REPAE – Revista Ensino e Pesquisa em Administração e Engenharia
Volume 2, número 1 – 2016
ISSN: 2447-6129
Editor Científico: Vitória Catarina Dib
Avaliação: Melhores práticas editoriais da ANPAD

Qual modalidade de "Computação em Nuvem" a organização deve optar?

João Carlos Lopes Fernandes
Doutorado em Engenharia Biomédica pela Universidade de Mogi das Cruzes
Faculdade ENIAC
joao.carlos@eniac.edu.br

RESUMO. Este trabalho elucida a Cloud Computing (computação em nuvem); nele é abordado seu funcionamento e suas vantagens e desvantagens. A Cloud Computing já é uma realidade mundial e deve ser compreendida nas organizações como uma nova tendência tecnológica. A visão operacional da computação em servidores locais e de controle interno, muda bastante com esta solução tecnologia. Mas entre os empresários a maior dúvida ainda é quando utilizá-la.

Palavras-Chave: Computação em nuvens; Tendências Tecnológicas; Tecnologia da Informação.

Data do recebimento do artigo: 27/3/2016
Data do aceite de publicação: 7/6/2016

INTRODUÇÃO

O surgimento da computação em nuvem possui efeitos de longo alcance sobre os sistemas e redes de computadores das organizações públicas e privadas. Muitas características tornam a computação em nuvem atraente, no entanto, os modelos tradicionais de segurança e controles ainda não são os ideais. O objetivo deste trabalho é fornecer uma visão geral da computação em nuvem e as considerações de segurança e privacidade envolvidas, que devem ser levadas em contata no caso de sua contratação. Mais especificamente, ele descreve algumas das ameaças, os riscos tecnológicos e as possíveis garantias que cercam o ambiente e seu tratamento.

A computação em nuvem foi definida pelo NIST (*National Institute of Standards and Technology*) como um modelo para permitir conveniente, acesso à rede “sobe demanda” a um “pool” compartilhado de recursos computacionais configuráveis (por exemplo, redes, servidores, armazenamento, aplicações e serviços) que podem ser rapidamente provisionados e liberados com o mínimo esforço de gerenciamento ou interação com o provedor da nuvem [15].

As tecnologias de computação em nuvem podem ser implementadas em uma ampla variedade de arquiteturas, sobe diferentes modelos de serviços e de implantação, e coexistir com outras tecnologias e abordagens de “design" de software.

Os desafios nesta modalidade de computação são imensos, especialmente para as nuvens públicas, cuja infraestrutura e os recursos são compartilhados com o público em geral.

O modelo de implantação da computação em nuvem Pública é uma opção viável para muitas aplicações e serviços. No entanto, as responsabilidades pela segurança e privacidade nesta categoria de nuvem continuam a ser uma obrigação para a organização que contrata este serviço.

1. DIRETRIZES DE SEGURANÇA E PRIVACIDADE.

A computação em nuvem pode ser considerada um novo paradigma de computação na medida em que permite a utilização de uma infraestrutura de computação em um ou mais níveis de abstração, como um serviço "on-demand" disponibilizado através da Internet ou qualquer outra rede de computadores. Por causa das implicações para uma maior flexibilidade e disponibilidade a baixo custo, a computação em nuvem é um assunto que tem recebido muita atenção.

O interesse na computação em nuvem tem crescido rapidamente nos últimos anos devido às vantagens de uma maior flexibilidade e disponibilidade de recursos de computação com um custo menor. A segurança e privacidade, no entanto, ainda necessitam de uma especial preocupação pelo lado das organizações, que pretendem realizar a migração de suas aplicações para ambientes de computação em nuvem pública ou até mesmo privada.

Os serviços de computação em nuvem oferecem economia de escala conseguida através do uso versátil de recursos disponibilizados. No entanto, ela é uma forma emergente de computação distribuída que ainda está em implementação. O próprio termo é frequentemente usado com uma gama de significados e interpretações [5]. Muito do que já foi escrito sobre ela tem como objetivo identificar os paradigmas importantes de seu uso e fornecimento de uma taxonomia geral para conceituar facetas importantes do serviço.

A computação em nuvem pública é um dos vários modelos de implementação possíveis. Uma nuvem pública é aquela em que a infraestrutura e outros recursos computacionais são colocados à disposição do público em geral, através da Internet. Estes tipos de serviços são comercializados por um provedor de serviços de nuvem. Na outra extremidade estão as nuvens privadas. Uma nuvem privada é aquela em que o ambiente de computação é operado exclusivamente para uma determinada organização. Pode ser gerida pela própria organização ou por um terceiro, ela pode ser hospedada no próprio "Data Center" da organização ou fora dele. Uma nuvem privada dá à organização um maior controle sobre os recursos de infraestrutura computacionais do que em uma nuvem pública.

Dois outros modelos de implantação que se situam entre nuvens públicas e privadas são nuvens "comunitárias" e nuvens "híbridas". Uma nuvem de comunidade é semelhante a uma nuvem privada, mas a infraestrutura e os recursos computacionais são compartilhados por várias organizações que têm privacidade em comum, segurança e considerações

regulatórias, mais do que para o uso exclusivo de uma única organização. A nuvem híbrida é uma composição de duas ou mais nuvens que permanecem como entidades únicas, mas são unidas por uma tecnologia padronizada ou proprietária que permite a interoperabilidade.

Assim como os diferentes modelos de implantação podem afetar o alcance e controle do ambiente computacional de uma organização em uma nuvem, também existem modelos de serviços suportados pela nuvem. Três modelos de serviços são conhecidos e frequentemente utilizados:

- *Software-as-a-Service.* O Software como Serviço (SaaS) é um modelo de implantação de software pela qual uma ou mais aplicações e seus recursos computacionais são fornecidos para uso sobe demanda, como um serviço. Seu principal objetivo é reduzir o custo total de hardware e desenvolvimento de software e a manutenção. A segurança é realizada, principalmente, pelo provedor de nuvem. O assinante deste serviço não gerencia nem controla a infraestrutura subjacente da nuvem ou aplicativos individuais; ele apenas pode selecionar as preferências e configurações de aplicativos limitados administrativamente.

- *Platform-as-a-Servic*e. A Plataforma como Serviço (PaaS) é um modelo de implantação de software em que a plataforma de computação é fornecida como um serviço sobe demanda. Os aplicativos podem ser desenvolvidos e implantados pelo cliente. Seu principal objetivo é reduzir o custo e a complexidade da compra, habitação e gestão dos componentes de hardware e software subjacentes da plataforma, incluindo qualquer programa necessário e ferramentas de desenvolvimento de banco de dados. O ambiente de desenvolvimento é tipicamente de propósito específico determinado pelo provedor da nuvem e "sobe medida" para o design e arquitetura de sua plataforma. O assinante da nuvem tem controle sobre os aplicativos e configurações do ambiente de aplicativos da plataforma. Normas de segurança são divididas entre o provedor da nuvem e o assinante.

- *Infrastructure-as-a-Service.* A Infraestrutura como Serviço (IaaS) é um modelo de implantação de software em que a infraestrutura de computação básica de servidores, software e equipamentos de rede é fornecido como um serviço "sobre demanda" em que existe uma plataforma para desenvolver e executar aplicações. Seu principal objetivo é evitar a compra, habitação e gestão dos componentes básicos de infraestrutura de hardware e software e, em vez obter esses recursos utilizá-los de forma virtualizada e controlada através de uma interface de serviço. O assinante desta nuvem geralmente tem ampla liberdade para escolher o ambiente de sistema operacional e de desenvolvimento a ser hospedado. Normas de segurança básica da infraestrutura são realizadas principalmente pelo assinante da nuvem.

A Figura 1 ilustra as diferenças de alcance e de controle entre o assinante de uma nuvem e o provedor de nuvem, para cada um dos modelos de serviço acima discutidos. Cinco camadas conceituais de um ambiente de nuvem generalizada são identificadas no diagrama que são aplicados a nuvens públicas, bem como cada um dos outros modelos de implementação. As setas à esquerda e à direita do diagrama denotam o intervalo aproximado do provedor de nuvem, escopo e controle sobre o ambiente de nuvem para cada modelo de serviço. Em geral, quanto maior o nível de suporte disponível a partir de um provedor de nuvem, menor será o controle do assinante sobre o sistema.

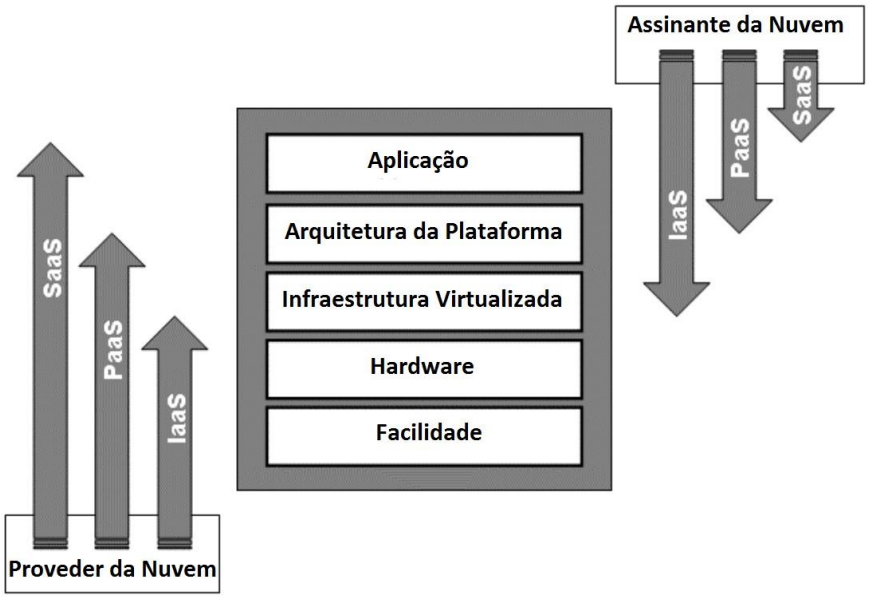

Figura 1: Diferenças no Escopo e Controle entre os modelos Cloud Service

As duas camadas mais baixas (facilidade e hardware) denotam os elementos físicos de um ambiente de nuvem, que estão sobe o controle total do provedor da nuvem, independentemente do modelo de serviço. Troca térmica, ventilação, ar condicionado (HVAC), energia elétrica, comunicações de dados fazem parte da camada de facilidade, enquanto os componentes de computadores, rede e armazenamento, e outros elementos de infraestrutura de computação física compreendem a camada de hardware.

As demais camadas denotam os elementos lógicos de um ambiente de nuvem. A camada de infraestrutura virtualizada envolve elementos de software, tais como hypervisors, máquinas virtuais, armazenamento de dados virtuais e componentes de middleware de apoio utilizados para realizar a infraestrutura sobre a qual uma plataforma de computação pode ser estabelecida. Embora a tecnologia de máquina virtual seja comumente usada nesta camada, existem outros meios de fornecer as abstrações de software necessárias. Da mesma forma, a camada de arquitetura implica em compiladores, bibliotecas, utilitários e outras ferramentas de software e ambientes de desenvolvimento necessários para implementar as aplicações. A camada de aplicação representa aplicações de software implementadas e direcionadas para os clientes (usuário final) ou outros programas, e disponibilizados através da nuvem.

2. CONTRATOS DE SERVIÇOS

As especificações para serviços de nuvem pública e acordos de serviços são geralmente chamadas de Acordos de Nível de Serviço (SLAs). Um SLA representa o entendimento entre o assinante da nuvem e o provedor de nuvem sobre o nível esperado de serviço a ser entregue e, no caso em que o fornecedor não entregar o serviço ao nível especificado, à compensação (normalmente financeira) disponível para o assinante. Um SLA, no entanto, geralmente constitui apenas uma parte dos termos de serviço estipuladas no acordo global do contrato ou serviços. Os termos de serviço cobrem outros detalhes importantes como o licenciamento de serviços, critérios de utilização, a suspensão do serviço e cancelamento, limitações de responsabilidade, política de privacidade e modificações nos termos de serviço.

Existem dois tipos de SLAs: os acordos não negociáveis predefinidos e os acordos negociáveis [2, 13]. Os acordos não negociáveis fornecem a base da economia em escala para o cliente e são normalmente aplicados em nuvens públicas. Não são apenas os termos de serviço previstos pelo provedor de nuvem, mas algumas ofertas, que o provedor também pode fazer e modificar nos termos de forma unilateral, sem dar qualquer notificação direta para o assinante (por exemplo, ao publicar uma versão atualizada de software, ou mudar as regras de armazenamento) [13].

Os SLAs negociáveis são equivalentes aos contratos tradicionais de "outsourcing" (terceirização) de tecnologia da informação. Eles podem ser usados para diminuir às preocupações de uma organização sobre a segurança e a política de privacidade. Neles são negociados os procedimentos e controles técnicos, como: a habilitação dos funcionários, os direitos de propriedade de dados manipulados, o isolamento de aplicações hospedadas, a criptografia de dados e sua segregação, monitoramento, relatórios de eficácia do serviço, conformidade com leis e regulamentos entre outros. Para os dados e aplicativos críticos podem exigir outros tipos de negociação no contrato para realizar sua adequação a realidade do cliente [15]. Estes pontos de negociação podem modificar significativamente o valor a ser cobrado. Um SLA negociável é normalmente menos rentável. O resultado de uma negociação também dependerá do tamanho da organização e de sua área de atuação. Independentemente do tipo de SLA, a obtenção de aconselhamento jurídico e técnico adequado é recomendado para garantir que os termos de serviço possam atender adequadamente às necessidades da organização.

2.1. OS PARÂMETROS DE SEGURANÇA

Enquanto o maior obstáculo enfrentando pela computação em nuvem seja sua segurança, o fornecimento de serviços em nuvem está crescendo e os provedores de nuvem possuem uma perspectiva de melhorar seu nível de segurança. A segurança não depende apenas do prestador de serviço, ela deve ser efetiva e discutida junto às organizações. Os maiores beneficiários são as pequenas organizações que possuem um número reduzido de administradores de segurança da informação (em muitos casos nenhum) e não possui economia de escala igual a disponível para grandes organizações.

As potenciais áreas das organizações podem obter benefícios com a transição para um ambiente de computação em nuvem, dentre elas vale ressaltar:

Os especialistas de computação alocados junto à empresa, podem se preocupar com o "Core Business" em profundidade, tomando ações estratégicas para melhoria do negócio. A estrutura das plataformas de computação em nuvem é tipicamente mais uniforme do que a maioria dos centros de computação tradicionais, a "elasticidade" pode ser vista como um parâmetro importante (deve fazer parte do contrato de SLA). A maior uniformidade e homogeneidade facilitam quando a plataforma necessita ser alterada e permite uma melhor automação de atividades de gerenciamento de segurança como: controle de configuração, testes de vulnerabilidade, auditorias de segurança e correções de componentes da plataforma de segurança. As atividades de resposta a incidentes, a garantia da privacidade das informações e o nível de segurança também melhoram com uma infraestrutura de nuvem homogênea e uniforme, assim como as atividades de gerenciamento do sistema, como gerenciamento de falhas, balanceamento de carga e manutenção do sistema. Muitos provedores de nuvem para atender aos padrões de conformidade operacional são certificados em áreas como a saúde, finanças e auditoria.

A escalabilidade na computação em nuvem permite uma maior disponibilidade (depende do "Link de Comunicação"). A redundância e a capacidade de recuperação de desastres também são características desta modalidade de computação.

As políticas e procedimentos de backup e recuperação de um serviço de nuvem podem ser superiores aos das organizações e, se as cópias de segurança são mantidas em diversas localizações geográficas, pode ser uma solução mais segura. Os dados mantidos dentro de uma nuvem podem ser disponibilizados, mais rapidamente para restauração em muitas circunstâncias do que os mantidos em um centro de dados tradicional. Sendo assim os serviços em nuvem também podem servir como um meio de armazenamento de backup "Off Site" para um "Data Center" de uma organização, em vez de mais soluções de armazenamento externo tradicional baseados em fitas [14]. No entanto, o desempenho da rede por meio da Internet e da quantidade de dados envolvidos são fatores limitantes que podem afetar a restauração.

Os dados mantidos e processados na nuvem podem apresentar menos riscos para uma organização do que tê-los dispersos em computadores portáteis ou mídia removível, onde o roubo e a perda de dispositivos ocorrem rotineiramente. Muitas organizações já fazem a transição para apoiar o acesso aos dados organizacionais a partir de dispositivos móveis para uma melhor gestão do fluxo de trabalho e obter outras eficiências operacionais na nuvem, um simples exemplo pode ser o "DropBox".

2.2. A DESVANTAGEM DE SEGURANÇA

Além de seus muitos benefícios potenciais para a segurança e a privacidade, a computação em nuvem também traz consigo potenciais áreas de preocupação, quando comparado com ambientes de computação encontrados em centros de dados tradicionais. Algumas das preocupações mais fundamentais incluem o seguinte:

A Complexidade do Sistema. Um ambiente de computação em nuvem é extremamente complexo em comparação com o de um centro de dados tradicional. A segurança depende não só da correção e da eficácia de muitos componentes, mas também sobre as interações entre eles. O número de possíveis interações entre componentes aumenta com o número de componentes, o que eleva o nível de complexidade. A complexidade se relaciona inversamente com a segurança, quanto maior for à complexidade maior serão as vulnerabilidades.

Os serviços de uma nuvem pública oferecidos por provedores podem possuir muitas organizações compartilhando os recursos e assim complicações subjacentes podem acontecer, ocasionadas por componentes e recursos dos outros assinantes.

O acesso aos dados e recursos organizacionais poderia ser inadvertidamente exposto a outros subscritores através de um erro de configuração ou software. Um invasor também pode se colocar como um assinante para explorar as possíveis vulnerabilidades do ambiente de nuvem para obter acesso não autorizado.

Embora as preocupações de segurança e privacidade em serviços de computação em nuvem são semelhantes aos de serviços tradicionais de computação, eles podem ser amplificados através de uma má gestão da organização (não se preocupar com a filosofia de acesso). Quando existe a migração para uma nuvem pública, por exemplo, é exigida uma transferência de controle para o provedor da nuvem, bem como os componentes do sistema que anteriormente estavam sob o controle direto da organização. A perda de controle sobre os aspectos físicos e lógicos do sistema e dos dados diminui a capacidade da organização para manter o controle sobre as situações adversas, alternativas, definir prioridades, e as mudanças de efeito em segurança e privacidade que são de interesse da organização.

Da mesma forma como acontece com qualquer tecnologia, serviços de computação em nuvem podem ser voltadas para atividades impróprias ou ilegais. Como exemplo, os botnets, montados e controlados por hackers são uma forma primitiva de computação em nuvem. Eles têm sido utilizados para o envio de spam e a realização de ataques de injeção de conteúdo contra sites [11]. Sua utilização também pode ser à base de um ataque de negação de serviço contra a infraestrutura de um provedor de nuvem. A possibilidade de que um serviço de nuvem ser contaminado por uma botnet já ocorreu; em 2009, um nó de controle foi descoberto a partir de uma nuvem IaaS [10, 12]. Os Spammers também utilizam os serviços de nuvem para o envio de phishing, com malwares através de técnicas de engenharia social [4].

CONCLUSÃO

A computação em nuvem já é uma realidade mundial, a adequação das empresas é apenas questão de tempo.

Em relação às necessidades de uma melhor segurança, as empresas prestadoras de serviço de nuvem já estão mobilizadas neste sentido.

A opção por utilizar uma nuvem publica, deve ser bem analisa e dosada pelas organizações, quando a principal necessidade for financeira (redução de custo) esta

solução se tornar interessante. A utilização de nuvens públicas atualmente é recomendada para as empresas de pequeno e médio porte.

Já se a empresa busca novas soluções tecnológicas, disponibilidade de acesso, facilidade de acesso por dispositivos móveis, elasticidade de recursos e uma maior segurança, a opção por uso de nuvens públicas não é a mais indicada.

De qualquer maneira sempre um projeto de migração deve ser realizado junto ao departamento de tecnologia da informação, independente de qual modalidade de nuvem for ser utilizada, os contratos também devem ser analisados pelo departamento jurídico e o nível se SLA definido entre o prestador de serviços de nuvem e a organização em caso de nuvens privadas.

REFERÊNCIAS

Brian Krebs, Amazon: Hey Spammers, Get Off My Cloud! The Washington Post, July 1, 2008, disponível em: <URL: http://blog.washingtonpost.com/securityfix/2008/07/amazon_hey_spammers_get_off_my.html>, acessado em 20 de Set de 2014.

Cloud Computing Use Cases White Paper, Version 4.0, Cloud Computing Use Case Discussion Group, July 2, 2010, disponível em: <URL: http://opencloudmanifesto.org/Cloud_Computing_Use_Cases_Whitepaper4_0.pdf> , acessado em 30 de Set de 2014.

Daniel E. Geer, Complexity Is the Enemy, IEEE Security and Privacy, Vol. 6, No. 6, November/December 2008.

Frederick M. Avolio, Best Practices in Network Security, Network Computing, March 20, 2000, disponível em: <URL: http://www.networkcomputing.com/1105/1105f2.html>, acessado em 1 de Ago de 2014.

Geoffrey Fowler, Ben Worthen, The Internet Industry Is on a Cloud – Whatever That May Mean, The Wall Street Journal, March 26, 2009, disponível em: <URL: http://online.wsj.com/article/SB123802623665542725.html>.

Lamia Youseff, Maria Butrico, Dilma Da Silva, Toward a Unified Ontology of Cloud Computing, Grid Computing Environments Workshop (GCE08), held in conjunction with SC08, November 2008, disponível em: <URL:

http://www.cs.ucsb.edu/~lyouseff/CCOntology/CloudOntology.pdf>, acessado em 10 de Mar de 2014.

Lance Whitney, Amazon EC2 Cloud Service Hit by Botnet, Outage, December 11, 2009, CNET News, disponível em: <URL: http://news.cnet.com/8301-1009_310413951-83.html>, acessado em 8 de Out de 2014.

Luis M. Vaquero1, Luis Rodero-Merino1, Juan Caceres, Maik Lindner, A Break in the Clouds: Towards a Cloud Definition, Computer Communication Review (CCR) Online, Short technical Notes, January 2009, disponível em: <URL: http://ccr.sigcomm.org/online/files/p50-v39n1l-vaqueroA.pdf>, acessado em 22 de Jul de 2014.

[1] Matt Williams, All Eyes are on Los Angeles as City Deploys Cloud-Based EMail, Government Technology, February 10, 2010, disponível em: <URL:

http://www.govtech.com/gt/744804?id=744804&full=1&story_pg=1>, acessado em 19 de Jun de 2014.

[2] Neal Leavitt. Is Cloud Computing Really Ready for Prime Time? IEEE Computer, January 2009.

Niels Provos, Moheeb Abu Rajab, Panayiotis Mavrommatis, Cybercrime 2.0: When the Cloud Turns Dark, Communications of the ACM, April 2009.

[3] Robert McMillan, Hackers Find a Home in Amazon's EC2 Cloud, Infoworld, IDG News Network, December 10, 2009, disponível em: <URL: http://www.infoworld.com/d/cloud- computing/hackers-find-home-in-amazonsec2-cloud-742>>, acessado em 25 de Mai de 2014.

[4] Simon Brad Shaw, Christopher Millard, Ian Walden, Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services, Queen Mary School of Law Legal Studies, Research Paper No. 63/2010, September 2, 2010, disponível em: <URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374>, acessado em 18 de Ago de 2014.

[5] Sushil Kumar, Oracle Database Backup in the Cloud, White Paper, Oracle Corporation, September 2008.

[6] Peter Mell, Tim Grance, The NIST Definition of Cloud Computing, Version 15, October 7, 2009, disponível em: <URL: http://csrc.nist.gov/groups/SNS/cloudcomputing>, acessado em 29 de Mar de 2014.

WHAT TYPE OF "CLOUD COMPUTING" SHOULD THE ORGANIZATION CHOOSE?

João Carlos Lopes Fernandes
Doutorado em Engenharia Biomédica pela Universidade de Mogi das Cruzes
Faculdade ENIAC
joao.carlos@eniac.edu.br

ABSTRACT

This work elucidates the Cloud Computing, it is approached its operation and its advantages and disadvantages. The Cloud Computing is now a global reality and must be understood in organizations as a new technological trend. The business vision for computing local servers and internal control changes dramatically with this technology solution. But among entrepreneurs is even greater doubt when to use it.

Keywords: Cloud Computing; Technological Trends; Information Technology.