Pedro Ramos Brandão

(Investigador do CIDHEUS – Universidade de Évora)

CLOUD DATA SECURITY

Um dos temos atualmente abordados com muita frequência é a questão da segurança nos sistemas de *Cloud Computing*. Grande parte das pessoas/empresas não sabem ou não entendem como podem estar seguros os seus dados e a sua informação se armazenados em sistemas de *Cloud Computing*. É perfeitamente legítimo e compreensível este receio: a segurança em *Cloud Computing*.

Manter a confidencialidade, integridade, autenticidade e disponibilidade de dados e informação em *Cloud Computing* não requer métodos especiais de proteção, nem novas técnicas! A proteção de dados em *Cloud Computing* é muito similar à proteção de dados nos tradicionais centros de dados. Autenticação e identificação, controlo de acesso, sistema anti "*delete*", verificação de integridade, dados mascarados e principalmente encriptação. Hoje em dia a base da segurança quer em centros de dados tradicionais e muito mais em sistemas de *Cloud Computing* "obriga" à utilização estruturada de encriptação.

Atualmente a criptografia expandiu os seus limites de utilização para efeitos de confidencialidade em comunicações e dados privados mas também a inclusão de técnicas que asseguram a integridade dos conteúdos, a autenticação da identidade bem como as assinaturas digitais seguras, através de um desenvolvimento acentuado de técnicas computacionais sofisticadas. Por este facto a criptografia é considerada uma tecnologia crítica e indispensável para a segurança em Cloud Computing.

Para obtermos a confidencialidade de dados criptográficos, o texto simples é convertido em texto cifrado através de vários possíveis meios, mas os de maior valor prático são todos baseados em funções matemáticas que devem atender a vários requisitos, incluindo:

- O algoritmo e a implementação devem ser computacionalmente eficientes na conversão de texto simples para texto criptografado, bem como na descodificação,
- O algoritmo deve estar aberto a ampla análise por uma comunidade de criptógrafos e outros,
- A saída resultante deve suportar o uso de ataques de força bruta mesmo por um grande número de computadores (como numa rede de computação ou em *Cloud Computing*).

Em operação, o texto simples é criptografado em texto cifrado usando uma chave de criptografia e o texto cifrado resultante é posteriormente descriptografado usando uma chave de descriptografia.

Em criptografia simétrica, essas chaves são as mesmas. A criptografia simétrica tem ampla aplicabilidade, mas quando é usada na comunicação entre as partes, a complexidade

da gestão de chaves pode tornar-se insustentável, pois cada par de comunicadores deve partilhar uma chave secreta única, também é muito difícil estabelecer uma chave secreta entre partes comunicantes quando um canal seguro já não existe para que eles possam trocar de forma segura uma chave secreta partilhada.

Em contraste, a criptografia assimétrica, também conhecida como criptografia de chave público-privada, a chave criptografada (chave pública) é diferente, mas matematicamente relacionada com chave privada no processo de descodificação.

A principal vantagem da criptografia assimétrica é que somente a chave privada deve ser mantida em segredo. É inviável calcular computacionalmente uma chave privada a partir de uma chave pública.

Portanto a melhor forma de manter os seus dados seguros em *Cloud Computing* é utilizar um sistema de criptografia assimétrico em todos os dados e informações armazenadas nestas estruturas.