Estudo propõe técnicas para a segurança de dados em nuvens

Pesquisador da FEEC define requisitos para que sistema de armazenamento seja simples, seguro e confiável

LUIZ SUGIMOTO
sugimoto@reitoria.unicamp.br

Foto: Antonio Scarpinetti

Vitor Hugo Galhardo Moia, autor da dissertação: "O uso da criptografia em nomes e outros atributos do arquivo cria uma camada a mais de proteção"

Um estudo sobre segurança e privacidade no armazenamento de dados em nuvens destaca um conjunto de problemas e preocupações neste sentido e sugere técnicas para amenizá-los, além de avaliar custos e benefícios destas técnicas e de suas possíveis combinações para oferecer melhor proteção ao usuário. Em sua dissertação de mestrado, Vitor Hugo Galhardo Moia fez um levantamento de soluções comerciais e acadêmicas para o armazenamento de dados em nuvens, definiu requisitos considerados essenciais para um sistema seguro, confiável e simples de utilizar, e ainda desenvolveu uma aplicação que chamou de CPG (Cloud Privacy Guard). A pesquisa foi orientada pelo professor Marco Aurélio Amaral Henriques e apresentada na Faculdade de Engenharia Elétrica e de Computação (FEEC).

Vitor Moia observa que a computação em nuvens já é uma tecnologia conhecida e consolidada, que pode trazer várias vantagens para os usuários. "Dentre outras facilidades, os provedores de serviços de nuvens (CSP – Cloud Service Providers) disponibilizam um espaço em seus servidores para que sejam depositados arquivos pessoais, por exemplo. As vantagens são diversas, como o backup, pois provedores mantêm servidores espalhados pelo mundo: armazenado um arquivo na nuvem, cópias são disparadas para todos os pontos, livrando o cliente da preocupação de fazer backups para guardar seus dados em locais seguros. É preciso atentar, entretanto, para o fato de que provedores gratuitos não garantem que dados não serão perdidos."

O autor da dissertação ressalta também a vantagem financeira, já que o usuário pode contar com recursos computacionais potentes sem os custos associados a infraestrutura e manutenção locais, pagando apenas pelo tempo e espaço que consome (modelo pay-as-you-go). "Contudo, talvez a maior vantagem seja a possibilidade de acessar seu arquivo de qualquer local e em qualquer momento, bastando um dispositivo com acesso a internet. O armazenamento em nuvem é interessante também para empresas, que às vezes compartilham uma mesma base de dados, como cadastro de clientes ou de produtos, que os funcionários podem acessar e atualizar."

Enumeradas as vantagens, Moia retoma o foco de seu estudo, sobre os riscos trazidos pelo armazenamento em nuvens quanto a segurança e privacidade, a começar pelo fato de o serviço ser terceirizado. "Quando uma pessoa armazena seus dados na nuvem, acaba entregando o controle do arquivo ao provedor que, intencionadamente ou não, pode acessá-lo de maneira inadequada. Existem vários CSPs ditos gratuitos, mas sempre existe um preço, que não fica explícito para o usuário. O provedor pode, por exemplo, utilizar as informações em benefício próprio ou vendê-las a empresas de marketing. Mesmo serviços que garantem proteção aos dados, não são tão seguros assim, pois não atendem a requisitos essenciais."

Recurso da criptografia

A dissertação traz um estudo sobre as principais preocupações dos usuários quanto a sua privacidade, assim como técnicas para amenizá-las. "Quem quer sigilo dos dados pode recorrer à criptografia, codificando-os de forma que apenas quem detenha um segredo (chave) consiga acessá-los. Outra técnica de proteção é a fragmentação dos dados, dividindo-se um arquivo em muitos fragmentos que são armazenados em nuvens diferentes, impedindo assim que terceiros, incluindo os provedores, tenham acesso à íntegra do conteúdo."

Mais uma preocupação diz respeito à nomeação e atributos dos arquivos, que geralmente recebem nomes sugestivos demais, como "extrato bancário", por exemplo, direcionando os atacantes para dados do seu interesse. "O uso da criptografia em nomes e outros atributos do arquivo cria uma camada a mais de proteção. Outros usuários querem manter segredo de sua localização em relação ao provedor e, para isso, também existem soluções. Uma última preocupação é quanto à posse dos dados, ou seja, impedir que o provedor consiga, através das informações armazenadas, chegar à identidade real do usuário; como solução, podemos recorrer a serviços de identificação auxiliares, como os utilizados em sistemas de identidades federadas."

Vitor Moia explica que diante dos inúmeros problemas de segurança a serem solucionados, ateve-se à criptografia para um estudo mais detalhado. "Levantamos e classificamos vários provedores de serviços de nuvem que também oferecem a criptografia entre suas soluções. Com base nesse estudo, definimos requisitos de segurança que um provedor deve apresentar para tornar o serviço o mais confiável possível. Avaliamos 17 provedores de serviços de nuvens e aplicações com esta finalidade e, no final, concluímos que eles não são tão seguros como anunciam; nenhum deles cumpriu com todos os requisitos que definimos, havendo ainda muito espaço para melhorias."

Solução simples de usar

Identificadas as lacunas neste contexto, o autor da pesquisa propôs uma solução para dar uma camada de proteção aos arquivos armazenados em nuvens. "Depois de comparar os sistemas existentes e de chegar a um conjunto de requisitos essenciais para a privacidade e segurança, apresentamos, como prova de conceito, uma aplicação baseada nesses mesmos requisitos. Esta solução que chamamos de CPG (Cloud Privacy Guard), serve justamente para criptografar os dados dos usuários antes do envio para a nuvem. É uma versão ainda em desenvolvimento, mas que já permite realizar vários testes."

De acordo com Moia, o maior desafio foi chegar a uma aplicação simples de ser utilizada, requisitando o menor esforço possível do usuário. "Um dos problemas identificados em relação à criptografia é a carga extra de trabalho exigida do usuário, com uma série de procedimentos complexos e enfadonhos até para profissionais da área. Com o CPG, o usuário simplesmente arrasta o arquivo para dentro de uma pasta e o próprio aplicativo vai criptografar e migrar os dados para a pasta padrão da nuvem."

Vitor Moia considera que sua dissertação traz informações bastante úteis para o uso da tecnologia de armazenamento de dados em nuvens, como o levantamento e comparação dos principais provedores que estão no mercado, a fim de ajudar o usuário a diferenciá-los e escolher aquele que melhor atende às suas necessidades; o estudo sobre técnicas, chamando a atenção para outros problemas associados a este serviço e não apenas quanto ao sigilo; e ainda os custos e benefícios para cada técnica, quando aplicadas individualmente ou combinadas. "É possível obter maior proteção em diversos aspectos a um custo bem menor do que se imagina. Elaboramos vários requisitos, mas cada usuário tem sua necessidade e talvez não precise de um provedor que atenda a todos eles."

A segurança num provedor

Requisito	Preocupação
Segurança das chaves criptográficas	Gerenciamento correto das chaves criptográficas. São considerados fatores como o tempo de vida de uma chave e sua guarda correta.
Deduplicação segura	Garantir que técnicas de economia de espaço, usadas por provedores para evitar duplicação de dados que possam comprometer a privacidade dos usuários.
Alto nível de sigilo	Buscar modos de implementação de criptografia em serviços de nuvem, que possam trazer mais segurança e menos riscos à privacidade do usuário.
Trust no one (Não confie em ninguém)	Oferecer mais garantias de que o usuário seja o único capaz de acessar seus dados, através do uso exclusivo de uma chave criptográfica (senha) não compartilhada com o provedor da nuvem.
Sigilo dos atributos dos arquivos	Proteger os atributos de um arquivo (nome, datas de criação e última modificação, tamanho, etc.) contra acesso não autorizado por terceiros.
Open Source (Código fonte aberto)	Manter em domínio público o código fonte da aplicação de proteção a fim de evitar vulnerabilidades ou "*portas dos fundos*" que possam comprometer a segurança e privacidade dos usuários.
Autenticidade do software	Permitir que usuários possam verificar a autenticidade de uma aplicação, isto é, que ela foi realmente gerada pelo seu desenvolvedor, a fim de evitar que atacantes possam alterá-la sem serem detectados.
Autenticação Multi-fator	Aumentar a segurança do processo de autenticação, utilizando dois ou mais fatores para este fim. Ex. de fatores de autenticação: algo que o usuário saiba (senha), algo que ele possua (smartphone ou cartão com chip) e algo que ele seja (características biométricas como digitais, íris, etc.).
Usabilidade	Reduzir a complexidade do software criptográfico a fim de facilitar sua utilização, exigindo um menor esforço sem o comprometimento da segurança.

Fonte: Divulgação

Publicação

Dissertação: *"A Study about the Security and Privacy on Cloud Data Storage"*
Autor: Vitor Hugo Galhardo Moia
Orientador: Marco Aurélio Amaral Henriques
Unidade: Faculdade de Engenharia Elétrica e de Computação (FEEC)