UNIVERSIDADE PAULISTA – UNIP

JEAN CARLOS O. TEIXEIRA

ASPECTOS DE SEGURANÇA EM *CLOUD COMPUTING*

LIMEIRA

2014

JEAN CARLOS O. TEIXEIRA

ASPECTOS DE SEGURANÇA EM

CLOUD COMPUTING

Trabalho de Conclusão de Curso para obtenção do título de Bacharel em Ciência da Computação pela Universidade Paulista.

Professores e orientadores: Marcos Gialdi, Mateus Locci e Cassiano M. Lopes

Limeira

2014

FOLHA DE APROVAÇÃO

JEAN CARLOS O. TEIXEIRA

ASPECTOS DE SEGURANÇA EM
CLOUD COMPUTING

Trabalho de Conclusão de Curso apresentado como requisito para obtenção do titulo de Bacharel no curso de Ciência da Computação da Universidade Paulista – Unip/Campus Limeira.

Aprovado em ____ de _____ de _____.

Componentes da banca examinadora:

_____
Prof. Marcos Vinícius Gialdi

Universidade Paulista – UNIP

Campus Limeira

_____
Prof. Amaury André

_____
Prof[a] Sandra Crippa

Limeira
2014

Dedico todo este trabalho,
principalmente a minha mãe,
a toda minha família e amigos.

AGRADECIMENTOS

Meu sincero e carinhoso obrigado a minha mãe, pelo apoio em diversas fases da minha vida e por sempre ter se esforçado para me ensinar caráter, respeito, educação e força de vontade.

Agradeço a todos os professores e orientadores envolvidos neste trabalho, pela sugestão do tema e pelas intervenções sempre precisas e didáticas ao longo dos meses de estudo.

Meu agradecimento, ainda, aos demais professores, cujos ensinamentos em muito contribuíram para que mais esta etapa fosse cumprida.

1 LISTA DE SIGLAS E ABREVIATURAS

E2EE - End-to-end *encryption*

RSA - é um algoritmo de criptografia de dados, que deve o seu nome a três professores do Instituto de Tecnologia de Massachusetts (MIT),

RonaldRivest, Adi Shamir e Leonard Adleman fundadores da atual empresa RSA Data Security, Inc., que inventaram este algoritmo.

DMZ - Demilitarized Zone (Zona desmilitarizada).

2 RESUMO

Cloud Computing chegou ao conhecimento de muitas pessoas recentemente, mas tudo indica que ouviremos este termo ainda por um bom tempo. Também conhecida no Brasil como computação nas nuvens ou computação em nuvem, Cloud Computing se refere, essencialmente à ideia de utilizarmos em qualquer lugar e independente de plataforma, as mais variadas aplicações por meio da internet.

Este modelo traz inúmeros benefícios como redução de custos, escalabilidade, sustentabilidade, portabilidade, flexibilidade, porém seu grande problema esta relacionado com a segurança da informação. Questões como localização, segregação e recuperação dos dados, direito sobre a informação, jurisdição, segurança na transmissão dos dados influenciam na adoção deste modelo.

Neste trabalho, serão abordados aspectos de segurança como: técnicas de criptografia na transmissão da informação, aspectos jurídicos, crimes eletrônicos, perícia digital forense e marco civil.

Palavras-chave: Criptografia, *Tokenization*, Crimes Digitais, Legislação Brasileira aplicada ao processo de pericia digital Forense, Pericia Digital, Marco Civil.

ABSTRACT

Many people knew Cloud Computing recently, and we will listen about it frequently from now on. Cloud computing refers essentially to the idea of using platform-independent and several applications through the internet.

This model brings many benefits such as lower costs, scalability, sustainability, portability, flexibility, however its big problem is information security. Issues such as data location, data segregation, data recovery, information about law, jurisdiction and data transmission security impact this model adoption.

This work mentions security aspects as encryption techniques for information transmission, legal issues, electronic crimes, digital forensic expertise and civil March.

Keywords: Encryption, Tokenization, Digital Crimes, Brazilian legislation applied to the digital process expertise Forensic, Digital Skill, Marco Civil.

SUMÁRIO

3 INTRODUÇÃO

A computação em nuvens é uma tecnologia amplamente utilizada atualmente, seja em empresas ou em nosso dia-a-dia, oferecendo grande flexibilidade e capacidade computacional.

Apesar dos benefícios desta tecnologia, é crescente a preocupação com a segurança de aplicações e informações nestes ambientes, o que faz com que as questões relativas à segurança sejam o principal obstáculo para adoção da computação em nuvens.

Diante deste cenário, este trabalho apresenta diversas questões relacionadas à segurança como: Criptografia, *Tokenization*, Crimes Digitais, Legislação Brasileira aplicada ao processo de perícia digital Forense, Perícia Digital, Marco Civil.

4 DESENVOLVIMENTO

4.1 Cloud Computing

Cloud Computing[1] ou computação nas nuvens – tradução literal para o português é um novo paradigma da informática que, conforme alguns especialistas pode representar o fim dos computadores pessoais, tornando-os autênticos terminais burros, com os dados e o processamento na nuvem. Google, Microsoft, Yahoo já oferecem serviços com base neste conceito. Mas afinal, o que é *Cloud Computing*?

Segundo definição encontrada em (Ramos/2010), *Cloud Computing* é:

> [...] um modelo que possibilita acesso de modo conveniente e sob demanda, a um conjunto de recursos computacionais configuráveis como redes, servidores, armazenamento, aplicação e serviços que podem ser rapidamente adquiridos e liberados com mínimo esforço gerencial ou interação com o provedor de serviços.

Em resumo, *Cloud Computing* pode ser entendido como um conceito em acesso a serviços, estruturas e ferramentas hoje presentes nos computadores pessoais ou locais através da Internet.

O modelo de computação em nuvem é composto, por cinco características essenciais, três modelos de serviços e quatro modelos de implantação da nuvem conforme citado no Art. de (Verdi, Fábio Luciano. 2010) seguem descrições:

4.2 Características Essenciais

−Serviço sob demanda: as funcionalidades computacionais são providas automaticamente sem a interação humana como o provedor do serviço;

−Amplo acesso aos serviços: os recursos computacionais estão disponíveis através da Internet e são acessados via mecanismos padronizados, para que possam ser utilizados por dispositivos móveis e computadores.

---

[1] Neste trabalho, tanto o termo em inglês quanto o termo em português serão utilizados sem distinção.

–Resource Pooling[2]: os recursos computacionais, físicos ou virtuais do provedor são utilizados para servir a múltiplos usuários, sendo alocados e realocados dinamicamente conforme a demando do usuário. Neste cenário, o usuário do serviço não tem a noção da localização exata do recurso, mas deve ser capaz de definir a localização em um nível mais alto como país, estado ou região.

–Elasticidade: as funcionalidades computacionais devem ser rápidas e elasticamente providas a partir da demanda do serviço. O usuário possui recursos ilimitados, que podem ser adquiridos a qualquer momento.

–Medição dos serviços: os sistemas de gerenciamento utilizados para computação em nuvem monitoram automaticamente os recursos para armazenamento, processamento e largura de banda. O serviço deve ser transparente para o provedor e para o usuário.

4.3 Modelos de Serviços

Fonte: Blogbrasil[3]

–Software como um serviço (Software as a Service – SaaS): aplicações de interesse para uma grande quantidade de usuários passam a ser hospedadas na

[2] O termo *resource pooling* é utilizado para definir um conjunto de recursos que se comportam como se fossem um único recurso. O objetivo desta técnica é aumentar a confiabilidade, flexibilidade e eficiência do sistema como um todo.
[3] Disponível em: http://blogbrasil.comstor.com/blog/bid/294730/O-que-%C3%A9-SaaS-PaaS-e-IaaS. Acesso em: 24 Nov. 2014

nuvem como uma alternativa ao processamento local. As aplicações são fornecidas como serviço pelos provedores e acessadas pelos clientes através de aplicações como o browser. O armazenamento é feito pelo provedor de serviço. Google Apps é um exemplo de SaaS. Conforme (Verdi, Rothenberg, Pasquini, & Magalhães, 2010) conclui-se que ao usar o Google Apps, as empresas podem economizar de 50% a 70% em comparação com outras soluções de e-mail.

−Plataforma como um Serviço (Plataform as a Service – PaaS): é a capacidade oferecida pelo provedor para o usuário desenvolver aplicações que serão executadas e disponibilizadas em nuvem. Neste sentido, surge outro conceito conhecido como *utility computing*, utilizado para denominar toda a plataforma de suporte ao desenvolvimento e fornecimento de aplicações em nuvem. Toda aplicação requer um modelo de computação, um modelo de armazenamento e um modelo de comunicação. As plataformas para desenvolvedores de aplicações em nuvem fornecem tais modelos e permitem utilizar conceitos implícitos tais como virtualização e compartilhamento de recursos.

−Infraestrutura como um Serviço (*Infraestructure as a Service – IaaS)*: é a capacidade que o provedor tem de oferecer uma infraestrutura de processamento e armazenamento de forma transparente. Neste cenário, o usuário não tem o controle da infraestrutura física, mas, através de mecanismos de virtualização, possui controle sobre os sistemas operacionais, armazenamento, aplicações instaladas e, possivelmente, um controle limitado dos recursos de rede. Um exemplo de *Utility Computing* disponibiliza como uma IaaS é a Amazon EC2.

4.4 Modelos de implantação

−Nuvem Privada (*Private Cloud*): compreende uma infraestrutura de nuvem operada unicamente por uma organização. Os serviços são oferecidos para serem utilizados internamente pela própria organização, não estando disponíveis publicamente.

−Nuvem Comunidade (*Community Cloud*): fornece uma infraestrutura compartilhada por uma comunidade de organizações com interesses em comum.

–Nuvem Pública (*Public Cloud*): a nuvem é disponibilizada publicamente através do modelo *pay-per-use*[4]*.* Tipicamente, são oferecidas por companhias que possuem grandes capacidades de armazenamento e processamento;

–Nuvem Hibrida (*Hybrid Cloud*): a infraestrutura é uma composição de duas ou mais nuvens privadas, comunitárias ou públicas que continuam a ser entidades únicas, porém, conectadas através de tecnologia proprietária ou padronizadas.

Ao analisarmos as definições expostas acima, é possível destacar três novos aspectos em relação ao *hardware*[5], introduzidos em *Cloud Computing*. São eles:

–A ilusão de recurso computacional infinito disponível sob demanda;

–A eliminação de um comprometimento antecipado por parte do usuário;

–A capacidade de alocar e pagar por recursos usando uma granularidade de horas.

Esta elasticidade para obtenção e liberação de recursos é um dos aspectos chaves da computação em nuvem, sendo uma das principais diferenças quando comparada com computação em grade.

[4] *Pagar pela quantidade que usar.*

[5] É a parte física de um computador, é formado pelos componentes eletrônicos, como por exemplo, circuitos de fios e luz, placas, utensílios, correntes, e qualquer outro material em estado físico, que seja necessário para fazer com o que computador funcione.

5 GRADES E COMPUTAÇÃO EM NUVEM

Muitas das características encontradas em grades computacionais são encontradas na computação em nuvem. Isto ocorre porque ambos os modelos possuem objetivos comuns tais como redução dos custos computacionais, compartilhamento de recursos e aumento de flexibilidade e confiabilidade. Entretanto, existem algumas diferenças que precisam ser enfatizadas.

Estas semelhanças e diferenças têm causado confusões e sobreposição de características e funcionalidades. No trabalho de (Verdi, Rothenberg, Pasquini, & Magalhães, 2010) foi realizado um estudo das diferentes características associadas à computação em nuvem que as compara às características de grades computacionais.

Algumas comparações importantes:

−Modelo de pagamento e origens: as grades computacionais surgiram através de financiamento público, na maioria das vezes patrocinadas por projetos dentro de universidades. O modelo *Cloud Computing* é motivado por aspectos comerciais onde grandes empresas criam estratégias de mercado com interesses nos lucros. Tipicamente, os serviços em grade são vendidos à taxa fixa por serviço, enquanto que os usuários dos serviços oferecidos nas *clouds* são cobrados pelo modelo *pay-per-use.*

Muitas aplicações não usam a mesma capacidade computacional de armazenamento e recursos de rede. O modelo de cobrança deve considerar o pagamento separado para cada tipo de recurso utilizado;

−Compartilhamento de recursos: as grades computacionais compartilham os recursos entre as organizações usuárias através do modelo adequado. Esta noção de recurso dedicado é possível através do uso de virtualização, aspecto ainda pouco explorado pelas grades;

Virtualização: as grades computacionais usam interfaces para esconder a heterogeneidade dos recursos computacionais. A virtualização utilizada em *Cloud Computing* ocorre de forma plena, possibilitando que usuários instalem máquinas virtuais e sistemas operacionais específicos nas mesmas. A migração e mobilidade de máquinas virtuais também é um aspecto comum dentro da nuvem e permite a otimização do uso de recursos de energia e resfriamento;

−Escalabilidade e gerenciamento: a escalabilidade em grades ocorre através do aumento no número de pontos de processamento. A escalabilidade em *Cloud*

Computing ocorre através de um redimensionamento do hardware virtualizado[6]. O gerenciamento das grades computacionais é difundido, pois não há uma única entidade proprietária de todos os sistemas. Por outro lado, as c*louds* encontradas atualmente são controladas por uma única entidade administrativa, muito embora exista uma tendência em se criar federações de nuvens;

Padronização: a maturidade das grades computacionais fez com que vários fóruns fossem criados para definição de padronização. Esforços para padronização de interfaces para os usuários assim como padronização de interfaces internas alavancaram a interoperabilidade de grades computacionais. Em *Cloud Computing*, as interfaces de acesso aos serviços são muito parecidas com as interfaces das grades, as interfaces internas são proprietárias e dificultam a criação de federações de nuvens. Atualmente existem várias iniciativas para definição de padrões para computação em nuvem conforme (Verdi, Rothenberg, Pasquini, & Magalhães, 2010), um dos desafios principais é a padronização do formato das imagens virtuais e APIS de migração.

Em termos gerais, grade computacional se refere ao processamento distribuído e paralelo, ou seja, quebrar uma tarefa em várias, distribuir em nós para processamento e então unir as partes para obter o resultado final. Na maioria das vezes, isto significa executar a mesma tarefa em diferentes conjuntos de dados para agilizar o resultado. Para isso, distribui-se a atividade no número máximo de unidades de processamento possível, enquanto que em *Cloud Computing*, obtém-se a quantidade de recursos suficientemente necessária para realização da tarefa computacional em determinado tempo.

[6] É o nome dado a uma máquina, implementada através de *software*, que executa programas como um computador real, também chamado de processo de virtualização

6 SEGURANÇA EM NUVEM, ASPECTOS JURÍDICOS.

A maior preocupação dos executivos atualmente refere-se à transferência do gerenciamento de atividades críticas a terceiros, que podem colocar em risco o controle dos processos e informações considerados competitivos para o negócio, bem como os contratos de *outsourcing*[7] que necessitam estabelecer um forte alinhamento de todo o cenário em questão, como também um compromisso explícito de colaboração entre cliente e provedor.

Em *Cloud Computing* o risco relativo à segurança da informação tornou-se uma das principais preocupações entre os gestores. O ritmo de sua disseminação está diretamente relacionado à confiabilidade do modelo. A incerteza se torna obstáculo uma vez que a tomada de decisão pode colocar em risco os ativos da organização.

Os aspectos jurídicos caminham a passos lentos e a ausência de uma legislação específica surge a partir do desenvolvimento da tecnologia, onde o Direito não acompanha algumas questões.

A dificuldade desse enfrentamento reside na variedade dos serviços ofertados. Os controles de segurança vão se perdendo lentamente, uma vez que, as responsabilidades dos mesmos podem ser repassadas a terceiros.

Nessa perspectiva, como visto por (Santos & Machado, 2010) surge o maior paradigma da *Cloud Computing*: Manter a segurança dos dados desses clientes. Em razão a ausência de leis que criminalizem ilícitos virtuais, surge a dificuldade em se punir os autores de atos praticados através da internet.

No Brasil, leva-se em consideração que a internet é só o meio utilizado para as práticas dos crimes e assim sendo, as diretrizes do direito penal são igualmente aplicáveis, bastando apenas adequá-las e modernizá-las pelos órgãos oficiais.

Por outro lado, é um caso atípico por não serem caracterizados todos os elementos inerentes aos crimes de danos, previstos no Código Penal.

No Brasil, temos alguns artigos no Código Penal que ditam como as perícias devem ser realizadas, entre eles, o Art. 158. Por não termos uma regulamentação ou padronização em *Cloud Computing*, não são previstas garantias dos dados para a realização de uma perícia que permita colher informações para exames como os

[7] É uma expressão em inglês normalmente traduzido para português como terceirização.

de corpo de delito, por exemplo. Mas, conforme o Art. 167: "[...] *não sendo possível o exame de corpo de delito a prova testemunhal poderá supri-lhe a falta".* Em meios digitais se torna complicado devido à necessidade de conhecimentos técnicos para narrar os fatos e a volatilidade das informações, essa que em *Cloud Computing* é bem maior do que nos modelos tradicionais.

No cenário atual, métodos e técnicas tradicionais da perícia forense podem se mostrar pouco eficientes. Assim,

> *Serviços de Cloud são especialmente difíceis de investigar, porque os logs e dados de vários clientes podem estar localizados conjuntamente e também estar distribuídos com uma constante mudança no conjunto de máquinas e data centers. (HEISER, 2009).*

Conforme art. 169 [...] "*para o efeito de exame do local onde houver sido praticada a infração, a autoridade providenciará imediatamente para que não se altere o estado das coisas até a chegada dos peritos*" [...]. Porém, em *Cloud Computing*, essa preservação não é garantida, pois o ambiente em nuvem será utilizado por várias pessoas e dependendo do crime, nem sempre saberemos o momento exato que ele foi cometido.

Para que uma perícia seja bem sucedida, é necessário que existam registros de auditoria, ou logs, íntegros e confiáveis. Não importa quão segura é a rede a ser auditada, nunca será possível confiar num registro que tenha sido comprometido ou avariado. Assim, a maneira como os logs são armazenados torna-se um fator de extrema relevância e os mesmo necessitam conter informações suficientes para identificação do usuário, endereço de IP[8], *login* e a data e o horário dos acessos.

Alguns prestadores de *Cloud Computing* não vêem razões para armazenar seus logs fora da nuvem, mas os riscos devem ser em considerados. A paralisação no serviço, com os logs armazenados em nuvem, impede que a empresa os acesse. Numa invasão, dependendo do nível de controle que o invasor tiver sobre os dados,

[8] É uma identificação de um dispositivo (computador, impressora, etc) em uma rede local ou pública. Cada computador na internet possui um IP (Internet Protocol ou Protocolo de internet) único, que é o meio em que as máquinas usam para se comunicarem na Internet.

poderá facilmente apagar os logs, eliminar possíveis provas e encobrir seus rastros; e a chance de descobrir qual foi à vulnerabilidade que possibilitou a invasão ou ataque é mínima.

7 CRIMES ELETRÔNICOS

A preocupação com os crimes eletrônicos não está relacionada apenas a nuvem e aos profissionais de Tecnologia da Informação (T.I.) e sim estendida a todas as arquiteturas, mecanismos, usuários e profissionais envolvidos com o universo digital. Esta nova modalidade de crime faz-se do uso dos meios computacionais como meio ou fim para as práticas de atividades ilícitas e já no ano de 2006, segundo pesquisa conduzida pela IBM, 100% dos usuários temiam mais o crimes cibernéticos do que os delitos físicos conforme visto em (Ramos & Eses, 2013). Neste mesmo material é visto também que a receita dos crimes cibernéticos é mais lucrativa do que a do narcotráfico[9] e indica que a incidência deste tipo de crime tende a aumentar.

Este aumento no número de ocorrências está provocando no Brasil, um impacto, não apenas em relação à discussão quanto à criação ou não de novas leis para tipificação dos crimes eletrônicos, mas, principalmente, no que se refere à perícia forense. Abaixo, uma lista de alguns crimes recentes relacionados à Cloud.

7.1 Apple, iCloud

O caso das fotos íntimas vazadas das celebridades continua gerando grande especulação sobre como os criminosos tiveram acesso aos arquivos pessoais. Enquanto alguns especialistas sugerem uma brecha de segurança que permitiu a invasão do iCloud, outros afirmam que ocorreu um ataque do tipo phishing[10], em que os usuários recebem mensagens falsas que solicitam seus dados de acesso e senha a um determinado serviço de Internet - neste caso, a nuvem do iPhone e Mac, o iCloud.

---

[9] Narcotráfico ou tráfico de drogas é o tráfico de substâncias ilícitas, entorpecentes.

[10] Termo oriundo do inglês (fishing) que quer dizer pesca, é uma forma de fraude eletrônica, caracterizada por tentativas de adquirir dados pessoais de diversos tipos; senhas, dados financeiros como número de cartões de crédito e outros dados pessoais. O ato consiste em um fraudador se fazer passar por uma pessoa ou empresa confiável enviando uma comunicação eletrônica oficial. Isto ocorre de várias maneiras, principalmente por email, mensagem instantânea, SMS, dentre outros. Como o nome propõe (Phishing), é uma tentativa de um fraudador tentar "pescar" informações pessoais de usuários desavisados ou inexperientes.

Segundo a Symantec, empresa fabricante do Norton Antivírus, as evidências apontam que as celebridades sofreram ataques do tipo phinshing ou SMSishing[11]. Sendo assim, a estratégia dos criminosos pode ter sido enviar e-mails ou mensagens de texto se passando por funcionários do setor de suporte da Apple. Nestes casos, as mensagens exigem as credenciais de acesso do usuário, do contrário a conta será bloqueada por algum motivo pelo suporte técnico.

A tese da Symantec também é reforçada pela Trend Micro. Segundo o presidente da companhia de segurança digital, Rik Ferguson, empresas grandes como a Apple mantêm equipes de segurança que trabalham intensamente para evitar brechas em seus serviços que exponham os usuários. Ele acredita que a causa provável para grandes vazamentos das fotos como este são ataques do tipo phishing.

7.2 Falha de segurança do serviço da Apple

Segundo a Via Forensics, uma empresa especializada em segurança em dispositivos móveis, a vulnerabilidade no iCloud seria um problema antigo, e que já estava sendo estudada pelo grupo. A ideia também é aceita pelo fundador do site HackApp, Alexey Troshichev, que direciona a responsabilidade do vazamento para o descuido da Apple que pode ter exposto milhares de usuários do serviço.

Porém, caso a brecha de segurança seja confirmada, o script o iBrute poderá ser apontado como a principal ferramenta utilizada pelos criminosos no roubo das fotos íntimas. O código malicioso, que utiliza a tática de força bruta para adivinhar as senhas, precisa que o atacante possua o e-mail utilizado pela vítima para acessar determinados serviços como o iCloud e o Find my iPhone.

7.3 Vazamento de senhas do DropBox

Centenas de nomes de usuário e senhas usados para acessar o Dropbox vazaram, e a pessoa responsável pela ação afirma ter informações de cerca de sete milhões de pessoas para divulgar.

---

[11] Semelhante ao phishing, SMSishing (ou phishing SMS) é quando um ladrão de identidade potencial envia-lhe uma mensagem de texto pedindo informações pessoais ou conta. Porque o texto parece ser de um contato respeitável, muitas pessoas respondem, e aí começa o roubo.

Os dados foram postados no Reddit e alguns usuários confirmaram a veracidade deles. Quem criou um dos posts informou que, caso lhe dêem pagamentos em bitcoin, ele fará divulgações de mais lotes.

Em nota enviada ao The Next Web, o Dropbox confirmou que houve o vazamento, mas garantiu que não foi culpa sua. Os nomes dos usuários e suas respectivas senhas infelizmente foram roubados de outros serviços.

Segundo a empresa, antes mesmo que o problema viesse à tona a maioria dos usuários afetados teve de mudar as senhas. Sabendo disso, os demais também alteraram. Sempre que o Dropbox detecta alguma atividade suspeita, realiza procedimentos de redefinição de senha.

7.4 Vazamento de cinco milhões de contas do Gmail

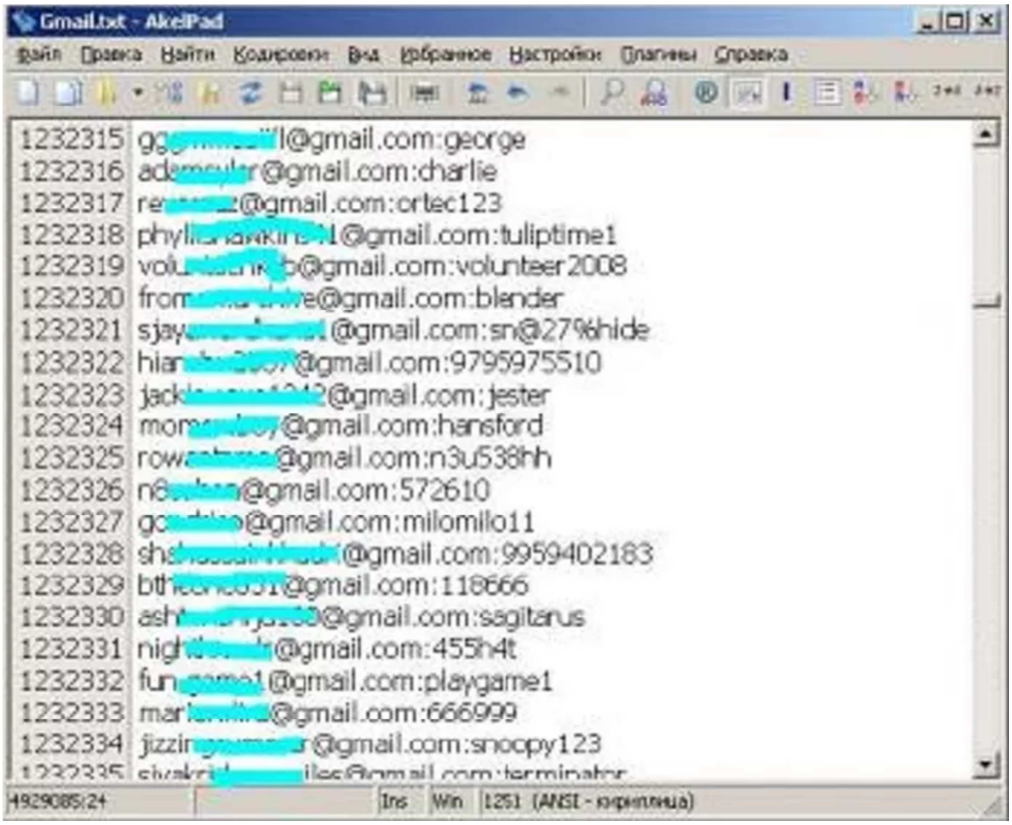
Cerca de cinco milhões de nomes de usuários do Gmail foram publicados em um fórum russo de Bitcoin. De acordo com o Google, a maioria das informações está ultrapassada, uma vez que muitas destas contas já foram suspensas há anos e algumas senhas vazadas são muito antigas. A gigante disse ainda que o vazamento não é resultado de nenhum tipo de falha de segurança:

> A segurança das informações de nossos usuários é uma prioridade para nós. Não temos nenhuma evidência de que os nossos sistemas tenham sido comprometidos, mas sempre que tomamos consciência de que contas podem ter sido violadas, tomamos medidas para ajudar esses usuários a se protegerem.

Pouco tempo depois que as informações foram expostas, administradores do fórum apagaram as senhas do arquivo postado, deixando apenas os logins.

Além disso, tvskit – nome de usuário do autor do post – afirmou que 60% dos dados capturados eram válidos. O arquivo inclui, principalmente, contas americanas, espanholas e russas.

O fórum Bitcoin russo tem sido palco de vários grandes vazamentos ao longo dos últimos dias. Só nesta semana, 4.660.000 contas Mail.ru foram expostas. Nomes de usuários e senhas de 1,26 milhões de outras contas Yandex também foram publicados em um arquivo de texto.



FONTE: TECHTUDO[12]

[12] Disponível em: http://www.techtudo.com.br/noticias/noticia/2014/09/lista-vaza-senhas-de-5-milhoes-de-contas-gmails-mas-google-nega-invasao.html. Acesso em: 12 Nov. 2014

8 CLOUD COMPUTING E A PERÍCIA FORENSE DIGITAL

A ausência atual de normas formais previstas contratualmente na oferta de serviços de *Cloud Computing* cria um ambiente de apreensão não só para profissionais da perícia forense, mas em todos envolvidos na busca da verdade processual. Para reforçar ainda mais este clima de apreensão e dúvidas Jeff Barr, em outubro de 2008, foi incapaz de responder a perguntas sobre quais cuidados os vendedores estão tendo para permitir que futuras investigações forenses no ambiente de *Cloud Computing* procedam de forma eficaz. Conforme visto em (Ramos & Eses, 2013) esta falta de aspectos formais na oferta deste tipo de serviço é apenas um dos desafios atuais, neste novo cenário, para a perícia digital.

Atualmente, software e também a infraestrutura estão localizados na nuvem em servidores que são propriedades de terceiros e não mais de forma local. Desta forma, o perito poderá não ter mais, em muitas ocasiões, o acesso ao disco rígido, infraestrutura e o controle sobre a rede do ambiente a ser investigado, o que hoje são requisitos fundamentais em muitas das perícias a serem realizadas para obter-se um laudo pericial completo e fundamentado.

8.1 Legislação Brasileira aplicada ao processo de perícia forense

No Brasil temos, tanto no código penal como no civil, alguns artigos que ditam como as perícias devem ser realizadas. A seguir, alguns dos artigos do decreto de lei 3689/41, do Código de Processo Penal, que determinam o processo de perícia e os problemas relacionados aos novos desafios traduzidos pelo *Cloud Computing*.

Do Capitulo II - Do Exame de Corpo de Delito e das Perícias em Geral

Art. 158. Quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado.

Art. 167. Não sendo possível o exame de corpo de delito, por haverem desaparecido os vestígios, a prova testemunhal poderá suprir-lhe a falta.

Há necessidade de realização da perícia quando existe a ocorrência de um crime, mesmo com o conhecimento da autoria e se, ao comprovar o desaparecimento dos vestígios, terem-se o testemunho como seu substituto.

Não há formalização quanto às normas contratuais na oferta de serviços de *Cloud Computing*, desta forma não estão previstas atualmente ferramentas e a garantia de que os dados ainda estarão disponíveis para a realização da perícia o

que pode impossibilitar o exame de corpo de delito. Para apoiar esta preocupação segundo a consultoria Gartner (Ramos & Eses, 2013):

> Serviços de Cloud são especialmente difíceis de investigar, porque os logs[13] e dados de vários clientes podem estar localizados conjuntamente e também estar distribuídos com uma constante mudança no conjunto de máquinas e data centers. Se não houver um compromisso contratual para apoiar formas específicas de investigação – juntamente com evidencias de que o vendedor já tenha apoiado com sucesso tais atividades, a única suposição segura é de que os pedidos de investigação e descoberta serão impossíveis.

Na possibilidade do exame de corpo de delito a prova testemunhal poderá supri-lo falta. Porém é muito complicado em meios digitais, devido à volatilidade das informações e a necessidade muitas vezes do conhecimento técnico para a narrativa dos fatos. Raramente serão questionadas quanto a sua veracidade.

Art. 159. Parágrafo Sexto. Havendo requerimento das partes, o material probatório que serviu de base à perícia será disponibilizado no ambiente do órgão oficial, que manterá sempre sua guarda, e na presença de perito oficial, para exame pelos assistentes, salvo se for impossível a sua conservação, Incluído pela Lei nº 11.690, de 2008.

Art. 169. Para o efeito de exame do local onde foi praticada a infração, a autoridade providenciará imediatamente para que não se altere o estado das coisas até a chegada dos peritos, que poderão instruir laudos com fotografia, desenhos ou esquemas elucidativos.

Art.169. Paragrafo único. Os peritos registrarão, no laudo, as alterações do estado das coisas e discutirão, no relatório, as consequências dessas alterações na dinâmica dos fatos. (Incluído pela Lei nº 8.862, de 28.3.194).

Resumindo o que está descrito nos artigos citados acima, o material fruto da investigação deve ser preservado. Uma boa prática para isso é, conforme visto a

[13] É uma expressão utilizada para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para restabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais.

cadeia de custodia, porém o *Cloud Computing* também traz problemas à preservação deste material, como o que segue:

Como esta nova tendência, o material probatório estará armazenado em servidores de terceiros. A cadeia de custódia do material em nuvem será feita, basicamente, a através da verificação de cada passo da investigação a integridade do material através do [14]hash, porém, quando este estiver armazenado em rede, muitas vezes não haverá a capacidade de acesso, seja de forma lógica ou mesma física, que poderá impossibilitar desta maneira uma cadeia de custodia adequada.

Cloud Computing é uma nova tendência tecnológica, assim como telefones celulares, rede sem fio e novos tipos de criptografia, a computação em nuvens está trazendo mais complexidade e novos desafios que exigirão uma adaptação e também a evolução tanto para o processo de perícia digital como também tudo envolvido a ele.

No Brasil, esta evolução justifica-se pela análise dos artigos da lei 3689/41 do nosso código penal:

Título VII – da Prova Capítulo I – Disposições Gerais.

Art. 157. São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais (Redação dada pele Lei nº 11.690, de 2008).

Parágrafo Primeiro. São também inadmissíveis as provas derivadas das ilícitas, salvo quando não evidenciado o nexo da causalidade entre umas e outras, ou quando as derivadas puderem ser obtidas por uma fonte independente das primeiras. (Incluído pela Lei nº 11.690, de 2008).

Do Capitulo II – Do Exame do Corpo de Delito e das Perícias em Geral

Art. 181. No caso de inobservância de formalidade ou no caso de omissões, obscuridades ou contradições, a autoridade policial ou judiciária manterá suprir a formalidade ou completar ou esclarecer o laudo.

Parágrafo único. A autoridade poderá também ordenar que se proceda a novo exame, por outros peritos, se julgar conveniente. Art. 182. O juiz não ficará adstrito ao laudo, podendo aceita-lo ou rejeitá-lo, no todo ou em parte.

---

[14] Uma função hash é um algoritmo que mapeia dados de comprimento variável para dados de comprimento fixo. Os valores retornados por uma função hash são chamados valores hash, códigos hash, somas hash (hash sums), checksums ou simplesmente hashes.

Analisando estes artigos comprova-se a preocupação com a preservação, e a adoção de procedimentos adequados na produção da prova pericial de forma que a mesma não seja questionada, considerada como ilícita ou mesmo rejeitada pelo juiz.

A formalização dos procedimentos, pelo menos os globais, que são utilizados na produção da prova pericial digital e também, principalmente, dos que se referem à garantia da cadeia de custódia levando-se em conta as mudanças trazidas pelo *Cloud Computing*.

Um tratado internacional de colaboração em investigação de crimes digitais assinado, de preferencia, pela maior parte dos países. Com isto, poderão ser evitados problemas legais nos casos em que a investigação possa ferir a jurisdição de um país onde está localizada fisicamente a nuvem bem como facilitar a captura e preservação das evidências.

E uma presença cada vez maior de iniciativa como o da ENISA e outros órgãos para promover, entre outras coisas, a formalização das normas contratuais na oferta destes tipos de serviço garantindo a preservação e acesso adequado às evidências, de forma a não violar a privacidade de outros usuários da nuvem.

9 MARCO CIVIL E A COMPUTAÇÃO EM NUVEM

O projeto de lei 21626/11, conhecido popularmente como o Marco Civil, é uma constituição que rege o uso da rede no Brasil definindo direitos e deveres de usuários e provedores da web no país. No dia 25 de março de 2014, após quase três anos de tramitação na Câmara, o plenário da Casa aprovou o projeto. Segue os principais pontos do Marco Civil:

–Neutralidade na rede: O principio da neutralidade diz que a rede deve ser igual para todos, sem diferença quanto ao tipo de uso. Assim, ao comprar um plano de internet, o usuário paga somente pela velocidade contratada. Ou seja: o usuário poderá acessar o que quiser independente do tipo de conteúdo. Paga, de acordo, com o volume e velocidade contratados. Em acordo com a oposição ao governo, o texto na Câmara aprovado e confirmado no Senado, prevê que a neutralidade será regulamentada por meio de decreto após consulta a Agência Nacional de Telecomunicações e ao Conselho Gestor da Internet (CGI).

–Privacidade na web: Além de criar um ponto de referência sobre a web no Brasil, o Marco prevê a inviolabilidade e sigilo de suas comunicações. O projeto de lei regula o monitoramento, filtro, análise e fiscalização de conteúdo para garantir o direito à privacidade. Somente por meio de ordens judiciais para fins de investigação criminal será possível ter acesso a esses conteúdos.

Outro ponto da proposta garante o direito dos usuários à privacidade, especialmente à inviolabilidade e ao sigilo das comunicações pela internet. O texto determina que as empresas desenvolvam mecanismos para garantir, por exemplo, que os e-mails só serão lidos pelos emissores e pelos destinatários da mensagem. O projeto assegura proteção a dados pessoais e registros de conexão e coloca na ilegalidade a cooperação das empresas de internet com órgãos de informação estrangeiros. As empresas que descumprirem as regras poderão ser penalizadas com advertência, multa, suspensão e até proibição definitiva de suas atividades. E ainda existe a possibilidade de penalidades administrativas, civis e criminais.

–Logs ou registros de acesso: Segundo o Marco Civil, os provedores de conexão são proibidos de guardar os registros de acesso a aplicações de internet. Ou seja, o seu rastro digital em sites, blogs, fóruns e redes sociais não ficará armazenado pela empresa que fornece acesso. Mas, pelo Art. 15 do PL, toda empresa constituída juridicamente no Brasil (classificada como provedora de aplicação) deverá manter o registro desse traço por seis meses. Elas também

poderão usá-los durante esse período nos casos em que usuário permitir previamente. Mesmo assim, são proibidas de guardar dados excessivos que não sejam necessários à finalidade do combinado com o usuário.

–Data centers fora do Brasil: O relator do projeto retirou do texto a exigência de data centers no Brasil para armazenamento com grande capacidade de armazenamento e processamento de dados onde ficam, normalmente, os arquivos dos sites, e-mails e os logs de acesso. Com as denúncias de espionagem eletrônica feita pelos Estados Unidos, o governo brasileiro tinha proposto o armazenamento de dados somente em máquina dentro do território brasileiro, mas essa obrigação saiu do texto aprovado.

9.1 Alicerces do Marco Civil e da Computação em Nuvem

Como fica a computação em nuvem? Se o Marco Civil tem o seu alicerce no tripé a neutralidade, privacidade e liberdade de expressão pode-se dizer que a tríplice da computação em nuvem seria: Acesso via internet, arquitetura e elasticidade. No entanto, o Marco Civil, pela aprovação dos termos da neutralidade de rede, impede diferenciação na qualidade/velocidade do acesso em função do tipo de tráfego gerado, ou da aplicação acessada.

9.2 Temas Controversos e Vantagens aos Clientes

A guarda dos dados em datacenters brasileiros tema tão debatido, acabou sendo retirado do documento, transformando-se em uma diretriz para atuação da União, dos Estados, do Distrito Federal e dos Municípios, conforme (Cascão, 2014) na forma de um "[...] estimulo à implantação de centros de armazenamento, gerenciamento e disseminação de dados no País."

O tema é controverso. A aplicação hospedada em território brasileiro tem vantagens práticas para o cliente. A primeira é a garantia que em caso de controvérsias será adotado o foro brasileiro. A segunda vantagem é a própria privacidade dos dados assegurada pelo Marco Civil, em que a quebra de sigilo somente pode ser feita com ordem judicial. Nos Estados Unidos não funciona assim, desde o incidente de 11 de setembro e a promulgação do Ato Patriota[15]. Outro

[15] Permite, entre outras medidas, que órgãos de segurança e de inteligência dos EUA interceptem ligações telefônicas e e-mails de organizações e pessoas

benefício é o uso de aplicações residentes em território nacional que têm menor latência e, consequentemente, melhor experiência de uso para os clientes brasileiros.

Outras formalizações do Marco Civil também são corretas e não representam ônus para os provedores sérios, como a obrigatoriedade dos provedores de aplicação guardarem os registros de acesso por seis meses, e a responsabilidade por danos de terceiros ser admissível somente se o provedor de aplicação não tomar as medidas técnicas cabíveis, após notificado judicialmente. O escândalo internacional do caso Snowden foi um alerta e o Brasil deu um importante passo na regulamentação da Internet. Que venham outros passos no rumo e no tempo certo.

---

supostamente envolvidas com o terrorismo, sem necessidade de qualquer autorização da Justiça, sejam elas estrangeiras ou americanas.

10 A IMPLEMENTAÇÃO DE CRIPTOGRAFIA TOTALMENTE HOMOMORPHIC

Cloud Computing tem sido a inovação mais promissora da computação nas últimas décadas. Seu uso ainda é dificultado pelos problemas de segurança relacionados com dados críticos. A criptografia dos dados armazenados remotamente tem sido a técnica mais utilizada para preencher esta lacuna na segurança, visto que a nuvem ainda é um grande risco.

O método de Criptografia *Homomorphic* é uma boa base, para melhorar a segurança e armazenamento de dados sensíveis. O modelo aceita entradas criptografadas e, em seguida, executa o processamento cego para satisfazer a consulta do usuário, sem conhecimento do seu conteúdo. Os dados cifrados somente serão decifrados pelo usuário que inicia a comunicação. Isso permite que os clientes contem com os serviços oferecidos pelas aplicações remotas sem arriscar sua privacidade.

10.1 Cloud Security

No cenário atual, tanto na nuvem pública quanto na privada a criptografia tenta garantir a segurança dos dados armazenados. Com o avanço das tecnologias foi possível criar uma transmissão segura de uma máquina local, para um armazenamento de dados em nuvem. Os dados armazenados são codificados e o canal de transmissão de dados bem protegido com as trocas de chaves. Mas, realizar cálculos sobre os dados armazenados na nuvem requer codificação. Isto prejudica o processo de *Data Mining*.

A proposta aqui é para criptografar os dados antes de enviar para o provedor de nuvem. Assim, para permitir que o fornecedor execute cálculos sobre os dados dos clientes como analise de padrões de vendas, sem expor os dados originais. Para alcançar este objetivo, também é necessário manter os *Cryptosystems* baseados em criptografia *Homomorphic* ou totalmente *Homomorphic* (*Encryption* (FHE) ou criptografia pouco *Homomorphic* (SHE)).

11 SISTEMA DE CRIPTOGRAFIA *HOMOMORPHIC*

Fonte: Technology Review[16]

Neste exemplo, queremos adicionar 1 e 2. Os dados são criptografados para que 1 se torne 33 e 2 torna-se 54. Os dados criptografados são enviados para a nuvem e processados, o resultado (87) pode ser baixado a partir da nuvem e descriptografado para proporcionar a resposta final (3).

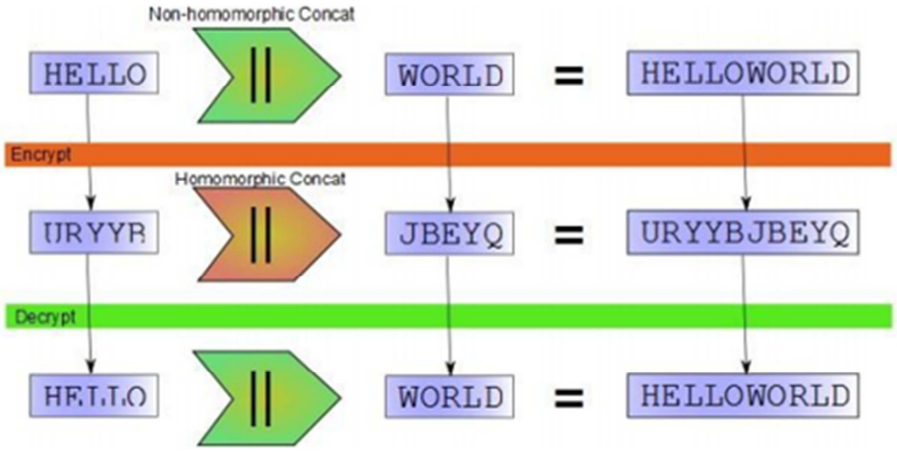
O problema é que, enquanto os dados podem ser enviados para o centro de dados em um provedor de nuvem criptografada, os servidores que alimentam uma nuvem não podem realizar qualquer trabalho no mesmo. Gentry, um pesquisador da IBM, mostrou que é possível analisar os dados sem decodifica-los. A chave é para encriptar os dados, tal como a realização de uma operação matemática da informação cifrada. A descodificação do resultado produz a mesma resposta que a realização de uma operação análoga em dados descriptografados. A correspondência entre as operações sobre os dados criptografados e as operações a serem executadas com dados criptografados é conhecido como um homomorfismo. Conforme dito por Craig Gentry em (Bajpai & Srivastava, 2014), “algo como isto poderia ser usado para proteger as operações através da Internet”.

Com a criptografia *Homomorphic*, uma empresa pode criptografar todo o seu banco de dados de e-mails e envia-lo para a nuvem. Os resultados serão baixados e descodificados sem expor os detalhes de um único e-mail.

[16] Disponível em: http://www2.technologyreview.com/article/423683/homomorphic-encryption/ Acesso em 24 Nov. 14

Gentry começou a estudar criptografia *Homomorphic* em 2008. No começo, ele era capaz de realizar apenas algumas operações básicas sobre dados criptografados antes de seu sistema começar a produzir lixo. Uma tarefa como encontrar um pedaço de texto em um e-mail requer encadeamento de milhares de operações básicas. Sua solução foi usar uma segunda camada de criptografia, essencialmente para proteger os resultados intermediários quando o sistema entrou em colapso e precisava ser reposto. "O problema de como criar uma verdadeira criptografia *Homomorphic* tem sido debatida por mais de 30 anos, e Craig foi a primeira pessoa a realizar o cálculo de matemática [...]" diz Paul Kocher, o presidente da empresa de segurança Pesquisa *Cryptography*. No entanto, adverte Kocher, como o esquema de Gentry atualmente requer uma enorme quantidade de computação, há um longo caminho a percorrer antes que sejam amplamente utilizáveis.

Gentry reconhece que a forma como ele se candidatou a dupla camada de criptografia era um pouco de um truque e que o sistema é executado muito lentamente para o uso prático, mas ele está trabalhando na otimização para aplicações específicas, tais como pesquisar bancos de dados para os registros. Ele estima que esses aplicativos possam estar prontos para o mercado dentro de cinco a 10 anos.



Fonte: Ripublication[17]

Em primeiro lugar, a noção de processamento de dados, sem acesso real ao mesmo é paradoxal. Vamos considerar um problema análogo no mundo físico.

Sita é dona de uma loja de jóias e possui materiais preciosos como ouro, diamantes, prata etc. Ela quer que seus trabalhadores montem de forma corretas todos os anéis e joias, porém anda desconfiada de alguns trabalhadores e presume que roubarão suas joias se houver oportunidade. Em outras palavras, ela quer que seus trabalhadores montem os materiais em peças acabadas, sem ter acesso aos materiais.

Ela usa um porta-luvas impenetrável transparente, protegido por um bloqueio para os quais tem a chave. Coloca os materiais preciosos dentro da caixa, trava-os e os entrega a um trabalhador.

O empregado, usando luvas, monta o anel ou colar dentro da caixa. A mesma é impenetrável, o trabalhador não pode chegar aos materiais preciosos. Sita abre a caixa com a chave e extrai o anel ou colar. Em suma, o trabalhador transforma a matéria-prima em uma peça acabada, sem ter um verdadeiro acesso aos materiais.

Em 2009, Craig Gentry da IBM propôs o primeiro sistema de criptografia *Full Homomorphic* que avalia um número arbitrário de adições e multiplicações e, assim, calcula qualquer tipo de função em dados codificados. O funcionamento interno acrescenta outra camada de criptografia a cada operação e usa uma chave

[17] Disponível em: http://www.ripublication.com/irph/ijict_spl/ijictv4n8spl_05.pdf. Acesso em: 24 Nov. 14

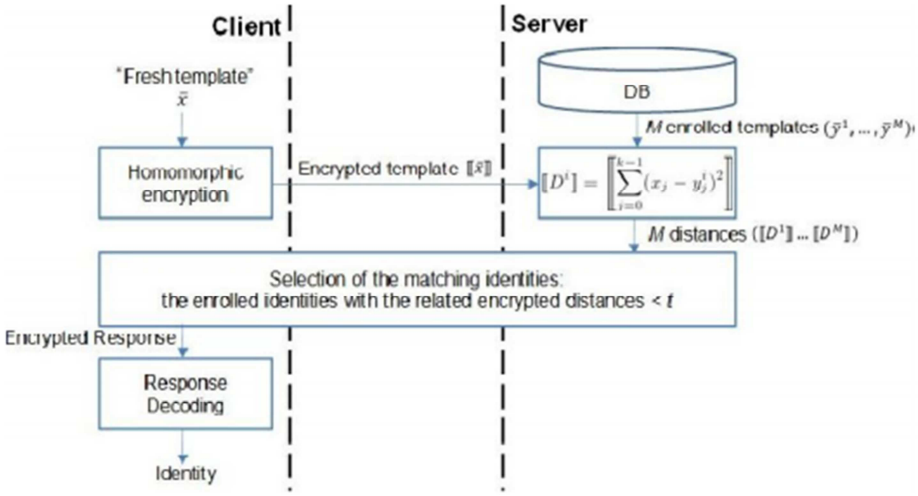
criptografada para desbloquear a camada interna de cifragem. Esta descriptografia recupera os dados sem expô-lo, permitindo um número infinito de cálculos sobre o mesmo.

Fonte: Ripublication[18]

12.1 FHE em Nuvem

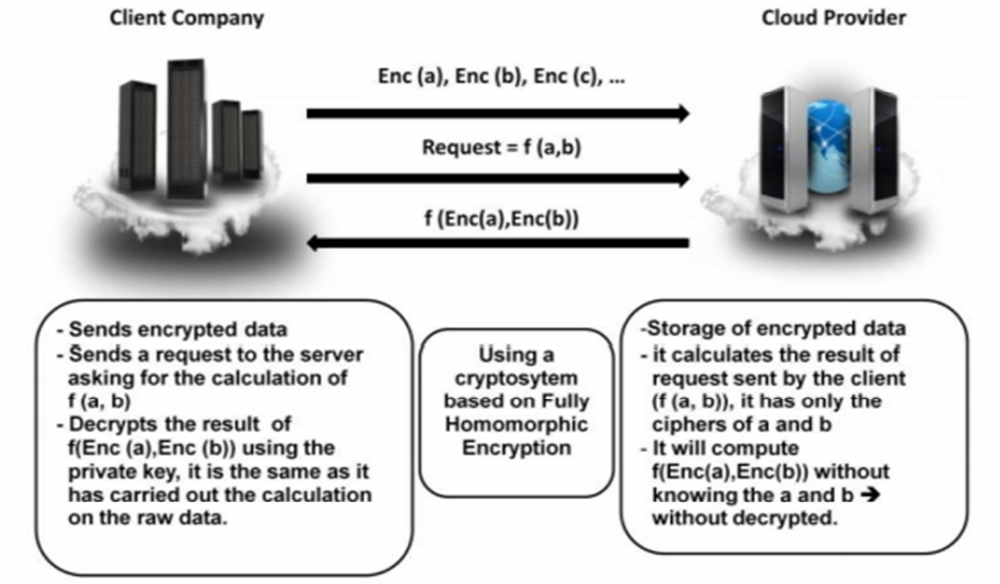
A aplicação da criptografia totalmente *Homomorphic* é um passo importante na segurança em nuvem. De modo geral, a terceirização dos cálculos sobre os dados confidenciais para o servidor da nuvem é possível, mantendo a chave secreta que pode decifrar o resultado do cálculo. Vamos analisar o desempenho dos tipos existentes de sistemas de criptografia *Homomorphic*, utilizados em uma plataforma virtual como um servidor de nuvem, uma rede VPN que liga a nuvem com o cliente, e em seguida, simulação de diferentes cenários. Por exemplo, um servidor de base de dados que se comunica com cliente utilizando um sistema de criptografia FHE, como mostra a figura abaixo:

[18] Disponível em: http://www.ripublication.com/irph/ijict_spl/ijictv4n8spl_05.pdf. Acesso em: 24 Nov. 14



Fonte: Ripublication[19]

Na mesma linha o cenário de computação na nuvem, pode ser ilustrado como a seguir:



Fonte: Ripublication[20]

Segurança da computação na nuvem baseado em criptografia totalmente *Homomorphic* é um novo conceito de segurança, que permite fornecer os resultados dos cálculos em dados criptografados sem conhecer as entradas de matérias em que o cálculo foi realizado respeitando a confidencialidade dos dados.

[19] Disponível em: http://www.ripublication.com/irph/ijict_spl/ijictv4n8spl_05.pdf. Acesso em: 24 Nov. 14.
[20] Disponível em: http://www.ripublication.com/irph/ijict_spl/ijictv4n8spl_05.pdf. Acesso em: 24 Nov. 14.

13 TOKENIZATION

As duas principais tecnologias para obscurecer os dados sensíveis são a criptografia e *tokenization*, sendo que a primeira é a mais usada. “Entre os nossos clientes, cerca de 80% usam a criptografia e 20% *tokenization*”, disse Pravin Kothari, CEO da empresa de segurança da informação em nuvem CipherCloud.

Tokenization, criada em 2005, é diferente de criptografia em vários pontos. Primeiro, os dados nunca deixam as instalações do proprietário. Em vez disso, os dados sensíveis, tais como o número do cartão de crédito é substituído por uma sequencia aleatória de caracteres, o *token.* É esse símbolo que é passado para a aplicação, seja na nuvem ou em qualquer outro lugar, para processamento. Ao contrario de criptografia, não há nenhuma maneira do sinal ser reverso.

“A indústria de cartões de pagamento tem sido o padrão de fato a anos”, disse David Canellos, CEO da empresa de segurança na nuvem na nuvem PerspecSys. “Mas agora estamos vendo casos novos para uso no paradigma da nuvem”.

O maior interesse em *tokenization* foi inicialmente impulsionado por clientes na Europa, preocupados com o Patriot Act dos EUA, disse Canellos.

> Os dados criptografados deixando a sua localização são ainda dados que deixam suas instalações. Nossos clientes em todo o mundo, que pretendem contratar uma nuvem com fornecedores norte-americanos, estão cada vez mais, optando por *tokenization*.

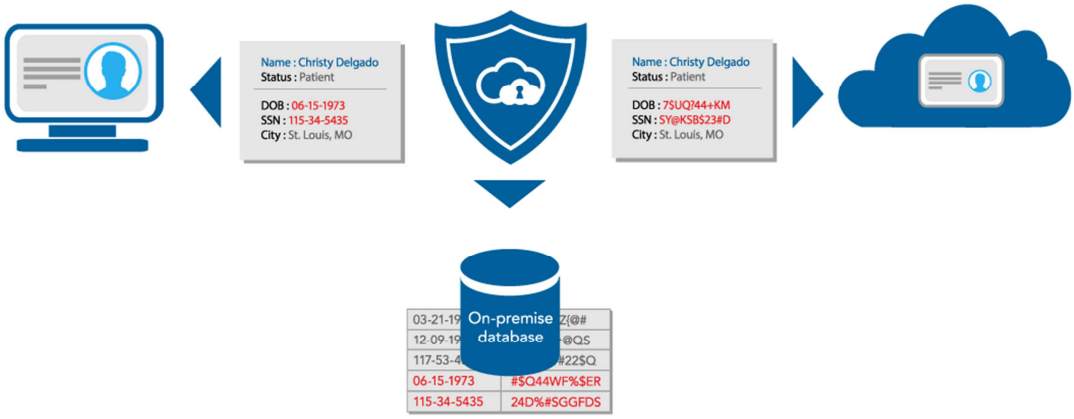
O fato de que os dados sensíveis permanecem completamente sob o controle da organização que possui a relativa simplicidade de *tokens* de manipulação na nuvem em comparação com dados criptografados leva a crer que a *tokenization* vai se tornar uma forma cada vez mais importante do tratamento de dados de forma segura na nuvem.

Prós:

- Controle completo de localização de dados.
- Nenhuma chave, aplicações em nuvem são mais fáceis de gerenciar.
- *Tokens* não podem ser revertidos, são projetados para recuperar dados de texto sem formatação.

Contras:

- Criptografia forte, segurança física e redundância necessária para abóbada símbolo.
- Possível vulnerabilidade. Os dados são armazenados sem criptografia no local.
- Não é aceito por todos os regimes regulatórios.



Fonte: Ciphercloud[21]

[21] Disponível em: http://www.ciphercloud.com/wp-content/uploads/2013/10/tokenization-assured-data-sovereignty-white-text-large.png Acesso em 24 Nov. 14

14 TOKENIZATION OU CRIPTOGRAFIA?

Há prós e contras em cada abordagem. Tokenization proporciona flexibilidade. É possível selecionar e limitar os dados que precisam ser protegidos como números de cartão de crédito.

Outro exemplo de como *Tokenization* é muitas vezes utilizado é no processamento de números de Segurança Social.

Todos nós sabemos o quão importante esses dígitos são. As pessoas roubam esses números dourados, roubam identidades. O Isolamento de um número de Segurança Social permite que ele seja substituído por um sinal durante o transporte e substituído posteriormente com os números reais. Este processo assegura que os números foram obtidos de forma legal.

No entanto, para fazer isso com sucesso, é preciso identificar os dados específicos para criptografia.

O *Tokenization* como sua metodologia de segurança minimiza o custo e a complexidade da conformidade com os padrões da indústria e regulamentações governamentais. Certamente a partir de uma questão de conformidade com o PCI DSS, alavancando *Tokenization* como proteção dos dados do cartão de crédito é menos caro do que E2EE.

O sistema de criptografia protege todos os dados, independentemente da sua composição, a partir de uma extremidade do processo até o destino. Essa proteção "full" não deixa chance de perder dados que devem ser protegidos. Criptografia end-to-end garante a proteção de dados a partir da fonte ao longo de toda a transmissão. Todos os dados são passados de forma segura através da rede, incluindo redes públicas, até ao seu destino, onde são de-encriptadas e geridas pelo destinatário.

Embora haja muito a ser dito no mercado sobre o desempenho, isso não deve ser um disjuntor do negócio, tecnologias de otimização e metodologias podem minimizar a diferença de desempenho. Em uma pesquisa recente conduzida Hubspan em segurança na nuvem, mais de 77% dos entrevistados disseram que estavam dispostos a sacrificar algum nível de desempenho, a fim de garantir a segurança dos dados. O desempenho da criptografia completa é aceitável para a maioria das implementações.

Não é preciso escolher um método em detrimento de outro. Tal como acontece com as implementações de nuvem, muitas empresas estão adotando uma

abordagem híbrida quando se trata de segurança de dados na nuvem. Se os mesmos são bem conhecidos e definidos, e o subconjunto de dados é sensível, então *Tokenization* é um método confiável e comprovado para implementação.

É claro que há uma série de abordagens para proteger seus dados contra *malware*[22] e outras falhas de segurança. *Tokenization* e E2EE são duas das formas mais populares hoje.

Também é importante compreender que cada um destes métodos requer um conjunto diferente de infraestruturas de apoio. O custo de implementação pode variar.

[22] É um *software* destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações (confidenciais ou não).

15 COMPARAÇÕES ENTRE CRIPTOGRAFIA E TOKENIZATION

Alguns argumentam que a criptografia ameaça o ótimo desempenho, este é um pequeno preço a pagar para garantir que a computação em nuvem não ameace a integridade os dados.

Um argumento interessante a favor do uso de *token* é o fato de que os dados sensíveis são substituídos por símbolos aleatórios para mitigar a mudança.

Os dados devem ser autorizados a sair da organização, especialmente quando eles são usados para acelerar o desempenho. Isso certamente aumenta o risco para a organização e pode até mesmo fazer a computação em nuvem menos atraente.

Há também considerações de implantação. Como uma tecnologia mais estabelecida, criptografia é mais amplamente entendida e, portanto, pode ser mais fácil de implementar. No entanto, há um par de capturas.

As chaves podem potencialmente ser roubadas por *insiders*, ou, como no caso do *backudoor* RSA, por agências que exploram pontos fracos do próprio algoritmo de criptografia.

Além da questão de segurança, há também a funcionalidade. As maiorias dos aplicativos na nuvem ainda estão usando bancos de dados em texto simples. Isto significa que os dados sensíveis devem ser decifrados antes de processados e então criptografados novamente, quando ele se move on. Uma das principais questões sobre o uso de criptografia é que existem múltiplas partes envolvidas.

A questão do controle de chaves é resolvida através do uso de *proxy*[23], tais como os fornecidos pelas empresas Cinphercloud e PerspecSys, entre outras. Estes *proxys* ou *gateways* estarão entre a organização e o provedor da nuvem, seja atrás do firewall[24] ou na rede de perímetro DMZ (zona desmilitarizada). Todo o tráfego na nuvem passa por eles. Os dados sensíveis são criptografados ou *tokenizados* antes de enviados para a nuvem, a organização que detém todas as chaves de criptografia.

Consultas de banco de dados, como pesquisas são realizadas localmente em índices, no caso da criptografia, o banco de dados completo na tokenização. Os dados ou *tokens* criptografados são enviados para as aplicações em nuvem para o

---

[23] É um servidor (um sistema de computador ou uma aplicação) que age como um intermediário para requisições de clientes solicitando recursos de outros servidores.

[24] Em português: Parede de fogo é um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.

processamento. Os dados de retorno são então convertidos novamente para os valores reais através do *proxy.*

Tais serviços podem limitar as ameaças internas também, como o tráfico de dados na nuvem e para múltiplas aplicações através do *proxy*, permitindo a visibilidade sobre todo o sistema, com comportamento anômalo como o download de grandes quantidades de informação, acionando alertas.

No final do dia, a organização que lançou uma estratégia de computação em nuvem deve decidir se eles podem ou não estar confortáveis com *Tokenization* - que pode ou não acarretar vazamento de informações sigilosas - ou criptografia *end-to-end*, o que prejudica o desempenho.

	Criptografia	**Vs**	***Tokenization***
Utilização no mercado	80%	x	20%
Implementação	Técnica mais conhecida	x	Está sendo adaptada à *Cloud Computing*
Gerenciamento de Chaves	Difícil gerenciamento, além do risco de se perder a chave	x	Não utiliza chaves, apenas troca os valores dos dados
Reversão do algoritmo	Pode ser revertido ao seu estado inicial	x	Não pode ser revertida, utilizada valores aleatórios.
Disponibilidade dos dados	Dados deixam sua instalação inicial (trafegado via internet)	x	Dados nunca deixam sua instalação inicial
Desempenho	Perca causada na criptografia/descriptografia	x	Tokens são menores do que os dados que representam

Fonte: O Autor

16 CONCLUSÃO:

Como outras tecnologias, a *Cloud Computing* traz diversos benefícios, mas também diversas dúvidas sobre o uso de seus modelos, custos, aplicação, migração de ambiente além da questão mais discutida, a segurança da informação.

Redução de custos, escalabilidade, sustentabilidade, portabilidade, flexibilidade são alguns dos benefícios.

Diversas empresas ainda não adotaram este modelo, temendo a perda dados, divulgação ou modificação.

Serviços e soluções entregues em qualquer lugar do planeta. Essa característica da *Cloud Computing* desafia o atual modelo jurídico que se baseia em leis locais. Em razão disso, os riscos legais são até maiores do que os de outros contratos tradicionais de outsourcing de TI.

Entrar nesse mundo sem fronteiras exige cautela na elaboração dos contratos firmados com os prestadores de serviço. É importante que o contrato contenha cláusulas sobre questões de privacidade e disponibilidades dos dados. As empresas têm que ficar atentas à jurisdição de outros países, em caso de armazenamento de dados fora do território nacional. É muito importante estabelecer qual legislação prevalecerá. Em caso de ordem judicial, o sigilo dos dados pode ser quebrado, dependendo da lei de privacidade aplicada pelo país onde o servidor estiver instalado.

Armazenar informações em datacenters no Brasil traz algumas vantagens. A primeira é a garantia que em caso de controvérsias será adotado o foro brasileiro. A segunda vantagem é a própria privacidade dos dados assegurada pelo Marco Civil, em que a quebra do sigilo somente pode ser feita com ordem judicial.

Para se transmitir uma informação através da internet é de vital importância que este meio seja seguro. As técnicas de criptografia *Homomorphic*, totalmente *Homomorphic* e *Tokenization*, visam à integridade dos dados que serão transmitidos para o datacenter.

A *Cloud Computing* proporciona diversos benefícios e diversos problemas relacionados à segurança. Não é possível afirmar se este modelo é o mais seguro.

17 REFERENCIAS

Portal da Segurança. (03 de Novembro de 2014). Acesso em 18 de Novembro de 2014, disponível em Jornal da Segurança: http://www.portaldaseguranca.com.br/Noticia/Visualizar/2215

Aranha, O. (07 de Julho de 2014). ***QUEIRA O SR. PERITO - Blog sobre computação forense, e-discovery e direito digital*.** Acesso em 19 de Novembro de 2014, disponível em http://qperito.com/: http://qperito.com/2014/07/07/queira-o-sr-perito-comentar-sobre-cloud-computing-os-desafios-ao-ordenamento-juridico-e-a-pericia-forense/

Bajpai, S., & Srivastava, P. (2014). **A Fully Homomorphic Encryption Implementation on Cloud Computing.** *International Journal of Information & Computation Technology., 4*(N. 08).

BURDUŞEL, L. (2013). **NEW CRYPTOGRAPHIC CHALLENGES IN CLOUD COMPUTING ERA.** *14*.

Canal Comstor. (04 de Junho de 2013). ***Canal Comstor*.** Acesso em 19 de Novembro de 2014, disponível em O Blog dos negócios de TI: http://blogbrasil.comstor.com/blog/bid/294730/O-que-%C3%A9-SaaS-PaaS-e-IaaS

Cascão, M. (25 de Abril de 2014). *Terra.com.br*. Acesso em 21 de Novembro de 2014, disponível em CIO.com.br: http://cio.com.br/opiniao/2014/04/25/marco-civil-e-a-computacao-em-nuvem/

Costa, M. (02 de Novembro de 2014). *Globo.com*. Acesso em 19 de Novembro de 2014, disponível em TechTudo: http://www.portaldaseguranca.com.br/Noticia/Visualizar/2215

Dara, S. (2013). **Cryptography Challenges for Computational Privacy in Public Clouds.**

Exame.com. (01 de Setembro de 2014). *Exame.com*. (Exame) Acesso em 10 de Novembro de 2014, disponível em http://exame.abril.com.br/: http://exame.abril.com.br/tecnologia/noticias/icloud-pode-ter-causado-parte-do-vazamento-de-fotos-intimas

Freire, K. (10 de Setembro de 2014). *http://www.techtudo.com.br/*. (Globo) Acesso em 17 de Novembro de 2014, disponível em Techtudo: http://www.techtudo.com.br/noticias/noticia/2014/09/lista-vaza-senhas-de-5-milhoes-de-contas-gmails-mas-google-nega-invasao.html

Horton, T., & McMillon, R. (2011). ***A Primer on Payment Security Technologies: Encryption and Tokenization*.** (First Data) Acesso em 05 de Novembro de 2014, disponível em First Data: http://files.firstdata.com/downloads/thought-leadership/primer-on-payment-security-technologies.pdf

IDG News Service. (30 de Abril de 2014). *http://cio.com.br/*. (CIO Estratégias de negócios e TI para líderes corporativos) Acesso em 20 de Novembro de 2014, disponível em NBusiness: http://cio.com.br/noticias/2014/04/30/criprografia-na-nuvem-aumenta-mas-ainda-nao-e-habito-corrente/

Lisk, S. (20 de Abril de 2011). ***Cloud Security Alliance Industry Blog*.** (CSA.org) Acesso em 15 de Novembro de 2014, disponível em https://blog.cloudsecurityalliance.org: https://blog.cloudsecurityalliance.org/2011/04/20/is-tokenization-or-encryption-keeping-you-up-at-night/

Mohanta, B. K., & Gountia, D. (2013). **Fully homomorphic encryption equating to cloud security: An approach.** *IOSR Journal of Computer Engineering (IOSR-JCE), 09*.

Mukhopadhyay, D., Sonawane, G., Gupta, P. S., Bhavsar, S., & Mittal, V. (s.d.). ***Enhanced Security for Cloud Storage using File Encryption.*** Acesso em 23 de Novembro de 2014, disponível em Cornell University Library: http://arxiv.org/ftp/arxiv/papers/1303/1303.7075.pdf

Olhar Digital. (11 de Setembro de 2014). ***Olhar Digital*.** (UOL) Acesso em 15 de Novembro de 2014, disponível em http://olhardigital.uol.com.br/: http://olhardigital.uol.com.br/noticia/44050/44050

Pescatore, J. (28 de Maio de 2012). *http://www.computerworld.com.pt/*. (Computer World) Acesso em 12 de Novembro de 2014, disponível em Computer World: http://www.computerworld.com.pt/2012/05/28/cloud-computing-exige-seguranca-especifica/

Ramos, R. d., & Eses, N. I. (Julho de 2013). ***O Impacto do Cloud Computing no Processo de Perícia Digital.*** Acesso em 19 de Novembro de 2014, disponível em Rennecloud Files: https://rennecloud.files.wordpress.com/2013/07/o-impacto-do-cloud-computing-no-processo-de-pericia-digital.pdf

Sadeghi, A.-R., Schneider, T., & Winandy, M. (s.d.). ***Token-Based Cloud Computing: Secure Outsourcing of Data and Arbitrary Computations with Lower Latency.*** Acesso em 24 de Novembro de 2014, disponível em Technische

Universitat Darmstadt: https://www.tk.informatik.tu-darmstadt.de/fileadmin/user_upload/Group_TRUST/PubsPDF/SSW10.pdf

Santos, A. P., & Machado, M. (2010). **CLOUD COMPUTING: IMPASSES LEGAIS E NORMATIVOS.** *Revista Científica Intraciência*, 16 - 105.

Velte, A. T., Velt, T. J., & Elsenpeter, R. (2013). ***Computação em Nuvem: Uma Abordagem Prática.*** Rio de Janeiro: Alta Books.

Verdi, F. L., Rothenberg, C. E., Pasquini, R., & Magalhães, M. F. (2010). **Novas Arquiteturas de Data Center para Cloud Computing.**

Zanutto, B. G. (2012). ***Segurança em Cloud Computing.*** Acesso em 24 de Novembro de 2014, disponível em DComp Ufscar: http://www.dcomp.sor.ufscar.br/verdi/topicosCloud/Artigo-Seguranca-Cloud.pdf