Modelo econômico de segurança para nuvens híbridas

Mauro Storch*, César A. F. De Rose

[1]Programa de Pós-Graduação em Ciência da Computação
Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)
Av. Ipiranga, 6681 – Porto Alegre – RS – Brazil

firstname.lastname@acad.pucrs.br*

Resumo. *A adoção de técnicas de criptografia e de segurança em sistemas computacionais dão suporte a privacidade, principalmente em ambientes compartilhados. No entanto, essas técnicas oneram os mecanismos de comunicação, armazenamento e processamento de dados. Modelar os níveis de segurança e as técnicas de criptografia adotadas permite dimensionar os recursos alocados e balancear a execução de aplicações em nuvens híbridas.*

1. Introdução

A computação em nuvem tem um papel importante e consolidado atualmente. Organizações podem se valer dos seus benefícios sem sub-utilizar os recursos computacionais já existentes. Através da implantação de uma nuvem privada no *data center* local, é possível ampliar a capacidade computacional conectando a nuvem privada à uma nuvem pública, formando assim uma nuvem híbrida [Mell and Grance 2011].

Neste cenário, surgem demandas de segurança relacionadas, por exemplo, ao armazenamento e processamento de dados, e também à comunicação entre os ambientes públicos e privados [Hashemi and Ardakani 2012]. Combinando mecanismos e protocolos baseados em criptografia de dados é possível suportar comunicação segura, utilizando as redes virtuais privadas, o armazenamento de dados, utilizando sistemas de arquivos criptografados, e o processamento de dados utilizando instruções embarcadas do processador [Intel 2014] ou através de processamento homomórfico [Gentry 2009].

A medida que são adicionados mecanismos e algoritmos de criptografia mais seguros, mais recursos são necessários para suportar níveis mais altos de segurança. Como resultado, durante a alocação de recursos compartilhados e públicos sob-demanda, devem ser considerados também os custos dos níveis de segurança adotados.

2. Aspectos de Segurança em Nuvens Híbridas

Considerando a adoção de ambientes públicos e compartilhados como porção pública de nuvens híbridas, é necessário avaliar a segurança da comunicação entre os ambientes, do armazenamento persistente de dados na porção pública e também do processamento em ambientes compartilhados.

Atualmente a comunicação entre uma nuvem privada e uma nuvem pública é feita a partir da criação de um canal, seguindo padrões de rede como os das redes virtuais privadas (VPNs) ou da adoção de protocolos seguros como TLS/SSL. Visto que normalmente essa comunicação é feita via internet, a adoção de redes privadas tornou-se um requisito fundamental para que organizações possam adotar o modelo de nuvem híbrida [Sotomayor et al. 2009]. No entanto, para que os dados possam trafegar do forma

criptografada, exite um custo computacional para o processo de criptografia tanto no envio quanto no recebimento.

Além da comunicação entre as instâncias privada e pública, na intenção de garantir a segurança da informação baseada nos dados armazenados na nuvem pública, é fundamental adotar técnicas de armazenamento seguras. As técnicas podem ser utilizados pela aplicação, encriptando os dados antes do armazenamento, ou através dos sistemas de arquivos criptografados. A adoção desses sistemas de arquivos abstraem a responsabilidade da aplicação quanto a segurança dos dados, no entanto, o custo de criptografia será aplicado impreterivelmente a todos os dados da aplicação. Na intenção de utilizar os princípios de escalabilidade, onde se movem copias da aplicação da nuvem privada para a pública, a adoção de sistemas de arquivos criptografados oferecem transparência tanto do ponto de vista da aplicação, quanto do ponto de vista do armazenamento seguro no ambiente da nuvem pública, sendo assim um padrão para privacidade no armazenamento de dados.

Na intenção de atender altos níveis de segurança, um ambiente baseado em recursos públicos deve prover o processamento seguro de dados. Muitos provedores fornecem em contrato garantia de segurança na execução de aplicações com suporte pelo mecanismo de virtualização, através do conceito chamado Security-as-a-Service (Segurança como Serviço). No entanto, durante a execução da aplicação os dados precisam estar em texto plano e não há como garantir a sua blindagem, uma vez que o principio da virtualização (principal tecnologia da computação em nuvem) é o compartilhamento do hardware. Sendo assim, é possível adotar técnicas como a computação homomórfica ou a aquisição de hardware dedicado para processamento de dados criptografados, como os Co-processadores criptográficos.

3. Modelo de Segurança e Trabalhos Futuros

Modelar a utilização de técnicas de segurança de dados em um ambiente de nuvem, proporciona um meio de dimensionar recursos e auxiliar no escalonamento de aplicações e dados. Com base no conhecimento prévio da aplicação, dos dados a serem processados e da infra-estrutura privada e pública, é possível promover o armazenamento e o processamento de dados sensíveis atendendo aos requisitos de segurança da aplicação. Neste sentido, pretende-se modelar os impactos da segurança em nuvens híbridas considerando aspectos de desempenho da aplicação e de recursos adquiridos na porção pública da nuvem híbrida.

Referências

Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. In *STOC*, volume 9, pages 169–178.

Hashemi, S. M. and Ardakani, M. R. M. (2012). Taxonomy of the Security Aspects of Cloud Computing Systems - A Survey. *International Journal of Applied Information Systems*, 4(1):21–28. Published by Foundation of Computer Science, New York, USA.

Intel (2014). Intel Advanced Encryption Standard Instruction (AES-NI). https://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni.

Mell, P. and Grance, T. (2011). The NIST definition of cloud computing (draft). *NIST special publication*, 800(145):7.

Sotomayor, B., Montero, R. S., Llorente, I. M., and Foster, I. (2009). Virtual infrastructure management in private and hybrid clouds. *Internet Computing, IEEE*, 13(5):14–22.