Sigilo médico-paciente sobre criptografia ponta-a-ponta

Irlon de Souza Lamblet[1], **Jéssica A. S. Sanglard**[1], **Nilson Mori Lazarin**[1]

[1]Bacharelado em Sistemas de Informação – Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (Cefet/RJ) – Nova Friburgo, RJ – Brazil

{irloncefet,jessicaadelinyss}@gmail.com, nilson.lazarin@cefet-rj.br

Abstract. *Faced with the new scenario imposed by the COVID-19 pandemic, the physician-patient relationship has undergone significant changes. In some cases it is possible for the patient to be treated remotely, however, the delivery and analysis of exams are sensitive points for medical confidentiality / patient. There are some storage systems for medical history in the cloud, however closed solutions, do not provide for migration of patient data and do not guarantee that the data is safe for leaks. This work presents a model and a implementation that offering to patient the control over their medical information in compliance to the brazilian version of the GDPR.*

Resumo. *Diante do novo cenário imposto pela pandemia do COVID-19, a relação médico-paciente sofreu mudanças significativas. Em alguns casos é possível que o paciente seja atendido de forma remota, entretanto, a entrega e análise de exames são pontos sensíveis para o sigilo médico/paciente. Existem alguns sistemas de armazenamento de históricos médicos em nuvem, entretanto são soluções fechadas, não preveem migração de dados do paciente e não garantem que os dados estejam seguros a vazamentos. Este trabalho apresenta um modelo e uma implementação aderente a LGPD oferecendo ao paciente a capacidade de controlar e proteger o acesso a suas informações médicas.*

1. Introdução

A segurança da informação está baseada na integridade, disponibilidade e confidencialidade dos dados armazenados. Entretanto, a grande quantidade de exames médicos realizados ao longo da vida, a descentralização dos registros médicos de um único paciente e a dificuldade ao migrar o prontuário de um profissional para outro, afetam da segurança dos dados médicos de um paciente. Esta insegurança a que os dados médicos estão sujeitos podem dificultar a realização de um diagnóstico mais preciso, pois com o cruzamento de dados é possível realizar uma análise mais assertiva que podem levar a escolha de um tratamento mais eficaz para o indivíduo [ANS 2015] [KIM and SOLOMON 2014].

Atualmente não há um sistema único de saúde integrado para pacientes e médicos onde exista a possibilidade dos registros (prontuários, exames, receitas, etc...) ficarem disponíveis para ambos, além de que a rede particular e pública não contam com a possibilidade de unificação de informações de um paciente. Sendo assim, o médico não tem acesso ao histórico completo do paciente, pois as informações de consultas anteriores estão em posse de outros profissionais, gerando a necessidade de criação de novas fichas e solicitação de novos exames para inciar-se um novo acompanhamento [de Fátima Marin 2010].

Uma evolução dos registros tradicionais, são os sistemas de prontuário eletrônico (*Eletronic Health Record* - EHR), entretanto os dados permanecem em posse do profissional de saúde e não do paciente. Dessa forma, softwares de registros pessoais de saúde (*Personal Health Record* - PHR) se apresentam como contraponto ao definir o paciente como responsável pelo armazenamento de seus dados médicos. Diante deste cenário, o armazenamento em nuvem torna-se uma opção viável. Todavia, o vazamento imprevisto ou voluntário de informações de pacientes pode ser destrutivo. De modo que, sua manipulação necessita de grande cautela e sigilo para evitar grandes distúrbios para usuários dos serviços de saúde, seus familiares e médicos [Aaron Baird 2008] [Edimara Mezzomo Luciano 2011].

Este trabalho apresenta uma metodologia que visa garantir o sigilo médico/paciente, através de técnicas criptográficas e ao mesmo tempo permitir maior controle dos dados por parte do paciente, atendendo as novas orientações propostas pela Lei Geral de Proteção de Dados Pessoais (LGPD) que consolida o consentimento do titular sobre o tratamento de seus dados. É possível observar que aquele que o utiliza as informações de certa pessoa, ou até mesmo os que mantém em bancos de dados, não possuem o direito das mesmas, somente a pessoa a quem os dados dizem a respeito possuí o poder de consentimento do uso desses dados. Dessa forma, em uma relação médico/paciente, os dados do paciente no qual ficam armazenados em históricos médicos são de propriedade do paciente, e não em posse do médico.

2. Fundamentação Teórica

A criptografia de chave pública se baseia na utilização de um par de chaves, sendo estas a chave privada e a chave pública. A chave pública tem a função de cifrar os dados, e pode ser divulgada, ao mesmo tempo que a chave privada é mantida em segredo, e é utilizada para decifrar os dados e recuperar o seu conteúdo original. A segurança se baseia pelo fato de que apenas a chave privada pode decifrar as informações cifradas pela sua chave pública correspondente, o que a diferencia da criptografia simétrica, onde uma mesma chave é utilizada para cifrar e decifrar [Nunes 2007].

O algoritmo Diffie-Hellman é capaz de estabelecer um segredo compartilhado que pode vir a ser utilizado como uma chave simétrica compartilhada. O seu algoritmo se dá pela ideia onde duas pessoas são capazes de produzir um mesmo segredo a partir das suas próprias chaves privadas e a chave pública de sua contraparte, pois ao realizar a combinação de um valor privado com o outro público, cada um chegará ao mesmo valor secreto, que poderá ser usado para cifrar ou decifrar os dados [de Melo Pires 2010].

O algoritmo de chave simétrica AES (*Advanced Encryption Standard*), é uma especificação para criptografia de dados instituída pelo Instituto Nacional de Padrões e Tecnologia (NIST). O AES cifra blocos de dados de 128 bits utilizando chaves de 128, 192 ou 256 bits [Daemen and Rijmen 1999].

3. Trabalhos Relacionados

Em [Rewagad and Pawar 2013] é apresentada uma arquitetura para proteção de dados baseada em três etapas. A primeira utiliza o algoritmo Diffie-Hellman para a geração das chaves utilizadas na etapa de troca de chaves; Em seguida utiliza-se o algoritmo RSA para autenticar o cliente através de uma assinatura digital. Por fim, os dados são cifrados

ou decifrados, através do algoritmo AES. É prevista a utilização de dois servidores, um com a finalidade de cifrar ou decifrar e outro dedicado ao armazenamento dos dados do usuário.

Em [Mello 2015] é apresentada uma arquitetura para compartilhamento e armazenamento seguro de registros de saúde em nuvem que executam o papel de provedores de serviço em uma federação de identidades unidas com o objetivo de prover e gerenciar identidades, voltadas para a área da saúde. Para realizar o armazenamento de dados, o dono do registro primeiramente cifra o registro utilizando uma chave simétrica e em seguida o cifra novamente, utilizando uma política (*Attribute Based Encryption*) ABE, após a execução dos algoritmos, o dono pode armazenar seu registro de saúde cifrado na nuvem do provedor de serviço, através de uma solicitação de armazenamento, onde ele escolherá se autenticar por meio da federação de entidades, selecionando um provedor de identidade, onde está cadastrado. Devido às relações entre atributos estabelecidas na política ABE, não é necessário executar outra operação de delegação de acesso para compartilhar os registros de forma segura, pois ao cifrar o registro por meio do ABE o protocolo criptográfico garante o controle de acesso.

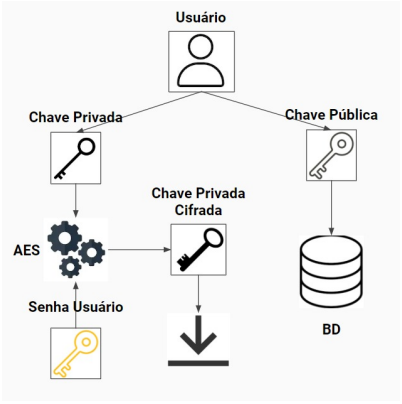
Este trabalho destina-se a proteção de dados e garantia do sigilo médico/paciente e nos dados providos pelo paciente. Diferente dos trabalhos [Rewagad and Pawar 2013] e [Mello 2015] utilizaremos técnicas criptográficas que operam com chaves assimétricas concedidas ao paciente e ao médico, além da combinação do AES e do algorítimo Diffie Hellman, que garante o acesso de informações ocorra de forma controlada, por meio de uma chave privada cifrada. Dessa forma, assegurando melhor controle e segurança ao paciente para auxílio de seu histórico médico e dados pessoais, portanto, para que o médico tenha acesso a essas informações será necessário ocorrer a troca de chaves com o paciente.

4. Proposta

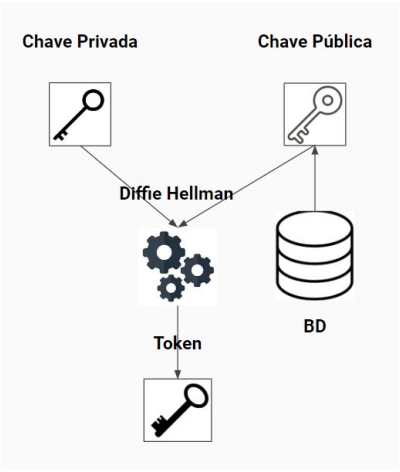
Este trabalho apresenta um modelo para proteção de dados e do sigilo médico/paciente, através do uso do algoritmo Diffie-Hellman. Além disso, foi implementada uma API (*Application Programming Interface*), que pode vir a ser utilizada em uma plataforma própria, ou auxiliar outros sistemas com o mesmo propósito de armazenar os históricos médicos de pacientes, reforçando a segurança dos dados, e permitindo aos seus usuários realizar o gerenciamento do controle de acesso destas informações.

Para utilizar este serviço, primeiramente será necessário que os usuários sejam cadastrados, informando uma senha, entre outras informações comuns ao cadastro de uma pessoa. A partir do cadastro do usuário, o servidor gerará um par de chaves assimétricas. A chave privada então é cifrada através do AES, utilizando-se da senha informada pelo usuário de forma que seja utilizada para ler e enviar dados, não transitando pela rede e Disponibilizando, assim, o download. No entanto a chave pública é armazenada no servidor para que possa ser utilizada posteriormente, conforme figura 1(a).

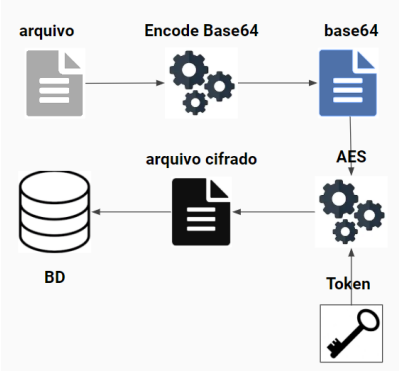
Utilizando-se das chaves assimétricas do paciente e do profissional da saúde, com o algoritmo Diffie-Hellman obtém-se um token de acesso, utilizado para cifrar ou decifrar dados. Desta forma, assegura-se que apenas o paciente, ou o profissional da saúde, possam visualizar as informações daquele arquivo. Na figura 1(b) podemos observar o processo de geração do token de acesso.



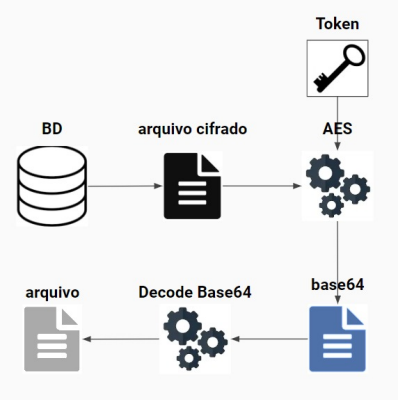
(a) Cadastro de Usuário



(b) Geração do token



(c) Armazenamento seguro



(d) Acesso aos dados armazenados

Figura 1. Processos do modelo de proteção de dados

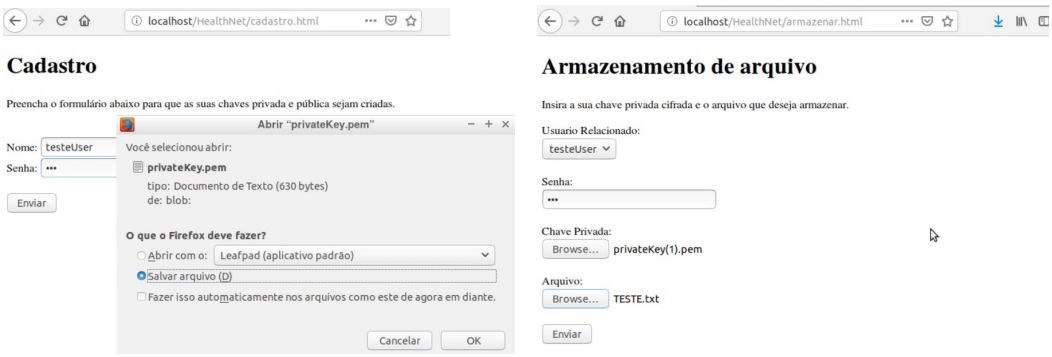
Durante o processo de armazenamento de uma informação no banco de dados, conforme apresentado na figura 1(c), deve-se utilizar a chave privada do paciente, além de informar o médico que receberá o acesso a estas informações. Os dados então passarão por um processo de codificação, utilizando Base64, e cifragem utilizando o token de acesso resultante da união da chave privada do paciente e da chave pública do médico. Após esta etapa, os dados estarão prontos para serem armazenados.

Para que um profissional da saúde recupere um dado armazenado, conforme apresentado na figura 1(d), será necessário que ele informe sua chave privada. O sistema deverá localizar a chave pública do paciente, e com o Diffie-Hellman gerará o token de acesso. O arquivo cifrado, armazenado no servidor, passará por um processo de decifragem utilizando o token, e em seguida será decodificado, para então estar disponível para leitura. Caso o profissional tenha recebido a devida permissão de acesso a estas informações, ou seja, o paciente tenha escolhido a chave pública do profissional para armazenar o dado, o arquivo terá sido perfeitamente decifrado.

4.1. Implementação

Como prova de conceito do modelo proposto, foi implementada a aplicação HealthNet disponível para download no GitHub[1]. Nesta seção serão demonstradas as funcionalidades da aplicação.

A Figura 2 apresenta a tela de cadastro de usuário e a tela de upload de arquivo digital. Na Figura 2(a) pode-se observar o cadastro de um novo usuário, onde, após o envio dos dados necessários a aplicação gera um par de chaves assimétricas e permite o download da chave privada que deve ser armazenada pelo usuário. A chave pública do usuário (médico ou paciente) fica armazenada no banco de dados para que possa servir de base na criação do token de acesso. Na Figura 2(b) pode-se observar o upload de um arquivo digital. Neste processo, o usuário utiliza-se de sua chave privada e senha de acesso, além de informar qual o usuário relacionado, ou seja o destinatário que terá acesso ao arquivo. A chave pública do usuário destino já está previamente cadastrada no banco de dados do sistema. Após isso ele deve indicar o arquivo a ser enviado e clivar em Enviar.



(a) Cadastro de Usuário (b) Upload de arquivo

Figura 2. Cadastro de usuário e Upload de Arquivo

A Figura 3(a) apresenta um comparativo entre o arquivo original enviado pelo usuário e o arquivo armazenado no disco do servidor do HealthNet. O arquivo enviado possuía o nome *TEXTE.txt* e ao ser armazenado no disco, o mesmo foi renomeado e recebeu um ID do usuário que o enviou e um ID incremental, referente os arquivos enviados pelo usuário. Neste caso o arquivo foi renomeado para *58_arquivo-1.txt*, mantendo a extensão original.

Na Figura 3(b) pode-se observar o processo de reaquisição ou visualização do arquivo. Nesta etapa é necessário que o usuário de destino selecione o arquivo desejado, insira sua senha de acesso e sua chave privada. Uma vez que a chave pública do usuário de origem já se encontra em banco de dados, o token é calculado e utilizado para decifrar o arquivo e liberar o download. É possível observar que contamos com a alternativa de guardar diversos arquivos, inclusive exames nos quais precisam ser refeitos ao longo do ano e no decorrer da vida do paciente, principalmente os que possuem doenças que precisam ser avaliada em períodos curtos de tempo, levando assim, o paciente a realizar mais de quatro, ou mais, exames repetidos no mesmo ano.

[1]https://github.com/nilsonmori/HealthNet

(a) Arquivo enviado x armazenado (b) Arquivo recuperado

Figura 3. Arquivo Enviado x Recuperado

5. Conclusão

Com o modelo apresentado buscamos contribuir com a redução da necessidade da refação de exames médicos através do desenvolvimento de um núcleo para uma plataforma que realize o armazenamento dos históricos médicos de pacientes, de maneira segura, ou seja, criptografado de ponta-a-ponta, através da combinação das ferramentas criptográficas apresentadas. Garantindo, dessa forma a privacidade dos dados dos pacientes, como também dar aos seus usuários a capacidade de decidir quais informações determinadas pessoas, com a devida permissão de acesso, poderão acessar. As funcionalidades fornecidas por este modelo também poderiam ser oferecidas a outros sistemas de armazenamento de históricos médicos, aumentando a sua confiabilidade.

A implementação da plataforma auxiliaria também no combate ao COVID-19, possibilitando melhoras significativas na área da saúde, tendo em vista o cenário mundial e principalmente na relação médico paciente de forma remota. Assegurando a confidencialidade e confiabilidade de forma igualitária para todos os usuários, de acordo com a Lei Geral de Proteção de Dados Pessoais (LGPD). Provendo segurança por meio da criptografia para consultas online seguras e com devidas proteções, além também do contato com o histórico médico do paciente.

Como trabalhos futuros, a aplicação de técnicas de extratores difusos (Fuzzy Extractors [Dodis et al. 2004]) neste contexto, tornariam a utilização de dados biométricos como entrada para técnicas criptográficas, tornando possível obter valores fixos necessários para os algoritmos criptográficos a partir de valores próximos, mas não idênticos, da chave original. Estes valores fixos, podem ser obtidos de leituras biométricas das digitais dos usuários, e utilizados como as suas chaves primárias, removendo a necessidade do usuário salvá-la, possibilitando algum acesso a informação em casos de emergências médicas, onde o usuário pode não estar apto a acessar determinados dados de seu histórico médico.

Referências

Aaron Baird, Frederick North, M. T. R. (2008). Personal health records (phr) and the future of the physician-patient relationship.

ANS, A. N. d. S. S. (2015). Mapa assistencial da saÚde suplementar.

Daemen, J. and Rijmen, V. (1999). Aes proposal: Rijndael.

de Fátima Marin, H. (2010). Sistemas de informação em saúde: considerações gerais.

de Melo Pires, R. (2010). Aplicação do algoritmo diffie-hellman no compartilhamento de volumes criptografados do truecrypt.

Dodis, Y., Reyzin, L., and Smith, A. (2004). Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In Cachin, C. and Camenisch, J. L., editors, *Advances in Cryptology - EUROCRYPT 2004*, pages 523–540, Berlin, Heidelberg. Springer Berlin Heidelberg.

Edimara Mezzomo Luciano, Carlos Eduardo Barbosa de Azevedo Bragança, M. G. T. (2011). Privacidade de informaÇÕes de pacientes de instituiÇÕes de saÚde: A percepÇÃo de profissionais da Área de saÚde.

KIM, D. and SOLOMON, M. G. (2014). Fundamentos de segurança de sistemas de informação. *Tradução Daniel Vieira*.

Mello, L. (2015). Uma nova arquitetura para compartilhamento e ar- mazenamento seguro de registros de saÚde na nuvem utilizando atributos de identidade federada.

Nunes, D. S. (2007). Criptografia assimétrica.

Rewagad, P. and Pawar, Y. (2013). Use of digital signature with diffie hellman key exchange and aes encryption algorithm to enhance data security in cloud computing. In *2013 International Conference on Communication Systems and Network Technologies*, pages 437–439.