Uma forma de tratar o desafio de proteger a privacidade dos usuários de armazenamento de dados em nuvens

Vitor Hugo Galhardo Moia[1], **Marco Aurélio Amaral Henriques**[1]

[1]Faculdade de Engenharia Elétrica e de Computação
Universidade Estadual de Campinas (Unicamp)
Campinas, SP, Brasil 13083-852

{vhgmoia,marco}@dca.fee.unicamp.br

Abstract. *Security and privacy are hot topics nowadays, mostly because the increasing number of news about cyber attacks in the Internet. Cloud data storage is a technology that brings several benefits to users, but, due to concerns related to its security, many users are reluctant to use it. The purpose of this article is to discuss the present problems in cloud data storage environment, as well as to propose a cryptographic application that tries to mitigate such problems and preserve user's privacy and security.*

Resumo. *Privacidade e segurança são temas que têm gerado muitas discussões ultimamente, principalmente devido ao crescente número de notícias sobre novas ameaças que surgem na internet. O armazenamento de dados nas nuvens é uma tecnologia em ascensão que traz diversas vantagens aos usuários em sua utilização. Entretanto, devido a preocupações com segurança, muitos usuários relutam em utilizar este serviço. O objetivo deste artigo é realizar uma breve discussão de alguns problemas presentes atualmente no ambiente de armazenamento de dados em nuvens, assim como propor uma aplicação criptográfica para mitigar tais problemas e preservar a privacidade e segurança dos usuários.*

1. Introdução

Devido às atraentes características do serviço de armazenamento de dados em nuvens, vários usuários migram seus dados para este ambiente. Contudo, recentes notícias sobre invasões à privacidade e segurança das pessoas e um possível monitoramento não autorizado por agências que deveriam proteger os usuários [Gellman and Soltani 2013] [Gellman 2013], contribuíram para gerar um sentimento de desconforto e receio nos mesmos, que passam muitas vezes a evitar a utilização de tais serviços. Diante deste cenário, técnicas baseadas em criptografia são cada vez mais requisitadas. Porém, a complexidade envolvida em sua utilização, muitas vezes agravada pela falta de experiência dos usuários, impede que muitos utilizem esta técnica para proteger suas informações e até sua privacidade neste meio.

Pensando em proporcionar um maior grau de confiança aos usuários, vários provedores de serviços de nuvem (CSP) começaram a oferecer serviços de criptografia em suas soluções. Contudo, existem vários obstáculos que devem ser superados, mas que às vezes são deixados de lado devido à complexidade envolvida. Neste artigo, são apresentados alguns problemas presentes no armazenamento de dados em nuvens, assim como é proposta uma abordagem, baseada em criptografia, com a finalidade de proteger a privacidade e dar mais segurança aos usuários que armazenam seus dados em nuvens. Assim

 ©2015 SBC — Soc. Bras. de Computação

como o TOR que utiliza camadas de encriptação para oferecer anonimato a seus usuários [Murdoch and Danezis 2005], um bom sistema de nuvem que garanta tanto a segurança dos arquivos como a privacidade de seus proprietários deve contar com várias camadas de proteção. Utilizando deste conceito, o CPG (Cloud Privacy Guard), como é chamada a proposta, utiliza técnicas criptográficas para proteger tanto o conteúdo como os atributos dos arquivos, além de utilizar um segundo fator para melhorar a segurança na autenticação dos usuários. Tais características destacam esta proposta entre os serviços disponíveis atualmente que utilizam a criptografia para cifrar os dados armazenados na nuvem. Além disso, o CPG se caracteriza pela sua facilidade de uso e configuração, requisitos destacados na concepção do mesmo, com a finalidade de viabilizar uma maior adoção tanto por parte de usuários leigos como dos mais experientes.

O restante deste trabalho está estruturado como segue: a seção II apresenta alguns problemas presentes no ambiente de armazenamento em nuvens. A seção III apresenta os trabalhos relacionados e a seção IV descreve a abordagem proposta, detalhando seu propósito, suas características e requisitos, funcionamento básico e algoritmos criptográficos utilizados. Já a seção V apresenta uma discussão sobre a autenticação multifator e como é implementada no CPG. Finalmente, a seção VI apresenta as conclusões e trabalhos futuros.

2. Problemas no armazenamento de dados em nuvens

Nesta seção são apresentados alguns riscos relativos ao armazenamento de dados em nuvens públicas. Alguns destes tópicos aparecem na lista das principais ameaças no ambiente de nuvem apontadas pela Cloud Security Alliance (CSA), entidade especializada em tecnologias de computação e segurança nas nuvens [CSA 2010].

- **Sigilo:** a maior parte dos usuários armazenam suas informações em claro na nuvem, ou seja, sem nenhuma proteção criptográfica sobre eles. Caso o servidor que esteja hospedando essas informações seja comprometido, os dados do usuário estarão vulneráveis a atacantes. Com isso, informações críticas de um usuário podem ser descobertas por outros e até usadas contra seus proprietários (por meio de chantagens, por exemplo). Outra exposição relativa ao armazenamento em claro dos dados é a possibilidade do monitoramento realizado pelos próprios CSPs nos dados, cuja finalidade pode ser o direcionamento de publicidade, por exemplo.
- **Localização:** normalmente os servidores de um CSP estão espalhados pelo mundo, de acordo com suas necessidades e também considerando fatores econômicos. Os dados dos usuários ficam armazenados de forma distribuída nestes servidores, e muitas vezes podem ser armazenados em um país diferente daquele do usuário. Isso pode implicar na mudança das leis pertinentes à privacidade do usuário em relação a estes dados. Este fato pode ser prejudicial aos usuários, uma vez que seus dados estão em posse de uma terceira parte, o CSP, que pode ser obrigado a entregar os mesmos para órgãos do governo, por exemplo.
- **Integridade:** detectar modificações não autorizadas em uma informação pode ser bastante útil na prevenção de ataques contra a segurança e privacidade dos usuários. Um dado armazenado na nuvem pode sofrer alguma modificação, como troca de algum conteúdo ou a adição de um código malicioso, como um vírus, por exemplo. Isso pode ocorrer tanto na transmissão do dado pela rede ou enquanto

 ©2015 SBC — Soc. Bras. de Computação

está armazenado nos servidores da nuvem. É importante que um usuário tenha meios de tomar conhecimento dessas alterações a fim de evitar danos maiores.

- **Aplicações inseguras:** a segurança dos dados de um usuário está vinculada a segurança do sistema que ele utiliza. Portas dos fundos, ou alçapões, são exemplos de ameaças que podem existir e que devem ser levados em consideração na análise de um sistema, uma vez que eles podem comprometer toda a segurança por terceiros que os conheçam. Por essa razão, antes da utilização de um software de um fabricante desconhecido, os usuários precisam se certificar que aquele software é realmente seguro e confiável.
- **Ataques internos:** este tipo de risco apresenta uma grande ameaça para os usuários uma vez que os atacantes são o pessoal de dentro da própria nuvem. Ex-empregados, ou atuais empregados descontentes que buscam fazer algum tipo de chantagem ou dano são exemplos do perfil destes atacantes. A grande vantagem que esses atacantes possuem em relação aos atacantes externos é o seu conhecimento sobre a infraestrutura da nuvem, e também o fato que algumas vezes eles têm acessos privilegiados, o que facilita a obtenção de alguma informação armazenada.
- **Sequestro de conta ou serviço:** esta ameaça está relacionada à tentativa de um atacante obter acesso a conta de um usuário, por meio de ataques como força bruta, phishing, fraude, exploração de vulnerabilidades de um software, ou outros. Normalmente, esse ataque é facilitado pelo reuso de credenciais (par login/senha) por parte dos usuários.

3. Trabalhos relacionados

Podemos dividir os trabalhos relacionados à proteção da privacidade dos usuários e da segurança dos seus dados em duas linhas: soluções da literatura e soluções comerciais. Na primeira linha, existem trabalhos que utilizam a criptografia para minimizar diversos problemas encontrados atualmente [Kumar et al. 2012], [Xu et al. 2012], [Kamara and Lauter 2010], [Gasti et al. 2010] e [Phuong et al. 2012]. Contudo, em muitos casos a solução proposta não é viável na prática e é tratada de forma superficial, onde não são levadas em consideração questões importantes que podem até comprometer toda a solução. Como exemplos podemos citar o gerenciamento das chaves criptográficas, a usabilidade da aplicação final, os meios para autenticação, dentre outros fatores, que são muitas vezes deixados de lado durante o projeto e considerados somente na implementação da solução. Estes fatores são tratados e discutidos neste trabalho, fato que o difere de outros na literatura.

Em relação as soluções comerciais [Schiessle 2013], [SpiderOak 2015], [Cyphertite], [Meisser 2011], [Credeon] e [Boxcryptor], muitas vezes a criptografia é utilizada nos servidores da nuvem, o que pode simplificar o uso das aplicações, por tirar dos usuários o fardo do gerenciamento de chaves. Porém, isto acontece com o custo de uma ilusão de privacidade, uma vez que a nuvem terá acesso aos dados do usuário por ter controle de todo o processo e, principalmente, das chaves. Os provedores de serviço que oferecem soluções que utilizam a criptografia no lado do usuário, são poucos. Nestas soluções o dado é cifrado antes de ser enviado para a nuvem e o usuário é responsável pelo gerenciamento de suas chaves, sendo o único com acesso a seus dados. Estas são as soluções consideradas ideais para os usuários que demandam uma maior privacidade.

 ©2015 SBC — Soc. Bras. de Computação

A abordagem proposta realiza a criptografia no lado do cliente, mas faz isso de forma a impactar o menos possível na usabilidade do sistema, exigindo o mínimo dos usuários. A autenticação utilizando dois fatores é um de seus diferenciais, pois não é adotada por nenhum CPS que fornece serviços criptográficos no lado do cliente. Esta tecnologia se faz cada vez mais necessária à medida que a autenticação por um único fator tem se mostrado insegura em vários casos. Além disso, a abordagem proposta também se preocupa com o controle do ciclo de vida das chaves criptográficas, característica muitas vezes não presente nos CSPs.

4. Uma abordagem para armazenamento seguro e privativo em nuvens

Como forma de avaliar a possibilidade de se ter um modelo de aplicação que proporcione segurança e privacidade aos usuários sem, contudo, diminuir a usabilidade com a qual os mesmos já se habituaram, propomos uma abordagem criptográfica para armazenamento de dados em nuvens que procura minimizar tanto quanto possível a sobrecarga imposta aos usuários no tocante ao seu uso e ao gerenciamento de chaves. Nesta seção, são apresentadas algumas características desta abordagem que buscam amenizar os riscos presentes no armazenamento em nuvens, discutidos na seção II.

4.1. Propósito

A proposta é realizar operações criptográficas sobre os dados que necessitam de proteção, antes de serem enviados e armazenados na nuvem. Também é propósito deste modelo ser independente dos CSPs disponíveis, podendo ser integrado com qualquer um que atenda alguns requisitos mínimos. Ele também deve ser fácil e amigável para configurar e utilizar, exigindo conhecimento mínimo em criptografia por parte de seus usuários.

4.2. Características e requisitos

Uma das características desta abordagem é ela poder ser integrada com diversos CSPs, como o Google Drive, OneDrive, Dropbox, Amazon entre outros, ou seja, ela pode ser integrada a qualquer CSP que trabalhe com um modelo de pasta de sincronismo, onde o usuário deposita seus arquivos para eles serem enviados para a nuvem. A aplicação também permite que os usuários compartilhem seus arquivos com outros usuários do sistema, através de certificados digitais, os quais podem ser certificados X.509 adquiridos no mercado (ICP-Brasil) ou emitidos pela ICP de Ensino e Pesquisa da RNP.

Em uma primeira utilização, o usuário cria um segredo, o qual será utilizado para proteger suas chaves criptográficas. Este segredo deverá ser fornecido sempre que uma operação criptográfica for necessária, exceto se ele já foi fornecido recentemente (chave ainda no estado ativada). Também é requisitado ao usuário nesta primeira utilização a definição dos diretórios a serem utilizados, tais como o diretório onde o usuário depositará os arquivos a serem cifrados (*Arquivos Secretos*), bem como o diretório de sincronização com a nuvem (ou um subdiretório deste) onde ficará o subdiretório *Arquivos Cifrados*, contendo a versão cifrada dos arquivos ditos secretos.

As operações criptográficas no CPG são realizadas no lado do cliente. Com isso, problemas como sigilo, localização e ataques internos são minimizados, uma vez que o único que possui acesso aos dados é o usuário.

 ©2015 SBC — Soc. Bras. de Computação

Para o gerenciamento do ciclo de vida das chaves criptográficas, o CPG utiliza a infraestrutura de chaves públicas ICPEdu ou ICP-Brasil. Além disso, sempre que um arquivo sofrer qualquer modificação e necessitar ser cifrado novamente, sua chave simétrica é trocada. Também faz parte deste gerenciamento de chaves a funcionalidade de não permitir que nenhuma chave secreta ou privada fique armazenada em claro na memória por mais tempo do que o estritamente necessário para seu uso.

Outra característica de CPG é não ser vulnerável a ataques que se aproveitam do recurso de deduplicação de arquivos na nuvem [D. Harnik and Shulman-Peleg 2010], devido ao fato de usar chaves aleatórias e distintas para cada arquivo que for armazenado de forma cifrada.

A recuperação de senhas normalmente disponibilizada por vários serviços na internet e até mesmo por alguns CSPs, não esta presente no CPG. O segredo criado pelo usuário não é armazenado em nenhum local, sendo apenas utilizado para cifrar/decifrar a chave privada do mesmo. A vantagem desta abordagem é a maior segurança dos dados do usuário uma vez que ele será o único que possuirá o segredo necessário para decifrar sua chave privada e, consequentemente, seus dados. Em vários serviços criptográficos disponíveis, a senha do usuário está atrelada às suas chaves criptográficas, e CSPs que habilitam o serviço de recuperação de senhas, possuem meios para acessar as chaves dos usuários. Assim, os usuários não são os únicos que possuem acesso aos seus dados. O problema de não se prover um serviço de recuperação de senhas é que, se o usuário perder/esquecer seu segredo, não conseguirá mais decifrar seus dados e não poderá acessar o conteúdo dos mesmos.

O CPG, além de cifrar o conteúdo dos dados dos usuários, também cifra os atributos dos mesmos, como o nome, data de criação, data da última modificação etc., a fim de criar uma barreira extra de proteção contra atacantes, dificultando que os mesmos direcionem seus ataques aos dados mais valiosos de suas vítimas.

Com relação à usabilidade, a abordagem proposta procura utilizar conceitos já assimilados pelos usuários, como arrastar e soltar objetos em uma pasta específica, por exemplo. Este modelo é similar aos utilizados por vários CSPs, como Google Drive, One Drive, Dropbox, etc. Em CPG, para um usuário cifrar um arquivo, basta que ele o deposite na pasta chamada *Arquivos Secretos*. Este evento fará com que o CPG o cifre segundo um protocolo específico e grave o resultado na pasta *Arquivos Cifrados* já dentro da pasta de sincronismo padrão da nuvem.

Uma vez realizada a configuração inicial, o usuário deve apenas fornecer seu segredo cada vez que usar CPG ou de tempos em tempos. Deste modo, muitos dos detalhes do funcionamento deste modelo, o gerenciamento das chaves e outras atividades, são realizadas de forma transparente para o usuário.

Um protótipo de CPG foi desenvolvido em linguagem Java e o mesmo vem sendo testado com diferentes serviços de armazenamento em nuvens como ownCloud, Dropbox e Drive. A maior facilidade que os usuários têm de utilizá-lo é obtida ao custo de uma maior complexidade de desenvolvimento e depuração. Esperamos que a interface mais simples e direta proposta, sem exigir muito treinamento e aproveitando os conhecimentos já consolidados nos usuários leigos e avançados, possa tornar esta aplicação uma forte aliada de todos os que buscam por mais segurança e privacidade ao armazenar seus dados

 ©2015 SBC — Soc. Bras. de Computação

em nuvens públicas ou privadas.

4.3. Funcionamento básico

A aplicação sempre é iniciada junto com o sistema operacional e fica executando em plano de fundo. Há um ícone na barra de notificações do sistema que permite aos usuários visualizarem que a mesma está em execução e até interagirem com ela, para acessar suas configurações ou a encerrá-la. Cada arquivo que o usuário deseja enviar para a nuvem de forma criptografada deve ser depositado na pasta *Arquivos Secretos*, para ser cifrado e depositado automaticamente na pasta *Arquivos Cifrados*, de onde será enviado para nuvem pelo software padrão da mesma, conforme pode ser visualizado nas Figs. 1 e 2 (nuvem ownCloud neste caso).

A Fig. 3 ilustra o processo de interação básico do usuário com CPG quando se deseja enviar um arquivo para a nuvem de forma cifrada. É importante destacar que os usuários podem trabalhar com o arquivo em claro diretamente na pasta *Arquivos Secretos* e, a cada alteração que o mesmo sofrer, ele será novamente cifrado e atualizado na nuvem.

Se a nuvem é acessada a partir de outro dispositivo que tenha a aplicação instalada, esta irá verificar as diferenças de conteúdo entre as pastas *Arquivos Secretos* (do dispositivo) e *Arquivos Cifrados* (da nuvem) e sempre que detectar um novo arquivo criptografado na nuvem, procurará decifrá-lo (mediante fornecimento de um segredo) e disponibilizá-lo ao usuário na pasta de *Arquivos Secretos*. O usuário ficará limitado a acessar seus arquivos criptografados somente através do CPG.

Para o compartilhamento de dados, o proprietário dos mesmos necessita criar e compartilhar uma pasta na nuvem com os interessados através da interface da própria nuvem, e então depositar os certificados destes interessados nesta pasta (Fig. 4). O CPG reconhece os certificados e cifra os arquivos (na verdade, cifra uma chave simétrica que é utilizada na cifragem do arquivo) da pasta utilizando estes certificados. Para revogar o acesso compartilhado de um determinado usuário, o proprietário necessita apenas remover o certificado deste usuário da pasta. Assim, na próxima vez que algum arquivo da mesma for modificado, ele será cifrado com base somente nos certificados presentes naquele momento deixando de ser acessível para o usuário (certificado) removido.

4.4. Algoritmos criptográficos

Os algoritmos criptográficos utilizados na abordagem proposta são o RSA e o AES, devido a ampla disponibilidade e reputação de segurança de ambos. Cada usuário deverá possuir um par de chaves assimétricas (recomenda-se 2048 bits), onde a chave pública é armazenada em forma de certificado e a privada cifrada com o segredo do usuário. A fim de possibilitar o acesso por meio de outros dispositivos aos arquivos do usuário, uma cópia destas chaves também é armazenada na nuvem em uma pasta específica criada pela aplicação. Cada arquivo é cifrado com uma chave simétrica aleatória (256 bits), que é lacrada pelas chaves públicas dos usuários que têm acesso ao mesmo. No momento da decifragem, o usuário deve fornecer seu segredo para que seja derivada uma chave simétrica (por meio do algoritmo Password Based Key Derivation Function 2 - PBKDF2 [IETF 2000] - 10 mil iterações e 192 bits de salt) que será utilizada para decifrar a chave privada e então obter a chave que decifra o arquivo. Este processo está detalhado nas Figs. 5 e 6, que tratam da geração das chaves criptográficas e sua recuperação, respectivamente.

 ©2015 SBC — Soc. Bras. de Computação

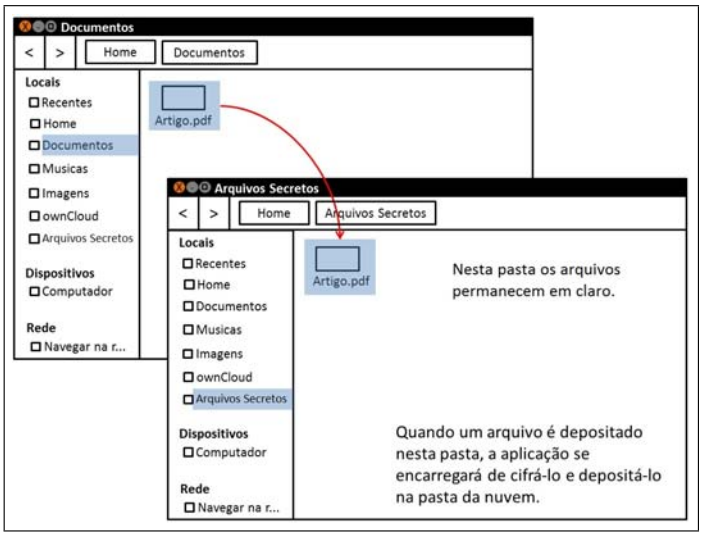

Figure 1. Processo para criptografar um arquivo a ser armazenado na nuvem

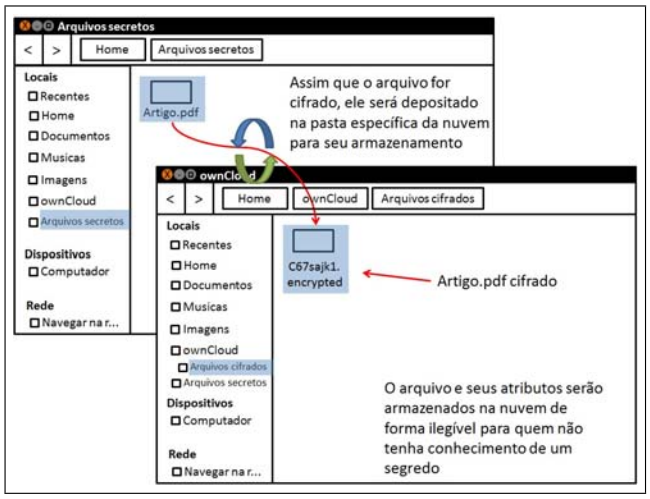

Figure 2. Criptografia e guarda do arquivo na pasta da nuvem

5. Autenticação Multi-fator

A autenticação multi-fator consiste na combinação de dois ou mais métodos de autenticação para verificar a identidade de um usuário. O método mais empregado hoje em dia é baseado em algo que o usuário saiba, como seu par login/senha. Este método é o mais bem aceito pela maioria dos usuários, justamente por já estar consolidado e a maioria estar familiarizada com ele. Outro motivo pelo seu sucesso é seu baixo custo, já que não necessita de um equipamento extra para a autenticação. Existem também outros métodos de autenticação que se baseiam em algo que o usuário tenha, como um dispositivo criptográfico, ou algo que o usuário é, considerando fatores biométricos (impressão digital, íris, retina, voz etc.). Porém, devido à necessidade de utilização de um equipamento extra de leitura (em alguns casos) e ao maior custo, os dois últimos métodos não são amplamente adotados como o primeiro. Contudo, com o crescente aumento da popularidade de telefones móveis, vários sistemas começaram a utilizá-los como um segundo fator de autenticação. Um exemplo da utilização desta abordagem é descrita por Lee et al [S. Lee 2010], que utiliza os telefones celulares dos usuários em conjunto com um par

 ©2015 SBC — Soc. Bras. de Computação

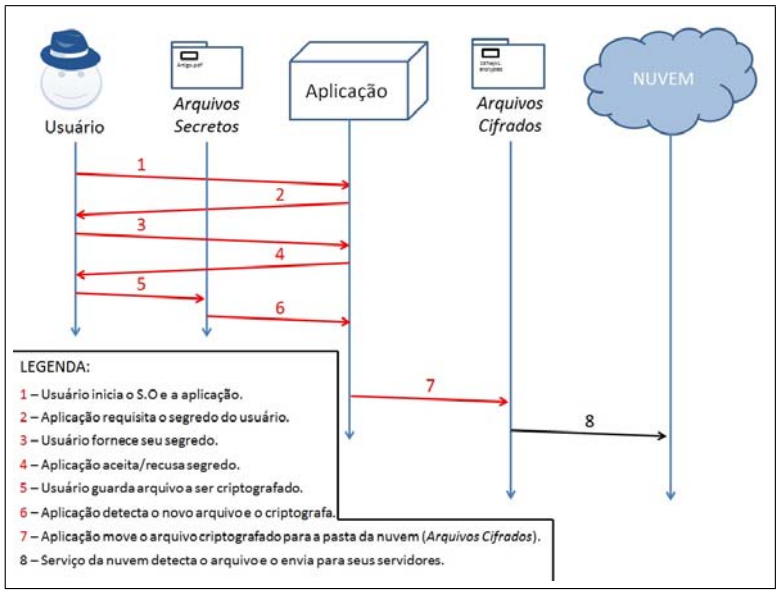

Figure 3. Interação básica da aplicação com o usuário

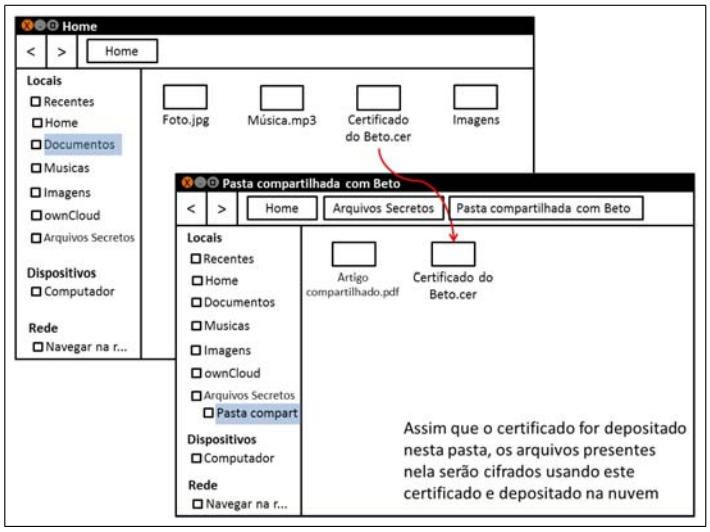

Figure 4. Compartilhamento de pasta com Beto

login/senha.

A necessidade de melhoria dos métodos de autenticação é devida à vulnerabilidade dos usuários frente a métodos que utilizam apenas o login/senha. Vários serviços na Internet que necessitam de autenticação obrigam os usuários a criarem novas identidades (um novo par login/senha). Com o tempo, usuários passam a acumular vários pares login/senha, o que se torna difícil de gerenciar. Com isso, os usuários tendem a utilizar a mesma senha muitas vezes, ou até reduzir a complexidade de suas senhas, de modo a torná-las fáceis de lembrar. Porém, isso gera grandes vulnerabilidades e facilita a vida dos atacantes. Até o governo dos Estados Unidos da América reconhece a fragilidade deste modelo nos dias atuais, e começa a exigir a adoção da autenticação de dois fatores para melhorar a segurança dos órgãos do governo e evitar certos ataques [Sternstein 2015].

No ambiente de armazenamento de dados em nuvens, o tipo de autenticação mais

 ©2015 SBC — Soc. Bras. de Computação

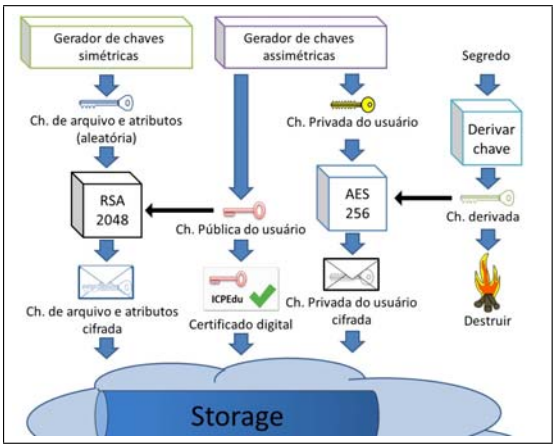

Figure 5. Armazenamento das chaves criptográficas

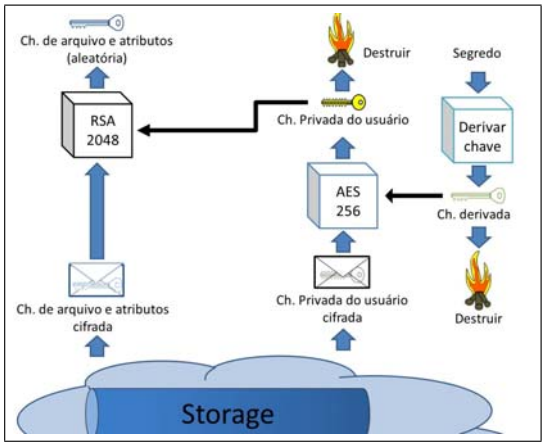

Figure 6. Recuperação das chaves criptográficas

empregado também é por meio de login/senha. Apenas dois CPSs se destacam por utilizar um segundo fator de autenciação em suas soluções: Onedrive [Onedrive] e Google Drive [Drive]. Ambos utilizam os telefones móveis de seus usuários para autenticá-los, porém usam a criptografia apenas no tráfego dos dados pela rede (protocolo TLS [IETF 2008]), e não no armazenamento dos mesmos. Contudo, quando se utiliza a criptografia para proteger os dados, a autenticação do usuário se torna ainda mais relevante, uma vez que vários CSPs usam a senha de seus usuários para derivar uma chave simétrica utilizada para cifrar/decifrar a chave privada dos mesmos. Neste contexto, a credencial se torna um dos pontos mais vulneráveis de todo o sistema. Por esta razão, a autenticação multi-fator pode ser um grande aliado para evitar que atacantes obtenham facilmente os dados dos usuários, adicionando uma camada de proteção extra. Desta forma, é de suma importância que ela seja considerada em um projeto de um sistema que procure proteger a privacidade dos usuários e a segurança de seus dados. Como alternativa a este modelo, um sistema poderia oferecer ao usuário a escolha da utilização ou não do segundo fator de autenticação, uma vez que alguns usuários podem ter limitações quanto aos recursos necessários da autenticação, como por exemplo, a posse de um leitor de cartão em sistemas que requerem *Smart Cards* ou até mesmo a posse de um celular. Mas para oferecer um melhor nível de segurança, tal sistema deveria permitir o uso apenas de login/senha por um período limitado e/ou obrigar uma troca mais frequente de senhas (sem permitir senhas fracas ou o reaproveitamento de senhas antigas).

CPG adota a autenticação multi-fator utilizando algo que o usuário saiba (uma senha) e algo que o usuário possua (um dispositivo móvel). Com isso, quando o usuário escolher utilizar o segundo fator de autenticação (2FA), o sistema irá integrar o processo de autenticação por segredo com o processo de autenticação do segundo fator, sendo o último requisitado após o usuário fornecer o segredo correto. Na ativação do segundo fator para autenticação, é exigido que o usuário passe por uma etapa de cadastramento, onde o mesmo irá seguir um processo simples para configurar o seu dispositivo e sua aplicação. O *Google Authenticator*, que utiliza o protocolo TOTP (*Time-Based One-Time Password Algorithm* [IETF 2011]), foi o escolhido para uma etapa inicial de testes com o CPG, pois, apesar de suas vulnerabilidades [Dmitrienko et al. 2014], é de fácil utilização e acesso por muitos usuários. Na etapa inicial de cadastro, o CPG gera uma sequência

 ©2015 SBC — Soc. Bras. de Computação

de 16 caracteres que deve ser inserida no dispositivo do usuário, que deve ter instalado em seu dispositivo o *Google Authenticator*. Esta inclusão do código pode ser realizada manualmente ou através de um código QR gerado no momento do cadastro. Já no processo de autenticação, a cada 30 segundos, o *Google Authenticator* gerará um código que deve ser inserido no CPG quando solicitado. Se o código inserido for o mesmo que o gerado pela aplicação, o usuário tem acesso ao CPG; caso contrário, o acesso é rejeitado e, após 3 tentativas erradas, é finalizado. Para tentar novamente, o usuário deve iniciar novamente o CPG e proceder com o processo de autenticação desde o início, incluindo fornecer o primeiro fator de autenticação novamente. O processo completo de autenticação utilizando o segundo fator de autenticação está resumido na Fig. 7.

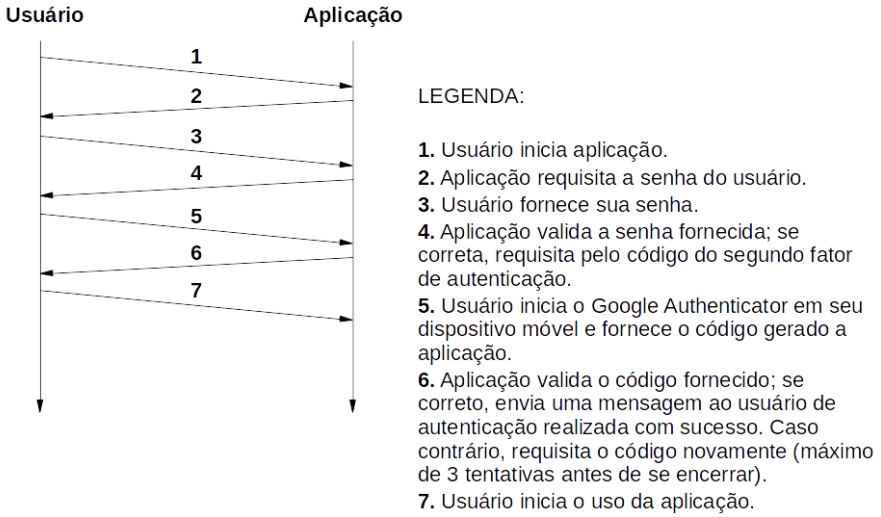

Figure 7. Autenticação 2FA

Da forma como está proposto aqui, o 2FA é requerido todas as vezes que o usuário tenta se autenticar. Entretanto, há situações em que o 2FA pode ser usado apenas para dar acesso a dados mais sensíveis. Há ainda o caso de autenticação contínua, no qual o usuário deve prover credenciais de tempos em tempos para provar que ainda está de posse de todas as credenciais. O uso de formas mais sofisticadas de 2FA será deixado para trabalhos futuros.

6. Conclusões e Trabalhos Futuros

Neste artigo foram apresentados alguns problemas presentes no ambiente de armazenamento de dados em nuvens, assim como uma proposta de uso de criptografia para mitigar tais problemas a fim de preservar a privacidade dos usuários e proteger seus dados enquanto armazenados nas nuvens. A proposta foi concebida considerando-se a questão da usabilidade, de maneira a ser atrativa para o maior número de usuários possível, exigindo o mínimo de esforço em sua utilização. Este fato pode ser observado tanto no uso como na configuração do CPG, os quais são simples e intuitivos, por se basearem em conceitos comuns aos usuários. Basta o usuário depositar um arquivo em uma pasta específica para que o mesmo seja cifrado e enviado para a nuvem. Acreditamos que esta simplicidade, alinhada a boas práticas de segurança, possa fazer com que a privacidade nas nuvens seja algo mais comum e fácil de alcançar.

 ©2015 SBC — Soc. Bras. de Computação

Destacamos também a utilização da autenticação de dois fatores. Como pode ser observado nos vários CSPs disponíveis atualmente, a identidade do usuário é fortemente ligada à proteção de suas chaves criptográficas. Por essa razão, é de suma importância a proteção da senha de autenticação (segredo) dos usuários, uma vez que ela se torna o elo mais fraco de todo um sistema, possibilitando acesso as chaves dos usuários e, consequentemente, a seus dados. É justamente para minimizar este risco, que o CPG adota a autenticação de dois fatores, a fim de dificultar certo tipos de ataques e propiciar mais proteção aos usuários.

Como trabalho futuro, será realizado um estudo sobre a implementação de outros protocolos de autenticação multi-fator a fim de realizar uma comparação entre eles, analisando principalmente fatores relacionados a segurança e usabilidade. Serão também buscadas formas de implementar de maneira mais eficiente e intuitiva a proteção de dados oferecida pela criptografia no lado do cliente.

References

Boxcryptor. Technical overview. https://www.boxcryptor.com/en/technical-overview. Acesso: 10 jul 2015.

Credeon. Cloud data protection. http://psg.hitachi-solutions.com/credeon/cloud-data-protection-overview. Acesso: 10 jul 2015.

CSA (2010). Top threats to cloud computing v1.0. http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf. Acesso: 10 jul 2015.

Cyphertite. Cryptography. https://www.cyphertite.com/papers/WP_Crypto.pdf. Acesso: 10 jul 2015.

D. Harnik, B. P. and Shulman-Peleg, A. (2010). Side channels in cloud services: Deduplication in cloud storage. *Security & Privacy, IEEE*, 8(6):40–47.

Dmitrienko, A., Liebchen, C., Rossow, C., and Sadeghi, A.-R. (2014). Security analysis of mobile two-factor authentication schemes. *Intel® Technology Journal*, 18(4).

Drive. Visao geral das conexoes SSL. https://support.google.com/a/answer/100181?hl=pt-BR. Acesso: 10 jul 2015.

Gasti, P., Ateniese, G., and Blanton, M. (2010). Deniable cloud storage: Sharing files via public-key deniability. In *Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society*, WPES '10, pages 31–42, New York, NY, USA. ACM.

Gellman, B. (2013). Nsa broke privacy rules thousands of times per year, audit finds. https://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html. Acesso: 03 set 2015.

Gellman, B. and Soltani, A. (2013). NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-

 ©2015 SBC — Soc. Bras. de Computação

2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html. Acesso: 03 set 2015.

IETF (2000). Password-Based Cryptography Specification: Version 2.0. https://www.ietf.org/rfc/rfc2898.txt. Acesso: 10 jul 2015.

IETF (2008). The Transport Layer Security (TLS) Protocol: Version 1.2. https://tools.ietf.org/html/rfc5246. Acesso: 03 set 2015.

IETF (2011). TOTP: Time-based One-Time Password algorithm. https://tools.ietf.org/html/rfc6238. Acesso: 02 set 2015.

Kamara, S. and Lauter, K. (2010). Cryptographic cloud storage. In *Proceedings of the 14th International Conference on Financial Cryptograpy and Data Security*, FC'10, pages 136–149. Springer-Verlag, Berlin, Heidelberg.

Kumar, A., Lee, B. G., Lee, H., and Kumari, A. (2012). Secure storage and access of data in cloud computing. In *ICT Convergence (ICTC), 2012 International Conference on*, pages 336–339.

Meisser, L. (2011). Wuala blog. wuala's encryption for dummies. https://www.wuala.com/blog/2011/04/wualas-encryption-for-dummies.html. Acesso: 10 jul 2015.

Murdoch, S. and Danezis, G. (2005). Low-cost traffic analysis of tor. In *Security and Privacy, 2005 IEEE Symposium on*, pages 183–195.

Onedrive. A sua vida em um único lugar. https://onedrive.live.com/about/pt-br/. Acesso: 10 jul 2015.

Phuong, T., Omote, K., Luyen, N., and Thuc, N. (2012). Improvement of multi-user searchable encrypted data scheme. In *Internet Technology And Secured Transactions, 2012 International Conference for*, pages 396–401.

S. Lee, I. Ong, H. L. H. L. (2010). Two factor authentication for cloud computing. *Journal of information and communication convergence engineering*, 8(4):427–432.

Schiessle, B. (2013). Owncloud: Introduction to the new owncloud encryption app. http://blog.schiessle.org/2013/05/28/introduction-to-the-new-owncloud-encryption-app/. Acesso: 10 jul 2015.

SpiderOak (2015). Engineering. the details behind what we do. https://spideroak.com/engineering_matters. Acesso: 10 jul 2015.

Sternstein, A. (2015). White house tells agencies to tighten up cyber defenses 'immediately'. http://www.nextgov.com/cybersecurity/2015/06/white-house-tells-agencies-tighten-online-security-immediately/115216/. Acesso: 10 jul 2015.

Xu, L., Wu, X., and Zhang, X. (2012). Cl-pre: a certificateless proxy re-encryption scheme for secure data sharing with public cloud. In *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*, pages 87–88. ACM.

 ©2015 SBC — Soc. Bras. de Computação