

Elaboração de Modelo para Proteção de Dados em Discos Virtuais usando os Esquemas IBE e ICP

Paulo Renato de Moraes Vieira, Luciano Ignaczak

Escola Politécnica – Universidade do Vale do Rio dos Sinos (UNISINOS)

São Leopoldo – RS – Brasil

paulo.renato@terra.com.br, lignaczak@unisinos.br

Abstract. *The new data storage' structure provided by virtual disk services has allowed users to develop different methods for sharing files over the internet. However, the data security level available on these services is limited by definition, requiring an option to ensure the protection of the files on the cloud, like data cryptography. This paper introduces a new model of cryptography on such scenario, converging the asymmetric schemas IBE and ICP, hence establishing the data confidentiality based on users' identity and the authentication using digital certificates.*

Resumo. *Os serviços de discos virtuais proporcionaram novas estruturas de armazenamento de dados, alterando a forma como as pessoas passaram a compartilhar arquivos por meio da internet. Entretanto, por definição, esses serviços apresentam limitações em relação à capacidade de garantir a segurança da informação, exigindo métodos de controle que assegurem a proteção dos arquivos na nuvem, como o uso de criptografia de dados. Este artigo propõe um modelo de criptografia voltado a esse cenário, associando a estrutura dos esquemas assimétricos IBE e ICP de proteção, garantindo assim, a confidencialidade dos dados com base na identidade dos usuários e a autenticação através de certificados digitais.*

1. Introdução

A estrutura da sociedade em rede, termo que caracteriza o comportamento atual das pessoas está lastreada em definições como as publicadas pelo [NIST (2011)] e em citações como a de [Newcombe (2012)], que apresentam a tecnologia de computação em nuvem (*cloud computing*) disponibilizando um alto nível de computação com reduzido custo de investimento e novas estruturas de produtos e serviços de Tecnologia da Informação (TI) no mercado. Dentre as soluções, os discos virtuais (*cloud storages*) são aqueles que permitem aos usuários fazerem *download*, *upload* e compartilhamento de arquivos pela *internet*, sendo uma opção enxuta para armazenamento de dados, devido ao custo de investimento reduzido frente à estrutura proporcionada pelos Provedores de Serviços na Nuvem (PSN). Alguns exemplos de mercado são o Google Drive, Amazon S3, Microsoft OneDrive e o Dropbox, sendo que o último conta com uma carteira de 500 milhões de clientes em todo o mundo, refletindo aproximadamente em 3.3 bilhões de conexões de compartilhamento de arquivos, segundo matéria do site [UOL (2016)].

No entanto, conforme texto publicado na revista [ZDNET (2015)], utilizando técnicas particulares de exploração das vulnerabilidades de sincronia desses serviços, uma pessoa mal intencionada é capaz de acessar os arquivos armazenados na nuvem mesmo sem ter conhecimento das credenciais do usuário, ratificando a afirmação de

[Newcombe (2012)], que aponta fatores de comprometimento e de riscos à informação devido a essa flexibilidade dos serviços sob demanda, requerendo uma atenção maior ao processo de segurança da informação às soluções dispostas na rede.

Nesse contexto, a criptografia é identificada como a solução ideal na busca por métodos para promover a confidencialidade dos dados, podendo passar a percepção de segurança à informação, situação capaz de justificar a alta demanda, nos últimos anos, de usuários em busca de opções de criptografia, segundo [Martin (2008)]. Das opções disponíveis no mercado, a Infraestrutura de Chaves Públicas (ICP) é o esquema criptográfico que promove métodos avançados de autenticação da identidade dos atores envolvidos na transação. A base do processo está na troca de chaves-públicas autenticadas previamente por uma entidade denominada Autoridade de Certificação (AC), resultando em estrutura de dados conhecida como certificados digitais. A utilização de certificados digitais permite a replicação da estrutura física de autenticação no ambiente eletrônico, conforme cita [Adams e Lloyd (2003)].

Uma das principais características da estrutura ICP de proteção é o alto custo computacional e de processos que esse esquema apresenta. Nesse contexto, segundo [Martin (2008)], o modelo criptográfico com base na identidade é aquele com maior simplicidade e praticidade de implementação, sendo essa talvez a principal característica, que justifica a rápida aceitação e adoção do referido padrão criptográfico. O *Identity-Based Encryption* (IBE) é um esquema assimétrico de proteção, que permite o cálculo da chave pública com base em um fator pseudorrandômico utilizado para identificar os atores da comunicação, fator que torna desnecessária a negociação prévia das chaves públicas ou utilização de um diretório de segurança para publicação das mesmas, como apresenta o padrão ICP. Dessa forma, é garantido aos atores um modo mais simples e prático de assegurar a confidencialidade da informação, mesmo ressaltando que é fundamental a integração com as bases de autenticação presente em outra solução para garantir que a aplicação sustente todos requisitos de segurança exigidos no cenário atual.

Das soluções de proteção presentes no mercado, aquelas voltadas para a segurança dos arquivos dispostos na nuvem, em sua grande maioria, estão apoiadas no uso de senhas ou estruturas complexas com base no esquema ICP de criptografia. Diante desse cenário, este trabalho busca responder a seguinte questão: é possível apresentar uma solução alternativa de proteção, capaz de garantir a confidencialidade dos arquivos na nuvem, associando a praticidade do modelo IBE e o esquema ICP de proteção?

Para responder a essa pergunta, o objetivo deste artigo é propor um modelo criptográfico capaz de sincronizar a capacidade de garantir a confidencialidade dos dados do esquema IBE ao padrão de autenticação presente no esquema ICP de proteção. O modelo permitirá aos autores avaliar a viabilidade de implementação em um ambiente real, garantindo a proteção de arquivos armazenados em discos virtuais e possibilitando o compartilhamento de dados de forma segura.

A organização deste artigo está distribuída em quatro seções, a segunda apresenta os trabalhos de diferentes autores que se relacionam ao objeto deste artigo, buscando pontuar os conceitos, percepções e conclusões. A terceira seção descreve o modelo criptográfico proposto, fornecendo informações gerais acerca dos componentes presentes e as respectivas relações. Por fim, a seção quatro apresenta as considerações finais, indicando os pontos de relevância ao projeto e proposta de segurança apresentada neste documento.

2. Trabalhos Relacionados

São apresentadas, nesta seção, visões de diferentes autores quanto aos principais tópicos relacionados e trabalhados ao longo desse projeto, buscando pontuar os conceitos, percepções e conclusões que facilitarão na identificação dos diferenciais presentes na solução projetada. Para tanto, o trabalho de pesquisa focou na busca por artigos em bases de dados acadêmicas, como a ACM, IEEE e Springer Link.

Dos desafios de segurança da computação em nuvem, a grande maioria das vulnerabilidades e ameaças elencadas pelos autores estão ligadas às características intrínsecas da tecnologia ou à implementação, em especial aos fatores da terceirização do controle e compartilhamento de recursos (estrutura “multi-inquilinos”). Para [Bouayad et al. (2012)] é preciso que haja uma visão holística do processo de proteção, garantindo que cada camada do serviço (da física à lógica) esteja devidamente avaliada e controlada, sob padrões de segurança que melhor representam os diferentes modelos presentes no ambiente, os quais contemplam diferentes atores envolvidos no cenário. Com o estudo dirigido à estrutura dos PSNs, [GroBauer et al. (2010)] propõem uma estrutura de referência dos principais componentes que orbitam os serviços na nuvem, permitindo assim uma visão mais ampla das vulnerabilidades e ameaças do ambiente. No trabalho de [Prakash e Dasgupta (2016)] estão descritos 9 dos principais pontos de vulnerabilidade do ambiente em nuvem considerados pela Aliança de Segurança da Computação em Nuvem (CSA), bem buscam apontar métodos de atender a essa demanda. Dentre os pontos citados, é possível constatar que o nível de segurança dos métodos de autenticação que é usualmente baixo, do tipo usuário e senha, demandando que haja maior atenção nesse quesito.

Quanto aos trabalhos que referenciam a estrutura de segurança do esquema IBE de proteção, [Lee (2010)] descreve uma solução híbrida que faz uso das tecnologias ICP e IBE, denominada Unified Public Key Infrastructure (UPKI). Na descrição desta solução, o autor propõe a criação de uma entidade que contemple os papéis de uma CA e uma PKG no ambiente, denominada Key Generation and Certification Authority (KGCA), além de agentes responsáveis pela recuperação da respectiva chave privada do esquema IBE, denominados Key Privacy Agents (KPAs). O sistema proposto [Sharma e Joshi (2016)] trata dos paradigmas de revogação das chaves utilizadas para criptografia de arquivos, sincronizando as características do esquema IBE com aquele que tem a base em atributos aleatórios, conhecido como ABE. Além da PKG, nesse ambiente há uma entidade denominada KU-CSP, que pode ser gerenciada pelo provedor da nuvem e é responsável por parte importante do processo de revogação das chaves. Propondo um método avançado de troca de chaves, [Júnior et al (2004)] apresentam solução alternativa à associação disjuntiva descrita por [Boneh e Franklin (2003)] na descrição original do esquema IBE.

Para proteção de arquivos na nuvem, desde acesso, armazenamento e troca, [Kumar e Singh (2015)] propõem um protocolo de autenticação dos usuários com base em criptografia utilizando uma estrutura de cálculo baseada em curvas elípticas, além de uma senha, do tipo One Time Password (OTP), gerado por um webserver na nuvem. Já no trabalho publicado por [Wei, Liu e Hu (2013)], os autores utilizam a estrutura IBE de proteção para proteger arquivos na nuvem, porém contam com a presença de uma terceira entidade responsável pela revogação da chave, denominada proxy re-encryption.

O modelo proposto neste artigo garante a confidencialidade da informação e autenticação dos usuários na troca e armazenamento de dados na nuvem, integrando o uso de certificados digitais ao processo de proteção com base no esquema IBE. Há similaridade com a proposta e estudos descritos em [Lee (2010)], porém contando com entidades distintas pelas ações de AC e PKG. A ideia central é utilizar as chaves IBE somente para garantir a confidencialidade dos dados e se apoiar na estrutura ICP presente no mercado para garantir os requisitos de autenticação e comprometimento legal das ações presentes nesse serviço, sendo um modelo avançado frente a processos como o apresentado por [Kumar e Singh (2015)].

3. Modelo Proposto

O objetivo central do modelo proposto neste artigo é apresentar um método de garantir a confidencialidade dos arquivos armazenados na nuvem. Conforme descrito na Figura 1, o modelo está estruturado na presença de cinco elementos, segmentados em locais e remotos, sendo os locais aqueles que iniciam e finalizam os processos, o Remetente e o Destinatário da informação. Fica a cargo dos elementos remotos sustentar as estruturas de armazenamento de dados na nuvem (Disco Virtual), recuperar as chaves de segurança utilizadas nos processos de criptografia e decriptografia (PKG), além de garantir a confiabilidade no processo de autenticação da identidade (AC).

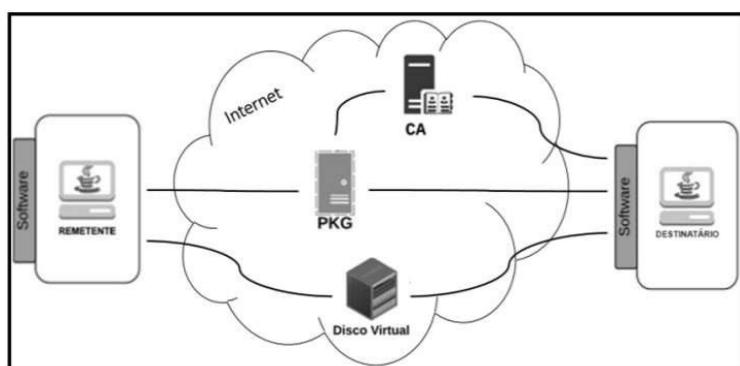


Figura 1 - Componentes e relacionamentos presentes no modelo criptográfico

Dos elementos ilustrados na Figura 1, o usuário “Remetente” é aquele que dá início ao processo de criptografia, buscando por um método de compartilhamento seguro de arquivos na nuvem, com controle de acesso aos dados mesmo que nunca tenha havido contato entre os envolvidos, independente do serviço de disco virtual utilizado. Serviço web de armazenamento de dados, o “Disco Virtual” é utilizado como ponto de distribuição online de arquivos, promovendo a disponibilidade da informação aos métodos de compartilhamento de dados utilizado pelos usuários. Os usuários podem enviar e baixar arquivos de qualquer lugar desde que haja conexão com a internet, através de páginas ou por aplicativos, *desktop* ou de dispositivos móveis. Entidade responsável pela emissão do certificado digital utilizado pelo Destinatário para autenticação, além de responder às requisições online de verificação do status do certificado, a “AC” pode fazer parte de uma estrutura ampla de confiança, e estar disponível na internet, ou de perímetro reduzido, de acesso limitado à rede local, conforme descrito na Figura 1. A “PKG” é responsável pela custódia das chaves de segurança dos usuários e validação da identidade do destinatário, atuando como ponto crucial tanto no processo de criptografia quanto de decriptografia dos arquivos. Para funcionamento pleno do sistema, é primordial que esse

componente esteja disponível na internet. Elemento final do fluxo do modelo proposto, o “Destinatário” é o usuário com o qual se deseja estabelecer a troca segura de arquivos na nuvem, sendo utilizado o respectivo email como informação chave para proteção dos arquivos e controle de acesso aos dados.

O método de criptografia escolhido para este modelo contempla a utilização de uma informação de domínio público, de fácil recuperação e diretamente ligado à identidade dos usuários. A informação elencada nesta proposta foi o endereço de correio eletrônico, permitindo que os usuários possam trocar dados de forma confidencial mesmo que nunca tenham estabelecido um canal seguro de compartilhamento anteriormente. O Remetente envia uma solicitação online à PKG, indicando no conteúdo da requisição o email daquele com quem se quer compartilhar a informação na nuvem. O processamento desses dados pela PKG irá gerar um código enviado na resposta ao Remetente, permitindo que o *software* local do usuário criptografe o conteúdo do arquivo utilizado, pronto para envio e armazenamento na nuvem através dos serviços de discos virtuais. Não há comunicação com a AC nas operações de criptografia de arquivos, uma vez que o usuário que inicia o processo é a origem, bem como não é foco neste modelo garantir a autenticidade e o não repúdio da informação.

Aspecto muito importante presente neste modelo é o bloqueio do acesso à informação original por usuários não autorizados. Isso ocorre no processo de decriptografia do arquivo, no qual o usuário Destinatário precisa autenticar-se junto à PKG, utilizando certificado digital válido e emitido junto a uma AC presente na raiz de confiança da PKG, para obter acesso à chave privada correspondente ao email utilizado no processo de criptografia. Somente após essa validação a PKG irá retornar os valores necessários para que o software local recupere a chave de proteção utilizada para criptografar o arquivo, permitindo assim acesso ao conteúdo original da informação.

Importante ressaltar que é pré-requisito para o sucesso deste modelo, a presença de certificado digital válido para autenticação da identidade do Destinatário. O esquema proposto fornece um amplo suporte para customizações acerca da área de atuação das entidades AC e PKG, de modo que estas atendam da melhor forma possível às necessidades do ambiente, exigindo apenas que haja um alinhamento prévio entre esses componentes.

4. Considerações Finais

A estrutura apresentada neste documento torna viável a convergência do que há de melhor nos esquemas IBE e ICP de criptografia, assegurando o sigilo da informação a um custo reduzido de complexidade operacional. Indo além, o projeto fornece suporte para resposta aos desafios relacionados aos fatores de retenção e gerenciamento do número extensivo de chaves criptográficas, demonstrando uma capacidade atemporal de decriptografia, não importando a versão das chaves assimétricas associadas aos certificados dos usuários.

O padrão criptográfico gerado após a associação de dois esquemas assimétrico de proteção, permite afirmar que a proposta atende aos requisitos de confidencialidade da informação, conforme descrito nos padrões internacionais de segurança ISO 27001 e 27002, fornecendo suporte necessário para elevar o nível de proteção dos dados armazenados em discos virtuais, enquanto garante o controle de acesso à informação somente para o usuário autorizado.

5. Referências

- Adams, C. e Lloyd, S. "Understanding pki. Boston", Massachusetts - EUA: Pearson Education, Inc, 2003.
- Boneh, D. e Franklin, M. "Identity-based encryption from the weil pairing". SIAM J. of Computing., [S.l.], v. 32, n. 3, p. 586–615, 2003.
- Bouayad, A. et al. "Cloud computing: security challenges". 2012 Colloquium in Information Science and Technology., [S.l.], p. =26–31, Out 2012.
- Grobauer, B. e Wallosche, T. e Stöcker, E. "Understanding cloud computing vulnerabilities". IEEE Security & Privacy., [S.l.], v. 2, n. 9, p. =50–57, Jun 2010.
- Júnior, W. D. B. e Terada, R. et al. "An ibe scheme to exchange authenticated secret keys". IACR Cryptology ePrint Archive 2004., [S.l.], p. =71, 2004.
- Kumar, V. e Singh, S. "Secured user's authentication and private data storage- access scheme in cloud computing using elliptic curve cryptography". 2th International Conference on Computing for Sustainable Global Development (INDIACoM)., [S.l.], p. 791–795, Mar 2015.
- Lee, B. "Unified public key infrastructure supporting both certificate-based and id-based cryptography". ARES'10 International Conference on Availability, Reliability and Security. [S.l.], p. 54–61, Fev 2010.
- Martin, L. "Introduction to identity-based encryption". Norwood, Massachusetts - EUA: Artech HouseIT, 2008.
- Newcombe, L. "Securing cloud services". Cambridgeshire, UK: IT Governance Publishing, 2012.
- NIST. "The nist definition of cloud computing (september 2011)". Disponível em: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> . Acesso em: 1 maio 2016.
- Prakash, C. e Dasgupta, S. "Cloud computing secuity analysis: Challenges and possible solutions." Electrical, Electronics, and Optimization Techniques (ICEEOT), International Conference on. IEEE, 2016.
- Sharma, R. e Joshi, B. "H-IBE: Hybrid-identity based encryption approach for cloud security with outsourced revocation." Signal Processing, Communication, Power and Embedded System (SCOPES), 2016 International Conference on. IEEE, 2016.
- UOL. "Dropbox comemora meio bilhão de usuários". Disponível em: <http://codigofonte.uol.com.br/noticias/dropbox-comemora-meio-bilhao-de-usuarios> . Acesso em: 30 maio 2016.
- Wei, J. e Liu, W. e Hu, X. "Secure data sharing in cloud computing using revocable-storage identity-based encryption". IEEE Transactions on Cloud Computing., [S.l.], p. 1–6, Ago 2013.
- ZDNET. "Attackers can access dropbox, google drive, onedrive files without a user's password". Disponível em: <http://www.zdnet.com/article/dropbox-google-drive-onedrive-files-man-cloud-attack> . Acesso em: 23 Junho 2016.