecidos pelos parceiros de negócio da OV que se relacionaram com os provedores de nuvem. Além disso, armazena os valores de QoS atuais obtidos pelo módulo de monitoramento, durante a fase de operação da OV.

Figura 15 – Interações com o repositório de dados



Fonte: Produção do próprio autor.

A abordagem de armazenamento adotada no repositório de dados permite que as informações que compõem os indicadores de confiança (QoS e *feedbacks*) possam ser utilizadas em ambientes com diferentes configurações de pesos, ou seja, pesos diferentes podem ser definidos para cada indicador de QoS no cálculo da confiança multicritério e no valor agregado subjetivo.

Assim, o módulo de agregação efetua a consulta ao repositório de dados para recuperar as informações referentes aos valores históricos de indicadores de QoS e os valores referentes aos *feedbacks* fornecidos pelos parceiros de negócio. Isso é feito para calcular a reputação do provedor de nuvem durante a fase de criação da OV, ou durante a operação da OV, quando são também considerados os valores de QoS monitorados juntamente com os valores históricos de QoS.

Durante a fase de dissolução da OV, o repositório de dados recebe os *feedbacks*, através do *Reputation Broker Service*, fornecidas pelos parceiros de negócio da OV, tornando-os aptos a serem utilizados pelo módulo de agregação. No momento da execução da fase de operação da OV os dados monitorados são armazenados no repositório de dados.

Por fim, o módulo de agregação utiliza os valores históricos (objetivos e subjetivos) e monitorados armazenados no repositório de dados, para calcular a reputação dos provedores de nuvem.

4.5 *REPUTATION BROKER SERVICE*

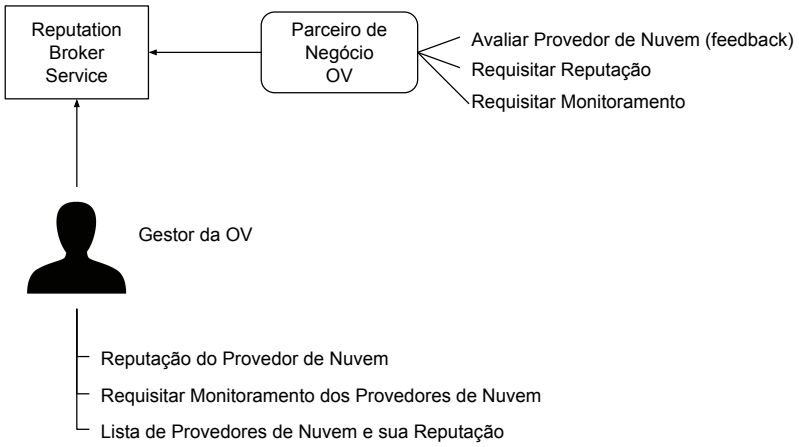
O *Reputation Broker Service* (RBS) é uma entidade centralizada que disponibiliza o acesso às funcionalidades propostas pela arquitetura de reputação para outros membros, por exemplo, o gestor da OV e os parceiros de negócio da OV.

Essa entidade é responsável por fornecer acesso as seguintes funcionalidades:

- Requisição dos valores de reputação de um determinado provedor de nuvem;
- Lista da reputação dos provedores de nuvem presentes no Repositório de Dados ou usados pela OV;
- Recebimento de requisições para realização de operações de monitoramento; e
- Recebimento dos valores referentes aos *feedbacks* fornecidos pelos parceiros de negócio para atualizar a participação de um provedor de nuvem no repositório de dados.

A atualização dos indicadores de QoS via RBS, é feita através de ações de monitoramento automático (*pooling*) dentro de um intervalo de tempo definido pelo gestor da OV ou por meio da solicitação de uma ação de monitoramento. Em resumo, as funcionalidades com os respectivos papéis (gestor da OV e parceiro de negócio da OV) são apresentadas na Figura 16.

Figura 16 – Funcionalidades propostas pelo *reputation broker service*



Fonte: Produção do próprio autor

Essas funcionalidades são aplicadas no contexto da integração entre organizações virtuais e computação em nuvem, para auxiliar os processos de tomada de decisão, como por exemplo, a busca e seleção de provedores de nuvem apoiada pela reputação.

4.6 CONSIDERAÇÕES PARCIAIS

O capítulo apresentou a arquitetura de reputação de confiança destacando seus requisitos funcionais, não funcionais, camadas, seus módulos e também a interação com a OV no contexto da integração com computação em nuvem.

A arquitetura é composta por três camadas: camada de aplicação, camada de reputação e a camada de dados e além disso foi dividida em quatro módulos: módulo de monitoramento, módulo de agregação, repositório de dados e o RBS.

Esse capítulo também apresentou o módulo de monitoramento que tem como principal objetivo, realizar o monitoramento de alguns indicadores de QoS dos provedores de nuvem durante a fase de operação da OV.

Posteriormente, o módulo de agregação foi apresentado, contemplando os métodos de cálculo para a reputação e também para cada indicador de confiança que a compõe, tanto objetivo quanto subjetivo. O indicador de confiança objetiva foi desenvolvido através de uma abordagem que analisa a eficiência relativa e a importância relativa (confiança multicritério) em relação ao histórico de participações dos provedores de nuvem. Por outro lado, o indicador de confiança subjetiva foi baseado no método de cálculo proposto em Noor et al. (2016b). Esse indicador é calculado através dos va-

lores agregados subjetivos dos *feedbacks* fornecidos pelo parceiro de negócio da OV ao provedor de nuvem, ponderado por um fator de credibilidade.

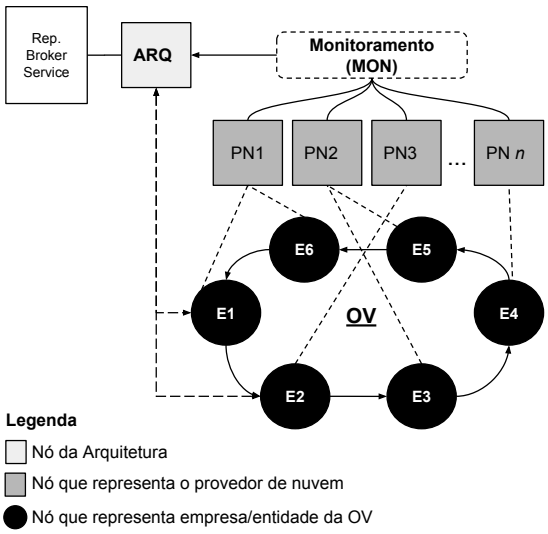
Por fim, outros módulos da arquitetura foram apresentados e descritos, como, por exemplo, o repositório de dados e o RBS. O repositório de dados busca armazenar os valores históricos de QoS e os *feedbacks* fornecidos pelos parceiros de negócio da OV que se relacionaram com os provedores de nuvem. Já o RBS disponibiliza as funcionalidades propostas pela arquitetura de reputação para outros membros, como por exemplo o gestor da OV e os parceiros de negócio da OV.

5 AVALIAÇÃO DA ARQUITETURA DE REPUTAÇÃO

Esse trabalho foi avaliado através de um ambiente simulado envolvendo a utilização da arquitetura de reputação por parte da organização virtual. O ambiente das simulações foi construído no simulador de redes P2P, denominado PeerFactSim.KOM (STINGL et al., 2011), na linguagem de programação Java. Tal simulador foi escolhido pelo fato de permitir a criação de uma rede P2P de forma a simular a conexão entre os componentes de uma OV, possibilitar a criação de nós de rede personalizados exercendo os papéis distintos e necessários da arquitetura proposta e efetuar a troca de mensagens entre os elementos, nesse caso, a arquitetura proposta e a OV baseada na nuvem.

O ambiente de integração proposto, apresentado na Figura 17, busca avaliar a construção dos valores dos indicadores de confiança objetiva e subjetiva, e consequentemente o valor final de reputação dos provedores de nuvem, bem como analisar as trocas de mensagens existentes entre os parceiros de negócio da OV e a arquitetura de reputação proposta. Dessa forma, diferentes nós de rede foram criados para representar cada elemento da arquitetura, como, por exemplo, nó da arquitetura (`ARQ`) (que tem implementado o *Reputation Broker Service* (RBS)) , provedores de nuvem (`PN`), parceiros de negócio da OV (`E`) e o módulo de monitoramento (`MON`).

Figura 17 – Ambiente proposto para os experimentos



Fonte: Produção do próprio autor.

O nó da arquitetura de reputação (ARQ) recebe as mensagens que são destinadas à arquitetura de reputação, como por exemplo recebimento de *feedbacks* dos parceiros de negócio da OV aos provedores de nuvem, requisição da reputação de um provedor de nuvem, requisição da lista de reputação (todos os provedores de nuvem) e o recebimento das informações de monitoramento. Esse nó tem implementada a funcionalidade do RBS, presente na seção 4.5, e comunica-se com o restante dos módulos presentes nas camadas da arquitetura de reputação.

O nó referente à entidade/empresa (E) representa o parceiro de negócio da OV. Esses nós são configurados/organizados através de uma topologia lógica em anel e interagem com a arquitetura de reputação. O parceiro de negócio da OV pode requisitar a reputação de algum provedor de nuvem, enviar *feedbacks* referentes ao provedor de nuvem usado e também requisitar ações de monitoramento. Além disso, os nós desse tipo podem trocar mensagens de colaboração, de forma simulada para realizar o atendimento da oportunidade de colaboração, durante a fase de operação da OV.

O nó provedor de nuvem (PN) representa um provedor de nuvem que fornece os seus serviços ou recursos para a OV. Desse modo, quando um novo parceiro de negócio é configurado na OV, por exemplo na fase de criação, um recurso/serviço de um provedor de nuvem é atribuído a ele. Sendo assim, o PN, nas simulações realizadas, atua como a entidade que está associada a um parceiro de negócio (E) e que será por ele avaliada. Além disso, desempenha o papel de fornecimento de dados para o módulo de monitoramento da arquitetura.

O nó de monitoramento (MON) é responsável por interagir com os n provedores de nuvem e coletar informações referentes ao QoS durante a simulação. Assim, quando o módulo de monitoramento é considerado, durante a fase de operação da OV, as informações coletadas são repassadas à arquitetura de reputação para que seja possível calcular o valor atual de reputação do(s) PN(s) através dos indicadores de confiança objetiva (histórico de QoS + dados monitorados) e subjetiva (*feedback* dos parceiros da OV) e atualizar a sua participação no repositório de dados.

Após a definição e detalhamento do ambiente de simulação proposto, torna-se necessário definir alguns parâmetros iniciais que são utilizados tanto pelo simulador quanto pela arquitetura de reputação durante a execução das simulações. Assim, os parâmetros são apresentados na Tabela 2.

Cada simulação a ser executada deve ter um tempo de duração, sendo que este tempo foi definido como 10080 min, ou seja, uma semana. Esse tempo de simulação é compreendido pelo tempo entre a criação da OV até sua dissolução e é utilizado para a distribuição de operações de colaboração, reputação, envio de *feedbacks*, entre outras.

Tabela 2 – Parâmetros iniciais utilizados nas simulações

Tempo de Simulação	10080 min	**Vetor de Pesos**	[0.3830, 0.2317, 0.1861, 0.1350, 0.0642]
Provedores de Nuvem	10	**Núm. de Participações**	10
Empresas na OV	5 - 25	**Núm. de Execuções**	10
Ope. da Arquitetura	100 - 200		

Fonte: Produção do próprio autor.

Inicialmente foi definido que dez provedores de nuvem estão presentes no repositório de dados da arquitetura e podem disponibilizar seus recursos para que os parceiros de negócio da OV utilizem durante a fase de operação da OV. Cada provedor de nuvem participou em 10 OVs passadas (histórico de participações) (LEMOS et al., 2014; VIEIRA; ALVES JUNIOR; FIORESE, 2015). Esse histórico refere-se aos valores utilizados para calcular cada indicador de confiança objetiva e subjetiva.

O histórico de dados usado no cálculo do indicador de confiança objetiva é composto pelos valores de cada um dos indicadores de QoS, apresentados na seção 2.4.1, nas participações anteriores em OVs. Esse histórico foi gerado de forma aleatória e para garantir a representatividade estatística desse conjunto de dados, determinou-se o tamanho mínimo amostral (MONTGOMERY; RUNGER, 2002). O tamanho mínimo amostral considerou um intervalo de confiança de 95%, um erro amostral de 5% e uma probabilidade de 2% para cada valor de amostra. Desse modo, cada valor histórico é referente a média aritmética de n valores, definido pelo tamanho mínimo amostral (30 amostras).

Diversos históricos de valores relativos ao QoS, compostos por dez participações em OVs, foram gerados usando algumas distribuições de probabilidade, como linear, exponencial, beta e triangular (MONTGOMERY; RUNGER, 2002). Através disso é possível analisar a aplicação dos fatores de penalização e recompensa no indicador de confiança objetiva, quando um provedor de nuvem apresenta um histórico de participações com maior variabilidade.

Por sua vez, o histórico de *feedbacks* do indicador de confiança subjetiva dos provedores de nuvem foi composto pelos dados reais, ou seja notas para os indicadores de QoS (conjunto de avaliações), presentes na base de dados disponível em Noor et al. (2016b)[1]. Nesse sentido, cada *feedback* é representado por um conjunto de avaliações composto por notas (avaliações) de 0 a 5 para cada indicador de QoS avaliado.

[1] <http://cs.adelaide.edu.au/~cloudarmor/ds.html>

Em algumas simulações, como por exemplo naquelas para obtenção do *overhead* e tempo de resposta médio, diversas OVs foram formadas contendo entre 5 e 25 parceiros de negócio. A quantidade de parceiros de negócio presentes na OV é usada para verificar o efeito de cenários diferentes nos tempos de utilização da arquitetura.

Outro parâmetro definido para a avaliação da arquitetura proposta é o número de requisições à arquitetura de reputação. Durante a fase de operação de uma OV, as requisições à arquitetura de reputação (reputação, lista de reputação e monitoramento), por parte dos membros da OV, são distribuídas uniformemente ao longo do tempo de simulação. Nesse sentido, considerou-se um cenário com 100 e outro com 200 requisições à arquitetura, sendo que 70% são referentes a operações de solicitação de reputação e 30% são relativas a operações de monitoramento. Além disso, considerou-se que na fase de dissolução da OV, cada parceiro de negócio realiza o envio do seu *feedback* referente ao provedor de nuvem utilizado à arquitetura de reputação (módulo RBS da arquitetura).

Os métodos de cálculo adotados no indicador de confiança objetiva e subjetiva de um provedor de nuvem utilizam diferentes pesos de importância para os indicadores de QoS utilizados. Esses pesos são calculados através da manipulação da matriz de julgamento do método multicritério AHP, presente na subseção 4.3.1.2. Essa matriz utiliza a escala de Saaty (SAATY, 1990) para definir a relação de importância pareada entre os indicadores de QoS. Tal relação de importância entre os indicadores de QoS foi definida de forma empírica.

Por fim, o número de execuções de cada simulação no ambiente proposto foi definido como dez repetições, com o propósito de aumentar a relevância estatística dos resultados (LAW, 2007; FREITAS, 2008), e foi considerado um intervalo de confiança de 95% em relação à média na análise dos resultados.

Todas as simulações presentes na análise de resultados foram realizadas no seguinte ambiente computacional: Intel Core i5 2.7 GHz, 8 GB RAM DDR3 utilizando o sistema operacional GNU/Linux distribuição Mint 18 64 bits.

A seção 5.1 apresenta o planejamento das avaliações realizadas. Tal planejamento tem como objetivo descrever as avaliações que serão feitas, parâmetros utilizados e os resultados esperados.

5.1 PLANEJAMENTO DE AVALIAÇÕES

O Módulo de Agregação é avaliado em função dos indicadores de confiança objetiva, subjetiva e a reputação dos provedores de nuvem na seção 5.2. A avaliação do indicador de confiança objetiva compreende a análise dos fatores de penalização e recompensa quando submetidos à vários históricos objetivos gerados por diferentes distribuições de probabilidade. Nesse caso, espera-se que históricos com maiores variações sejam mais penalizados do que recompensados.

A avaliação do indicador de confiança subjetiva será composta pela análise do fator de credibilidade em conjuntos de *feedbacks* normais e maliciosos. No conjunto de *feedbacks* normal, cada parceiro de negócio envia *feedbacks* sem apresentar conteúdo e comportamento malicioso. No conjunto de *feedbacks* malicioso, cada parceiro de negócio envia uma determinada quantidade aleatória de *feedbacks* maliciosos (simula ataques). Para realizar essa avaliação diversas OVs são simuladas e os *feedbacks* fornecidos pelos parceiros de negócio da OV aos provedores de nuvem são coletadas. Dessa forma, pode-se calcular o valor atualizado do indicador de confiança subjetiva.

A avaliação da reputação em um primeiro caso será analisada através dos valores históricos objetivos e subjetivos presentes no repositório de dados. Através disso, os valores dos indicadores de confiança objetiva e subjetiva são calculados e por conseguinte a reputação dos provedores de nuvem é calculada usando duas configurações de pesos para os indicadores de confiança. Em um segundo caso, o método de cálculo do valor de reputação da arquitetura proposta será comparado com o método utilizado no sistema de reputação Beta (JØSANG; ISMAIL, 2002). A comparação será realizada através de dois conjuntos de dados: normal e malicioso. Os conjuntos são compostos pelo histórico e valores monitorados de QoS e *feedbacks* dos parceiros de negócio. No entanto, o conjunto malicioso, apresenta *feedbacks* gerados através de OVs em que os parceiros de negócio apresentam comportamento malicioso, ou seja, ataques de colusão de avaliações e de avaliações injustas são efetuados. Através disso, pretende-se verificar o funcionamento dos dois métodos de cálculo quando submetidos a esses conjuntos.

O desempenho da arquitetura de reputação será avaliado na seção 5.3, sendo composto pelas avaliações: (i) tempo de resposta de cada operação disponibilizada pela arquitetura, como, monitoramento, cálculo e retorno da reputação e envio de *feedbacks*; (ii) *overhead* de utilização da arquitetura e (iii) análise de escalabilidade. Para realizar as avaliações i e ii, diversas OVs com tamanhos diferentes serão simuladas, contendo entre 5 e 25 parceiros de negócio. Em cada OV simulada, os provedores de nuvem são alocados de forma aleatória, seguindo uma distribuição uniforme, para

cada parceiro de negócio. Ainda, em cada simulação realizada, considerou-se um cenário com 100 e 200 requisições à arquitetura, conforme mencionado nos parâmetros da simulação. Portanto, por meio das avaliações planejadas, pretende-se analisar a aplicação da arquitetura de reputação em OVs com diferentes tamanhos, bem como verificar o tempo de resposta de cada operação e o *overhead* de utilização da arquitetura.

A análise de escalabilidade das operações da arquitetura (iii) será realizada através da simulação de diversas OVs com diferentes quantidades de parceiros de negócio, variando entre 5 e 100. Além disso, serão utilizados três cenários de avaliação apresentados no Quadro 2.

Quadro 2 – Cenários de avaliação da análise de escalabilidade

Cenário	**Descrição**
Cenário 1	Quantidade fixa de provedores de nuvem (10 provedores)
Cenário 2	Quantidade igual de parceiros e provedores de nuvem (ex: 20 parceiros usam recursos de 20 provedores de nuvem)
Cenário 3	Quantidade variável de provedores de nuvem (1:n), ou seja, um provedor pode disponibilizar seus recursos para mais de um parceiro de negócio da OV

Fonte: Produção do próprio autor.

Na análise de escalabilidade o tempo de resposta é considerado como métrica de avaliação. Desse modo, as operações relacionadas à requisição do valor de reputação (um provedor de nuvem), requisição da lista de reputação (valor de reputação de todos os provedores usados na OV) e envio de *feedbacks* são analisadas. Por fim, espera-se identificar o comportamento de cada operação em relação a quantidade de parceiros de negócio presentes na OV bem como os provedores de nuvem usados.

5.2 MÓDULO DE AGREGAÇÃO

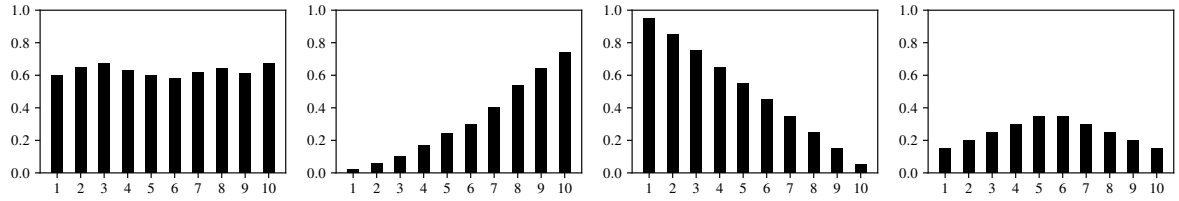
O Módulo de Agregação tem como principal objetivo realizar o cálculo do valor da reputação dos provedores de nuvem no contexto da OV, utilizando dois indicadores históricos de confiança: objetivo e subjetivo. Desse modo, os resultados de avaliação apresentados nesta seção, são divididos da seguinte forma:

- Indicador de Confiança Objetiva: avaliação do fator de penalização e recompensa quando aplicado em diversos conjuntos históricos gerados de acordo com diferentes distribuições de probabilidade;
- Indicador de Confiança Subjetiva: análise do indicador de confiança subjetiva quando aplicado a um conjunto de *feedbacks* normais e maliciosos;
- Reputação: comparação do valor de reputação gerado pela arquitetura proposta em relação a outro método de cálculo de reputação disponível no sistema de reputação Beta (JØSANG; ISMAIL, 2002).

5.2.1 Indicador de Confiança Objetiva

A aplicação dos fatores de penalização e recompensa no cálculo do indicador de confiança objetiva é analisada nesta subseção. Para possibilitar essa análise, vários históricos de valores relativos aos indicadores de QoS, especificados na seção 2.4.1, foram gerados. Os históricos foram gerados através de algumas distribuições de probabilidade, apresentadas na Figura 18, sendo elas: linear, exponencial crescente, beta e triangular (MONTGOMERY; RUNGER, 2002). Essas distribuições foram escolhidas para verificar qual é o impacto da variabilidade do conjunto histórico de dados durante o cálculo dos fatores de penalização e recompensa e consequentemente na geração do valor do indicador de confiança objetiva.

Figura 18 – Distribuições de probabilidade usadas na geração dos valores de QoS

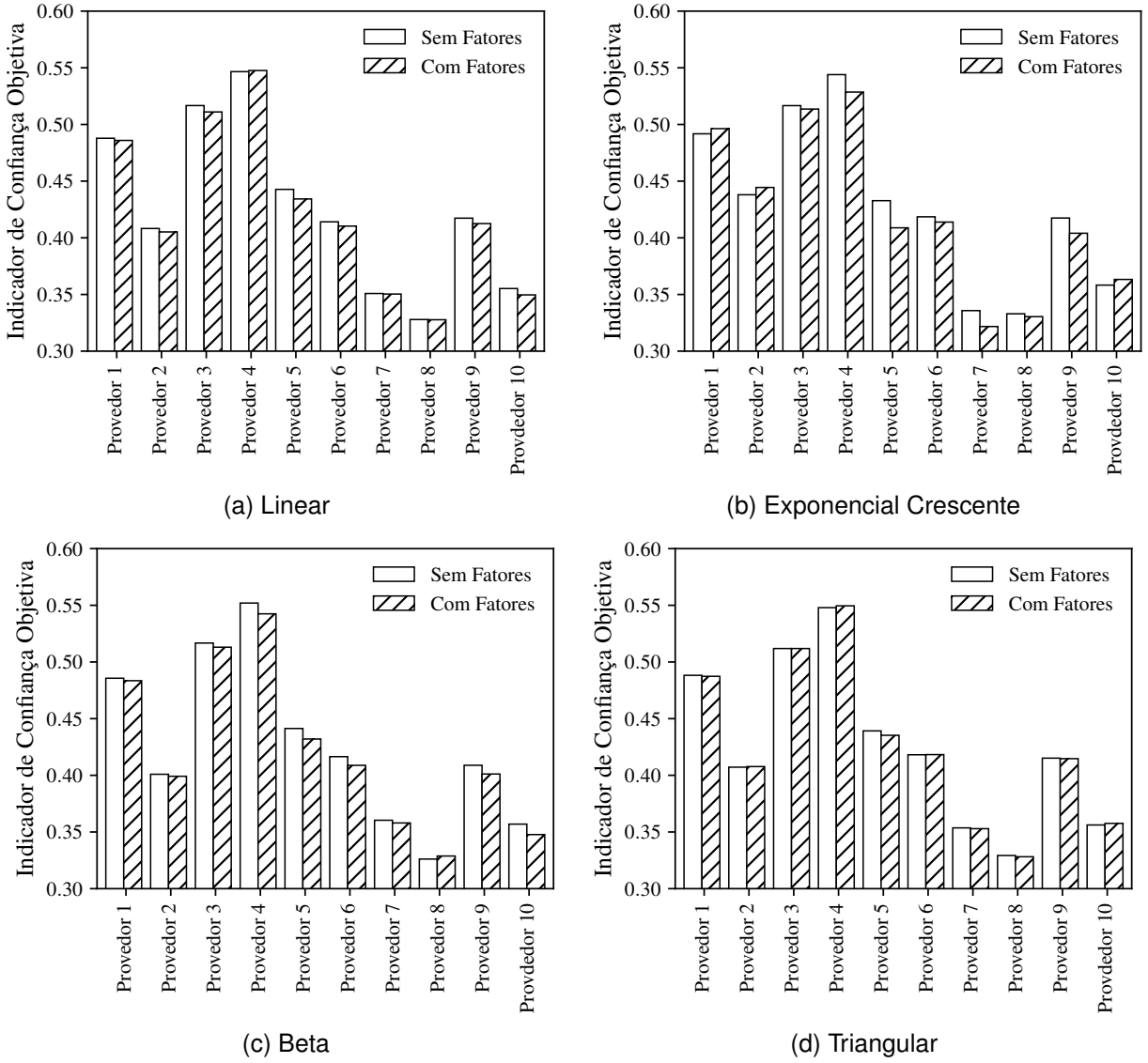


(a) Linear (b) Exp. Crescente (c) Beta (d) Triangular

Fonte: Produção do próprio autor.

Desse modo, os gráficos presentes na Figura 19 apresentam os resultados da utilização dos fatores de penalização e recompensa no cálculo do indicador de confiança objetiva para cada distribuição de probabilidade mencionada. Os resultados apresentados consideram duas alternativas: (i) **Sem Fatores**: o indicador de confiança objetiva é calculado sem utilizar os fatores de penalização e recompensa e (ii) **Com Fatores**: nesse caso os fatores de penalização e recompensa são utilizados.

Figura 19 – Análise do indicador de confiança objetiva



(a) Linear

(b) Exponencial Crescente

(c) Beta

(d) Triangular

Fonte: Produção do próprio autor.

Através dos resultados apresentados, pode-se notar que os valores do indicador de confiança objetiva gerados através de uma distribuição linear e triangular não apresentam diferenças tão relevantes entre as alternativas. Nessas distribuições de probabilidade, as participações históricas não apresentaram tanta variabilidade afe-

tando o cálculo da eficiência relativa e interferindo no cálculo dos fatores de penalização e recompensa. Assim, pode-se dizer que devido aos valores históricos estarem presentes dentro da margem aceitável (apresentada na seção 4.3.1.2) houve mais recompensa do que penalização em relação ao histórico.

O mesmo caso não pode ser observado em relação aos resultados alcançados, quando os valores históricos objetivos (valores dos indicadores de QoS) seguem as distribuições de probabilidade exponencial e beta, pois apresentam uma maior variabilidade, impactando no cálculo da eficiência relativa e na confiança multicritério particularmente nos fatores de penalização e recompensa, e consequentemente no valor resultante do indicador de confiança objetiva. Nesse caso, nota-se que a maioria dos provedores de nuvem tiveram o valor do indicador de confiança objetiva reduzido quando foram aplicados os fatores de penalização e recompensa, como por exemplo, para os dados referentes à distribuição exponencial, nota-se o provedor 7 (0.3357 para 0.3217) e o provedor 5 (0.4327 para 0.4088).

Assim, conclui-se que um determinado provedor de nuvem que apresente maiores variações em seu histórico de participações em OVs apresentará uma menor eficiência relativa e sofrerá mais penalizações em relação ao seu comportamento histórico.

5.2.2 Indicador de Confiança Subjetiva

Esta seção tem como objetivo avaliar a aplicação do fator de credibilidade no cálculo do indicador de confiança subjetiva, quando submetido a conjunto de dados que apresentam *feedbacks* normais e maliciosos.

Assim, para a realização dessa avaliação, diversas OVs foram formadas para simular a existência de dois cenários de coleta de *feedbacks*: normal e malicioso. Dessa forma, as OVs são compostas por dez parceiros de negócio que utilizaram os recursos de cinco provedores de nuvem (1, 2, 3, 4 e 10). Os provedores de nuvem, disponíveis no repositório de dados da arquitetura, são alocados a cada parceiro de negócio da OV de forma aleatória, seguindo uma distribuição de probabilidade uniforme, pois considerou-se que todos apresentam a mesma capacidade no fornecimento de recursos para colaborar com o atendimento da oportunidade de negócio da OV.

Os parceiros de negócio colaboraram entre si e utilizaram os recursos dos provedores de nuvem. Assim, no final da OV (fase de dissolução), a arquitetura de reputação recebe os *feedbacks* que foram fornecidos pelos parceiros de negócio, de acordo com os cenários mencionados anteriormente (normal e malicioso). Desse modo, dois conjuntos de *feedbacks* são gerados e analisados:

- **Conjunto de *feedbacks* normal**: considerou-se que os parceiros de negócio

da OV avaliaram subjetivamente, sem conteúdo e comportamento malicioso, os provedores de nuvem com os quais interagiram, ou seja, os *feedbacks* não são provenientes de ataques gerados pelos usuários/parceiros da OV;

- **Conjunto de *feedbacks* malicioso**: nesse caso, os parceiros de negócio da OV enviaram avaliações com conteúdo e comportamento malicioso, ou seja, cada parceiro de negócio enviou uma quantidade aleatória de avaliações à arquitetura de reputação, justamente para simular as duas formas de ataque: colusão de avaliações e avaliações injustas. Para tanto, dois cenários são analisados: quantidade fixa e variável de *feedbacks* maliciosos.

Para efeitos de relevância estatística, a OV mencionada em cada cenário foi simulada dez vezes. Dessa forma, para efeitos de cálculo do indicador de confiança subjetiva utilizaram-se os valores agregados subjetivos ($Q_c(c, s, z)$) gerados pelos *feedbacks* dos usuários (conjuntos normal e malicioso), juntamente com os valores agregados subjetivos gerados pelos *feedbacks* disponíveis no repositório de dados, que representam os dados históricos de participações anteriores em OVs.

No cálculo do indicador de confiança subjetiva considerou-se duas alternativas:

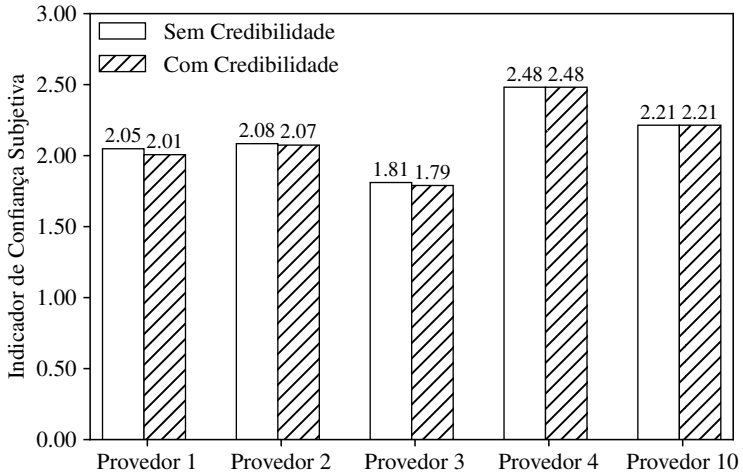
- **Sem Credibilidade**: o fator de credibilidade é desconsiderado no cálculo do indicador de confiança subjetiva;

- **Com Credibilidade**: nesse caso, o fator de credibilidade é usado. Considerou-se que os subfatores que identificam os ataques (colusão e avaliações injustas) apresentam a mesma importância, ou seja, os pesos são iguais.

Desse modo, no primeiro conjunto de *feedbacks* normal, os parceiros de negócio avaliaram subjetivamente cada provedor de nuvem, em que cada *feedback* teve seu conjunto de avaliações (notas para os indicadores de QoS) gerado de forma aleatória através de uma distribuição de probabilidade linear. Nesse conjunto, considerou-se que os *feedbacks* fornecidas pelos parceiros de negócio não apresentam conteúdo nem comportamento malicioso.

A Figura 20 apresenta os resultados para o indicador de confiança subjetiva no conjunto de *feedbacks* normal. Dessa forma, o valor do indicador de confiança subjetiva para cada provedor é calculado usando os *feedbacks* presentes no histórico acrescidos do conjunto normal.

Figura 20 – Indicador de confiança subjetiva no conjunto de *feedbacks* normal



Fonte: Produção do próprio autor.

Por meio dos valores do indicador de confiança subjetiva, percebe-se que nesse cenário de avaliação, por não apresentar *feedbacks* com conteúdo e comportamento malicioso, os valores das alternativas analisadas para os provedores de nuvem são próximos. Isso justifica-se pelo fator de credibilidade, o qual atua com mais eficiência quando ataques são realizados ao valor do indicador, sendo que no caso analisado, o fator de credibilidade manteve um valor próximo a 1.

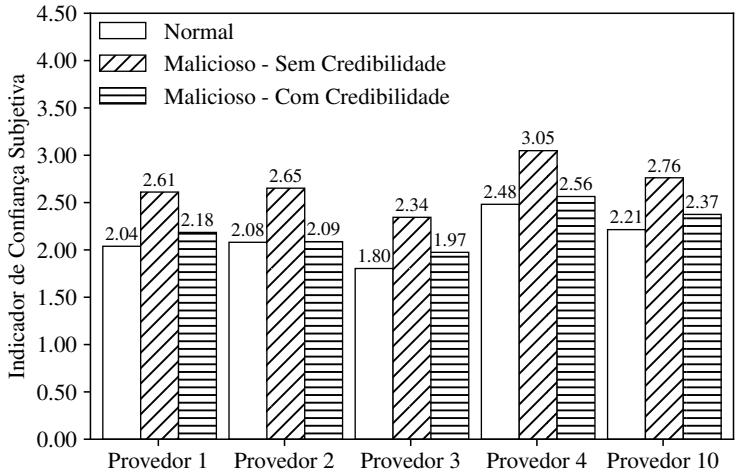
Em contrapartida, no segundo conjunto de *feedbacks*, foi simulado um cenário em que os parceiros de negócio da OV forneceram avaliações com comportamento e conteúdo malicioso. Em que o comportamento refere-se ao ataque de colusão, ou seja, mais *feedbacks* do que o esperado e o conteúdo refere-se aos valores presentes no conjunto de avaliações do *feedback*, por exemplo, muitos *feedbacks* que apresentam valores entre 4 e 5, que são os mais altos valores para as notas dos indicadores de QoS. Nesse caso, o conjunto de *feedbacks* analisado apresenta o propósito de promover o valor do indicador de confiança subjetiva de um provedor de nuvem e consequentemente sua reputação.

Assim, considerou-se dois casos de teste. No primeiro caso, cada parceiro de negócio da OV forneceu uma quantidade aleatória de *feedbacks*, sendo que uma quantidade fixa era maliciosa (50%). Por exemplo, um parceiro qualquer forneceu 30 *feedbacks* dos quais 15 apresentam conteúdo malicioso. No segundo caso, a quantidade de *feedbacks* maliciosos varia entre 0% (nenhuma) e 100% (todos são maliciosos).

Os resultados do primeiro caso são apresentados na Figura 21 e três alternativas são consideradas:

- **Normal**: valor do indicador de confiança subjetiva gerado através do conjunto de *feedbacks* normal apresentado anteriormente;
- **Malicioso – Sem Credibilidade**: o indicador de confiança subjetiva é calculado sem considerar a utilização do fator de credibilidade no conjunto de *feedbacks* maliciosos; e
- **Malicioso – Com Credibilidade**: nesse caso, a utilização do fator de credibilidade é considerada.

Figura 21 – Indicador de confiança subjetiva no conjunto de *feedbacks* malicioso - fixo



Fonte: Produção do próprio autor.

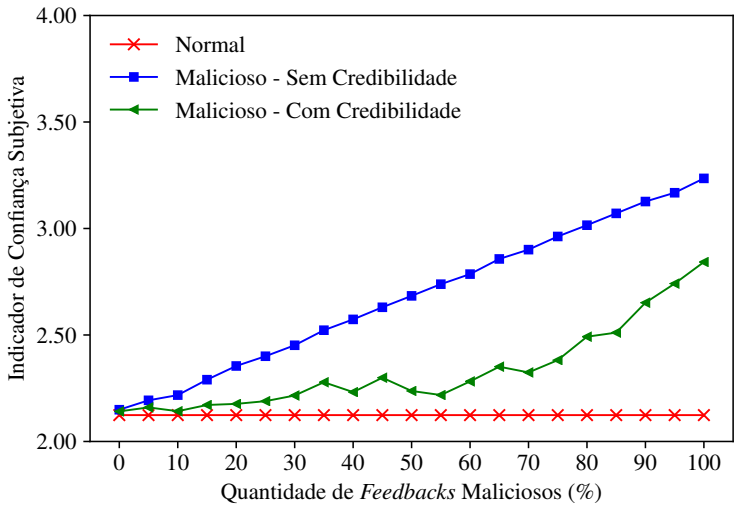
Dessa forma, pelos resultados apresentados, nota-se que o valor do indicador de confiança subjetiva apresenta valores diferentes entre os conjuntos normais e maliciosos de *feedbacks*, principalmente quando a credibilidade não é levada em consideração. Para tratar os ataques ocorridos no conjunto malicioso de *feedbacks*, o fator de credibilidade é aplicado. Assim, em comparação com o conjunto de *feedbacks* normal, nota-se que a alternativa que considera a credibilidade no conjunto malicioso, apresenta os valores do indicador de confiança subjetiva mais próximos do que seria o comportamento normal dos *feedbacks* (sem ataques de colusão e avaliações injustas) emitidos pelos membros da OV que utilizaram os provedores de nuvem.

Ainda, no segundo conjunto de avaliações, analisou-se uma outra situação em que os parceiros de negócio enviaram uma quantidade variável de *feedbacks* maliciosos. Esse cenário foi idealizado para analisar o comportamento do fator de credibilidade em função da quantidade de *feedbacks* maliciosos. Para isso os resultados apresentados na Figura 22 referem-se a média aritmética do valor do indicador de

confiança subjetiva dos cinco provedores de nuvem (1, 2, 3, 4 e 10) em relação a quantidade de *feedbacks* maliciosos (representadas por porcentagem). Nesse sentido, cada linha do gráfico pode ser entendida como:

- **Normal**: o valor médio é calculado através dos valores dos indicadores subjetivos dos provedores usando o conjunto de *feedbacks* normal;
- **Malicioso - Sem Credibilidade**: nesse caso, o conjunto malicioso é usado e o fator de credibilidade não é considerado no cálculo do indicador;
- **Malicioso - Com Credibilidade**: conjunto malicioso é usado e o fator de credibilidade é considerado.

Figura 22 – Indicador de confiança subjetiva no conjunto de *feedbacks* malicioso - variável



Fonte: Produção do próprio autor.

Por meio dos resultados apresentados percebe-se que quando a porcentagem de *feedbacks* maliciosos aumenta, a média do indicador de confiança subjetiva sem a utilização do fator de credibilidade também aumenta proporcionalmente quando o fator de credibilidade não é considerado. Por exemplo, o valor médio do indicador subjetivo para o caso analisado, é de 2.1491 para 0% de *feedbacks* maliciosos, apresentando um valor próximo a média normal (2.1238), e finalizou em 3.2352 quando todos os *feedbacks* são considerados como maliciosos.

Para auxiliar no tratamento quando um conjunto de *feedbacks* com comportamento e conteúdo malicioso é enviado à arquitetura de reputação, o fator de credibilidade é aplicado para minimizar os efeitos dos ataques no valor do indicador de

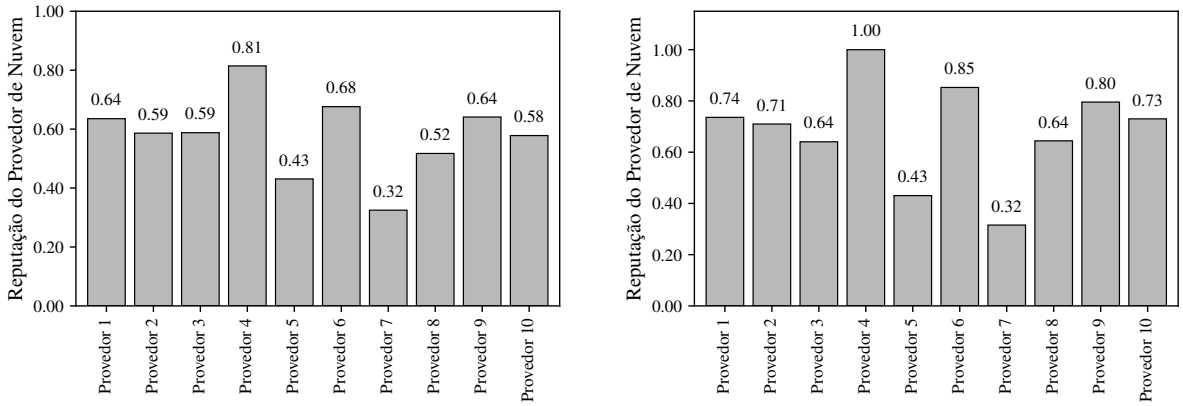
confiança subjetiva, ou seja, pondera o valor agregado subjetivo de cada *feedback* com o valor do fator de credibilidade. Através disso, pode-se notar que o valor médio do indicador com a utilização do fator de credibilidade é menor em relação ao que desconsidera a credibilidade dos *feedbacks* em ambos os casos, justamente para tentar representar o que seria o comportamento normal dos *feedbacks* fornecidos pelos membros da OV aos provedores de nuvem.

5.2.3 Reputação

Esta seção tem por objetivo apresentar os resultados relacionados ao valor da reputação dos provedores de nuvem. Em um primeiro caso, o valor da reputação referente ao histórico de participações de cada provedor de nuvem é apresentado. Em um segundo caso, o método de cálculo do valor da reputação é comparado com o método utilizado no sistema de reputação Beta (JØSANG; ISMAIL, 2002).

Através do ambiente de integração proposto, a reputação dos provedores de nuvem é calculada usando dois indicadores de confiança objetiva e subjetiva. Desse modo, para o cálculo do indicador de confiança objetiva considerou-se os valores históricos de QoS gerados através de uma distribuição de probabilidade linear. O indicador de confiança subjetiva de cada provedor de nuvem foi calculado usando os dados apresentados na seção 5.2.2 referentes ao conjunto de *feedbacks* normal. Além disso, no cálculo da reputação, definiu-se empiricamente duas configurações de pesos, sendo elas: A) com 0.85 para o indicador de confiança objetiva e 0.15 para o indicador de confiança subjetiva e B) com 0.75 para o indicador de confiança objetiva e 0.25 para o indicador de confiança subjetiva. Os resultados dessa avaliação são apresentados na Figura 23.

Figura 23 – Valores de reputação dos provedores de nuvem



(a) Configuração de peso A

(b) Configuração de peso B

Fonte: Produção do próprio autor.

Assim, percebe-se que o cálculo da reputação dos provedores de nuvem é dependente do peso atribuído a cada indicador de confiança. Dessa forma, os provedores de nuvem que apresentam maiores valores no indicador objetivo (ou seja, são eficientes e apresentam uma boa pontuação multicritério) apresentam os maiores valores de reputação.

Em um cenário real, os pesos devem ser escolhidos pelo gestor da OV para definir qual indicador é mais relevante no cálculo da reputação. Dependendo da combinação dos pesos escolhidos, por exemplo, um cenário que priorize as avaliações subjetivas, a aplicação do fator de credibilidade durante o cálculo do indicador de confiança subjetiva é usada com grande proveito. Caso ocorram ataques com o objetivo de promover ou prejudicar o valor do indicador de confiança subjetiva e consequentemente a reputação, o fator de credibilidade atua como um meio de tratamento dos efeitos decorrentes dos ataques. Dessa forma, o fator de credibilidade previne uma situação em que provedores que estavam com uma reputação baixa em OVs passadas tenham sua reputação maliciosamente aumentada e sejam selecionados em virtude do seu valor de reputação, fornecendo um serviço que não é condizente com as avaliações recebidas.

Por fim, na seção 5.2.3.1, o método de cálculo da reputação da arquitetura proposta é comparado com o método utilizado em outro sistema de reputação, o Beta (BRS) (JØSANG; ISMAIL, 2002).

5.2.3.1 Comparação entre os Métodos de Cálculo da Reputação

A comparação dos valores de reputação gerados pelo método de cálculo da arquitetura proposta com outros trabalhos é dificultada pelas diferentes características adotadas nos métodos desses outros trabalhos, pois a arquitetura proposta é aplicada em OVs baseadas na nuvem e calcula a reputação através da combinação de dois indicadores de confiança: objetiva e subjetiva.

Entretanto, é possível comparar o método de cálculo da reputação da arquitetura proposta com o método usado no sistema de reputação Beta (BRS) (JØSANG; ISMAIL, 2002). O sistema de reputação BRS foi desenvolvido inicialmente para *e-commerce*, porém pode ser aplicado a qualquer cenário e serve de base para muitas pesquisas, sendo largamente utilizado (HALLER, 2009), conforme pode ser visto em Josang, Hayward e Pope (2006), Momani, Aboura e Challa (2007), Ganeriwal, Balzano e Srivastava (2008) e Arshad e Moessner (2011).

O método de cálculo presente no BRS (JØSANG; ISMAIL, 2002) utiliza a função de densidade de probabilidade da distribuição Beta para calcular a reputação, através da contagem de transações/interações positivas e negativas. O valor da reputação,

no sistema BRS, é representado pela Equação 5.1. Esse valor é calculado através de uma função de expectativa (valor esperado, $E(\varphi\,(p|r,s)\,)$) gerado pela distribuição Beta, que é equivalente a uma razão que considera a contagem de transações/interações positivas (r) e negativas (s) (JØSANG; ISMAIL, 2002; JØSANG; ISMAIL; BOYD, 2007).

$$Rep(r,s) = E(\varphi(p|r,s)) = \frac{r-s}{r+s+2} \tag{5.1}$$

De modo a exemplificar o cálculo da reputação pelo BRS, considere que um provedor de nuvem em suas participações passadas em OVs, contabiliza 10 transações/interações positivas (r) e 5 negativas (s) realizadas com os parceiros de negócio. Assim, conforme a Equação 5.1, a reputação desse provedor é 0.2941. Dessa forma, nota-se que os parceiros de negócio da OV avaliam as interações realizadas com os provedores de nuvem de forma qualitativa, seja positiva ou negativa, e a reputação é calculada através da quantidade de interações para cada forma.

Para efetuar a comparação entre os valores de reputação calculados pelos dois métodos, deve-se adaptar os dados usados pelo método da arquitetura proposta para a aplicação no BRS. O método da arquitetura proposta usa os valores de dois indicadores de confiança: objetiva e subjetiva para o cálculo da reputação, enquanto o BRS utiliza a contagem de interações positivas e negativas, sendo que essas interações são avaliadas pelos usuários.

Dessa forma, para calcular a reputação via BRS, deve-se adaptar os valores dos indicadores confiança objetiva e subjetiva para possibilitar a contagem de interações positivas e negativas. Nesse sentido, na comparação entende-se que uma interação objetiva refere-se ao valor do indicador de confiança objetiva em uma participação em OV. Desse modo, pode representar n valores, ou seja, n interações que são referentes à participações anteriores em OVs, que além do histórico incluem os valores de QoS atuais, ou seja, que foram obtidos através do monitoramento. Nesse caso, no valor da interação objetiva, somente é considerado o valor da eficiência relativa e contribuição multicritério sem os fatores de penalização e recompensa.

Uma interação subjetiva tem um valor agregado subjetivo associado que é calculado sobre os valores das avaliações subjetivas (*feedback*). Esse *feedback* é fornecido pelo parceiro de negócio na dissolução de uma OV qualquer. Desse modo, um *feedback* é referente a uma ou mais interações em participações nas OVs.

Nesse sentido, a Tabela 3 apresenta os valores limite que definem o que é considerado uma interação positiva e negativa para o cálculo da reputação via BRS, possibilitando assim a contagem das interações.

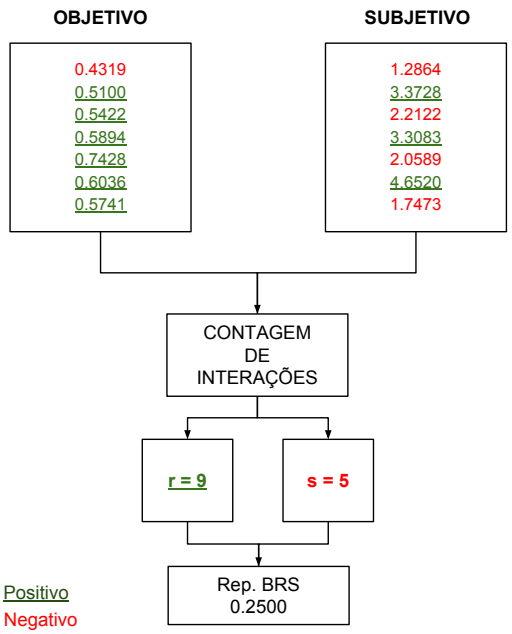
Tabela 3 – Representação das interações positivas ou negativas em relação aos indicadores de confiança objetiva e subjetiva

	Negativa	Positiva
Interação Objetiva	$[0.0, 0.5]$	$]0.5, 1.0]$
Interação Subjetiva	$[0.0, 2.5]$	$]2.5, 5.0]$

Fonte: Produção do próprio autor.

De modo a ilustrar o procedimento de comparação realizado com o método proposto no BRS considere a Figura 24. A Figura apresenta os dados referentes ao indicador de confiança objetiva nas participações passadas em OV, em que cada valor é referente a uma interação em OV, ou seja uma participação de um provedor de nuvem qualquer, incluindo os valores obtidos com o monitoramento. Além disso, apresenta os valores agregados subjetivos gerados através dos *feedbacks* fornecidos pelos parceiros de negócio para um provedor de nuvem qualquer. Nesse sentido, a contagem das interações positivas (r) e negativas (s) é realizada e a reputação é calculada pelo método do BRS. Portanto, para o exemplo apresentado, a reputação (BRS) desse provedor de nuvem é 0.25.

Figura 24 – Exemplo dos dados usados para comparação com o método do Beta



Fonte: Produção do próprio autor.

De modo a realizar a comparação entre os valores de reputação calculados pelos dois métodos, diversas OVs foram formadas para coletar os valores referentes a dois conjuntos de dados: normal e malicioso. As OVs foram compostas por dez parceiros de negócio que utilizaram os recursos de cinco provedores de nuvem (1, 2, 3, 4, e 10). Os provedores de nuvem foram alocados de forma aleatória, seguindo uma distribuição uniforme, a cada parceiro da OV, pois considerou-se que todos apresentam a mesma capacidade de fornecer recursos para o processo de colaboração da OV.

Assim, ambos os conjuntos de dados mencionados são compostos de valores históricos e monitorados de QoS e *feedbacks*. Os valores históricos de QoS, referem-se as participações do provedor de nuvem em OVs já finalizadas (histórico). O histórico de participações foi gerado através de uma distribuição de probabilidade linear, mencionado no capítulo 5. Na abordagem do BRS, considera-se que cada participação em OV representa uma interação objetiva, conforme apresentado no exemplo. Além disso, os valores de QoS monitorados são obtidos através das OVs formadas no ambiente de integração. Desse modo, obtém-se a contagem de interações objetivas que é referente tanto ao histórico como ao desempenho atual desse provedor (monitorado).

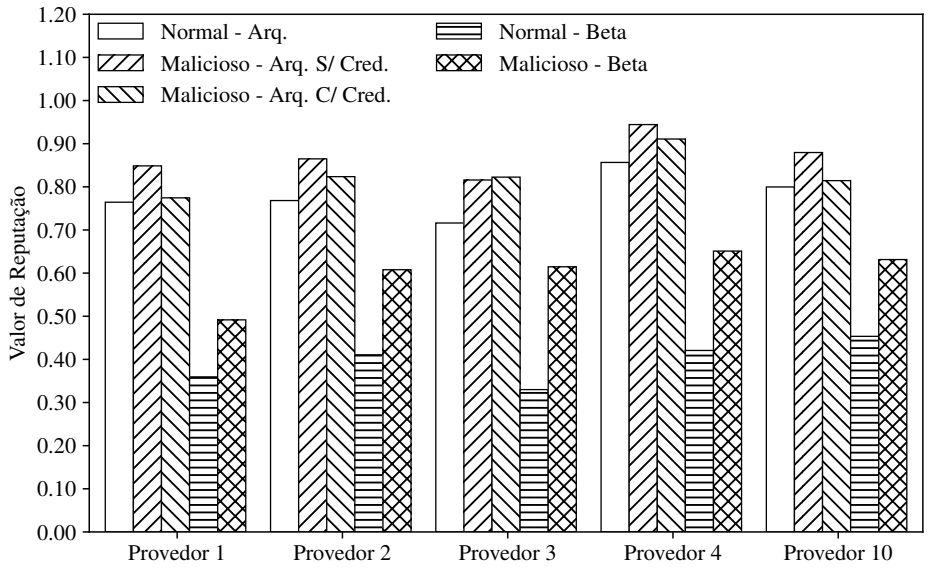
Os *feedbacks* referem-se as avaliações dadas pelos parceiros de negócio da OV nas participações passadas. A diferença entre os conjuntos de dados normal e malicioso, consiste na forma como os *feedbacks* são fornecidos. No conjunto normal considera-se que os *feedbacks* não apresentam conteúdo e comportamento malicioso. Em contrapartida, no conjunto malicioso, os parceiros da OV enviam diversas avaliações com o propósito de promover ou prejudicar um provedor de nuvem, ou seja, ataques de colusão e avaliações injustas são efetuados.

Os resultados referentes à comparação dos valores de reputação são apresentados na Figura 25. Para o método de cálculo da arquitetura proposta consideraram-se pesos para cada indicador de confiança, sendo 0.85 para o objetivo e 0.15 para o subjetivo. Dessa forma, as alternativas usadas na comparação, são entendidas como:

- **Normal - Arq.**: cálculo da reputação pelo método da arquitetura proposta no conjunto de dados normal;
- **Malicioso - Arq. S/ Cred.**: cálculo da reputação pela arquitetura proposta não considerando o fator de credibilidade das avaliações no conjunto malicioso;
- **Malicioso - Arq. C/ Cred.**: similar ao anterior, porém considera o fator de credibilidade;
- **Normal - Beta**: reputação calculada pelo método do sistema de reputação beta (BRS) no conjunto de dados normal;

- **Malicioso - Beta**: reputação calculada pelo método do sistema de reputação beta (BRS) no conjunto de dados malicioso.

Figura 25 – Comparação dos valores de reputação gerados pelos métodos da arquitetura proposta x sistema beta



Fonte: Produção do próprio autor.

Através dos resultados apresentados é possível notar que as alternativas referentes a arquitetura de reputação, no conjunto de dados malicioso, fornecem meios para tratar ataques que ocorrem ao indicador de confiança subjetiva dos provedores de nuvem. Dessa forma, a aplicação do fator de credibilidade nos valores subjetivos agregados é usada com grande proveito. Assim, percebe-se que o valor de reputação considerando o uso do fator de credibilidade (Malicioso - Arq. C/ Cred) é menor do que na outra opção (Malicioso - Arq. S/ Cred), pois ataques de colusão e avaliações injustas foram promovidos. Logo, durante o cálculo do indicador subjetivo, o valor agregado subjetivo de cada *feedback* fornecido é ponderado pelo valor do fator de credibilidade do parceiro de negócio, impactando no cálculo da reputação pelo método apresentado na arquitetura proposta.

Porém, o mesmo não acontece no método proposto pelo sistema beta (BRS). Pois, o BRS não apresenta um fator ou mecanismo que identifique quando ataques são promovidos, ou seja, não identifica quando um provedor de nuvem tem muitas (além do considerado normal) interações avaliadas como positivas ou negativas. Dessa forma, não considera o fator de credibilidade do usuário que está avaliando a interação realizada com o provedor de nuvem. Isso nota-se, por exemplo, no valor de

reputação calculado para o provedor 3 em que no conjunto normal apresenta o valor de 0.3300, enquanto no malicioso o valor é 0.6146.

Por fim, nota-se que o método de cálculo da reputação adotado no sistema BRS pode ser adaptado e aplicado a qualquer contexto além do *e-commerce*. No entanto, percebe-se que os dois métodos comparados (arquitetura e BRS) apresentam diferenças na forma como a reputação é calculada e também nos valores de reputação. No método presente na arquitetura proposta, a reputação é calculada através da agregação dos valores de dois indicadores de confiança objetiva e subjetiva por meio de uma abordagem ponderada. Já no método do BRS, a reputação é calculada através da quantidade de interações/transações positivas e negativas referentes à alguma entidade. Dessa forma, a diferença observada entre os valores pode ser explicada pela forma como a reputação é calculada no BRS, pois não considera o valor de cada indicador e sim a quantidade de interações. Além disso, o método adotado no BRS, não considera o fator de credibilidade dos usuários que avaliam as interações ou transações com as entidades, desse modo, permitindo que uma entidade receba muitas avaliações positivas ou negativas em sequência, para promover ou prejudicar a reputação de uma entidade.

5.3 DESEMPENHO DA ARQUITETURA DE REPUTAÇÃO

Esta seção apresenta os resultados relativos ao desempenho da arquitetura de reputação quando utilizada pela OV. Os resultados contemplam a análise do tempo de resposta de cada operação disponibilizada pela arquitetura, o *overhead* de utilização e a análise de escalabilidade.

5.3.1 Tempo de Resposta

O tempo de resposta de cada operação da arquitetura é medido em milissegundos e é compreendido pelo tempo de troca de mensagens entre o solicitante e arquitetura, bem como o tempo de processamento para atender a operação.

Desse modo, na análise do tempo de resposta, considerou-se as seguintes operações da arquitetura proposta: (i) Requisição do valor de reputação de um provedor de nuvem (PN); (ii) Requisição da lista dos valores de reputação de todos os PNs que já participaram de alguma OV; (iii) Envio de avaliação (*feedback*) do parceiro de negócio da OV em relação ao PN usado e (iv) Requisição de monitoramento dos indicadores de QoS de um PN ou de todos os provedores utilizados na OV.

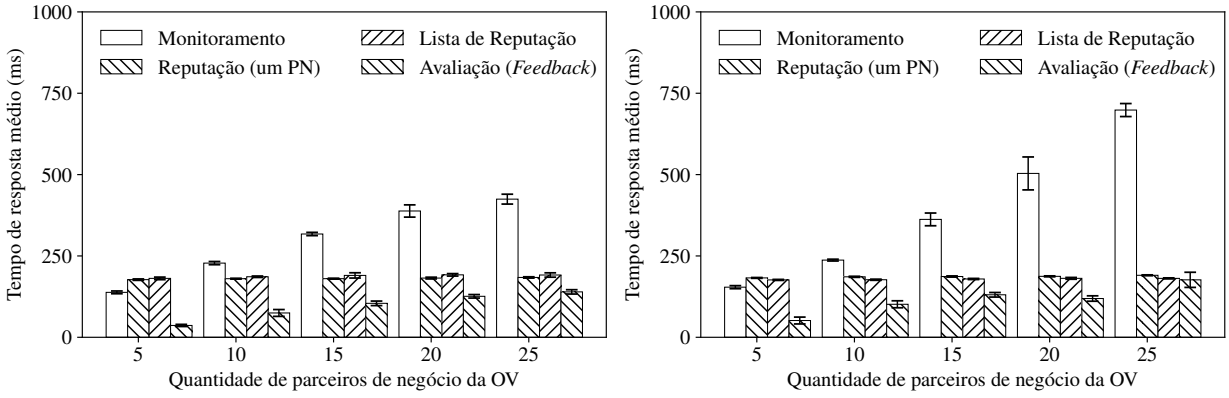
Diversas OVs foram simuladas contendo entre 5 e 25 parceiros de negócio e em cada OV, durante a fase de operação, os parceiros de negócio realizaram requisições de operações à arquitetura, totalizando um cenário com 100 e 200 requisições,

conforme mencionado no planejamento das avaliações. Além disso, para cada OV formada, considerou-se os recursos disponibilizados pelos dez provedores de nuvem disponíveis no repositório de dados, e esses recursos foram alocados de forma aleatória, seguindo uma distribuição uniforme, para cada parceiro de negócio da OV. Dessa forma, a quantidade de provedores de nuvem se manteve fixa durante as simulações realizadas.

As requisições à arquitetura proposta são distribuídas através de uma abordagem consistente, ou seja, 70% referem-se à requisições de reputação (valor de reputação de um PN e lista de reputação) e 30% são relativas ao monitoramento de QoS. Ainda, considerou-se que cada parceiro de negócio presente na OV avaliou o provedor de nuvem que disponibilizou serviços/recursos.

Nesse sentido, a Figura 26 apresenta o tempo médio de resposta para cada operação da arquitetura durante o atendimento da oportunidade de colaboração da OV, considerando os dois cenários mencionados, 100 requisições à arquitetura (Figura 26 a) e 200 requisições à arquitetura (Figura 26 b).

Figura 26 – Tempo de resposta médio para cada operação da arquitetura



(a) 100 requisições

(b) 200 requisições

Fonte: Produção do próprio autor.

Em relação aos resultados apresentados, nota-se que o tempo de resposta da operação de envio de avaliações (*feedbacks*), ou seja quando um membro da OV fornece seu *feedback* em relação à um provedor de nuvem, está associado com a quantidade de parceiros de negócio presentes na OV. Dessa forma, em cenários que apresentam mais parceiros de negócio, naturalmente mais avaliações são enviadas no final na dissolução da OV, pois houve uma maior quantidade de interações. Assim, percebe-se que o tempo de resposta é maior devido a quantidade de requisições que

a arquitetetura recebe, ou seja, é necessário receber os *feedbacks* e armazená-los no repositório de dados, através da abordagem centralizada adotada via RBS. Por fim, o tempo de resposta dessa operação é composto na sua maior parte pelo processamento, ou seja, o armazenamento no repositório, sendo que em média o tempo despendido com a comunicação (troca de mensagens entre o membro da OV e o RBS) é de 8 ms.

A operação de monitoramento, quando usada na OV, realiza a troca de mensagens entre a arquitetura de reputação, nó de monitoramento (módulo de monitoramento), e os recursos/serviços de nuvem utilizados pela OV. Desse modo, a troca de mensagens tem como meta coletar os valores atuais de QoS para que a arquitetura possa armazenar essas informações no repositório de dados.

Em relação aos resultados referentes ao tempo de resposta médio de monitoramento, percebe-se que o tempo de resposta se destaca em relação aos demais tempos em ambos os cenários (100 e 200 requisições). Inicialmente nota-se que o tempo da operação de monitoramento é dependente da quantidade de provedores de nuvem que estão fornecendo seus recursos/serviços para o ambiente da OV. A abordagem de alocação de recursos aleatória, seguindo uma distribuição de probabilidade uniforme, resultou nas seguintes configurações de OVs: 5 parceiros e 3 provedores, 10 parceiros e 5 provedores, 15 parceiros e 7 provedores, 20 parceiros e 8 provedores, e 25 parceiros e 9 provedores. Através disso, é possível observar que em ambos os cenários (100 e 200 requisições) o tempo de resposta da operação de monitoramento aumenta em decorrência do aumento do número de provedores, pois mais alvos necessitam ter o QoS coletado e consequentemente a arquitetura de reputação processa e armazena mais informações.

Em outros cenários que exigem uma maior quantidade de operações, ou seja, mais requisições de operação de monitoramento bem como monitoramento mais constante, o tempo de resposta da operação é maior. Isso pode ser notado por meio dos cenários simulados (100 e 200 requisições (req.)), os quais devido a abordagem consistente adotada, apresentam diferentes quantidades de requisições de monitoramento, sendo 30 operações de monitoramento (cenário com 100 req.) e 60 operações (cenário com 200 req.). Dessa forma, a arquitetura proposta necessita processar e armazenar uma maior quantidade de informações que são geradas em decorrência do aumento das requisições, o que acaba impactando no tempo de resposta dessa operação.

Em ambos os cenários analisados, 100 e 200 requisições, para a operação de monitoramento, o tempo médio de troca de mensagens é de 8 ms, sendo que o restante do tempo de resposta da operação é referente ao processamento, ou seja, compreende a coleta do QoS, envio do QoS monitorado à arquitetura e a atualização

da participação desse provedor de nuvem no repositório de dados. Em um cenário real, a operação de monitoramento pode apresentar um tempo de resposta diferente, pois depende das ferramentas de *hardware* ou *software* utilizadas para essa função.

As operações relacionadas com a reputação, valor de reputação de um PN e lista dos valores de todos os PNs, apresentam um tempo de resposta linear em relação ao número de parceiros de negócio da OV e também da quantidade de requisições recebidas pela arquitetura de reputação. As duas operações de reputação apresentam tempos praticamente semelhantes nos cenários analisados. Isso deve-se ao fato da abordagem adotada no indicador de confiança objetiva (apresentado na subseção 4.3.1), em que adota a eficiência relativa, ou seja, para calcular a eficiência de um provedor é necessário comparar essa eficiência com a eficiência dos outros que estão sendo utilizados na OV, através do DEA, sendo dessa forma necessário obter e processar os históricos de QoS de todos os provedores. Devido a isso, a única diferença existente entre as duas operações, é a sua forma de retorno para o solicitante, na qual uma delas retorna apenas o valor de reputação de um provedor de nuvem, enquanto a outra retorna a lista de valores de reputação de todos os provedores de nuvem (nesse caso, 10 provedores).

Embora a operação de lista de reputação seja mais relevante para a fase de criação da OV, na fase de operação ela também pode ser utilizada, por exemplo quando o gestor da OV necessita substituir um provedor de nuvem ou associar mais um recurso a um parceiro de negócio, dessa forma, pode utilizar a lista de valores de reputação como meio de auxílio ao processo de tomada de decisão.

5.3.2 *Overhead*

Na computação, o *overhead* é visto como um tempo computacional que é exigido para desempenhar alguma tarefa ou incluir uma nova funcionalidade em um *software*, ambiente, entre outros. Nesse trabalho, o *overhead* é usado para calcular o tempo computacional total decorrente da aplicação da arquitetura proposta em uma OV. Ou seja, mensura o tempo médio que é acrescido à operação de uma OV, quando a mesma utiliza as funcionalidades disponibilizadas pela arquitetura, como por exemplo, requisições de reputação, monitoramento, entre outras. Assim, considera o tempo gasto com o processamento das operações e troca de mensagens entre a arquitetura e os solicitantes.

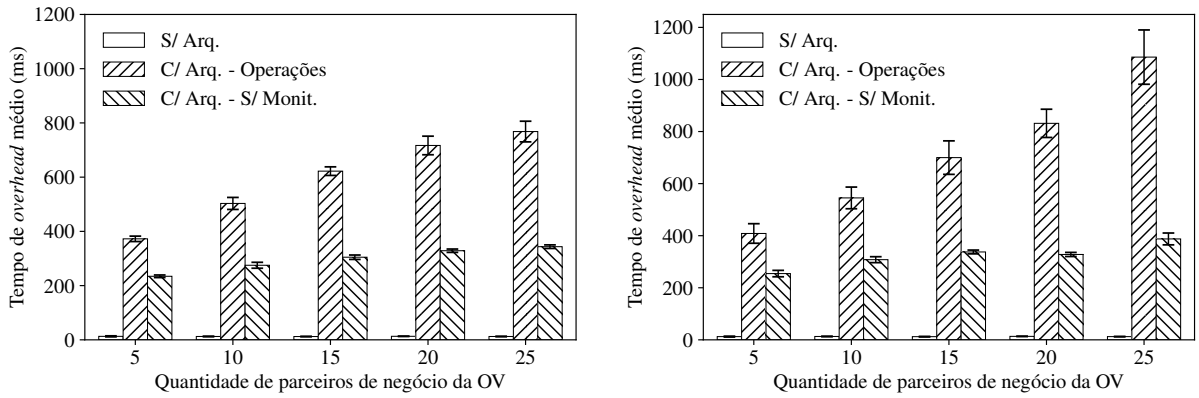
Dessa forma, o *overhead* médio de utilização da arquitetura foi analisado por meio de diversas OVs simuladas com tamanhos diferentes, ou seja, entre 5 e 25 parceiros de negócio, durante uma semana de tempo (86400 s), e também considerando-se que a arquitetura de reputação recebeu 100 e 200 requisições de operações (reputação de um provedor de nuvem e monitoramento), além das requisições de envio de

avaliações (*feedbacks*), realizadas na fase de dissolução da OV por cada parceiro de negócio.

Os resultados do *overhead* médio de utilização, de acordo com as simulações realizadas, são apresentados na Figura 27, considerando 100 requisições (Figura 27 a) e 200 requisições (Figura 27 b). Três configurações foram consideradas para a análise do *overhead*, sendo elas:

- **S/ Arq.**: a arquitetura de reputação não é utilizada na OV. Nesse caso, somente a operação de colaboração entre os parceiros de negócio é considerada, ou seja, não há nenhum *overhead* decorrente da aplicação da arquitetura de reputação. Essa configuração é desenvolvida para efeito de comparação com o *overhead* produzido pela utilização da arquitetura;
- **C/ Arq. - Operações**: utilização da arquitetura de reputação na OV, considerando as operações de requisição do valor de reputação (um provedor), monitoramento de QoS durante a fase de operação da OV e o envio de *feedbacks* na fase de dissolução da OV;
- **C/ Arq. - S/ Monit.**: nesse caso o uso do módulo de monitoramento (operação de monitoramento de QoS) foi desconsiderado no cálculo do *overhead*.

Figura 27 – *Overhead* médio



(a) 100 requisições

(b) 200 requisições

Fonte: Produção do próprio autor.

A opção (S/ Arq.) não considera o uso da arquitetura de reputação na organização virtual, ou seja, a OV é criada, operada e dissolvida sem o suporte das operações disponibilizadas pela arquitetura proposta. Nesse caso, temos o tempo de execução

baseline, ou seja, sem nenhum *overhead* relativo à arquitetura de reputação proposta, sendo que o único tempo gasto é com a operação de colaboração. A operação de colaboração, implementada de forma simulada, é referente à troca de mensagens entre os parceiros de negócio da OV. Ou seja, um parceiro envia uma mensagem para outro, sendo que nessa operação o único tempo existente é para a criação, envio e recebimento da mensagem, considerando uma latência fixa definida no simulador como 10 ms.

Através dos resultados apresentados em ambos os cenários (100 e 200 requisições), percebe-se que na opção (S/ Arq.), o tempo médio gasto é de 12.6 ms que é referente a troca de mensagens entre os parceiros da OV, dessa forma apresentando menos variações entre as alternativas (tamanhos de OVs). Em um cenário real o tempo médio referente a colaboração pode ser diferente, pois no ambiente de integração adotado não foi implementada a colaboração entre os parceiros, visto que não é o foco do trabalho. Dessa forma, no cenário real além da troca de mensagens é possível considerar outras variáveis, tais como, consultas a dados e sistemas de informações empresariais (ex: SAD, SIG, SPT, SAE, etc), bem como processos de tomada de decisão.

Nas opções que envolvem o uso da arquitetura de reputação por parte da OV (C/ Arq. - Operações e C/ Arq. - S/ Monit.), nota-se que há um acréscimo de tempo em relação ao que seria o tempo normal para uma OV desempenhar suas atividades, pois novas funcionalidades são adicionados ao ambiente de colaboração trazendo também benefícios à OV e seus membros.

Assim, na opção C/ Arq. - Operações, é considerada a utilização da arquitetura de reputação com todas as suas operações na OV, ou seja, valores de reputação são requisitados, o monitoramento de QoS ocorre na fase de operação da OV e os parceiros de negócio enviam seus *feedbacks* à arquitetura na dissolução da OV. Nesse sentido, percebe-se que o tempo para execução das operações, ou seja, o *overhead* em relação ao *baseline* aumenta proporcionalmente em relação a quantidade de parceiros de negócio presentes na OV e das requisições recebidas pela arquitetura. Isso é motivado principalmente pelas operações de envio de avaliações subjetivas e monitoramento de QoS.

A operação de envio de avaliações influencia no *overhead* de utilização, pois quanto mais parceiros de negócio estão presentes na OV, mais *feedbacks* necessitam ser processados pela arquitetura, ou seja, envolve o recebimento das avaliações pela arquitetura através do RBS e a atualização do repositório de dados com os novos *feedbacks*.

O *overhead* de utilização (C/ Arq. - Operações) também é dependente da ope-

ração de monitoramento de QoS. Quanto mais parceiros de negócio estão presentes na OV, mais serviços/recursos dos provedores de nuvem são utilizados. Dessa forma, o *overhead* de utilização da arquitetura é maior, pois o número de recursos de nuvem a serem monitorados é maior, logo mais operações de monitoramento são necessárias.

Além disso, observa-se que nos cenários de 100 e 200 requisições, o valor do *overhead* é diferente em relação a quantidade de parceiros de negócio. Isso está relacionado com a quantidade de requisições, pois considerou-se uma abordagem de utilização em que 70% refere-se a requisições de reputação e 30% é relativo a monitoramento de QoS. Desse modo, em um cenário com mais requisições, o *overhead* de utilização da arquitetura é maior, devido a uma maior quantidade de operações de monitoramento, pois haverá mais valores de QoS a serem enviados para a arquitetura e atualizados no repositório de dados.

Em outro cenário de utilização da arquitetura, denominado de *C/ Arq. - S/ Monit.*, o cálculo do *overhead* desconsiderou a operação de monitoramento. Nesse caso, o *overhead* de utilização da arquitetura é baseado somente no tempo computacional das operações de requisição de reputação e envio de avaliações (*feedbacks*). Assim, pelos resultados apresentados pode-se perceber que o *overhead* nesse caso sofre poucas variações em relação a quantidade de parceiros de negócio e requisições à arquitetura. A partir disso, pode-se concluir que a operação de monitoramento é a que mais influencia no tempo de *overhead* de utilização da arquitetura como um todo.

Por fim, conforme os resultados apresentados notou-se que a arquitetura de reputação quando utilizada pela OV apresenta um *overhead* em consequência das operações que são disponibilizadas. Em contrapartida, o uso dessa arquitetura traz alguns benefícios para a rede de colaboração, como por exemplo, busca e seleção de provedores de nuvem pela reputação, verificação da reputação na fase de operação da OV e auxílio na tomada de decisão em uma possível fase de evolução da OV.

5.3.3 Análise de Escalabilidade

Essa seção tem por objetivo apresentar os resultados referentes a análise de escalabilidade. A análise de escalabilidade realizada compreende a avaliação do tempo de resposta das operações de cálculo da reputação e envio de avaliações disponibilizadas pela arquitetura.

Para verificar a escalabilidade dessas operações e da arquitetura, simularam-se várias OVs com diferentes quantidades de parceiros de negócio, considerando entre 5 e 100 parceiros de negócio. Considerou-se que cada parceiro de negócio da OV avaliou o provedor de nuvem utilizado, na fase de dissolução da OV. Durante a operação da OV, cada parceiro de negócio requisitou o valor de reputação de um provedor de

nuvem ou de todos os provedores (lista de reputação). Nas simulações realizadas, as operações referentes à reputação, foram distribuídas de forma uniforme no tempo de simulação (10080min), e cada parceiro de negócio realizou uma quantidade empiricamente definida de requisições de reputação, sendo 5 de cada tipo (valor de um PN e lista de reputação). Dessa forma, três cenários de avaliação são analisados.

No **primeiro cenário**, considerou-se uma quantidade fixa de provedores que fornecem seus recursos para os membros da OV em todas as simulações realizadas na análise, ou seja, os dez provedores de nuvem presentes no repositório de dados.

O **segundo cenário** apresenta uma quantidade igual de parceiros de negócio e provedores de nuvem, sendo crescentes na relação de um para um. Por exemplo, uma OV com quinze parceiros de negócio apresenta um repositório de dados da arquitetura com quinze provedores e todos os provedores são usados pela OV.

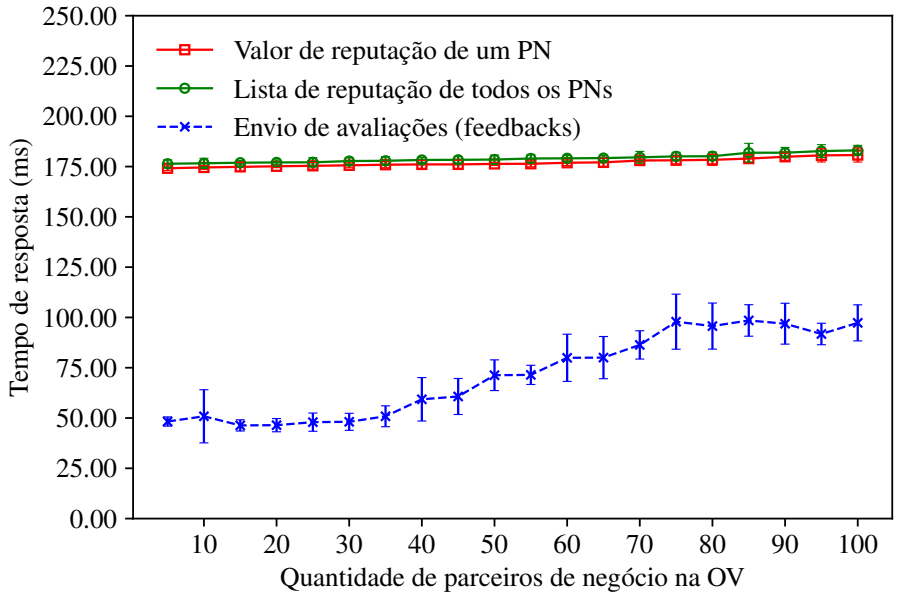
No **terceiro cenário**, a quantidade de provedores de nuvem usados é variável e cada provedor pode estar sendo utilizado por mais de um parceiro de negócio, estabelecendo uma relação de 1 para n. Inicialmente é estabelecido um repositório de dados com 100 provedores de nuvem. Na fase de formação da OV, os recursos dos provedores de nuvem são alocados de forma aleatória, seguindo uma distribuição de probabilidade uniforme, para cada parceiro de negócio. Dessa forma, é possível ter OVs configuradas com 20 parceiros e 12 provedores que fornecem seus recursos durante a operação da OV, por exemplo.

Os três cenários de avaliação são usados para analisar o tempo de resposta das operações mencionadas em contextos que apresentam mais parceiros de negócio utilizando as operações da arquitetura e também quando a quantidade de provedores de nuvem usada pela OV é alterada, ou seja, se mantém fixa (10 provedores) ou variável. Cada cenário de avaliação foi simulado dez vezes para fins de relevância estatística e os resultados representam a média do tempo de resposta das operações analisadas, considerando um intervalo de confiança de 95%.

Dessa forma, os resultados para o primeiro cenário são apresentados na Figura 28. Nesse caso, a quantidade de provedores de nuvem se manteve fixa (10) e três operações disponibilizadas pela arquitetura proposta foram analisadas:

- **Envio de avaliações (*feedbacks*)**: cada parceiro de negócio envia uma avaliação referente ao provedor de nuvem utilizado;
- **Requisição do Valor de Reputação**: refere-se a requisição do valor de reputação de um único provedor de nuvem;
- **Requisição de Lista de Reputação**: retorna a lista dos valores de reputação dos provedores usados na OV.

Figura 28 – Análise de escalabilidade - Quantidade de provedores de nuvem fixa (cenário 1)



Fonte: Produção do próprio autor.

Em relação aos resultados de escalabilidade do cenário 1, percebe-se que o tempo de resposta da operação de envio de avaliações depende da quantidade de membros da OV, assim como foi observado nos experimentos realizados na seção 5.3.1. Em uma OV composta por 5 parceiros de negócio, o tempo de resposta médio da operação de envio de avaliações é de 48.26 ms e com 100 parceiros de negócio é 97.30 ms. Essa diferença de tempo é explicada pela quantidade de requisições que a arquitetura necessita processar, pois quanto maior a OV mais *feedbacks* são coletados e armazenados no repositório de dados.

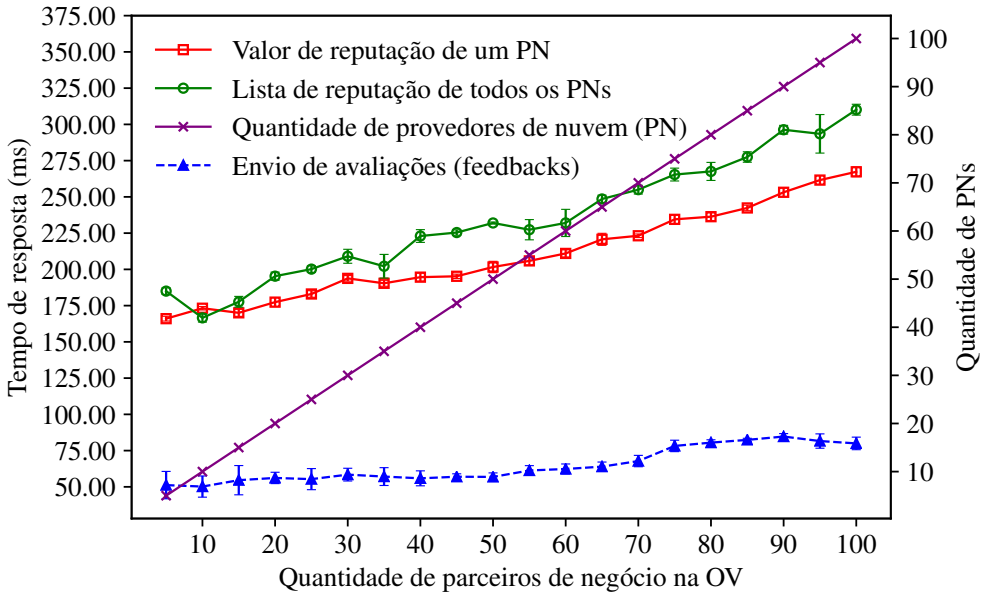
Nas operações relacionadas com a reputação (valor de um PN e lista de reputação) percebe-se que o tempo de resposta apresenta pouca variação em relação as alternativas, ou seja, quantidade de parceiros de negócio presentes na OV. Além disso, nota-se que, nesse cenário, o tempo de resposta entre as duas operações de reputação apresenta valores próximos nas configurações de OVs analisadas.

A diferença média de tempo de resposta entre as duas operações de reputação é aproximadamente 1.18%. Isso é explicado pela abordagem adotada no cálculo do indicador de confiança objetiva. Esse indicador considera em sua composição o cálculo da eficiência relativa de um provedor de nuvem. Para calcular a eficiência de um provedor é necessário comparar o valor da eficiência do provedor sendo analisado com a eficiência relativa dos demais provedores usados pela OV, tudo isso através do DEA. Uma vez que o DEA calcula a eficiência relativa de todos os provedores en-

volvidos (para que seja possível fazer a comparação) a cada requisição, a diferença de tempo existente entre as duas operações, está presente na forma de retorno da requisição, em que a operação de reputação retorna somente a reputação (valor) de um provedor de nuvem, enquanto a outra retorna a lista de valores de reputação de todos os provedores envolvidos.

Os resultados apresentados na Figura 29 são referentes às simulações realizadas no cenário 2. Esse cenário apresenta uma distribuição diferente de recursos dos provedores de nuvem, ou seja, foi estabelecido uma relação de 1 para 1. Por exemplo, uma OV composta por 15 parceiros de negócio utiliza os recursos de 15 provedores de nuvem. Nesse cenário, analisou-se o tempo de resposta das seguintes operações: requisição do valor de reputação (um provedor), requisição da lista de reputação (todos os provedores) e o envio de avaliações (*feedbacks*).

Figura 29 – Análise de escalabilidade - Mesma quantidade de provedores de nuvem e membros da OV (cenário 2)



Fonte: Produção do próprio autor.

Dessa forma, para os resultados do cenário 2, nota-se que a operação de envio de avaliações apresenta um comportamento similar ao observado no cenário 1, ou seja, é crescente em relação ao número de parceiros de negócio. Além disso, nota-se que as operações referentes à reputação são influenciadas pela quantidade de provedores de nuvem que fornecem seus recursos para a OV. O aumento de tempo observado deve-se à abordagem adotada no indicador de confiança objetiva. O indicador de confiança objetiva depende do cálculo da eficiência relativa que é baseada

na eficiência de um provedor em comparação com a eficiência dos demais provedores de nuvem, através do DEA. Logo, aumenta o tempo necessário para o processamento das operações de reputação.

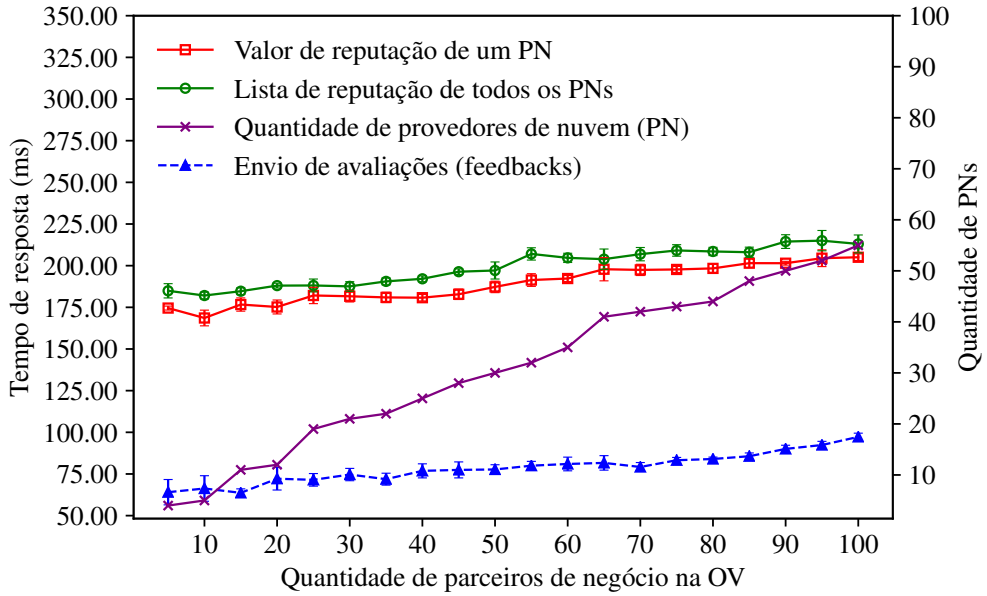
No mesmo cenário, percebe-se que a diferença média de tempo entre as duas operações de reputação (10.41 %) nas diversas configurações de OVs é maior do que o observado no cenário 1 (1.18 %), quando se considerou uma quantidade fixa (10) de provedores de nuvem. Essa diferença é ocasionada principalmente pela quantidade de provedores de nuvem usados. Desse modo, em uma OV que utilize mais recursos de nuvem, o tempo necessário para processar a operação de lista de reputação é diferente quando utiliza-se uma quantidade fixa, ou seja, 10 provedores conforme analisado no cenário 1. Isso é explicado tanto pela abordagem ponderada de cálculo adotada, pois é necessário calcular mais valores de reputação, quanto aos indicadores de confiança.

Nesse sentido, em relação aos indicadores de confiança, o aumento de tempo observado é motivado tanto pelo acesso ao repositório de dados, ou seja é necessário obter uma quantidade maior de informações referentes aos históricos de QoS e *feedbacks* de cada provedor, quanto pelos métodos de cálculo adotados em cada indicador de confiança (ex: confiança multicritério e valor agregado subjetivo), os quais são influenciados pela quantidade de provedores de nuvem. Assim, essas operações intermediárias acabam impactando no tempo de processamento da operação de lista de reputação quando utilizada em cenários com maiores quantidades de provedores.

Por fim, os resultados do cenário 3, são apresentados na Figura 30. Esse cenário é o que mais se aproxima de um cenário real de utilização da arquitetura em relação à escalabilidade. Assim, foi considerado uma relação de 1 para n, ou seja, cada provedor de nuvem pode disponibilizar seus recursos/serviços para mais de um parceiro de negócio da OV. Por exemplo, uma OV com 20 parceiros de negócio pode estar usando os recursos/serviços de 12 provedores de nuvem, devido à abordagem aleatória de alocação baseada em uma distribuição de probabilidade uniforme. Desse modo, foi analisado o tempo de resposta das operações de reputação (valor e lista) e envio de avaliações em função da quantidade de parceiros de negócio presentes na OV e provedores de nuvem usados na OV.

Nos resultados do terceiro cenário nota-se que os tempos de resposta são crescentes em relação a quantidade de parceiros de negócio e os provedores de nuvem usados, assim como observado no segundo cenário. Por exemplo, em uma OV formada com 50 parceiros de negócio, cerca de 30 provedores de nuvem estavam fornecendo recursos e serviços para a OV. Dessa forma, o tempo médio da operação de requisição de valor de reputação, nessa configuração, é de 187.25 ms. Em contrapartida, no cenário 2, para a mesma operação e quantidade de membros da OV o tempo

Figura 30 – Análise de escalabilidade - Quantidade de provedores de nuvem variável (cenário 3)



Fonte: Produção do próprio autor.

de resposta médio é 201 ms. Essa diferença de tempo é explicada pela quantidade de provedores usados, pois no cenário 2 a quantidade é equivalente ao número de membros da OV, ou seja, 50 provedores de nuvem. Desse modo, o tempo de resposta é maior devido a abordagem adotada no cálculo do indicador de confiança objetiva.

Portanto, através dos resultados de escalabilidade apresentados, pode-se concluir principalmente que as operações relacionadas à reputação (valor e lista) são dependentes da quantidade de provedores de nuvem que são utilizados durante o atendimento da oportunidade de colaboração. No primeiro cenário foi visto que as operações de reputação apresentam uma menor variação em seu tempo de resposta médio em relação a quantidade de parceiros de negócio presentes na OV. Isso deve-se ao fato de que a quantidade de provedores de nuvem usados se manteve fixa (10) em todas as OV formadas. Já, nos cenários 2 e 3, foi percebido que os tempos de resposta das operações de reputação apresentam valores diferentes entre os cenários, devido a forma como os recursos de nuvem são distribuídos aos parceiros de negócio, pois considerou-se um número variável de provedores de nuvem presentes no repositório de dados e disponíveis para a OV.

5.4 CONSIDERAÇÕES PARCIAIS

Este capítulo apresentou o ambiente de integração usado na avaliação da arquitetura de reputação bem como os resultados obtidos através de simulações no

ambiente proposto. O ambiente foi desenvolvido através do simulador de redes P2P, denominado PeerFactSim.KOM (STINGL et al., 2011). Além disso, os parâmetros usados nas simulações e o planejamento de avaliações foram apresentados.

Em sequência apresentou-se os resultados provenientes das avaliações. Inicialmente, o módulo de agregação foi avaliado no indicador de confiança objetiva, subjetiva e a reputação. No indicador de confiança objetiva avaliou-se os fatores de penalização e recompensa e notou-se que em históricos de valores de QoS com mais variações, como os gerados pelas distribuições exponencial e beta, houve mais penalização do que recompensa. Já, o indicador de confiança subjetivo, teve seu fator de credibilidade analisado quando submetido a dois conjuntos de dados: normal e malicioso. Através dessa avaliação, percebeu-se que o fator de credibilidade auxilia no tratamento dos ataques de colusão e avaliações injustas. Por fim, o valor de reputação da arquitetura proposta foi comparado com os valores gerados através do método disponível no sistema Beta notando-se uma diferença nos valores de reputação, devido a forma como a reputação é construída nos dois métodos analisados.

O desempenho da arquitetura de reputação foi avaliado. A avaliação compreendeu o tempo de resposta das operações, *overhead* de utilização e a análise de escalabilidade. Através das avaliações relacionadas com o tempo de resposta, notou-se que o tempo de resposta da operação de envio de avaliações (*feedbacks*) depende da quantidade de membros da OV e a operação de monitoramento apresentou tempos maiores nos cenários com mais requisições e recursos monitorados. Nos tempos observados referentes as operações de reputação, percebeu-se em cenários em que a quantidade de provedores de nuvem se manteve fixa (10), o tempo de resposta apresentou menos oscilações entre as alternativas, dessa forma notou-se que sofre menos influência da quantidade de membros da OV.

Em relação as avaliações relacionadas com o *overhead* de utilização, notou-se que o *overhead* foi influenciado pela quantidade de requisições e membros disponíveis na OV. Desse modo, observou-se que quando a arquitetura é utilizada pela OV acaba ocasionando um *overhead* durante o atendimento da oportunidade de colaboração em decorrência das operações disponibilizadas. Esse *overhead* é negligenciável, uma vez que, a utilização da arquitetura, apresenta benefícios para a OV, como, busca e seleção de provedores pela reputação, verificação da reputação na fase de operação, auxílio na tomada de decisão, entre outros.

A análise de escalabilidade realizada baseou-se na variação da quantidade de membros da OV e na quantidade de provedores de nuvem usados através da observação dos tempos de resposta para as operações de reputação e envio de avaliações. Desse modo, três cenários de avaliação foram elencados e estavam relacionados com a quantidade de provedores de nuvem usados. Assim, os resultados mostraram que

o tempo de resposta das operações de reputação são dependentes da quantidade de provedores de nuvem usados devido a abordagem adotada no indicador de confiança objetiva, o qual considera a eficiência relativa, ou seja, o valor de eficiência de um provedor de nuvem é baseado na comparação da eficiência com os demais, através do DEA. Por fim, notou-se que o tempo de resposta médio da operação de envio de avaliações está relacionada com a quantidade de parceiros de negócio presentes na OV.

6 CONSIDERAÇÕES E TRABALHOS FUTUROS

Esse trabalho apresentou uma arquitetura de reputação de confiança aplicada ao contexto da integração entre as organizações virtuais e computação em nuvem para suportar os processos de tomada de decisão existentes neste ambiente e auxiliar no estabelecimento de um relacionamento de confiança.

A arquitetura de reputação de confiança foi desenvolvida através de uma abordagem centralizada, seguindo alguns requisitos funcionais e não funcionais. Os requisitos funcionais estão relacionados com decisões de implementação que referem-se a forma como a reputação é calculada, disseminada e atualizada. Já, os requisitos não funcionais elicitam algumas restrições da arquitetura proposta para fornecer a reputação dos provedores de nuvem.

A arquitetura de reputação é composta por três camadas, Aplicação; Reputação; e Dados, e quatro módulos, referentes ao Módulo de Agregação, Módulo de Monitoramento, Repositório de Dados; e o *Reputation Broker Service* (RBS). O Módulo de Agregação calcula a reputação dos provedores de nuvem através de dois indicadores de confiança: objetiva (indicadores de QoS) e subjetiva (*feedback* dos parceiros de negócio aos provedores de nuvem). O Módulo de Monitoramento tem como papel monitorar e atualizar os indicadores de QoS de cada provedor de nuvem, enquanto a OV está em sua fase de operação. O Repositório de Dados armazena os valores referentes as participações passadas e atuais de cada provedor de nuvem em OVs. Por fim, o *Reputation Broker Service* fornece acesso às operações da arquitetura para outros elementos, como o parceiro de negócio da OV e o gestor da OV.

É importante notar que para a satisfação completa dos requisitos não funcionais, a arquitetura proposta depende da disposição dos parceiros de negócio em avaliar o(s) provedor(es) de nuvem com o(s) qual(is) se relacionam, de forma a possibilitar a atualização da reputação, bem como depende também de algum meio para armazenar as informações dos indicadores quantitativos bem como das avaliações qualitativas (*feedbacks*) (ex: banco de dados). Tal dependência constitui-se em um aspecto limitante da arquitetura proposta, mas que pode ser contornado com o estabelecimento de compromissos legais a partir do momento da sua utilização.

De forma a avaliar a arquitetura de reputação proposta foi desenvolvido um ambiente de integração no simulador de redes P2P PeerFactSim.KOM. Os experimentos realizados buscaram avaliar o cálculo dos valores dos indicadores de confiança objetiva, subjetiva, valor final de reputação dos provedores de nuvem, bem como analisar as trocas de mensagens e interações existentes entre os parceiros de negócio da OV

e a arquitetura de reputação.

Assim, através do ambiente proposto, foram avaliados os fatores de penalização e recompensa do indicador de confiança objetiva, o fator de credibilidade do indicador de confiança subjetiva, bem como a comparação do valor de reputação disponibilizado pela arquitetura com o valor gerado pelo método de agregação presente em outro sistema de reputação. Além disso, o desempenho da arquitetura de reputação foi avaliado, compreendendo o *overhead* de utilização baseado no tempo de resposta das operações fornecidas e uma análise de escalabilidade das operações disponibilizadas pela arquitetura.

Dessa forma, por meio dos resultados apresentados, pode-se perceber que a aplicação do fator de credibilidade nas avaliações subjetivas, auxiliou no tratamento dos ataques ao valor do indicador de confiança subjetiva, ponderando o valor dessas avaliações. Além disso, o uso do mecanismo de penalização e recompensa no indicador de confiança objetiva, mostrou que em históricos gerados por distribuições de probabilidade que apresentam maiores oscilações, o valor da confiança multicritério foi reduzido, pois houve mais penalizações do que recompensas.

Outros resultados relacionados à comparação mostraram as diferenças entre os métodos de cálculo de reputação. O método de cálculo da arquitetura considera os valores dos indicadores de confiança objetiva e subjetiva através de uma abordagem ponderada. Já, no método do sistema Beta (BRS), a reputação de uma entidade é calculada através de uma função de densidade de probabilidade a qual considera a quantidade de transações/interações positivas e negativas. Dessa forma, através dos resultados apresentados, pode-se observar que o método usado no BRS não apresenta meios para avaliar a credibilidade dos usuários que avaliam as interações, ou seja, permite que um usuário envie diversas avaliações positivas ou negativas para promover ou prejudicar a reputação de uma entidade.

Na análise de desempenho da arquitetura de reputação, os resultados apresentaram um *overhead* de utilização tolerável em relação as operações analisadas e as funcionalidades que a arquitetura de reputação disponibiliza para o ambiente de colaboração. Na análise de escalabilidade realizada verificou-se o comportamento da operação de envio de avaliações em função do aumento da quantidade de membros da OV. Na mesma análise, além do aumento de membros da OV considerou-se três cenários para avaliar as operações de reputação. Esses cenários são relativos aos provedores de nuvem usados, sendo que no primeiro a quantidade se manteve fixa (10), no segundo foi estabelecido uma relação de 1 para 1, ou seja, um provedor é usado por um membro da OV e o terceiro considerou que um provedor de nuvem pode ser usado por mais de um parceiro da OV (relação de 1 para n). Através desses cenários, percebeu-se que os tempos de resposta das operações de reputação estão

relacionados com a quantidade de provedores usados do que com a quantidade de membros da OV que enviam requisições de reputação para a arquitetura.

Por fim, destaca-se a necessidade de avaliar o indicador de confiança objetiva utilizando dados reais, pois na avaliação proposta utilizou-se dados gerados aleatoriamente seguindo algumas distribuições de probabilidade. Isso foi realizado em função da dificuldade de obtenção de dados reais e históricos dos provedores de nuvem em relação ao QoS para realizar a avaliação do módulo de agregação. Existem algumas ferramentas como, por exemplo, o *CloudHarmony*[1], que apresentam alguns dados, como capacidade de armazenamento, processamento, planos disponíveis, disponibilidade, etc.; no entanto, não apresentam outros dados relevantes como o tempo de resposta, estabilidade e segurança.

6.1 RECOMENDAÇÕES PARA TRABALHOS FUTUROS

Um possível trabalho futuro inclui a implementação dessa arquitetura de reputação em um cenário real, ou seja, disponibilizar suas funcionalidades como serviço através de uma plataforma. Essa implementação pode ser realizada através de diversas formas, como *web services*, plataforma *web*, entre outras. Nesse sentido, a arquitetura proposta deve ser adaptada para lidar com algumas situações, como, ataque de negação de serviço, disponibilidade com replicação e redundância para evitar ponto único de falha. Desse modo, algumas avaliações podem ser realizadas visando analisar questões como realocação dos nós, ataque de negação de serviço, disponibilidade da plataforma, acurácia dos resultados de reputação, entre outras.

Além disso, outro trabalho pode ser a incorporação de outros subfatores no fator de credibilidade do indicador de confiança subjetiva. Dessa forma, essa incorporação auxiliaria no tratamento de outros ataques além dos que foram analisados. Um desses ataques é o de múltiplas identidades, em que um um mesmo usuário assume diversas identidades para avaliar de forma maliciosa um provedor de nuvem (JØSANG; GOLBECK, 2009).

Outra recomendação de trabalho futuro é a extensão da arquitetura de reputação para os parceiros de negócio, ou seja, cada parceiro de negócio avalia a colaboração com os outros parceiros, gerando assim um valor de reputação para os membros da OV, além da reputação dos provedores de nuvem. Assim, deve-se investigar indicadores que possam representar a reputação dos parceiros de negócio, por exemplo, indicadores de desempenho que refletem o comportamento organizacional, ou seja, abordam aspectos financeiros, operacionais, logísticos, entre outros.

Além disso, tratamentos para outros tipos de ataque no contexto da reputa-

[1] https://cloudharmony.com/

ção entre os parceiros de negócios, como por exemplo re-entrada, *playbooks*, ataque *sybil*, *free riders*, entre outros (JØSANG; GOLBECK, 2009; HOFFMAN; ZAGE; NITA-ROTARU, 2009), podem ser incorporados à arquitetura de reputação. Também recomenda-se a análise de outros aspectos e conceitos no cálculo da reputação, como, uso da janela de tempo (intervalo de tempo entre interações), número de interações entre os parceiros de negócio, avaliações diretas (parceiro para parceiro), avaliações indiretas (visão da OV para o parceiro) e a utilização de pesos diferentes para os *feedbacks*, onde por exemplo, *feedbacks* mais recentes tenham peso maior que os mais antigos (LI; YU; HUANG, 2011).

No presente trabalho a reputação dos provedores de nuvem foi baseada em dois indicadores de confiança objetiva e subjetiva, sendo agregados para a geração do valor de reputação através de um abordagem ponderada, na qual o gestor da OV define a relevância de cada indicador de confiança, ou seja, o peso de importância. Desse modo, recomenda-se como trabalhos futuros, o estudo e análise de outros métodos de agregação, como, lógica *fuzzy*, métodos estocásticos, probabilísticos, entre outros. Além disso, pode-se incorporar outros indicadores ou fatores no cálculo da reputação que sejam justificados na literatura.

Por fim, a arquitetura proposta tem como objetivo apoiar a tomada de decisão no contexto da integração entre OV e computação em nuvem com a reputação. Desse modo, a arquitetura desenvolvida tanto como o ambiente de integração apresentado na avaliação da arquitetura, podem ser reaproveitados para outros fins, como:

- Análise de risco na fase de operação da OV, ou seja, além da reputação a arquitetura proposta poderia incorporar métodos e cálculo de análise de risco, quando opta-se por usar determinados provedores de nuvem e membros da OV;

- Uso do valor de reputação juntamente com as necessidades/preferências do usuário (gestor da OV ou membro da OV) em um *framework* de seleção de serviços ou provedores de nuvem (GARG; VERSTEEG; BUYYA, 2013; MORAES; FIORESE; MATOS, 2017), na qual a arquitetura seria utilizada como um serviço;

- Uso de políticas de segurança dos usuários e da OV juntamente com o gerenciamento da confiança no ambiente de integração proposto para a implementação de mecanismos que realizem a negociação e gerenciamento de políticas; e

- Extensão da arquitetura desenvolvida para o uso em outros cenários e outras formas de rede de colaboração (times virtuais, empresas virtuais), ambientes de *e-commerce*, entre outros.

6.2 PRINCIPAIS CONTRIBUIÇÕES

Além da principal contribuição levantada na conclusão, a proposição de uma arquitetura de reputação de confiança aplicada ao contexto da integração entre as organizações virtuais e computação em nuvem, pode-se definir as seguintes contribuições relacionadas:

- Criação de um indicador de confiança objetiva que compreende duas abordagens: eficiência relativa calculada pelo DEA e a confiança multicritério com mecanismos de recompensa e penalização;
- Criação de um indicador de confiança subjetiva baseado no que foi proposto por Noor et al. (2016b), com alguns diferenciais, como: adoção de uma abordagem ponderada e tratamento do ataque de avaliações injustas no fator de credibilidade das avaliações;
- Ambiente de integração desenvolvido para a avaliação da arquitetura que pode ser reaproveitado para outros fins, por exemplo análise de risco durante a fase de operação da OV; e
- Revisão sistemática de trabalhos aplicados em OVs que estejam relacionadas com confiança, reputação e computação em nuvem.

6.3 PUBLICAÇÕES

Até o momento da escrita, este trabalhou gerou as seguintes publicações:

Anais de Conferências:

- Publicados:
  - BILECKI, Luís Felipe; FIORESE, Adriano. Arquitetura para reputação de confiança no contexto da integração entre Organizações Virtuais e Computação em Nuvem. In: ESCOLA REGIONAL DE ALTO DESEMPENHO DO RIO GRANDE DO SUL, 16., 2016, São Leopoldo, RS, **Anais ...** Porto Alegre: SBC, 2016, p. 149-150.
  - BILECKI, Luís Felipe; FIORESE, Adriano. A Confidence Indicator Model for Virtual Organization Creation in Cloud Computing Environment. In: IFIP WG 5.5 WORKING CONFERENCE ON VIRTUAL ENTERPRISES, 17., 2016, Porto, **Proceedings ...**, Porto: Springer, 2016, p. 200-211.
  - BILECKI, Luís Felipe; FIORESE, Adriano. Uma proposta de indicador de confiança no contexto da integração entre Organizações Virtuais e Computação em Nuvem. In: ESCOLA REGIONAL DE ALTO DESEMPENHO DO

RIO GRANDE DO SUL, 17., 2017, Ijuí, RS, **Anais ...** Porto Alegre: SBC, p. 193 - 194.

  - BILECKI, Luís Felipe; FIORESE, Adriano; MATOS, Fernando. A Trust Reputation Architecture for Virtual Organization Integration in Cloud Computing Environment. In: INTERNATIONAL CONFERENCE ON ENTERPRISE INFORMATION SYSTEMS, 19., 2017, Porto, Portugal, **Proceedings ...** Porto: Scitepress, 2017, v. 2., p. 695-702.
  - BILECKI, Luís Felipe; FIORESE, Adriano. Uma Arquitetura de Reputação de Confiança Aplicada ao Ambiente de Computação em Nuvem. In: WORKSHOP DE COMPUTAÇÃO EM CLOUDS E APLICAÇÕES, 15., 2017, Belém, PA, **Anais ...** Porto Alegre: SBC, 2017, p. 130-143.
  - BILECKI, Luís Felipe; FIORESE, Adriano. A Classification Taxonomy for Reputation and Trust Systems Applied to Virtual Organizations. In: PRO-VE 2017: 18th IFIP WORKING CONFERENCE ON VIRTUAL ENTERPRISES, 18., 2017, Vicenza, **Proceedings ...**, Vicenza: Springer, 2017, p. 515-526.

- Aceito para publicação:

  - BILECKI, Luís Felipe; FIORESE, Adriano. A Trust Reputation Architecture for Cloud Computing Environment. In: 14TH ACS/IEEE INTERNATIONAL CONFERENCE ON COMPUTER SYSTEMS AND APPLICATIONS - AICCSA 2017.

Revistas:

- Publicados:

  - BILECKI, Luís Felipe; HOUNSELL, Marcelo da Silva; FIORESE, Adriano. Uma Revisão Sistemática sobre Abordagens em Organizações Virtuais no Contexto de Confiança, Reputação e Computação em Nuvem. **Revista de Informática Teórica e Aplicada**, v. 24, n. 1, 2017. ISSN 2175-2745.

REFERÊNCIAS

ACAMPORA, G.; CASTIGLIONE, A.; VITIELLO, A. A fuzzy logic based reputation system for E-markets. In: IEEE INTERNATIONAL CONFERENCE ON FUZZY SYSTEMS, 2014, Beijing. **Proceedings...** Beijing: IEEE, 2014. p. 865–872.

ACETO, G. et al. Cloud monitoring: A survey. **Computer Networks**, v. 57, n. 9, p. 2093 – 2115, 2013. ISSN 1389-1286.

ALAWAMLEH, M.; POPPLEWELL, K. Risk sources identification in virtual organisation. In: POPPLEWELL, K. et al. (Ed.). **Enterprise Interoperability IV: Making the Internet of the Future for the Future of Enterprise**. London: Springer, 2010. p. 265–277. ISBN 978-1-84996-257-5.

ALHAMAD, M.; DILLON, T.; CHANG, E. SLA-based trust model for cloud computing. In: INTERNATIONAL CONFERENCE ON NETWORK-BASED INFORMATION SYSTEMS, 13., 2010, Takayama, Gifu, Japan. **Proceedings ...** Takayama, Gifu, Japan: IEEE, 2010. p. 321–324.

ALVES JUNIOR, O. C. **Método de seleção de parceiros logísticos baseado em indicadores de desempenho para organizações virtuais**. 354 f. Tese (Doutorado em Engenharia de Automação e Sistemas) — Universidade Federal de Santa Catarina, Programa de Pós-Graduação em Engenharia de Automação e Sistemas, Florianópolis, 2011.

ANDRULIS, J. et al. Evaluating the STORE reputation system in multi-agent simulations. In: FERRARI, E. et al. (Ed.). **Trust Management III, Third IFIP WG 11.11 International Conference, IFIPTM 2009**. West Lafayette, IN, EUA: Springer, 2009. (IFIP Advances in Information and Communication Technology, v. 300), p. 267–282.

ARASTEH, M.; AMINI, M.; JALILI, R. A trust and reputation-based access control model for virtual organizations. In: INTERNATIONAL ISC CONFERENCE ON INFORMATION SECURITY AND CRYPTOLOGY, 9., 2012, Tabriz, Irã. **Proceedings ...** Tabriz, Irã: IEEE, 2012. p. 121–127.

ARENAS, A. E.; AZIZ, B.; SILAGHI, G. C. Reputation management in collaborative computing systems. **Security and Communication Networks**, John Wiley e Sons, Ltd., v. 3, n. 6, p. 546–564, 2010. ISSN 1939-0122.

AROCKIAM, L.; MONIKANDAN, S.; PARTHASARATHY, G. Cloud computing: A survey. **Int. J. Internet Comput**, v. 1, n. 2, p. 26–33, 2011.

ARSHAD, K.; MOESSNER, K. Robust collaborative spectrum sensing based on beta reputation system. In: FUTURE NETWORK & MOBILE SUMMIT (FUTURENETW), 2011, Warsaw, Polônia. **Proceedings ...** Warsaw, Polônia: IEEE, 2011. p. 1–8.

BANKER, R. D.; CHARNES, A.; COOPER, W. W. Some models for estimating technical and scale inefficiencies in data envelopment analysis. **Management science**, INFORMS, v. 30, n. 9, p. 1078–1092, 1984.

BARANWAL, G.; VIDYARTHI, D. P. A framework for selection of best cloud service provider using ranked voting method. In: INTERNATIONAL ADVANCE COMPUTING CONFERENCE, 2014, Gurgaon, India. **Proceedings ...** Gurgaon, India: IEEE, 2014.

BARBOSA, H.; MORAIS, T. Study on computational trust and reputation models. In: **High Performance Network Studies**. Porto: E-book, 2016. cap. 6, p. 58–66.

BEZERRA, E. **Princípios de Análise e Projeto de Sistemas com UML**. 2. ed. Rio de Janeiro: Elsevier, 2007. 369 p. ISBN 978-8535216967.

CAMARINHA-MATOS, L. M.; AFSARMANESH, H. The Virtual Enterprise Concept. **Infrastructures for Virtual Enterprises**, v. 153, p. 3–14, 1999.

CAMARINHA-MATOS, L. M.; AFSARMANESH, H. Virtual Enterprise Modeling and Support Infrastructures: Applying Multi-agent System Approaches. In: **Selected Tutorial Papers from the 9th ECCAI Advanced Course ACAI 2001 and Agent Link's 3rd European Agent Systems Summer School on Multi-Agent Systems and Applications**. London, UK, UK: Springer-Verlag, 2001. (EASSS '01), p. 335–364. ISBN 3-540-42312-5.

CAMARINHA-MATOS, L. M.; AFSARMANESH, H. Collaborative networks: a new scientific discipline. **Journal of intelligent manufacturing**, Springer, v. 16, n. 4-5, p. 439–452, 2005. ISSN 1572-8145.

CAMARINHA-MATOS, L. M. et al. Collaborative networked organizations–concepts and practice in manufacturing enterprises. **Computers & Industrial Engineering**, Elsevier, v. 57, n. 1, p. 46–60, 2009. ISSN 0360-8352.

CHAKRABORTY, S.; ROY, K. An SLA-based framework for estimating trustworthiness of a cloud. In: INTERNATIONAL CONFERENCE ON TRUST, SECURITY AND PRIVACY IN COMPUTING AND COMMUNICATIONS, 11., 2012, Liverpool, UK. **Proceedings ...** Liverpool, UK: IEEE, 2012.

CHARNES, A.; COOPER, W. W.; RHODES, E. Measuring the efficiency of decision making units. **European Journal of Operational Research**, Elsevier, v. 2, n. 6, p. 429–444, 1978. ISSN 0377-2217.

CHO, J.-H.; SWAMI, A.; CHEN, I.-R. A survey on trust management for mobile ad hoc networks. **IEEE Communications Surveys & Tutorials**, v. 13, n. 4, p. 562–583, 2011. ISSN 1553-877X.

COOPER, W. W.; SEIFORD, L. M.; TONE, K. **Introduction to data envelopment analysis and its uses: with DEA-solver software and references**. 1. ed. New York: Springer Science & Business Media, 2006.

COOPER, W. W.; SEIFORD, L. M.; ZHU, J. **Handbook on data envelopment analysis**. New York: Springer Science & Business Media, 2011. v. 164.

DHARMAADI, I. P. A. et al. Reputation system based on seller-buyer closeness degree for e-commerce. In: INTERNATIONAL CONFERENCE ON ICT FOR SMART SOCIETY, 2014, Bandung, Indonésia. **Proceedings ...** Bandung, Indonésia: IEEE, 2014. p. 226–231.

EDEN, A. H. Three paradigms of computer science. **Minds and Machines**, v. 17, n. 2, p. 135–167, 2007. ISSN 0924-6495.

ESPOSITO, E.; EVANGELISTA, P. Investigating virtual enterprise models: literature review and empirical findings. **International Journal of Production Economics**, v. 148, p. 145 – 157, 2014. ISSN 0925-5273.

FIRDHOUS, M.; GHAZALI, O.; HASSAN, S. Trust Management in Cloud Computing: A Critical Review. **International Journal on Advances in ICT for Emerging Regions (ICTer)**, v. 4, n. 2, p. 24–36, 2012. ISSN 1800-4156.

FOUSS, F.; ACHBANY, Y.; SAERENS, M. A probabilistic reputation model based on transaction ratings. **Inf. Sci.**, Elsevier Science Inc., New York, NY, EUA, v. 180, n. 11, p. 2095–2123, jun. 2010. ISSN 0020-0255.

FREITAS, P. J. d. **Introdução a modelagem e simulação de sistemas**. 2. ed. Florianópolis: Visual Books, 2008. 372 p. ISBN 8575022288.

GAMBETTA, D. et al. Can we trust trust. **Trust: Making and breaking cooperative relations**, Citeseer, v. 13, p. 213–237, 2000.

GANERIWAL, S.; BALZANO, L. K.; SRIVASTAVA, M. B. Reputation-based framework for high integrity sensor networks. **ACM Trans. Sen. Netw.**, ACM, New York, NY, EUA, v. 4, n. 3, p. 15:1–15:37, jun. 2008. ISSN 1550-4859.

GARCIA, A. L.; CASTILLO, E. F. del; PUEL, M. Identity federation with VOMS in cloud infrastructures. In: INTERNATIONAL CONFERENCE ON CLOUD COMPUTING TECHNOLOGY AND SCIENCE, 5., 2013, Santa Clara, CA, EUA. **Proceedings ...** Santa Clara, EUA: IEEE, 2013.

GARG, S. K.; VERSTEEG, S.; BUYYA, R. SMICloud: A Framework for Comparing and Ranking Cloud Services. In: INTERNATIONAL CONFERENCE ON UTILITY AND CLOUD COMPUTING, 4., 2011, Gurgaon, Índia. **Proceedings ...** Gurgaon, Índia: IEEE, 2011. p. 210–218.

GARG, S. K.; VERSTEEG, S.; BUYYA, R. A framework for ranking of cloud computing services. **Future Generation Computer Systems**, Elsevier, v. 29, n. 4, p. 1012–1023, 2013. ISSN 0167-739X.

GERHARDT, T. E.; SILVEIRA, D. T. **Métodos de pesquisa**. Porto Alegre: Plageder, 2009.

GIL, A. C. **Como elaborar projetos de pesquisa**. São Paulo: Atlas, 2008.

GRAHAM, R. L.; KNUTH, D. E.; PATASHNIK, O. **Concrete Mathematics: A Foundation for Computer Science**. 2nd. ed. Boston, MA, EUA: Addison-Wesley Longman Publishing Co., Inc., 1994. ISBN 0201558025.

GRANATYR, J. et al. Trust and reputation models for multiagent systems. **ACM Comput. Surv.**, ACM, New York, NY, EUA, v. 48, n. 2, p. 27:1–27:42, out. 2015. ISSN 0360-0300.

GRIVAS, S. G.; KUMAR, T. U.; WACHE, H. Cloud Broker: Bringing Intelligence Into the Cloud. In: INTERNATIONAL CONFERENCE ON CLOUD COMPUTING, 3., 2010, Miami, EUA. **Proceedings ...** Miami, EUA: IEEE, 2010. p. 544–545.

HABIB, S. M.; RIES, S.; MUHLHAUSER, M. Cloud computing landscape and research challenges regarding trust and reputation. In: INTERNATIONAL CONFERENCE ON UBIQUITOUS INTELLIGENCE & COMPUTING AND INTERNATIONAL CONFERENCE ON AUTONOMIC & TRUSTED COMPUTING, 7., 2010, Shaanxi, China. **Proceedings ...** Shaanxi, China: IEEE, 2010. p. 410–415.

HABIB, S. M.; RIES, S.; MUHLHAUSER, M. Towards a trust management system for cloud computing. In: INTERNATIONAL CONFERENCE ON TRUST, SECURITY AND PRIVACY IN COMPUTING AND COMMUNICATIONS, 10., 2011, Changsha, China. **Proceedings ...** Changsha, China: IEEE, 2011. p. 933–939.

HALLER, J. A bayesian reputation system for virtual organizations. **Negotiation, Auctions, and Market Engineering**, Springer, p. 171–178, 2008.

HALLER, J. STORE Stochastic Reputation Service for Virtual Organisations. In: KARABULUT, Y. et al. (Ed.). **Trust Management II. IFIPTM 2008. IFIP – The International Federation for Information Processing**. Boston, MA: Springer, 2008. v. 263, p. 367–370.

HALLER, J. **A Stochastic Reputation System Architecture to Support the Partner Selection in Virtual Organisations**. 167 p. Tese (Doutorado) — Universitat Karlsruhe (TH), Institut für Informationswirtschaft und management (IISM), Fakultät für Wirtschaftswissenschaften (WIWI), Karlsruhe, 2009.

HOFFMAN, K.; ZAGE, D.; NITA-ROTARU, C. A survey of attack and defense techniques for reputation systems. **ACM Comput. Surv.**, ACM, New York, NY, EUA, v. 42, n. 1, p. 1:1–1:31, dez. 2009. ISSN 0360-0300.

JAVAID, S.; MAJEED, A.; AFZAL, H. A reputation management system for efficient selection of disaster management team. In: INTERNATIONAL CONFERENCE ON ADVANCED COMMUNICATION TECHNOLOGY, 15., 2013, PyeongChang, Coreia do Sul. **Proceedings ...** PyeongChang, Coreia do Sul: IEEE, 2013. p. 829–834.

JØSANG, A.; GOLBECK, J. Challenges for robust trust and reputation systems. In: INTERNATIONAL WORKSHOP ON SECURITY AND TRUST MANAGEMENT, 5., 2009, Saint Malo, França. **Proceedings ...** Saint Malo, França: IFIP, 2009.

JOSANG, A.; HAYWARD, R.; POPE, S. Trust network analysis with subjective logic. **Conferences in Research and Practice in Information Technology Series**, v. 48, n. January, p. 85–94, 2006. ISSN 14451336.

JØSANG, A.; ISMAIL, R. The beta reputation system. In: BLED ELECTRONIC COMMERCE CONFERENCE, 15., 2002, Bled, Eslovênia. **Proceedings ...** Bled, Eslovênia: Citeseer, 2002. v. 5, p. 2502–2511.

JØSANG, A.; ISMAIL, R.; BOYD, C. A survey of trust and reputation systems for online service provision. **Decision Support Systems**, v. 43, n. 2, p. 618 – 644, 2007. ISSN 0167-9236.

KALIDINDI, R. R. et al. Trust Based Participant Driven Privacy Control in Participatory Sensing. **International Journal of Ad hoc, Sensor & Ubiquitous Computing**, v. 2, n. 1, mar. 2011. ISSN 1743-8233.

KAMVAR, S. D.; SCHLOSSER, M. T.; GARCIA-MOLINA, H. The eigentrust algorithm for reputation management in p2p networks. In: INTERNATIONAL CONFERENCE ON WORLD WIDE WEB, 12., 2003, Budapeste, Hungria. **Proceedings ...** New York, NY, EUA: ACM, 2003. p. 640–651.

KERSCHBAUM, F. A verifiable, centralized, coercion-free reputation system. In: ACM WORKSHOP ON PRIVACY IN THE ELECTRONIC SOCIETY, 8., 2009, Chicago, Illinois, EUA. **Proceedings ...** New York, NY, EUA: ACM, 2009. p. 61–70.

KERSCHBAUM, F. et al. Pathtrust: A trust-based reputation service for virtual organization formation. In: INTERNATIONAL CONFERENCE ON TRUST MANAGEMENT, 4., 2006, Pisa, Italy. **Proceedings ...** Berlin, Heidelberg: Springer-Verlag, 2006. p. 193–205.

KHURANA, R.; BAWA, R. K. Qos based cloud service selection paradigms. In: INTERNATIONAL CONFERENCE ON CLOUD SYSTEM AND BIG DATA ENGINEERING (CONFLUENCE), 6., 2016, Noida, Índia. **Proceedings ...** Noida, Índia: IEEE, 2016. p. 174–179.

KO, R. K. L. et al. TrustCloud: A Framework for Accountability and Trust in Cloud Computing. In: IEEE WORLD CONGRESS ON SERVICES, 7., 2011, Washington, DC, EUA. **Proceedings ...** Washington, DC, EUA: IEEE, 2011. p. 584–588.

KURDI, H. A. HonestPeer: An enhanced EigenTrust algorithm for reputation management in P2P systems. **Journal of King Saud University - Computer and Information Sciences**, v. 27, n. 3, p. 315 – 322, 2015. ISSN 1319-1578.

LAW, A. M. Statistical analysis of simulation output data: the practical state of the art. In: WINTER SIMULATION CONFERENCE, 39., 2007, Washington, DC, EUA. **Proceedings ...** Washington, DC, EUA: IEEE, 2007. p. 1810–1819.

LEE, C. A. A design space review for general federation management using keystone. In: INTERNATIONAL CONFERENCE ON UTILITY AND CLOUD COMPUTING, 7., 2014, Londres, UK. **Proceedings ...** Washington, DC, EUA: IEEE/ACM, 2014. p. 720–725.

LEE, C. A.; DESAI, N. Approaches for Virtual Organization Support in OpenStack. In: INTERNATIONAL CONFERENCE ON CLOUD ENGINEERING, 7., 2014, Anchorage, AK, EUA. **Proceedings ...** Anchorage, AK, USA: IEEE, 2014. p. 432–438.

LEMOS, F. S. B. de et al. A Hybrid Dea-Fuzzy Method for Risk Assessment in Virtual Organizations. **Decision Making Soft Computing**, p. 601–607, 2014.

LI, J. et al. CloudVO: Building a Secure Virtual Organization for Multiple Clouds Collaboration. In: ACIS INTERNATIONAL CONFERENCE ON SOFTWARE ENGINEERING, ARTIFICIAL INTELLIGENCE, NETWORKING AND PARALLEL/DISTRIBUTED COMPUTING, 11., 2010, Londres, UK. **Proceedings ...** Washington, DC, EUA: IEEE Computer Society, 2010. p. 181–186.

LI, M.; YU, Y.; HUANG, Z. A group-choose model for partner selection in virtual organization. In: INTERNATIONAL CONFERENCE ON DEPENDABLE, AUTONOMIC AND SECURE COMPUTING, 9., 2011, Sydney, Austrália. **Proceedings ...** Washington, DC, EUA: IEEE, 2011. p. 674–681.

LIN, H.; LI, Z.; HUANG, Q. Multifactor hierarchical fuzzy trust evaluation on peer-to-peer networks. **Peer-to-Peer Networking and Applications**, v. 4, n. 4, p. 376–390, 2011. ISSN 1936-6450.

LIU, S. et al. A Fuzzy Logic Based Reputation Model Against Unfair Ratings. In: INTERNATIONAL CONFERENCE ON AUTONOMOUS AGENTS AND MULTI-AGENT SYSTEMS, 6., 2013, Saint Paul, MN, EUA. **Proceedings ...** New York, NY, EUA: ACM, 2013. p. 821–828. ISBN 978-1-4503-1993-5.

MA, H.; HU, Z. Recommend trustworthy services using interval numbers of four parameters via cloud model for potential users. **Frontiers of Computer Science**, Springer, v. 9, n. 6, p. 887–903, 2015. ISSN 2095-2236.

MACHHI, S.; JETHAVA, G. B. Feedback based trust management for cloud environment. In: INTERNATIONAL CONFERENCE ON INFORMATION AND COMMUNICATION TECHNOLOGY FOR COMPETITIVE STRATEGIES, 2., 2016, Udaipur, India. **Proceedings ...** New York, NY, EUA: ACM, 2016. p. 114:1–114:5.

MACQUEEN, J. Some methods for classification and analysis of multivariate observations. In: **Proceedings of the Fifth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Statistics**. Berkeley, Calif.: University of California Press, 1967. p. 281–297.

MALIK, Z.; BOUGUETTAYA, A. RATEWeb: Reputation assessment for trust establishment among web services. **The International Journal on Very Large Data Bases**, Springer-Verlag New York, Inc., v. 18, n. 4, p. 885–911, 2009. ISSN 0949-877X.

MARTIĆ, M.; NOVAKOVIĆ, M.; BAGGIA, A. Data envelopment analysis-basic models and their utilization. **Journal of Management, Informatics and Human Resources - ORGANIZACIJA**, v. 42, n. 2, p. 37–43, 2009. ISSN 1318-5454.

MASHAYEKHY, L.; GROSU, D. A reputation-based mechanism for dynamic virtual organization formation in grids. In: INTERNATIONAL CONFERENCE ON PARALLEL PROCESSING, 21., 2012, Pittsburgh, PA, EUA. **Proceedings ...** Pittsburgh, PA, EUA: IEEE, 2012. p. 108–117.

MELL, P. M.; GRANCE, T. **SP 800-145. The NIST Definition of Cloud Computing**. Gaithersburg, MD, United States, 2011. Disponível em: <http://dx.doi.org/10.6028/NIST.SP.800-145>. Acesso em: 11 out. 2016.

MOMANI, M.; ABOURA, K.; CHALLA, S. Rbatmwsn: Recursive bayesian approach to trust management in wireless sensor networks. In: INTERNATIONAL CONFERENCE ON INTELLIGENT SENSORS, SENSOR NETWORKS AND INFORMATION, 3., 2007, Melbourne, Austrália. **Proceedings ...** Melbourne, Austrália: IEEE, 2007. p. 347–352.

MONTGOMERY, D. C.; RUNGER, G. C. **Applied Statistics and Probability for Engineers**. New York, NY, EUA: John Wiley and Sons, 2002.

MORAES, L. B. et al. Uma Taxonomia de Integração entre a Computação em Nuvem e as Organizações Virtuais. In: SEMINÁRIO INTEGRADO DE SOFTWARE E HARDWARE (SEMISH), 42., 2015, Recife, PE. **Anais ...** Recife, PE: Sociedade Brasileira de Computação, 2015.

MORAES, L. B. de; FIORESE, A.; MATOS, F. A multi-criteria scoring method based on performance indicators for cloud computing provider selection. In: INTERNATIONAL CONFERENCE ON ENTERPRISE INFORMATION SYSTEMS, 19., 2017, Porto, Portugal. **Proceedings ...** Porto, Portugal: ScitePress, 2017. p. 588–599.

MOUSA, H. et al. Trust management and reputation systems in mobile participatory sensing applications: A survey. **Computer Networks**, v. 90, p. 49 – 73, 2015. ISSN 1389-1286.

MSANJILA, S. S.; AFSARMANESH, H. Trust analysis and assessment in virtual organization breeding environments. **International Journal of Production Research**, v. 46, n. 5, p. 1253–1295, 2008. ISSN 0020-7543.

MUCHAHARI, M. K.; SINHA, S. K. A new trust management architecture for cloud computing environment. In: INTERNATIONAL SYMPOSIUM ON CLOUD AND SERVICES COMPUTING, 2012, Mangalore, Índia. **Proceedings ...** Mangalore, Índia: IEEE, 2012. p. 136–140.

MUN, J.; SHIN, M.; JUNG, M. A goal-oriented trust model for virtual organization creation. **Journal of Intelligent Manufacturing**, Springer, v. 22, n. 3, p. 345–354, 2011. ISSN 1572-8145.

NEATA, S.; URZICA, A.; FLOREA, A. M. Trust Model for Virtual Organizations. In: INTERNATIONAL SYMPOSIUM ON SYMBOLIC AND NUMERIC ALGORITHMS FOR SCIENTIFIC COMPUTING, 13., 2011, Timisoara, Romênia. **Proceedings ...** Washington, DC, EUA: IEEE, 2011. p. 357–364.

NIST. NIST SP - 500-293 US Government Cloud Computing Technology Roadmap. **Nist Special Publication**, I e II, p. 85, 2014. Disponível em: <http://www.nist.gov/manuscript-publication-search.cfm?pub_id=915112>. Acesso em: 11 out. 2016.

NOOR, T. H.; SHENG, Q. Z. Trust as a service: a framework for trust management in cloud environments. In: INTERNATIONAL CONFERENCE ON WEB INFORMATION SYSTEMS ENGINEERING, 12., 2011, Sydney, Austrália. **Proceedings ...** Sydney, Austrália: Springer, 2011. p. 314–321.

NOOR, T. H. et al. Managing trust in the cloud: State of the art and research challenges. **Computer**, v. 49, n. 2, p. 34–45, Feb 2016.

NOOR, T. H. et al. Cloudarmor: Supporting reputation-based trust management for cloud services. **IEEE transactions on parallel and distributed systems**, IEEE, v. 27, n. 2, p. 367–380, 2016.

NOOR, T. H. et al. Trust management of services in cloud environments: Obstacles and solutions. **ACM Comput. Surv.**, ACM, New York, NY, EUA, v. 46, n. 1, p. 12:1–12:30, jul. 2013. ISSN 0360-0300.

PAN, M.; LI, M.; YU, Y. A group-choose algorithm supporting virtual organization creation for workflow deployment in cloud environment. **Concurrency and Computation: Practice and Experience**, Wiley Online Library, v. 25, n. 13, p. 1894–1908, 2013.

PAPAIOANNOU, T. G.; STAMOULIS, G. D. Reputation-based estimation of individual performance in collaborative and competitive grids. **Future Generation Computer Systems**, Elsevier, v. 26, n. 8, p. 1327–1335, 2010.

PEARSON, S.; BENAMEUR, A. Privacy, security and trust issues arising from cloud computing. In: INTERNATIONAL CONFERENCE ON CLOUD, 2., 2010, Indianapolis, IN, EUA. **Proceedings ...** Washington, DC, EUA: IEEE, 2010. p. 693–702.

PETRI, I. et al. Trust modelling and analysis in peer-to-peer clouds. **International Journal of Cloud Computing**, Inderscience Publishers Ltd, v. 1, n. 2-3, p. 221–239, 2012.

RESNICK, P.; ZECKHAUSER, R. Trust among strangers in internet transactions: Empirical analysis of ebay's reputation system. **The Economics of the Internet and E-commerce**, v. 11, n. 2, p. 23–25, 2002.

ROUSSEAU, D. M. et al. Not so different after all: A cross-discipline view of trust. **Academy of management review**, Academy of Management, v. 23, n. 3, p. 393–404, 1998.

RUAN, A.; MARTIN, A. Repcloud: Achieving fine-grained cloud tcb attestation with reputation systems. In: WORKSHOP ON SCALABLE TRUSTED COMPUTING, 6., 2011, Chicago, Illinois, EUA. **Proceedings ...** New York, NY, EUA: ACM, 2011. p. 3–14.

RUARO, A. F.; RABELO, R. J. Avaliação de ferramentas de computação em nuvem para empresas virtuais. In: BRAZILIAN SYMPOSIUM ON INFORMATION SYSTEMS, 12., 2016, Florianópolis. **Proceedings ...** Florianópolis: SBC, 2016. p. 417–424.

RUARO, A. F.; RABELO, R. J. Do cloud computing tools support the needs of virtual enterprises? In: IFIP WG 5.5 WORKING CONFERENCE ON VIRTUAL ENTERPRISES (PRO-VE 2016), 17., 2016, Porto, Portugal. **Proceedings ...** Porto, Portugal: Springer International Publishing, 2016. p. 200–211.

SAATY, T. L. How to make a decision: the analytic hierarchy process. **European journal of operational research**, Elsevier, v. 48, n. 1, p. 9–26, 1990.

SABATER, J.; SIERRA, C. Regret: Reputation in gregarious societies. In: **Proceedings of the Fifth International Conference on Autonomous Agents**. New York, NY, EUA: ACM, 2001. (AGENTS '01), p. 194–195. ISBN 1-58113-326-X.

SABATER, J.; SIERRA, C. Review on Computational Trust and Reputation Models. **Artificial Intelligence Review**, v. 24, n. 1, p. 33–60, 2005. ISSN 1573-7462.

SCEKIC, O.; TRUONG, H.-L.; DUSTDAR, S. Modeling Rewards and Incentive Mechanisms for Social BPM. In: INTERNATIONAL CONFERENCE ON BUSINESS PROCESS MANAGEMENT, 10., 2012, Tallinn, Estônia. **Proceedings ...** Tallinn, Estônia: Springer Berlin Heidelberg, 2012. p. 150–155.

SHARMA, A.; BANATI, H. A framework for implementing trust in cloud computing. In: INTERNATIONAL CONFERENCE ON INTERNET OF THINGS AND CLOUD COMPUTING, 2016, Cambridge, United Kingdom. **Proceedings ...** New York, NY, EUA: ACM, 2016. p. 6:1–6:7.

SIEGEL, J.; PERDUE, J. Cloud Services Measures for Global Use: The Service Measurement Index (SMI). In: ANNUAL SRII GLOBAL CONFERENCE, 2012, San Jose, CA, EUA. **Proceedings ...** Washington, DC, EUA: IEEE, 2012.

SQUICCIARINI, A. C.; PACI, F.; BERTINO, E. Trust establishment in the formation of virtual organizations. **Computer Standards & Interfaces**, Elsevier, v. 33, n. 1, p. 13–23, 2011. ISSN 0920-5489.

STINGL, D. et al. PeerfactSim.KOM: A simulation framework for Peer-to-Peer systems. In: INTERNATIONAL CONFERENCE ON HIGH PERFORMANCE COMPUTING AND SIMULATION, 2011, Istambul, Turquia. **Proceedings ...** Istambul, Turquia: IEEE, 2011. p. 577–584.

TAN, Z. et al. A novel trust model based on SLA and behavior evaluation for clouds. In: ANNUAL CONFERENCE ON PRIVACY, SECURITY AND TRUST, 14., 2016, Auckland, New Zealand. **Proceedings ...** Auckland, New Zealand: IEEE, 2016. p. 581–587.

TANG, M. et al. Towards a trust evaluation middleware for cloud service selection. **Future Generation Computer Systems**, Elsevier BV, v. 74, p. 302–312, set. 2017. ISSN 0167-739X.

TAVAKOLIFARD, M.; ALMEROTH, K. C. A taxonomy to express open challenges in trust and reputation systems. **Journal of Communications**, v. 7, n. 7, p. 538–551, 2012.

THEOHARIDOU, M.; TSALIS, N.; GRITZALIS, D. In cloud we trust: Risk-assessment-as-a-service. In: IFIP WG 11.11 INTERNATIONAL CONFERENCE ON TRUST MANAGEMENT, 7., 2013, Málaga, Espanha. **Proceedings ...** Málaga, Espanha: Springer Berlin Heidelberg, 2013. p. 100–110.

VAVILIS, S.; PETKOVIĆ, M.; ZANNONE, N. A reference model for reputation systems. **Decision Support Systems**, Elsevier, v. 61, p. 147–154, 2014. ISSN 0167-9236.

VIEIRA, R. G.; ALVES JUNIOR, O. C.; FIORESE, A. Analyzing Virtual Organizations Formation Risk in P2P SON Environments. In: INTERNATIONAL CONFERENCE ON ENTERPRISE INFORMATION SYSTEMS (ICEIS), 16., 2014, Lisboa, Portugal. **Proceedings ...** Lisboa, Portugal: Springer International Publishing, 2015. p. 285–301.

VOSE, D. **Risk analysis: a quantitative guide**. 3. ed. New Jersey, EUA: John Wiley & Sons, 2008.

VOSS, M.; WIESEMANN, W. Using Reputation Systems to Cope with Trust Problems in Virtual Organizations. In: INTERNATIONAL WORKSHOP ON SECURITY IN INFORMATION SYSTEMS, 3., 2005, Miami, FL, EUA. **Proceedings ...** Miami, FL, EUA: SCITEPRESS, 2005. p. 186–195.

WAZLAWICK, R. **Metodologia de pesquisa para ciência da computação, 2a edição**. 2. ed. Rio De Janeiro: Elsevier, 2014.

WHITBY, A.; JØSANG, A.; INDULSKA, J. Filtering out unfair ratings in bayesian reputation systems. In: INTERNATIONAL JOINT CONFERENCE ON AUTONOMOUS AGENTS AND MULTI AGENT SYSTEMS, 3., 2004, Roma, Itália. **Proceedings ...** Roma, Itália: Citeseer, 2004. p. 106–117.

WINKLER, T. J. et al. Trust Indicator Modeling for a Reputation Service in Virtual Organizations. In: EUROPEAN CONFERENCE ON INFORMATION SYSTEMS, 2007, St. Gallen, Suiça. **Proceedings ...** St. Gallen, Suíça: University of St. Gallen, 2007. p. 1584–1595.

XIE, F. et al. A risk management framework for cloud computing. In: INTERNATIONAL CONFERENCE ON CLOUD COMPUTING AND INTELLIGENCE SYSTEMS, 2., 2012, Hangzhou, China. **Proceedings ...** Hangzhou, China: IEEE, 2012. p. 476–480.

XIE, J.; ZHONG, J.; DENG, P. A robust trust management model for e-commerce system. In: INTERNATIONAL CONFERENCE ON E-BUSINESS ENGINEERING, 11., 2014, Guangzhou, China. **Proceedings ...** Guangzhou, China: IEEE, 2014. p. 170–176.

XIONG, L.; LIU, L. Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities. **IEEE Transactions on Knowledge and Data Engineering**, IEEE, v. 16, n. 7, p. 843–857, 2004.

YU, H. et al. A Survey of Trust and Reputation Management Systems in Wireless Communications. **Proceedings of the IEEE**, v. 98, n. 10, p. 1755–1772, Out 2010. ISSN 0018-9219.

ZAMANIAN, M.; MOHSENZADEH, M.; NASSIRI, R. A novel framework for virtual organization creation on cloud. In: CAMARINHA-MATOS, L. M.; AFSARMANESH, H. (Ed.). **Proceedings ...** Amsterdã, Holanda: Springer Berlin Heidelberg, 2014. p. 435–442.

ZHANG, L. et al. Robustness of trust models and combinations for handling unfair ratings. In: IFIP WG 11.11 INTERNATIONAL CONFERENCE ON TRUST MANAGEMENT, 6., 2012, Surat, Índia. **Proceedings ...** Berlim: Springer, 2012. p. 36–51.

ZHANG, Q.; CHENG, L.; BOUTABA, R. Cloud computing: state-of-the-art and research challenges. **Journal of Internet Services and Applications**, v. 1, n. 1, p. 7–18, 2010. ISSN 1869-0238.

APÊNDICE A – MODELAGEM CONCEITUAL DA ARQUITETURA

Esse apêndice tem por objetivo apresentar a modelagem conceitual da arquitetura de reputação desenvolvida, considerando uma representação de mais alto nível. São apresentados os diagramas da *Unified Modeling Language* (UML): i) casos de uso e ii) sequência.

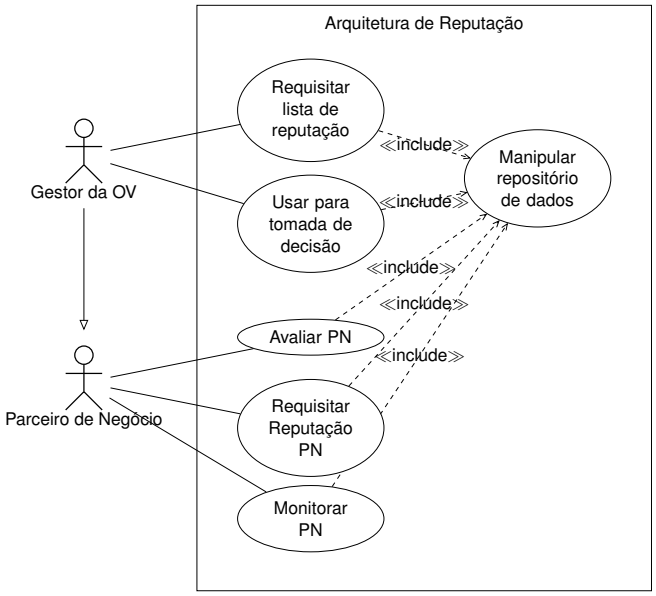
O diagrama de caso de uso apresenta as funcionalidades disponibilizadas pela arquitetura, enquanto o diagrama de sequência exibe a troca de mensagens e as interações entre os elementos da arquitetura.

A.1 DIAGRAMA DE CASOS DE USO

Tem como objetivo principal apresentar uma visão externa das funcionalidades do sistema ou objeto que está sendo analisado, sem se preocupar como essas funcionalidades serão implementadas. Ainda, este diagrama é utilizado como base para prosseguir com o desenvolvimento dos outros diagramas da UML, como por exemplo diagrama de sequência (BEZERRA, 2007).

O diagrama de casos de uso da arquitetura de reputação, ilustrado na Figura 31, apresenta as funcionalidades da arquitetura para dois atores, o gestor da OV e o parceiro da negócio da OV, e ainda PN representa o provedor de nuvem.

Figura 31 – Diagrama de casos de uso



Fonte: Produção do próprio autor.

Deste modo, através das funcionalidades presentes no diagrama de casos de uso, o gestor da OV pode utilizar as informações de reputação do PN para a tomada de decisão. O gestor da OV compartilha as mesmas funcionalidades que o parceiro de negócio é capaz de realizar com a arquitetura de reputação. Tais funcionalidades podem ser brevemente descritas como:

- **Requisitar lista de reputação**: O gestor da OV pode requisitar a lista de reputação dos PNs presentes no repositório de dados da arquitetura de reputação e utilizar esses valores para a tomada de decisão, por exemplo, seleção de provedores de nuvem com base na sua reputação;
- **Usar para tomada de decisão**: O gestor da OV utiliza as informações de reputação para a tomada de decisão durante o ciclo de vida da OV;
- **Avaliar PN**: O parceiro de negócio avalia subjetivamente o PN na fase de dissolução da OV;
- **Requisitar Reputação**: O parceiro de negócio/gestor da OV pode requisitar a reputação de um provedor de nuvem a qualquer momento;
- **Monitorar PN**: O parceiro de negócio/gestor da OV pode requisitar ações de monitoramento dos indicadores de QoS dos PNs à arquitetura de reputação;
- **Manipular o repositório de dados**: Todos os casos de uso bem como os demais módulos da arquitetura utilizam o repositório de dados para atender a solicitação do usuário da arquitetura.

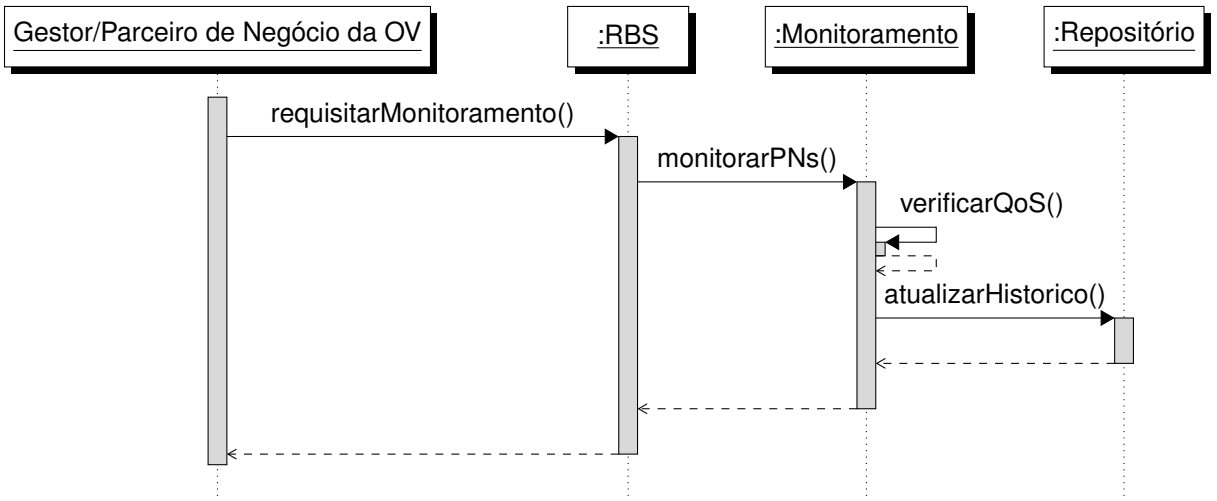
A.2 DIAGRAMAS DE SEQUÊNCIA

O diagrama de sequência busca representar a sequência de interações (mensagens trocadas entre objetos) de um módulo, componente ou sistema que está sendo analisado (BEZERRA, 2007).

Para analisar a arquitetura proposta, construiu-se diagramas de sequência para os principais casos de uso que são referentes as operações disponibilizadas pela arquitetura, como: monitoramento de QoS dos provedores de nuvem, requisição do valor de reputação dos provedores de nuvem e o envio de *feedbacks* dos parceiros de negócio ao provedor de nuvem.

Assim, a Figura 32, apresenta a troca de mensagens na operação de monitoramento de QoS. Tal operação, quando requisitada, verifica o QoS de cada provedor de nuvem, realiza a coleta de novas informações referentes ao QoS e atualiza os valores de QoS deste provedor de nuvem no repositório de dados da arquitetura de reputação.

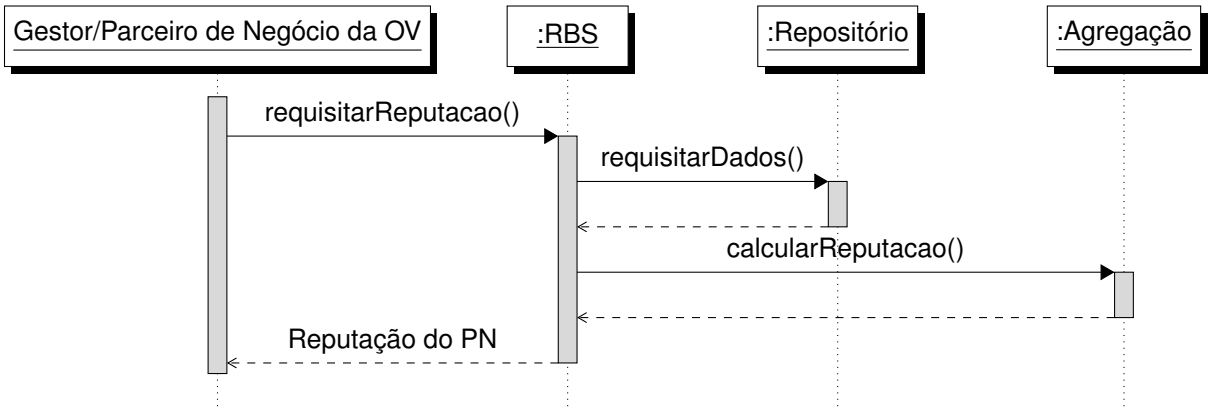
Figura 32 – Módulo de monitoramento



Fonte: Produção do próprio autor.

A operação de requisição do valor de reputação de um PN ou de todos os PNs (lista de reputação) tem seu diagrama de sequência apresentado na Figura 33.

Figura 33 – Interação na requisição da reputação de um PN



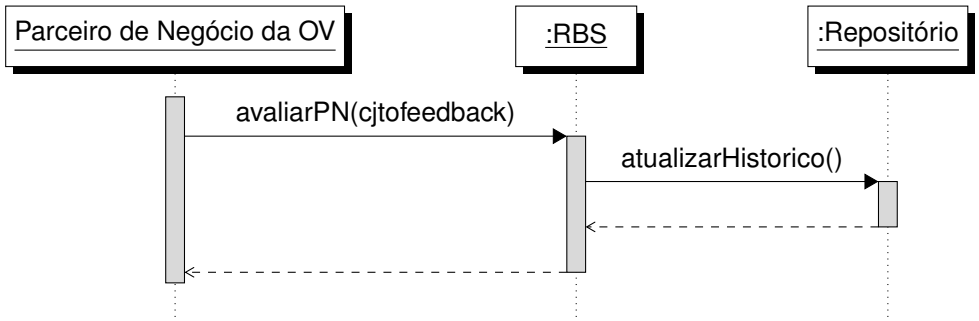
Fonte: Produção do próprio autor.

Por exemplo, o gestor da OV ou parceiro de negócio da OV solicita o valor de reputação de um determinado PN ao RBS, que busca o histórico de participações objetivas (combinando os dados de monitoramento (se existirem)) e subjetivas do PN no repositório de dados e, por fim, envia esses dados ao módulo de agregação que retorna a reputação do PN ao solicitante.

A operação de envio de *feedbacks* (avaliações), ocorre principalmente na fase de dissolução da OV, quando os parceiros de negócio avaliam subjetivamente os pro-

vedores de nuvem utilizados. A sequência de interações dessa operação é apresentada pelo diagrama presente na Figura 34.

Figura 34 – Envio de avaliação subjetiva do membro da OV ao PN



Fonte: Produção do próprio autor.

Desta forma, um parceiro de negócio da OV que deseja avaliar subjetivamente um PN envia seu *feedback*, composto de um conjunto de avaliações, ao RBS que verifica e atualiza o histórico do indicador de confiança subjetiva do PN no repositório de dados da arquitetura de reputação.