Uma Abordagem Estratificada à Monitorização de Serviços Cloud

Nuno Palhares, Solange Rito Lima
Departamento de Informática, Centro Algoritmi
Universidade do Minho
Campus de Gualtar
4710-057 Braga, Portugal
Email: nunopalhares89@gmail.com, solange@di.uminho.pt

***Resumo*—A monitorização de redes é uma tarefa essencial na gestão e engenharia das redes de comunicações atuais. Face a paradigmas como *Cloud Computing* e *Cloud Services*, os desafios colocados à monitorização de redes e serviços são ainda mais variados e exigentes. *Cloud Computing* inclui modelos de serviços distintos (IaaS, PaaS, SaaS), compartilhando algumas necessidades comuns na medição de infraestruturas, mas com especificidades de acordo com o tipo de serviço prestado e recursos envolvidos. Posto isto, é essencial ter uma visão geral dos distintos aspetos relacionados com a monitorização de serviços *Cloud*, para uma melhor compreensão dos pontos-chave e promover a qualidade dos serviços prestados. Neste contexto, este artigo apresenta uma abordagem estratificada à monitorização de Serviços *Cloud*. O objetivo principal prende-se com a identificação das várias dimensões da monitorização de serviços *Cloud*, combinando as perspetivas do fornecedor de infraestruturas e de serviços, e dos clientes. Consequentemente, a monitorização do estado dos recursos, da qualidade de serviço, qualidade de experiência e contratos de serviço são aspetos a cobrir. Este processo envolve a identificação de parâmetros e métricas relevantes para cada dimensão monitorizada.**

I. Introdução

Hoje em dia temos presenciado a um crescimento da oferta de serviços baseados em *Cloud Computing*. Este facto deve-se sobretudo à descida dos custos capitais e operacionais (CapEx e OpEx) associados à tecnologia, fruto do aumento da concorrência. Este fator, aliado às vantagens de *Cloud Computing* têm-se traduzido num aumento exponencial da tecnologia. Relativamente ao conceito, as *Clouds* são um grande conjunto de recursos virtualizados facilmente utilizáveis e acessíveis (como *hardware*, plataformas de desenvolvimento e/ou serviços). Esses recursos podem ser dinamicamente reconfigurados para se ajustarem a uma carga variável, permitindo também uma melhor utilização dos recursos. Este conjunto de recursos é tipicamente explorado por um modelo *pay-per-use* (também conhecido por *pay-as-you-go*), em que as garantias são oferecidas pelo fornecedor da infraestrutura, por meio de SLAs (*Service Level Agreements*) personalizados [1].

Uma das preocupações constantes das empresas está relacionada com a monitorização e gestão de redes e serviços. A gestão dos serviços *Cloud* é sustentada por ações como visualização, controlabilidade e automação em ambientes virtuais. Este tipo de ações assume um papel importante no apoio à gestão da complexidade associada a *Cloud Computing*. A visualização é uma vantagem para um gestor de serviços, na medida em que ajuda a responder rapidamente a eventos e a tomar melhores decisões, enquanto o controlo ajuda a gerir riscos e a automação a reduzir custos. Em *Cloud Computing*, na perspetiva do serviço *Cloud* para o fornecedor e cliente, a gestão destes serviços e a garantia de QoS (*Quality of Service*), tornou-se uma das dificuldades do desenvolvimento da tecnologia. Perante este cenário, torna-se essencial ter uma visão global de todos os aspetos que possam interferir na qualidade do serviço prestado e que por sua vez devem ser tidos em conta no processo de monitorização e gestão.

Uma das questões mais importantes passa pela monitorização dos diferentes modelos de implementação de serviços *Cloud*. De facto, cada modelo de implementação possuí as suas próprias características e necessidades, logo necessita de diferentes abordagens de monitorização. As diferenças existem principalmente entre as *Private Clouds* e as *Public Clouds* (ver conceitos na secção II). Nas *Private Clouds* uma empresa apenas tem de lidar com os seus próprios recursos. Devido às suas políticas de segurança, os dados relevantes estão sob o controle da organização. Por outro lado, as *Public Clouds* exigem um maior investimento na monitorização do tráfego, devido sobretudo à difusão geográfica e aos grandes conjuntos de recursos envolvidos, assim como à necessidade de mais flexibilidade, escalabilidade e segurança. As questões de segurança, tais como configurações de *firewalls*, podem afetar e limitar aspetos relacionados com a monitorização entre os fornecedores de serviços *Cloud*. As *Public Clouds* necessitam ainda de fornecer informações sobre a monitorização aos seus clientes, o que requer mais flexibilidade, segurança e customização.

As características das *Public Clouds* levantam ainda preocupações relacionadas com a distribuição geográfica dos recursos que constituem a base da infraestrutura *Cloud*. À primeira vista, pode parecer que em *Cloud Computing* já não existe a preocupação sobre a localização geográfica. Essa ideia advém da sua natureza permitir um amplo acesso à rede, característica herdada da Internet e na qual se baseia. Contudo, a computação em nuvem não pode sobrepor-se às leis da física e os atrasos consequentes numa transmissão de dados podem tornar-se um verdadeiro problema ao fornecimento de

um serviço de qualidade. Utilizadores em localizações remotas podem estar sujeitos a latências inaceitáveis, limitando o grau de interatividade e interferindo nos parâmetros relacionados com QoS e QoE (*Quality of Experience*).

De outra perspetiva, um tópico bastante pertinente e que deve ser tido em consideração na monitorização *Cloud* são cada vez mais as questões energéticas. As mudanças do clima e o aquecimento global são dois dos problemas mais relevantes para o nosso planeta, onde o aumento das temperaturas está diretamente relacionado com a quantidade de dióxido de carbono produzida. Posto isto, nos vários ramos da ciência e da tecnologia, nos últimos anos tem existido um investimento na investigação e desenvolvimento de soluções "amigas" do ambiente. Neste contexto surgiram termos como *Green IT* e *Green Cloud Computing*. O desafio em *Green Cloud Computing* passa por minimizar a utilização de recursos e continuar a satisfazer a qualidade dos serviços requisitados e a sua robustez, contribuindo não só para uma redução dos custos operacionais como também do impacto ambiental [6], [7]. Assim, as questões energéticas são sobretudo um aspeto a ser associado à monitorização das infraestruturas ao nível dos recursos físicos.

Outra das grandes preocupações inerentes à monitorização prende-se com as questões de segurança. Este é um tópico em que tem havido grande investigação por ser crucial para a implantação do paradigma pois relaciona-se com a confiança e adesão dos clientes. A segurança está associada a aspetos de elevada importância, tais como a integridade, disponibilidade, privacidade e autenticidade dos dados e dos utilizadores.

Numa perspetiva fornecedor/cliente, na prestação de serviços *Cloud* levantam-se questões económicas e contratuais, devendo os serviços ser prestados de acordo com os SLAs e requisitos de QoS e QoE estabelecidos. Um fornecedor de um serviço *Cloud* deve estar em constante contacto com o cliente e deve levar em consideração o seu *feedback* para melhorar a qualidade do serviço prestado. Assegurar a qualidade de serviço e outros requisitos pertinentes, como a segurança, são metas que se revelam um processo complexo e difícil, fruto do uso de ambientes virtuais e por vezes de infraestruturas de outras empresas. No caso da ocorrência de conflitos de interesse que possam surgir entre fornecedores e clientes, a adoção de uma *third-party* neutra, responsável pela monitorização do desempenho do serviço, parece ser a melhor solução [3]. Respeitar um SLA é o primeiro passo para uma boa interação entre fornecedores e clientes, já que o objetivo de um SLA é garantir que a QoS e QoE são compreendidas da mesma forma por ambos. Os SLAs funcionam como um dos instrumentos primários de controlo por parte do utilizador. Face a estes fatores, a necessidade de um sistema de monitorização eficiente e transparente revela-se um requisito de particular importância.

Neste contexto, e conciliando as várias vertentes da monitorização focadas, o presente artigo apresenta uma abordagem estratificada à monitorização dos serviços *Cloud*. Para cada camada do modelo proposto apresentam-se os principais parâmetros e métricas a considerar, reunindo assim num modelo integrado as diferentes necessidades de monitorização e as perspetivas das diferentes entidades participantes. Pretende-se, desta forma, reunir e clarificar os principais aspectos envolvidos na monitorização em *Cloud* e fomentar o desenvolvimento de plataformas de monitorização abrangentes e flexíveis.

Este artigo está organizado da seguinte maneira. Na secção II é fornecida uma contextualização das definições usadas em *Cloud Computing*. Na secção III é apresentado o trabalho relacionado na área da monitorização, com a identificação de ferramentas e plataformas/*frameworks* neste contexto. Seguidamente, na secção IV é apresentada a proposta estratificada à monitorização dos Serviços *Cloud*, identificando num modelo por camadas as várias dimensões envolvidas na monitorização destes serviços. Por fim, na secção V são apresentadas as principais conclusões do trabalho efetuado, assim como as propostas de trabalho futuro.

II. Conceitos

De seguida são apresentados alguns conceitos inerentes à tecnologia *Cloud Computing*, tais como os Modelos de Serviço e os Modelos de Implementação existentes.

A. Modelos de Serviço

Os serviços *Cloud Computing* estão divididos em modelos de serviço, de acordo com a sua natureza. Os três principais modelos que estruturam a arquitetura *Cloud* são os IaaS (*Infrastructure as a Service*), PaaS (*Platform as a Service*) e SaaS (*Software as a Service*), descritos de seguida. Os serviços relativos às infraestruturas são considerados a camada inferior, seguidos pelos ambientes/plataformas de desenvolvimento. As aplicações são o *front-end* do utilizador e residem no topo da pilha *Cloud* [2], [3]. Na Tabela I estão ilustrados alguns exemplos de serviços classificados segundo os modelos discutidos, assim como a relação Vendedor/Comprador de cada modelo de serviço.

- **Infrastructure as a Service (IaaS)**: este modelo de serviço fornece recursos computacionais virtuais, nomeadamente poder de processamento, de armazenamento e de comunicação. O cliente não tem privilégios para controlar a infraestrutura *Cloud* subjacente, porem possui controlo sobre as aplicações desenvolvidas, sistemas operativos, armazenamento e alguns componentes de rede.
- **Platform as a Service (PaaS)**: este é um modelo que disponibiliza um conjunto de ferramentas necessárias ao desenvolvimento de aplicações *online*, sem que haja preocupações com a sua hospedagem. As ferramentas disponibilizadas fornecem um conjunto bem integrado e especializado de serviços que incorporam tudo o que um programador necessita nas áreas de desenvolvimento, teste, publicação, hospedagem e manutenção de aplicações.
- **Software as a Service (SaaS)**: o objetivo deste tipo de modelo passa por disponibilizar aos clientes, aplicações que correm sobre uma infraestrutura *Cloud*. O ambiente de execução é a Internet e as aplicações estão acessíveis através de vários dispositivos clientes, com recurso a

interfaces como um *web browser*. O utilizador não está necessariamente a pagar pela compra de um sistema, ou seja, está apenas a adquirir o direito de utilizar um serviço, o que na sua essência é um *software* como muitos outros existentes.

Tabela I
EXEMPLOS DE SERVIÇOS.

Modelos de Serviço	Exemplos	Vendedores	Compradores
IaaS	Amazon Web Services, Microsoft Hyper-VGoGrid, Proofpoint, Rackspace, RightScale, IBM (Blue Cloud), VMWare VCloud, Sun (Project Carloine), HP Adaptative IaaS EMC, Windows Azure...	Fornecedores de Datacenters	Empresas
PaaS	Google App. Engine, Windows Azure, dotCloud, Salesforce, Redhat, Oracle, Cloudera, Cloud Foundry...	Fornecedores de Plataformas de Serviço	Companhias de Desenvolvimento de Software
SaaS	Office 365, Salesforce, Google Apps., Yahoo (Zimbra), Concur, Taleo, Netsuite, Proofpoint, Dropbox, Workday, Hotmail...	Companhias de Software	Utilizadores Finais

B. Modelos de Implementação

Numa perspetiva organizacional, existem formas básicas nas quais os serviços *Cloud* podem ser implementados. Os três modelos mais populares são os seguintes [2], [3]:

- **Public Cloud**: disponibilizam recursos de computação ao público em geral ou a um grande grupo de indústrias, através da Internet. Os utilizadores deste modelo utilizam serviços que são disponibilizados por organizações especializadas na venda de serviços *Cloud*. Neste caso o termo "*public*" nem sempre significa que o serviço não tem custos, apenas caracteriza o modo de acesso à sua interface. Os clientes alugam o acesso dos recursos conforme necessitam, baseando-se num modelo de pagamento *pay-as-you-go*.
- **Private Cloud**: neste tipo de implementação os serviços e os recursos computacionais estão exclusivamente dedicados a uma organização particular e não são partilhados com outras organizações. A diferença para as *Public Clouds* reside no facto dos dados e processos serem geridos dentro de uma organização. Não existem restrições ao nível da largura de banda da rede, exposições a falhas de segurança ou requisitos legais inerentes à sua utilização. As questões de segurança não são uma questão fundamental como nas *Public Clouds*, uma vez que os recursos estão protegidos pelas políticas de segurança (*firewall*) da própria empresa.
- **Community Cloud**: a infraestrutura *Cloud* é partilhada por várias organizações e suporta uma comunidade que partilha alguns interesses (e.g. uma missão comum, requisitos específicos de segurança, políticas entre outras considerações). Os membros da comunidade partilham o acesso aos dados e aplicações da *Cloud* em questão. Estão localizadas tanto no local como fora do estabelecimento e a sua gestão pode ser levada a cabo por uma organização ou por uma *third party*.
- **Hybrid Cloud**: este é um modelo que resulta da combinação das características dos tipos de modelos anteriormente descritos, tal como o nome sugere. Resumidamente, uma *Private Cloud* possui as suas infraestruturas locais complementadas com o poder de computação de uma *Public Cloud*.

III. TRABALHO RELACIONADO

Uma das preocupações constantes dos fornecedores de serviços está relacionada com a monitorização e gestão dos serviços *Cloud*. Existe a necessidade de identificar, antecipar e reportar falhas, com vista a uma otimização dos serviços e respetiva satisfação dos clientes. Os administradores de sistemas e os próprios utilizadores finais podem monitorizar e gerir os seus recursos de várias formas, dependendo do tipo de serviço em questão. Na Tabela II estão indicadas algumas das ferramentas de monitorização disponíveis, estando divididas de acordo com a técnica e paradigma a que obedecem. A monitorização local, tal como o nome indica, é feita localmente nos respetivos ambientes. Na monitorização remota, as ferramentas de monitorização são distribuídas e escaláveis, suportando sistemas de computação de alto desempenho, como *clusters* ou *grids*. Uma outra forma de monitorização é através de plataformas de gestão web, cuja oferta no mercado é maior, devido sobretudo à competitividade entre empresas de desenvolvimento deste tipo de produtos.

Tabela II
FERRAMENTAS DE MONITORIZAÇÃO.

Tipo	Exemplos
Local	Sysstat (Isag, Ksars), Dstat.
Remota	Nagios, Ganglia, GroundWork, Cacti, MonALISA, GridICE.
Plataformas de Gestão Web	RightScale, Landscape, Amazon CloudWatch, Gomez, Hyperic/Cloud Status, 3Tera, Zenos, Logic Monitor, Nimsoft, Monitis, Kaavo, Tap in systems, CloudKick, Enstratus, YLastic, TechOut, ScienceLogic, Keynote, NewRelic.

Para além das ferramentas acima citadas, existem ainda algumas propostas de *frameworks* e sistemas de monitorização que procuram dar os primeiros passos. Dois exemplos de projetos neste âmbito são o *Lattice* [4] e o *PCMONS* [5].

Em relação ao *framework Lattice*, este foi desenhada sobretudo para monitorizar recursos e serviços em ambientes virtuais. Resumidamente, este *framework* foi desenvolvido e implementado em conjunto com o projeto RESERVOIR. O RESERVOIR é um serviço *Cloud* que distingue fornecedores de serviços dos fornecedores de infraestruturas e tem como objetivo aumentar a eficácia da computação, permitindo o desenvolvimento de serviços complexos. São abrangidas questões geográficas e de QoS, tentando também assegurar garantias de segurança. Por sua vez, o *Lattice* recorre a

um sistema de monitorização de *probes* para coletar dados para o sistema de gestão. Os autores tiveram o cuidado de implementarem um sistema que não fosse intrusivo, de modo a não afetar adversamente o desempenho do sistema ou de qualquer aplicação em execução. Para aumentar o poder e a flexibilidade da monitorização é introduzido o conceito de "fonte de dados" (*data source*). As fontes de dados podem conter de uma maneira dinâmica múltiplos *probes*. As fontes de dados delineadas são os recursos físicos, os recursos virtuais e as aplicações de serviço. Contudo, o *framework Lattice* é flexível e não se limita somente a este tipo de fonte de dados. O seu design permite que tanto as fontes de dados como os próprios tipos de *probes* sejam desenhados e planeados conforme as necessidades e objetivos.

Quando ao PCMONS, é um sistema que tem presente a ideia de que a monitorização pode beneficiar de ferramentas e conceitos já estabelecidos na gestão de computação distribuída. O seu objetivo principal passa por implementar um sistema de monitorização em *Private Clouds*, com recurso a *software open source*, nomeadamente o Nagios. Os autores argumentam que devido às características únicas de cada modelo de serviço, não é possível chegar a uma solução de gestão genérica. Face a este facto, para a solução proposta, optaram por um modelo IaaS, devido sobretudo à sua flexibilidade, e por *Private Clouds*, uma vez que estão sob o controlo das políticas de segurança da respetiva empresa. A arquitetura do sistema de monitorização é composta por três camadas e equipara-se a um modelo centralizado onde é utilizada a ligação cliente/servidor. A camada base corresponde às infraestruturas e basicamente contém as instalações (*hardware* e rede), assim como *software*. A camada do meio (*Integration Layer*) é responsável por abstrair os detalhes das infraestruturas e é composta por vários módulos, permitindo ao sistema ser adaptável e extensível (*plug-ins*) a outros cenários/ferramentas. A camada superior corresponde à visualização e fornece uma interface (no caso a do Nagios) onde através da análise das várias informações disponíveis, pode ser comprovado o cumprimento das políticas e dos SLAs estabelecidos.

IV. Monitorização Estratificada de Serviços Cloud

Esta secção apresenta a abordagem estratificada proposta para a monitorização de serviços *Cloud*, indicando as várias dimensões da monitorização destes serviços. Para cada dimensão são identificadas e propostas métricas relevantes para a monitorização a efetuar. Após uma análise da bibliografia e de referências relevantes na área, é possível constatar que ainda não existe um consenso na classificação de métricas que satisfaçam todos os requisitos impostos pelos ambientes *Cloud*. Portanto, uma apropriada classificação das métricas e a sua normalização são um grande desafio a cumprir, tendo em vista uma gestão eficiente e a otimização dos serviços *Cloud*.

Na secção IV-C são abordadas questões relacionadas com QoE. Por fim é estabelecida uma relação entre a abordagem proposta e os modelos de serviço existentes.

A. Abordagem Estratificada Proposta

Conforme mencionado, o modelo definido tem como objetivo abranger as várias dimensões envolvidas na monitorização de serviços *Cloud*. O modelo está estratificado em 4 camadas principais, que por sua vez se subdividem em algumas categorias. As 4 camadas principais correspondem à Infraestrutura, à Rede, ao Serviço/Aplicação e à relação Cliente/Fornecedor, conforme ilustrado na Figura 1. A camada referente às Infraestruturas abrange tanto os recursos físicos como os recursos virtuais envolvidos no complexo ambiente de *Cloud Computing*. Para além da necessidade de monitorizar os diversos componentes que constituem toda uma infraestrutura, existem ainda outras questões que devem ser monitorizadas a este nível, como as questões energéticas e de segurança. Na camada de Rede são abrangidos aspetos relacionados sobretudo com o serviço IP, como o débito e as questões de desempenho e disponibilidade/fiabilidade. Ao nível da camada de Serviço/Aplicação, a monitorização incide em questões que permitem avaliar a disponibilidade/fiabilidade, desempenho e segurança de um serviço, entre outros aspetos. Por fim a relação Cliente/Fornecedor de serviço deve ser alvo de uma monitorização ao nível da auditoria dos SLA, da contabilização do uso/custo e dos aspetos de segurança. De seguida são abordadas as 4 camadas em maior detalhe.

Figura 1. Modelo estratificado proposto para a monitorização de serviços Cloud.

1) Infraestrutura: Como base e suporte de toda uma arquitetura complexa que envolve o ambiente *Cloud Computing*, as infraestruturas físicas são um dos focos principais a ter em conta no processo de monitorização. Todos os componentes físicos, desde dispositivos de processamento, armazenamento, até aos de rede (*switches*, *routers*) devem ser monitorizados. A maioria das referências na área é unânime em considerar como métricas mais relevantes a percentagem de utilização de CPU, RAM, memória de armazenamento, assim como as estatísticas das interfaces de rede das máquinas físicas [4], [6], [7], [8], [9]. Como já referido, os dispositivos de rede devem ser igualmente monitorizados, pois problemas ao nível dos *switches*, *routers* ou mesmo dos *links* podem afetar a conetividade da topologia. Uma topologia instável pode acarretar problemas que influenciem todo um conjunto de aspetos, como, por exemplo, a engenharia de tráfego, o débito, a disponibilidade de um serviço, violações dos SLA, questões económicas, entre outros.

No que toca às questões energéticas, uma parte significativa da energia elétrica consumida pelos recursos de computação

é transformada em calor, o que por sua vez acarreta alguns problemas. As altas temperaturas reduzem o tempo de vida dos dispositivos/componentes e acabam também por influenciar a fiabilidade e disponibilidade do sistema. Por sua vez, os procedimentos de gestão de energia podem afetar o desempenho do sistema de uma maneira complexa, dado que a taxa de computação global é resultado da velocidade e da coordenação de múltiplos elementos dentro de um sistema [10]. Assim, tendo em atenção as questões energéticas na monitorização *Cloud*, sobretudo ao nível das infraestruturas, na Tabela III estão indicadas algumas das métricas a considerar, retiradas de referências na área que podem ser associadas a este tópico. Segundo [10], onde são levados em consideração aspetos ecológicos e de desempenho no sistema de gestão de recursos (métricas, técnicas, modelos, políticas, algoritmos), o consumo de energia é uma boa métrica para abordar as questões relacionadas com a energia. Também em [7], o consumo de energia é uma métrica levada em consideração. Por sua vez, em [6] são propostas também métricas ao nível do controlo das temperaturas e sistemas de *backup* de energia (geradores, UPS). Estas são métricas que surgem no contexto da solução proposta pelos autores para a gestão de recursos, baseada em modelos organizados e compostos por agentes autónomos. O objetivo passa sobretudo por otimizar a utilização de energia e reduzir a emissão de dióxido de carbono.

Relativamente à segurança das infraestruturas ao nível dos recursos físicos é tido como base o trabalho proposto em [11], [12], onde são recomendadas algumas restrições e auditorias à segurança *Cloud*. Os autores baseiam-se no trabalho efetuado pela *Cloud Security Alliance* (CSA), onde a *Cloud* é modelada em sete camadas, nomeadamente: *Facility, Network, Hardware, OS, Middleware, Application e User*. Visto que nesta etapa são abordados os recursos físicos *Cloud*, podem ser associadas as três primeiras camadas propostas pela CSA. Portanto, tendo em conta a análise feita às camadas *Facility, Network* e *Hardware* podem ser extraídas métricas de alguns dos procedimentos propostos, conforme os exemplos apresentados na Tabela III. No que toca às instalações (*Facility*) a segurança é sobretudo ao nível físico, onde podem ser implementados controlos de acesso através de videovigilância, vários sistemas de autenticação, sistemas de alarmes e sensores, entre outros. Os objetivos principais passam por evitar infiltrações maliciosas, manipulações de dados e assegurar a própria integridade das instalações e componentes. Ao nível do *Hardware* propriamente dito, as medidas de segurança estão em conformidade com as adotadas nas instalações, onde devem ser seguidos os protocolos de segurança. No que diz respeito à camada *Network*, devido à sua natureza, que pode ser descrita como a fronteira entre os dados dos clientes e os próprios clientes (inseridos por vezes em redes sujeitas a ameaças), podem ser adotadas *Firewalls*, *Intrusion Detection Systems* (IDS), *Intrusion Prevention Systems* (IPS), entre outros mecanismos.

Ainda a nível das infraestruturas, os recursos virtuais assumem um papel muito interventivo num ambiente de *Cloud Computing*, pelo que a sua monitorização se torna um

Tabela III
EXEMPLOS DE MÉTRICAS PARA A CAMADA DOS RECURSOS FÍSICOS.

Layer	Categoria	Exemplo de Métricas
Infraestrutura	Componentes	CPU (percentagem de utilização, nº de cores), RAM (percentagem de utilização), memória de armazenamento (percentagem de utilização, velocidade de leitura e escrita), estatísticas das interfaces de rede, conectividade da topologia.
Recursos Físicos	Energia	Consumos de energia, temperaturas, estado dos geradores e UPS.
	Segurança	Alarmes/sensores de incêndio, vigilância, controlo de acessos, sistemas de autenticação, monitorização de *firewalls*, IDS, IPS.

aspeto essencial. Os processos envolvidos na virtualização são constituídos por algumas operações importantes, como a suspensão/reinício/migração e início/paragem de *Virtual Machines* (VMs). Estas são operações abordadas em muitos dos recentes trabalhos de investigação, tendo em vista o desenvolvimento de métricas, como por exemplo a "utilização" [10]. Várias referências apontam os diversos componentes dos recursos virtuais como aspetos a monitorizar. As métricas mais comuns a este nível estão relacionadas sobretudo com a percentagem de utilização do CPU, RAM e memória de armazenamento das VMs (ver Tabela IV). As estatísticas das interfaces de rede das VMs são igualmente relevantes. Operações relacionadas com os processos de criação e migração de VMs ou número de instâncias ativas são também informações úteis [4], [6], [7], [8], [9].

Quanto à segurança nos recursos virtuais das infraestruturas, podem ser associadas as camadas *OS* e *Middleware* abordadas em [11], [12]. Neste caso as métricas a serem levadas em consideração devem ser extraídas da monitorização dos Sistemas Operativos ao nível dos eventos assim como do sistema de chamadas entre as VMs e o *hardware*. O objetivo passa sobretudo por evitar a cópia e modificações de dados. A camada *Middleware*, segundo os autores em [12], é considerada um potencial ponto fraco, pois encontra-se entre as camadas do OS e das Aplicações, envolvendo assim bastantes componentes, conforme o serviço e respetiva arquitetura em questão. Nesta camada, as métricas devem estar assim associadas à monitorização da virtualização e dos sistemas de segurança em arquiteturas *Cloud* heterogéneas.

2) Rede: Passando para a camada de "Rede", a classificação das categorias que a caracterizam e as respetivas métricas são sobretudo ao nível do Serviço IP. A subdivisão nesta camada é efetuada nas seguintes categorias: Débito, Desempenho e Disponibilidade/Fiabilidade (ver Tabela V). As métricas propostas para estas categorias estão associadas às métricas tradicionais das redes de computadores e telecomunicações, provenientes sobretudo dos esforços dedicados a este tópico pela International Telecommunications Union - Telecommunication Standardization Sector (ITU-T) e pelo grupo de trabalho IP Performance Metrics (IPPM) do IETF.

No que diz respeito ao Débito são várias as referências que

Tabela IV
EXEMPLOS DE MÉTRICAS PARA A CAMADA DOS RECURSOS VIRTUAIS.

Layer	Categoria	Exemplo de Métricas
Infraestrutura Recursos Virtuais	Componentes	CPU (percentagem de utilização, nº de cores), RAM (percentagem de utilização), memória de armazenamento (percentagem de utilização, velocidade de leitura e escrita), estatísticas das interfaces da VM, migrações de VM, número de instâncias ativas.
	Segurança	Monitorização de eventos e do OS ao nível do sistema de chamadas entre VMs e o *hardware*.

Tabela V
EXEMPLOS DE MÉTRICAS PARA A CAMADA DE REDE.

Layer	Categoria	Exemplo de Métricas
Rede	Débito	Volume de tráfego por unidade de tempo, largura de banda utilizada e disponível, capacidade.
	Desempenho	Duplicação de pacotes, perda de pacotes (OWPL, OWLP, IPLR), atraso (OWD, RTT, IPTD, IPDV), IPER, SPR.
	Disponibilidade/ Fiabilidade	*UP time*, (in)disponibilidade da rede, conetividade (*one* ou *two-way*), tempo de resposta (médio e máximo), tempo médio de restauro em caso de falhas, tempo médio entre falhas.

o classificam como essencial no processo de monitorização *Cloud* [13], [14]. Para além da importância ao nível das decisões relacionadas com a engenharia de rede, as questões económicas também estão "atentas" a este aspeto. Devido à sua natureza, o débito pode variar constantemente, o que leva a que as métricas que lhe estão relacionadas sejam monitorizadas de perto e tendo em vista o cumprimento dos SLA [15]. Na análise do volume de tráfego por unidade de tempo, uma monitorização ao nível de classes de serviço pode trazer benefícios, nomeadamente para a otimização da utilização da rede, identificação de classes com problemas, etc. A largura de banda quantifica o volume de dados que um *link* ou caminho pode transferir por unidade de tempo. A largura de banda disponível, representa assim uma métrica variável no tempo, onde é identificada a capacidade disponível, levando em consideração a carga atual. A capacidade, representando o limite máximo à largura de banda disponível, é também uma métrica que se enquadra neste contexto.

Em [4], [8] as estatísticas referentes ao tráfego de rede são apontadas como fontes de dados importantes à monitorização. Esta informação pode ser útil também na camada de rede ao nível do serviço IP, para além da camada das Infraestruturas físicas e virtuais, tal como referido anteriormente.

Quanto às métricas referentes ao Desempenho ao nível da rede, estas englobam as tradicionais métricas de QoS como a duplicação de pacotes, perda de pacotes (OWPL - *One-way packet loss*, OWLP - *One-way loss pattern*, IPLR - *IP packet loss ratio*), atraso (OWD - *one-way delay*, RTT - *round-trip time*, IPTD - *IP packet transfer delay*, IPDV - *IP packet delay variation*), *IP packet error ratio* (IPER), *Spurious IP packet ratio* (SPR), entre outras [9], [16].

No que toca à Disponibilidade/Fiabilidade de uma rede, esta pode apresentar períodos de inatividade provocados por problemas que podem ter origem nos componentes de rede, configurações de routing, entre outros aspetos. Face a esta possibilidade, torna-se relevante monitorizar a (in)disponibilidade de uma rede, assim como o estado da conectividade. O tempo de resposta a uma configuração de rede também pode ser um indicador relevante para avaliar a disponibilidade da rede. Perante a ocorrência de falhas na rede, o tempo médio entre a ocorrência de falhas ou o tempo médio de restauro são bons fatores de avaliação da fiabilidade de uma rede.

3) Serviço/Aplicação: Na camada de Serviço/Aplicação, a natureza dos parâmetros monitorizados e a maneira como estes devem ser recolhidos depende essencialmente do *software* a ser monitorizado e não da infraestrutura *Cloud* em que está inserido. Uma das principais preocupações a ter em conta, passa pela disponibilidade de um Serviço/Aplicação. Um Serviço/Aplicação *Cloud* está sujeito a um conjunto de aspetos de diversas naturezas que podem afetar a sua disponibilidade, devido sobretudo à complexidade do ambiente *Cloud*. Posto isto, devem ser associadas métricas à disponibilidade de um Serviço/Aplicação, onde são registados os períodos de tempo em que um serviço está em funcionamento e quando se encontra indisponível. Este é um tópico que envolve questões económicas, pois em caso de indisponibilidade de um Serviço/Aplicação existem violações de SLA e posteriores penalizações do lado do fornecedor, uma vez que a qualidade do serviço foi afetada. Na Tabela VI estão ainda indicadas algumas métricas associadas à Disponibilidade e Fiabilidade de um Serviço/Aplicação. Quando estamos perante um cenário de falhas de serviço (indisponibilidade de um serviço ou quebra significativa da qualidade de serviço), a capacidade de recuperação e o tempo utilizado deve ser do conhecimento dos clientes ou de *third-parties* responsáveis pela monitorização. Para além dos aspetos relacionados com a recuperação de um dado Serviço/Aplicação, os intervalos de tempo entre a ocorrência de falhas também funcionam como indicadores da sua fiabilidade e eficiência.

Por sua vez, o tempo de resposta de um dado serviço pode funcionar como um fator de medição do seu desempenho. Neste contexto, em [15] são abordadas métricas referentes ao tempo de resposta médio e máximo num cenário de jogos *online* em *Cloud Computing*.

Devido à natureza insegura do ambiente onde alguns dos Serviços/Aplicações são disponibilizados, a segurança torna-se um aspeto relevante a controlar. Tal como indicado na Tabela VI, o número de vulnerabilidades de segurança deve ser uma métrica importante, uma vez que é necessário monitorizar comportamentos para detetar possíveis violações. Outros aspetos ao nível da camada da Aplicação que podem ser monitorizados e salvaguardados são sobretudo os certificados digitais, chaves privadas, *Domain Name System Security Extensions* (DNSSEC), etc. O comportamento do utilizador também pode ser associado a esta camada e as métricas relevantes prendem-

se sobretudo com os processos de *login*, padrões de acesso, IPs associados, entre outras. A monitorização deve incidir ainda na gestão de passwords, onde são fornecidos dados como o formato das *passwords* e frequência com que devem ser renovadas [13].

Para além das métricas e aspetos da monitorização referidos anteriormente, podem ainda ser acrescentadas métricas associadas especificamente ao tipo de Serviço/Aplicação em questão. Por outro lado, pode ser útil o registo de um histórico, onde podem constar os IPs de acesso e registos dos tempos de login referentes aos diversos clientes.

Tabela VI
EXEMPLOS DE MÉTRICAS PARA A CAMADA SERVIÇO/APLICAÇÃO.

Layer	Categoria	Exemplo de Métricas
Serviço / Aplicação	Disponibilidade Fiabilidade	*UP time*, (in)disponibilidade do serviço, tempo de restauro em caso de falhas, tempo médio entre falhas.
	Desempenho	Tempo de resposta (médio/máximo), processamento *batch*.
	Segurança	Número de vulnerabilidades de segurança, padrões de acesso, processos de login, gestão de passwords.
	Outras	Registos dos tempos de login e IPs de acesso (histórico), métricas específicas do tipo de aplicação.

4) Cliente/Fornecedor: A relação Cliente/Fornecedor envolve todo um conjunto de interesses comerciais, o que torna necessário o estabelecimento de um contrato onde sejam especificados todos os aspetos do serviço em questão. Neste contexto é importante esclarecer o conceito de SLA. Um SLA é um contrato estabelecido entre fornecedor e cliente e especifica quais as necessidades dos consumidores e o compromisso dos fornecedores para com eles. Num SLA estão contidos normalmente itens como: conjunto de serviços fornecidos, uma definição completa e específica de cada serviço, requisitos de QoS, tempo de atividade, segurança, privacidade, procedimentos de *backup*, responsabilidades de ambas as partes, entre outros [3]. Uma referência ainda para as questões relacionadas com a localização geográfica dos *datacenters* em relação às leis nacionais e internacionais. Este é tido como um critério importante pelas companhias que pretendem investir em soluções baseadas na *Cloud*. Para tal é necessário que os SLA incluam e abranjam este tipo de parâmetros. O estabelecimento de normas para *Cloud Computing*, que ainda não se encontram claramente definidas, podem ajudar a lidar com estes parâmetros geográficos e legais [17]. No que toca à gestão de serviços, o cliente deverá requerer sumários de todo um conjunto de auditorias, feitas pelo fornecedor do serviço, como parte da verificação do respetivo SLA. Os SLA funcionam assim como um dos instrumentos primários de controlo do utilizador. Portanto, uma das métricas vitais a este nível de monitorização passa pela auditoria dos SLAs, onde são registadas todas as violações e incumprimentos dos mesmos. Posto isto, a verificação do cumprimento dos SLAs está diretamente relacionada com as camadas anteriores, uma vez que pode ser necessário recorrer a métricas estabelecidas ao nível das infraestruturas, rede ou serviços. Por exemplo, em [7] é referida uma métrica relativa à média de violações de SLA, que representa a média de desempenho de CPU que não foi alocada a uma aplicação quando requerida. Em caso de ocorrência deste tipo de incumprimentos, existem consequências. Dependendo dos parâmetros dos SLAs estabelecidos entre clientes e fornecedores, podem ocorrer penalizações e compensações por parte dos fornecedores de serviço.

A monitorização da contabilização do uso do serviço também é um aspeto bastante importante, na medida em que existe a necessidade de assegurar os interesses económicos de ambas as partes. Devido à natureza elástica dos ambientes *Cloud*, aliado ao modelo comercial *"pay-as-you-go"*, a medição da utilização e o custo tornam-se aspetos vitais [9], [15]. A análise da contabilização dos serviços e respetiva receita, permite também aos fornecedores de serviço adaptarem os seus planos de preçários e estratégias comerciais conforme as necessidades do mercado. Este estudo pode fazer a diferença, numa altura onde a forte concorrência na área se notabiliza, fruto do aumento da oferta na web de ferramentas baseadas em *Cloud Computing*.

Relativamente à segurança, em [2] são abordados alguns parâmetros que devem estar incluídos num SLA, e que por sua vez se enquadram na relação entre cliente e fornecedor. Este tipo de parâmetros diz respeito sobretudo ao estado de aquisição e atualização dos padrões de segurança relevantes por parte do fornecedor, assim como dos certificados. Outros tipos de parâmetros indicados são o estado de certificação da parte responsável pela gestão; estado das restrições operacionais incluídas nas medidas de segurança impostas pelo sistema de gestão; estado da garantia de confidencialidade nas trocas de dados entre *Clouds*; localização dos dados; estado da aquisição de *logs* para a deteção de atos maliciosos e o período durante o qual estes são mantidos; estado do controlo da comunicação para bloquear comunicações maliciosas; estado das medidas que atuam contra o congestionamento da rede, evitando ataques *Denial of Service* (DoS)/*Distributed Denial of Service* (DDoS); estado das medidas contra *malware*.

Tabela VII
EXEMPLOS DE MÉTRICAS PARA A CAMADA CLIENTE/FORNECEDOR.

Layer	Categoria	Exemplo de Métricas
Cliente/ Fornecedor	Auditoria	Monitorização de violações e incumprimentos dos SLA, penalizações.
	Contabilização	Monitorização do uso e respetivo custo do serviço, receita.
	Segurança	Estado de aquisição e atualização dos padrões de segurança, certificados, localização dos dados.

B. Questões Relacionadas com QoE

Com a migração de aplicações pessoais e comerciais para a *Cloud*, a qualidade do serviço prestado torna-se um importante diferenciador entre os diversos fornecedores. Um fator que está diretamente relacionado com a QoS é a qualidade que é presenciada pelo utilizador final, ou seja, a qualidade de experiência (QoE) resultante da utilização de um dado serviço. Posto isto, torna-se também imprescindível monitorizar a QoE.

Neste tipo de monitorização são tidas em conta métricas como atraso, variações do atraso (*jitter*), perdas, latência, entre outras. Contudo, estes são aspetos que não fazem parte do conhecimento e do vocabulário comum dos utilizadores finais. Porém a sua opinião e *feedback* acerca da satisfação em relação aos serviços subscritos são um fator bastante relevante a ter em conta na avaliação de toda a infraestrutura. Devido aos diversos intervenientes de um ambiente *Cloud*, perceber e gerir a QoE dos serviços requer uma visão multidisciplinar, que integra a tecnologia, utilizador e aspetos comerciais da qualidade do acesso do utilizador final. O objetivo principal da gestão da QoE está assim relacionado com a intenção de fornecer uma aplicação *Cloud* de alta qualidade ao utilizador final e tentar minimizar os custos dos diversos intervenientes. Estes vão desde entidades relacionadas com os modelos de serviço da pilha *Cloud* (IaaS, PaaS e SaaS), até aos fornecedores das redes subjacentes (Telcos - *Telecommunications companies* e ISPs - *Internet Network Providers*).

No que toca aos atuais trabalhos de investigação da QoE na *Cloud*, estes focam-se sobretudo em aplicações multimédia, onde se encaixam serviços de *streaming* HTTP como o Youtube ou Netflix. O impacto dos tempos de espera na perceção do utilizador tem ganho especial atenção nas comunidades de investigação, dado o aumento de popularidade dos serviços multimédia *Cloud* [18]. Este paradigma dos tempos de espera pode ser também associado a aplicações interativas como *web browsing*. Quanto aos serviços *Cloud* mais complexos, como produtos *office*, edição colaborativa ou OS a correr na *Cloud*, os trabalhos de pesquisa relacionados com a QoE ainda estão a dar os primeiros passos. Existem ainda algumas questões em aberto como, por exemplo, o impacto da interatividade dos utilizadores e a sua influência na QoE ou o relacionamento da QoE com as expectativas dos utilizadores, resultantes do domínio do uso do serviço em questão, entre outras.

Relativamente à gestão da QoE em geral, em [18] são abordados os passos básicos a ter em consideração. Estes estão relacionados com o entendimento e mapeamento, monitorização e estimação, adaptação e controlo da QoE. Num primeiro passo, é necessário entender quais são os requisitos de uma aplicação e efetuar um mapeamento entre parâmetros mensuráveis e QoE. Um mecanismo típico de avaliação de QoE passa pelo cálculo de *Mean Opinion Scores* (MOS). O próximo passo consiste na monitorização (desde infraestruturas, condições da rede, SLAs e informações específicas das aplicações) e estimativa de QoE. A monitorização pode ser efetuada pelo fornecedor dentro da rede, onde são requeridas funções de mapeamento entre a QoS e QoE, ou ao nível de parâmetros específicos de uma aplicação, o que requer técnicas de *Deep Packet Inspection* (DPI). Como alternativa, existe ainda a opção da monitorização no utilizador final, dando a melhor perspetiva sobre a qualidade presenciada. Por fim, a adaptação e o controlo da QoE tem como objetivo possibilitar aos fornecedores que atuem antes que o utilizador possa notar algum problema e ficar insatisfeito ou abandonar o serviço.

Os mesmos autores identificam ainda alguns desafios que surgiram com a migração de serviços para a *Cloud* e que têm influência na qualidade presenciada pelos utilizadores finais. Os desafios identificados podem ir desde a distribuição geográfica do utilizador, artefactos introduzidos com o aumento das distâncias da rede entre o utilizador e o serviço, problemas de gestão de recursos derivados das localizações geográficas, ou até a questão do envolvimento de diversas entidades no fornecimento de um serviço. No caso da localização geográfica, esta pode limitar o grau de interatividade, uma vez que utilizadores em localizações remotas podem estar sujeitos a latências inaceitáveis, levando em consideração a distância entre o *data center* e o local onde o serviço é acedido. A grande quantidade de utilizadores em várias localizações geográficas também podem ter influência direta num serviço, pois podem ser afetados requisitos como a escalabilidade e a velocidade de acesso. Uma referência ainda para a dependência da QoE para com as condições da rede e os SLAs, na medida em que é definido o caminho entre o *datacenter* e o utilizador final, atravessando diferentes domínios administrativos.

C. Relação com os Modelos de Serviço

Devido às diferenças significativas entre os três modelos de serviço mais populares, é consensual que não exista uma solução genérica de monitorização *Cloud*. Cada modelo de serviço possui diferentes áreas e graus de controlo, assim como as suas próprias características de gestão. Posto isto é compreensível que seja difícil alcançar uma solução de gestão *Cloud* genérica. Face a este paradigma, um sistema de monitorização necessita de ser planeado e desenvolvido, com o intuito de ser adequado aos objetivos da gestão. Este processo para além de cobrir os vários constituintes de todo um ambiente *Cloud*, deve ainda levar em consideração aspetos como a QoS/QoE, os SLAs e características como a segurança, robustez, escalabilidade, elasticidade, entre outras [4].

Neste contexto torna-se útil relacionar o modelo estratificado proposto para a monitorização de serviços *Cloud* com os modelos de serviço. Essa relação está ilustrada na Tabela VIII, levando em consideração os três modelos de serviço mais populares (IaaS, PaaS e SaaS) e as camadas do modelo proposto (Infraestrutura, Rede, Serviço/Aplicação e Cliente/Fornecedor).

No que diz respeito à camada de monitorização das infraestruturas, esta pode ser essencialmente associada ao modelo de serviço IaaS. Na base desta associação estão as características dos componentes envolvidos, uma vez que são comuns. Na camada das infraestruturas estão incluídos componentes dos recursos físicos e virtuais relativos ao processamento, armazenamento e comunicação em rede, ou seja, aspetos que também caracterizam o modelo de serviço IaaS.

Quanto à camada de Rede, se for levada em consideração uma monitorização fim-a-fim, esta relaciona-se com os três modelos de serviço direta ou indiretamente. Tendo em consideração todo o ambiente *Cloud*, dependendo dos intervenientes e do serviço em questão, a monitorização da Rede pode ser efetuada de várias maneiras. No caso de um serviço fornecido a um cliente com base num modelo SaaS, as questões relacionadas com os aspectos de Rede (como Débito

e Desempenho), devem ser monitorizadas desde a origem (infraestruturas, *datacenters*) até ao local onde o utilizador acede ao serviço. Neste caso estão envolvidos os modelos de serviço IaaS e SaaS. No caso de existirem intermediários, como as companhias de desenvolvimento de *software*, ou seja, fornecedores de plataformas de serviço inseridos num modelo de serviço PaaS, a monitorização da camada de Rede também está relacionada com este modelo. Portanto esta camada pode estar relacionada com os diversos intervenientes, uma vez que pode atravessar os vários modelos de serviço, tendo em consideração uma monitorização fim-a-fim.

Por sua vez, a camada Serviço/Aplicação está associada ao modelo de serviço SaaS. Na base desta relação está a natureza da camada, uma vez que os parâmetros monitorizados e a maneira como devem ser recolhidos dependem sobretudo do *software* e não da infraestrutura.

Por fim, a camada Cliente/Fornecedor ao abordar aspetos como contabilização e auditorias, está diretamente relacionada com os três modelos de serviço. Devido à complexidade de um ambiente *Cloud* e à existência de diversos intervenientes, é normal existirem relações comerciais entre fornecedores e clientes a vários níveis. Os fornecedores tanto podem disponibilizar *datacenters*, como plataformas de serviço ou *software*, enquanto os clientes podem ser empresas de desenvolvimento de plataformas e *software* ou os utilizadores finais.

Tabela VIII
RELAÇÃO COM OS MODELOS DE SERVIÇO.

	IaaS	PaaS	SaaS
Infraestrutura	✓		
Rede	✓	✓	✓
Serviço/Aplicação			✓
Cliente/Fornecedor	✓	✓	✓

V. CONCLUSÃO E TRABALHO FUTURO

O rápido crescimento de *Cloud Computing* como um novo modelo de prestação de serviços é um facto que não pode ser negado. A noção da necessidade da existência de um sistema de monitorização para operar com eficiência um ambiente *Cloud* já está presente. Devido à falta de maturidade típica das novas tecnologias, podem ser apontadas algumas limitações, nomeadamente no controlo e gestão de uma *Cloud*. A monitorização *Cloud* pode beneficiar de metodologias, conceitos e ferramentas já consolidados na gestão da computação distribuída tradicional. Contudo, a natureza complexa de um ambiente *Cloud* torna difícil chegar a uma solução de gestão genérica, nomeadamente devido à natureza e às características próprias de cada modelo de serviço (IaaS, PaaS e SaaS) e de cada modelo de implementação (*Public* e *Private*).

Uma observação relevante que se constata no contexto da monitorização *Cloud* é a falta de normas. Este é um facto que assume particular importância quando se tenta realizar uma monitorização através de múltiplas *Clouds*, envolvendo questões geográficas e legais para além da QoS e QoE. Como parte dos esforços dedicados à normalização, o presente trabalho contribuí com algumas sugestões de parâmetros, métricas e boas práticas para uma monitorização eficiente dos serviços e ambientes *Cloud Computing*.

Como trabalho futuro, pretende-se aplicar os conhecimentos adquiridos num cenário prático, comprovando a utilidade do modelo proposto, nomeadamente as vantagens associadas a efetuar a monitorização de uma forma estratificada.

Agradecimentos: Este trabalho é financiado pelo FEDER através do Programa Operacional Factores de Competitividade-COMPETE e pela FCT - projeto FCOMP-01-FEDER-0124 022674.

REFERÊNCIAS

[1] Luis Vaquero, Luis Merino, Juan Caceres and Maik Lindner. *A Break in the Clouds: Towards a Cloud Definition*. SIGCOMM CCR, 39(1):50–55, January 2009.

[2] ITU-T FGCloud. *Part 1: Introduction to the Cloud Ecosystem: Definitions, Taxonomies, Use Cases and High-level Requirements*. Technical report, February 2012

[3] Cloud Computing Use Case Discussion Group. *Cloud Computing Use Cases white paper v4.0*. Technical report, July 2010

[4] Stuart Clayman, Alex Galis, Clovis Chapman, Giovanni Toffetti, Luis Merino, Luis Vaquero, Kenneth Nagin and Benny Rochwerger. *Monitoring Service Clouds in the Future Internet*. IOS Press, pages 115–126, April 2010.

[5] Shirlei Chaves, Rafael Uriarte, and Carlos Westphall. *Toward an Architecture for Monitoring Private Clouds*. IEEE Communications Magazine, pages 130–137, December 2011.

[6] Jorge Werner, Guilherme Geronimo, Carlos Westphall, Fernando Koch and Rafael Freitas. *Simulator Improvements to Validate the Green Cloud Computing Approach*. In Network Operations and Management Symposium (LANOMS) 7th Latin American, October 2011.

[7] Anton Beloglazov, Jemal Abawajy and Rajkumar Buyya. *Energy Aware Resource Allocation Heuristics for Efficient Management of Data Centers for Cloud Computing*. ELSEVIER, Future Generation Computer Systems, 28, pages 755–768, May 2012.

[8] Ya-Shiang Peng and Yen-Cheng Chen. *SNMP-Based Monitoring of Heterogeneous Virtual Infrastructure in Clouds*. In Network Operations and Management Symposium (APNOMS) 13th Asia-Pacific, September 2011.

[9] Taesang Choi, Nodir Kodirov, Tae-Ho Lee, Doyeon Kim and Jaegi Lee. *Autonomic Management Framework for Cloud-based Virtual Networks*. In Network Operations and Management Symposium (APNOMS) 13th Asia-Pacific, September 2011.

[10] Mehdi Sheikhalishahi and Lucio Grandinetti. *Revising Resource Management and Scheduling Systems*. In CLOSER 2012 - 2nd International Conference on Cloud Computing and Services Science, page 121 – 126, 2012.

[11] Jonathan Spring. *Monitoring Cloud Computing by Layer, Part 1*. IEEE Security & Privacy Magazine, pages 66–68, March/April 2011.

[12] Jonathan Spring. *Monitoring Cloud Computing by Layer, Part 2*. IEEE Security & Privacy Magazine, pages 52–55, May/June 2011.

[13] Shirlei Chaves, Carlos Westphall and Flavio Lamin. *SLA Perspective in Security Management for Cloud Computing*. In Sixth International Conference on Networking and Services, IEEE Computer Society, pages 212–217, March 2010.

[14] Flávio Sousa, Leonardo Moreira, Gustavo Santos and Javam Machado. *Quality of Service for Database in the Cloud*. In CLOSER 2012 - 2nd International Conference on Cloud Computing and Services Science, page 595 – 601, 2012.

[15] Pankesh Patel, Ajith Ranabahu, and Amit Sheth. *Service Level Agreement in Cloud Computing*. Technical report, September 2009.

[16] Solange Lima. A Distributed Admission Control Model for Class-based Networks. PhD thesis, University of Minho, Braga, 2005.

[17] Katerina Stamou, Jean-Henry Morin, Benjamin Gateau and Jocelyn Aubert. *Service Level Agreements as a Service - Towards Security Risks Aware SLA Management*. In CLOSER 2012 -2nd International Conference on Cloud Computing and Services Science, page 663 – 669, 2012.

[18] Tobias Hoßfeld, Raimund Schatz, Martin Varela and Christian Timmerer. *Challenges of QoE Management for Cloud Applications*. IEEE Communications Magazine, pages 28 – 36, April 2012.