ABORDAGENS E-SAUDE ARMAZENADAS NA COMPUTAÇÃO EM NUVEM: UMA REVISÃO SOBRE SEGURANÇA E PRIVACIDADE DE DADOS

Luís Rafaeli Coutinho – UFSC
Hidelbrando Rodrigues – UFAM

E-mail para contato: luisrafaelli29@gmail.com
hidelrodrigues@gmail.com

Eixo Temático: 2.1.6 Ciências da Informação

Categoria: comunicação oral

RESUMO
Neste artigo, apresentamos uma revisão da literatura para e-saude em ambiente de armazenamento na nuvem. Foram selecionados artigos principalmente por fontes da Medline e Google Scholar. Objetivando procurar recentes informações sobre esta tecnologia emergente para os serviços de saúde. Com relevância à segurança e privacidade de dados que diferentes estudos de computação em nuvem abordaram. Armazenar informações confidenciais como prontuários eletrônicos e informações de saúde na nuvem, significa que devem ser tomadas precauções para garantir a segurança e confidencialidade dos dados. Os provedores de serviços na nuvem devem garantir que todos os mecanismos de segurança estarão em vigor para evitar acesso não autorizado e violações de dados. Muitos estudos para aprimoramento da confiabilidade e privacidade dos dados estão sendo realizados. Os pacientes devem ser mantidos informados sobre como seus dados de saúde podem ser gerenciados. Esta pesquisa mostra também que a tecnologia da computação em nuvem pode ser aplicada em várias áreas de domínio e-saude.

Palavras-chave: nuvem, saúde, segurança**.**

INTRODUÇÃO

Os dados de saúde estão crescendo muito rapidamente em termos de tamanho, complexidade e velocidade. As técnicas de geração de banco de dados tradicionais e de mineração de dados não são mais eficientes em armazenando, processando e analise desses dados. Novas ferramentas inovadoras são necessárias para lidar com estes dados dentro da área de saúde em tempo hábil (YOUSSEF, 2014).

De acordo com definição do National Institute of Standards and Technology (NIST) dos EUA, a computação em nuvem é "um modelo que pode ser distribuído, rapidamente

provisionado e com recursos de computação configuráveis como servidores, armazenamento, aplicativos, redes e outros serviços" (MELL; GRANCE, 2009).

O compartilhamento de dados na nuvem está tornando-se vital para as organizações e usuários sociais. Os benefícios incluem maior produtividade e melhor gerenciamento de tempo, por exemplo, usando ferramentas colaborativas como o Google Docs. Com os usuários, os benefícios do compartilhamento de dados são claros, por exemplo, o Facebook, que permite compartilhar fotos e vídeos, além de compartilhar informações do dia-a-dia. Em relação aos prestadores de cuidados de saúde, estes, estão migrando rapidamente para a nuvem e os benefícios do compartilhamento também são evidentes, visto que, esta prática permite armazenar e compartilhar registros eletrônicos e, portanto, remover a dependência geográfica entre prestador de cuidados de saúde e paciente (THILAKANATHAN et al, 2014).

Porém, uma vez que uma das vantagens mais significativas da computação em nuvem é a sua enorme capacidade de armazenamento de dados, a nuvem é suscetível a muitos ataques de privacidade e segurança. Como resultado, muitos hospitais e organizações de saúde estão relutantes em adotar a tecnologia “Cloud”.

Vale ressaltar que, alta acessibilidade, disponibilidade e confiabilidade podem tornar a computação em nuvem uma solução para problemas de interoperabilidade na área de saúde. O novo paradigma, para a prestação de serviços de saúde, foi adotado por países como EUA, Canadá, Reino Unido, Coréia e União Européia (ABBAS; KHAN, 2014).

Os avanços na tecnologia da informação apontam grande progresso de tecnologias de saúde em vários domínios (KOTZ et al, 2015). No entanto, essas novas tecnologias também fizeram dados de saúde não só muito maiores, mas também muito mais difíceis para manusear e processar (UR REHMAN et al e LIU et al, 2016). Este artigo propõe uma revisão bibliográfica com base na segurança e privacidade em dados de saúde armazenados em ambiente de computação em nuvem.

METODOLOGIA

De modo restrito, consideramos pesquisa a busca sistemática de respostas a indagações científicas e soluções tecnológicas às necessidades da vida diária, entendendo ciência como a atividade restrita a pesquisa de novos conhecimentos e ampliação do entendimento daqueles já existentes. Entendemos tecnologia como o

desenvolvimento e análise de novos materiais, equipamentos e métodos de execução de determinadas tarefas (WAINER, 2006).

Este estudo trata-se de uma revisão bibliográfica. Para a análise e estudo de sistemas de registros eletrônicos de saúde baseados em nuvem, revisamos artigos publicados, pesquisas em segurança e problemas de privacidade, que diferentes estudos de computação em nuvem usam para o desenvolvimento em plataformas “Cloud”. Totalizando trinta artigos pesquisados no período de janeiro a abril de 2019. A literatura relacionada foi obtida principalmente por fontes da Medline e Google Scholar. Muitas publicações mostram a viabilidade de implementações da computação em nuvem. Foram selecionados vinte artigos e demais referências para a presente revisão. Todos foram revisados para procurar informações sobre esta tecnologia emergente para os serviços de saúde. A maioria deles mostra as vantagens que as soluções baseadas na nuvem podem fornecer a sistemas e-saude.

RESULTADOS E DISCUSSÃO

A capacidade de acessar universalmente todas as informações de saúde do paciente em tempo hábil é de extrema importância. Portanto, um alto nível de integração de dados, interoperabilidade e compartilhamento de dados entre diferentes profissionais da área de saúde são necessários. Principalmente em instituições que pretendem oferecer cuidados de saúde de alta qualidade aos pacientes atendidos (YOUSSEF, 2014).

Os requisitos de armazenamento e disponibilidade contínua de dados de e-saude favorecem o uso da computação em nuvem para prestação de serviços. A computação em nuvem está emergindo como uma promessa, um novo paradigma para a computação e está chamando a atenção tanto da academia como da indústria. A computação em nuvem mostrou grande potencial para melhorar a colaboração entre diferentes organizações de saúde para cumprir os requisitos comuns como escala agilidade, rentabilidade e disponibilidade. Além disso, a migração de registros de saúde do paciente para o armazenamento na nuvem alivia os provedores de saúde das tarefas de gerenciamento de infraestrutura (ABBAS; KHAN, 2014).

A vantagem de custo da computação em nuvem não é apenas relacionada como o armazenamento. Por não comprar ou instalar determinado hardware e software, usando menos energia, os usuários de computação em nuvem provavelmente também reduzirão significativamente suas emissões de carbono. Pesquisas sugerem que as tecnologias de

informação e comunicação (TIC) já são responsáveis por 2% das emissões globais de carbono e que sua participação relativa poderá aumentar ainda mais (HU; BAI, 2014).

Necessidades e os requisitos para a privacidade e-saude na nuvem

Os provedores de serviços em nuvem devem implantar sistemas de autenticação que assegurem a privacidade da informação do paciente. Os governos devem exigir que os prestadores de serviços “Cloud” atendam os requisitos de privacidade necessários para garantir a privacidade de dados do paciente. A implantação de um quadro legal ajudará a realizar um ambiente seguro. Políticas de privacidade foram legisladas em vários países para regular e preservar a privacidade dos registros de pacientes. Como exemplo, a Lei de Portabilidade e Responsabilidade do Seguro de Saúde que regula a privacidade da informática em saúde e a segurança dos dados dos pacientes nos EUA (HIPAA). É importante enfatizar que estas políticas dependem de cada país.

De acordo com a lei espanhola 41/2002, um RES (Registro Eletrônico de Saúde) é definido como uma documentação, que contém informações sobre a clínica evolução do paciente durante sua assistência no processo de saúde. Nesta lei, os usos dos RES são definidos, exigindo pessoal médico para manter a privacidade dos pacientes. A lei espanhola trata esse tipo de informação como "especialmente protegida". Este tipo de nomenclatura está definido na Lei 15/1999 com o objetivo de proteger a privacidade do paciente. O consentimento do paciente é necessário para gerenciar e acessar esses dados, exceto no caso de uma emergência em que a vida do paciente está em risco (RODRIGUES et al, 2013).

No Brasil ocorreu a criação de um processo de certificação de sistemas de registro eletrônico de saúde, com o estabelecimento dos requisitos obrigatórios e, acompanhando a legislação federal para documento eletrônico, reforçou a obrigatoriedade do uso de certificação digital (assinatura eletrônica) para a validade ética e jurídica de um Prontuário Eletrônico do Paciente (PEP) e Registro Eletrônico de Saúde (RES). Um marco regulatório importante foi à publicação da Resolução CFM Nº 1821/2007. A estrutura de um prontuário, independente de ser eletrônico ou em papel, deve seguir as orientações e determinações da Resolução CFM Nº 1638/2002 que define o prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde (SBIS, 2012).

Para a informatização em saúde, a integridade e confidencialidade são atributos desejáveis. A integridade significa preservar a precisão e consistência de dados e no sistema de saúde, refere-se ao fato de que os registros eletrônicos de saúde (RES) não foram adulterados por uso não autorizado. A confidencialidade é definida pela

Organização Internacional para Normalização (ISO) no ISO-17799 como "garantindo que a informação seja acessível apenas para aqueles autorizados a ter acesso" (YOUSSEF, 2014).

Aplicações da computação em nuvem

O modelo de computação em nuvem muda a infraestrutura da informática para provedores de serviços terceirizados que gerenciam os recursos de hardware e software com reduções significativas de custos. Uma plataforma que, além de armazenar volumes gigantescos dos dados de saúde, também serve como um gerenciamento estruturado dos dados em vários provedores de saúde.

Na área de saúde os dados podem ser extraídos de diferentes bancos de dados para tratamentos e outros fins analíticos. Normalmente, a nuvem consiste em elementos em camadas, como o armazenamento físico, infraestrutura de serviços, aplicativos e comunicação à infraestrutura. Essa tecnologia é aplicada para compartilhamento, processamento e gerenciamento de dados de saúde. Além disso, a infraestrutura da nuvem e-saúde pode ser: (a) implementado internamente pelo profissional de saúde (privado), (b) mantido por alguma parte externa (pública), (c) mantido pelo prestador de cuidados de saúde e por uma parte externa juntos (híbrido) podem ser categorizadas (ABBAS; KHAN, 2014).

Um novo tipo de serviço de computação em nuvem (nuvens da comunidade) também é promovido como outra adição possível aos outros modos. Em nuvens de comunidades, os serviços em nuvem podem ser fornecidos (muitas vezes por uma organização) e consumidos por grupos de organizações em negócios ou profissões semelhantes às da organização fornecedora. Atualmente, há poucos exemplos para demonstrar a viabilidade dessa abordagem (SULTAN, 2014).

Os avanços na tecnologia móvel permitiram dispositivos móveis, como smartphones e tablets, serem usados em uma variedade de diferentes aplicações dentro da área de saúde. Nos últimos anos, os dispositivos móveis começaram a se tornar abundantes em muitas aplicações de saúde. O motivo do crescente uso da computação móvel é a sua capacidade de fornecer uma ferramenta ao usuário quando e onde é necessário independentemente do movimento do usuário, portanto, suporte de localização e independência (YOUSSEF, 2014).

Com o advento do monitoramento eletrônico de saúde remota, sistemas prometem revolucionar a saúde convencional. Métodos de cuidados integrando o Internet of Things (IoT). Esses sistemas podem aumentar ainda mais a inteligência, flexibilidade e interoperabilidade na nuvem. Nos últimos anos tem visto um crescente interesse em

sensores portáteis e hoje vários dispositivos estão comercialmente disponíveis para cuidados de saúde pessoais, fitness e consciência de atividade. Estruturas seguras de armazenamento na nuvem foram, portanto, propostos para uso com registros médicos sensíveis. No entanto, proteger o processamento de dados na nuvem continua sendo um desafio, considerando a grande quantidade de aplicativos habilitados a IoT (HASSANALIERAGH et al, 2015 e HOSSAIN; MUHAMMAD, 2016).

Discussão de tópicos revisados nos artigos

Para médicos e outros profissionais da área da saúde, abraçar soluções mais seguras, consiste em que elas sejam úteis e adequadas dentro do seu fluxo de trabalho clínico. Ações de tecnologia da informação em saúde apresentam muitos problemas exigentes para os usuários se autenticarem com os sistemas. Novos mecanismos de autenticação que trabalhem com smartphones, tablets, desktops, e laptops possuem relevância (KOTZ et al, 2015).

Um pequeno e limitado estudo de caso de "prova de concepção" com base em um projeto piloto de e-saude bem-sucedido (usando simulador) implementado em um hospital de Londres foi apresentado em um artigo com as vantagens que os potenciais pacientes "reais" (e seus familiares) podem obter de um sistema de nuvem em ambiente hospitalar. Refletindo sobre o caso acima mencionado do Chelsea e Westmin-ster Hospital, os prestadores de cuidados de saúde que contemplaram a adoção de uma plataforma de computação em nuvem puderam ser mais bem atendidos por “cloudproviders” locais. O simulador denominado Flexiant forneceu exemplo de um provedor de pequenas nuvens que pode oferecer um projeto de saúde interessante (SULTAN, 2014).

A adoção da tecnologia da computação em nuvem é mais do que um projeto de grande escala. Portanto, a complexidade do sistema será um critério fundamental ao fazer uma decisão de adoção. Além disso, os sistemas de informação hospitalar, como o Sistema de Imagem e Comunicação (PACS), o Sistema de Informação Hospitalar (HIS) e o Sistema de Informação Radiológica (RIS) são únicos por natureza. Migrar esses sistemas para a plataforma de computação em nuvem também será um fator crítico que estas organizações precisam considerar (LIAN; YEN; WANG, 2014).

Na revisão bibliográfica em questão, foi possível encontrar uma série de trabalhos de pesquisa em redes de sensores sem fio WSN (Wireless Sensor Networks) para aplicações médicas. Na verdade, a enorme quantidade de dados gerados e recolhidos por redes de sensores médicos apresentam vários desafios que as arquiteturas existentes

ainda não podem resolver de forma mais eficiente com relação à segurança (LOUNIS et al, 2016).

Devido à terceirização de dados, o servidor da nuvem não pode ser totalmente confiável para fornecer serviço de controle de acesso a dados, o que significa que os métodos de controle de acesso existentes no servidor não são mais aplicáveis para sistemas de armazenamento em nuvem. Exigindo o uso de outras técnicas para privacidade dos dados (YANG et al, 2013).

A crescente necessidade do cuidado remoto dos pacientes em casa combinada com a crescente popularidade de dispositivos móveis devido à sua natureza onipresente resultou em muitos aplicativos desenvolvidos para permitir saúde móvel. A “Cloud”, em combinação com tecnologias móveis, permitiu que os médicos convenientemente monitorassem e avaliem a saúde do paciente enquanto o paciente está no conforto de sua própria casa (HOSSAIN; MUHAMMAD, 2016). Isso exige compartilhamento de informações de saúde entre equipes de saúde, como médicos e enfermeiros, a fim de fornecer melhor cuidados e de forma mais segura aos pacientes. No entanto, o compartilhamento de informações de saúde pode introduzir problemas de privacidade e de segurança que podem muitas vezes entrar em conflito com a própria legislação (CHEN; YANG; SHIH, 2014).

Mecanismos de segurança e controle de privacidade

Alguns dos problemas de segurança que devem ser considerados pelos provedores de serviços “Cloud” e seus clientes de cuidados de saúde são: o acesso baseado em função, mecanismos de segurança de rede, criptografia de dados, assinaturas digitais e monitoramento de acesso. Além disso, para garantir a segurança das informações e cumprir as políticas de privacidade, o provedor de serviços em nuvem deve ser compatível com várias certificações e requisitos de terceiros. Como SAS70 Type II, PCI DSS Level 1, ISO 27001 e Lei Federal de Gestão da Segurança da Informação (FISMA) por exemplo (RODRIGUES et al, 2013).

A confidencialidade e a integridade podem ser alcançadas através de técnicas do controle de acesso e criptografia. O controle de acesso é um efetivo método para proteger dados, e amplamente utilizado em muitos estudos. Técnicas com uma identidade baseada em sistema de criptografia (IBE) no controle de acesso de RES são bem difundidas (UR REHMAN, 2016). A criptografia baseada em atributo (ABE) é um dos sistemas de criptografia mais preferidos usados na computação de armazenamento de dados de saúde na nuvem. Alguns autores sugerem um modelo de nuvem híbrida que

contém controles de acesso e técnicas de proteção de segurança como uma solução confiável (HU; BAI, 2014).

A criptografia baseada em atributos (ABE) tem sido usada para projetar sistemas de compartilhamento do PEP. No entanto, as soluções existentes não conseguem alcançar vários aspectos importantes e objetivos de segurança. Um sistema de ABE multi-autoridade com texto cifrado com responsabilidade do usuário e aplicado para projetar um sistema de compartilhamento do PEP pode contribuir com uma segurança maior dos dados (XHAFA et al, 2015). É essencial que os esquemas ABE obtenham a revogação de atributos, pois os atributos dos usuários podem ser alterados com frequência (WANG et al, 2018).

O controle de acesso aos dados é uma maneira eficaz de garantir segurança de dados na nuvem. Uma política de texto cifrado com criptografia baseada em atributos (CP-ABE) é uma técnica promissora para controle de acesso de dados criptografados. No entanto, devido à ineficiência de decodificação e revogação, os esquemas CP-ABE existentes não podem ser aplicados diretamente para construir um esquema de controle de acesso a dados para sistemas de armazenamento em nuvem multiautorais, onde os usuários podem possuir atributos de múltiplas autoridades. Uma proposta para um controle de acesso para armazenamento em nuvem multi-autoridade (DAC-MACS), com um esquema de controle de acesso a dados eficaz e seguro com decodificação e revogação apresentou boas possibilidades em estudo (YANG et al, 2013).

Um novo modelo de privacidade acessível e autorizado pelo paciente com controle de privacidade multinível, preservando esquemas de autenticação cooperativa (PSMPA), realizando três níveis diferentes de requisitos de segurança e privacidade na computação em nuvem. Distribuída em dispositivos móveis (sistema proposto) com aplicações em saúde, ilustraram que o PSMPA pode resistir a vários tipos de ataques maliciosos e superar esquemas anteriores em termos de armazenamento, computação e sobrecarga de comunicação. Após prova formal de segurança e avaliações de eficiência (ZHOU et al, 2015).

CONSIDERAÇÕES FINAIS

O ambiente na nuvem alivia as organizações de saúde das tarefas de gerenciamento de infraestrutura e também minimiza custos de desenvolvimento e manutenção. Esta estrutura oferece um alto nível de integração, interoperabilidade,

disponibilidade e compartilhamento de dados de saúde entre prestadores de cuidados de saúde, pacientes e praticantes.

Mas precauções devem ser consideradas essencialmente com mecanismos de segurança e privacidade. A presente revisão mostra estudos crescentes e em desenvolvimento sobre a tecnologia de armazenamento na nuvem que devem ser aprimorados e otimizados futuramente.

A segurança e a privacidade estão emergindo como um novo desafio na informática no setor de saúde com o uso da tecnologia “Cloud”. Buscando a confidencialidade, o sigilo das informações pessoais, o armazenamento seguro de dados, a preservação da autenticidade e integridade das informações eletrônicas em saúde, assim como, de outros domínios comerciais.

REFERÊNCIAS

ABBAS, Assad; KHAN, Samee U. A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. **IEEE Journal of Biomedical and Health Informatics**, v. 18, n. 4, p. 1431-1441, 2014.

CENTERS FOR DISEASE CONTROL AND PREVENTION et al. HIPAA privacy rule and public health. Guidance from CDC and the US Department of Health and Human Services. **MMWR: Morbidity and mortality weekly report**, v. 52, n. Suppl. 1, p. 1-17, 19, 2003.

CHEN, Chin-Ling; YANG, Tsai-Tung; SHIH, Tzay-Farn. A secure medical data exchange protocol based on cloud environment. **Journal of medical systems**, v. 38, n. 9, p. 112, 2014.

HASSANALIERAGH, Moeen et al. Health monitoring and management using Internet-of-Things (IoT) sensing with cloud-based processing: Opportunities and challenges. In: **2015 IEEE International Conference on Services Computing**. IEEE, 2015. p. 285-292.

HOSSAIN, M. Shamim; MUHAMMAD, Ghulam. Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring. **Computer Networks**, v. 101, p. 192-202, 2016.

https://portal.cfm.org.br/crmdigital/Cartilha_SBIS_CFM_Prontuario_Eletronico_fev_2012.pdf

HU, Yan; BAI, Guohua. A systematic literature review of cloud computing in eHealth. **arXiv preprint arXiv:1412.2494**, 2014.

KOTZ, David et al. Security for mobile and cloud frontiers in healthcare. **Communications of the ACM**, v. 58, n. 8, p. 21-23, 2015.

LIAN, Jiunn-Woei; YEN, David C.; WANG, Yen-Ting. An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital. **International Journal of Information Management**, v. 34, n. 1, p. 28-36, 2014.

LIU, Zheli et al. Cloud-based electronic health record system supporting fuzzy keyword search. **Soft Computing**, v. 20, n. 8, p. 3243-3255, 2016.

LOUNIS, Ahmed et al. Healing on the cloud: Secure cloud architecture for medical wireless sensor networks. **Future Generation Computer Systems**, v. 55, p. 266-277, 2016.

MELL, Peter; GRANCE, Tim. The NIST Definition of cloud computing. v. 15, 10 jul. 2009. 2010.

RODRIGUES, Joel JPC et al. Analysis of the security and privacy requirements of cloud-based electronic health records systems. **Journal of medical Internet research**, v. 15, n. 8, p. e186, 2013.

SULTAN, Nabil. Making use of cloud computing for healthcare provision: Opportunities and challenges. **International Journal of Information Management**, v. 34, n. 2, p. 177-184, 2014.

THILAKANATHAN, Danan et al. A platform for secure monitoring and sharing of generic health data in the Cloud. **Future Generation Computer Systems**, v. 35, p. 102-113, 2014.

UR REHMAN, Muhammad Habib et al. Big data analytics in mobile and cloud computing environments. In: **Innovative Research and Applications in Next-Generation High Performance Computing**. IGI Global, 2016. p. 349-367.

WAINER, J. et al. **O que é pesquisa em informática em saúde?.** RITA, v. 13, n. 1, p. 42-56, 2006.

WANG, Shangping et al. Efficiently revocable and searchable attribute-based encryption scheme for mobile cloud storage. **IEEE Access**, v. 6, p. 30444-30457, 2018.

XHAFA, Fatos et al. Privacy-aware attribute-based PHR sharing with user accountability in cloud computing. **The Journal of Supercomputing**, v. 71, n. 5, p. 1607-1619, 2015.

YANG, Kan et al. DAC-MACS: Effective data access control for multiauthority cloud storage systems. **IEEE Transactions on Information Forensics and Security**, v. 8, n. 11, p. 1790-1801, 2013.

YOUSSEF, Ahmed E. A framework for secure healthcare systems based on big data analytics in mobile cloud computing environments. **Int J Ambient Syst Appl**, v. 2, n. 2, p. 1-11, 2014.

ZHOU, Jun et al. PSMPA: Patient self-controllable and multi-level privacy-preserving cooperative authentication in distributedm-healthcare cloud computing system. **IEEE transactions on parallel and distributed systems**, v. 26, n. 6, p. 1693-1703, 2014.