# O USO DA COMPUTAÇÃO EM NUVEM NA CRIAÇÃO DE UM PROTOCOLO DE RASTREABILIDADE

**MACEDO, Paulo Cesar de**
Faculdade Santa Lúcia
*paulo.macedo@fatec.sp.gov.br*

**CATINI, Rita de Cássia**
Faculdade Santa Lúcia
*ritacatini@gmail.com*

**CATINI NETO, Carlos**
Etec Pedro Ferreira Alves
***catini.it@gmail.com***

**RESUMO**

*Com a finalidade de garantir a privacidade dos dados provenientes dos sistemas automatizados da área da saúde, algumas informações de acesso precisam ser armazenadas. Esta área procura evitar que informações sigilosas, como as de prontuários de pacientes, fiquem disponíveis para qualquer tipo de usuário. O objetivo desse artigo é o desenvolvimento de um protocolo, disponibilizado em nuvem, capaz de responsabilizar os usuários desses sistemas pelos seus acessos, atendendo às normas indicadas pela HIPAA[1]. O protocolo define quais dados devem ser coletados, que formato os mesmos devem seguir, além das possíveis ações realizadas pela maioria dos sistemas. Como resultado, após a implementação, pode-se constatar que é perfeitamente viável a utilização do protocolo em sistemas de saúde.*

**PALAVRAS-CHAVE:** *Computação em Nuvem; HIPAA; Protocolo; Segurança; Mobile.*

[1] HIPAA - *Health Insurance Portability Accountability Act* - Lei de Responsabilidade de Portabilidade do Seguro de Saúde

Recebido em 08-12-2017 • Aceito em 27-02-2018

## INTRODUÇÃO

Sabe-se que os avanços tecnológicos visam contribuir com a automação dos processos em todas as áreas, agilizando assim a tomada de decisão por parte de qualquer profissional. Na área da saúde, isso não é diferente, ou seja, com o acesso à informação e quanto mais rápido um diagnóstico for feito, um tratamento se inicia. Existem diversas tecnologias capazes de permitir que as informações desta área sejam tratadas e disponibilizadas. Podemos citar, por exemplo, as redes locais usadas amplamente pelas instituições, onde os computadores são interligados e as informações trafegam utilizando programas específicos muitas vezes feitos especificamente para alguma atividade.

Existem também inúmeros programas (*softwares*) capazes de auxiliar as instituições médicas a controlarem seus atendimentos. Porém, a grande maioria deles é instalada localmente em suas redes, exigindo determinados tipos de equipamentos individuais de cada empresa desenvolvedora. Com essas novas tecnologias surgiram os problemas de infraestrutura, manutenção e segurança dos dados que a área tem que lidar diariamente. Segundo Maise *et al*. (2004), esses problemas vão desde uma rede que não funciona corretamente, equipamentos de má qualidade ou ultrapassados e, não menos importante, a exposição dos dados dos pacientes pelos sistemas desenvolvidos de qualquer forma.

As informações dos pacientes são mantidas em servidores que, com o passar dos anos, são substituídos por outros servidores mais potentes, ou seja, o fator tempo é significativamente um problema para as instituições que sempre têm que se atualizar frente aos avanços tecnológicos.

Os acessos externos a esses programas, e os dados gerados por eles, desencadeiam inúmeros problemas de segurança da informação, onde torna-se difícil garantir a privacidade dos dados trafegados. Utilizar a *Internet* como ferramenta para disponibilizar os dados de pacientes também se torna um problema ainda maior pois, além da segurança interna, as instituições têm que se preocupar com a segurança oferecida por terceiros, os provedores de acesso (ZANDIEH; KAHYUN; KUPERMAN, 2008).

Para Omogbadegun (2006), a *Internet* é outro ponto que requer muito cuidado das instituições de saúde e algumas optam por não utiliza-la, devido à falta de segurança que a mesma oferece. Outras instituições, porém, fazem o uso controlado e monitorado da *Internet*, já que seus departamentos precisam cada vez mais se conectarem a outras instituições, sejam particulares, como os bancos, ou públicas, como órgãos do governo que a mesma presta serviços. Outro fator é o uso pelos funcionários que, por sua vez, fazem uso de seus próprios aparelhos conectados à *Internet*,

Recebido em 08-12-2017 • Aceito em 27-02-2018

os *smartphones,* que estão presentes na vida da maioria das pessoas, com tendência de utilização cada vez maior. Um outro problema enfrentado por toda a área médica é manter as informações sob sigilo pois, caso os dados dos prontuários sejam compartilhados de forma indevida, inúmeras situações podem ser desencadeadas, como por exemplo:

- O que aconteceria se um funcionário conseguisse uma lista de pacientes com determinada doença e vendesse essa informação para um laboratório?;
- Se alguém invadisse o sistema anonimamente e divulgasse o nome dos pacientes com doenças infectocontagiosas?;
- Se um funcionário conseguisse realizar um acesso com a senha de um superior e alterasse algumas informações?;
- O que aconteceria se o sistema fosse contaminado por vírus de computador e todos os dados fossem perdidos; dentre outros problemas.

Alguns artigos pesquisados apresentam técnicas de criptografia de proteção dos dados dos pacientes, mas pouco se fala da responsabilidade após a liberação dos dados pelo paciente. Os dados são liberados aos médicos e profissionais, mas não existe uma forma de responsabilizá-los pelo acesso, de maneira formal e direta.

He e Johnson (2012) e Selvakumar e Sendhilkumar (2011), acreditam que os dados dos pacientes devem ser sempre protegidos a serem compartilhados em uma rede ou sistema devido a fragilidade das informações. Já para Kamalakannan e Arvind (2014), não há problemas em compartilhar as informações, desde que estejam criptografadas e só possam ser decifradas pelos proprietários das chaves de segurança.

Para Sobhy, El-Sonbaty e Elnasr (2012), o risco de as informações serem compartilhadas com pessoas de má fé podem provocar situações inconvenientes às instituições de saúde. Xue (2014) concorda que expor o paciente pode resultar em situações desconfortáveis ao mesmo e sua família.

Mediante a essas informações percebeu-se a necessidade do desenvolvimento de um protocolo de rastreabilidade aproveitando a ascensão da Computação em Nuvem (*Cloud Computing),* a qual atenda às normas da *Health Insurance Portability Accountability* (HIPAA).

Segundo a norma, os dados provenientes dos atendimentos realizados são de propriedade exclusiva do paciente (HIPAA, 2015). Essa norma foi criada pelos norte-americanos, mais especificamente pela *United States Department* (USD), a fim de estabelecer regras do uso correto das informações disponíveis e geradas pela área da saúde. Como a quantidade de informações

Recebido em 08-12-2017 • Aceito em 27-02-2018

pode ser gigantesca, percebe-se a necessidade do armazenamento em locais com maior disponibilidade (USD,2003).

Segundo Hauck *et al.* (2010), o termo *Cloud Computing* surgiu em meados de 2003, porém, sem a existência de tanta capacidade, mas com a ideia de que os *Data Centers* existentes pudessem ser compartilhados por qualquer tipo de pessoa, em qualquer lugar do planeta. Ryan e Loeffler (2010), afirmam que a *Cloud Computing* atua com muita segurança quando o assunto é armazenamento de informações com alto nível de confidencialidade. Isso implica que as instituições podem confiar cegamente em deixar seus dados disponíveis nesse tipo de rede. Para Jadeja (2012), o fato das informações serem de âmbito confidencial, a *Cloud Computing* pode ser a saída perfeita para armazenamento dos milhares de informações geradas pela área em questão.

## 2. METODOLOGIA

Esse artigo mostra a proposta de um novo protocolo de segurança de dados de paciente, intitulada Protocolo de Rastreabilidade (PR1). Foi utilizada uma linguagem de programação simples, possibilitando verificar se os dados de saúde estão sendo usados de acordo com os requisitos impostos pela norma HIPAA e, ao mesmo tempo, estabelecendo as responsabilidades pelo uso. Este protocolo é composto por uma forma de autenticação, localização e *token*, definição de dados e geração de *Short Message Service* (SMS).

Sendo assim, através dessa implementação, foi possível avaliar a eficiência e a segurança das informações.

Enquanto algumas pesquisas se pautam na segurança do acesso aos dados oferecidos de forma criptografada, esse artigo tem interesse na visão do outro lado envolvido, ou seja, no usuário da instituição que acessou os dados.

### 2.1 Protocolo de rastreabilidade (PR1)

Sua arquitetura será o modelo cliente servidor no qual todos os dispositivos envolvidos (clientes) irão acessar um único ponto (servidor), utilizando um arquivo para envio e recebimento em um formato universal. Dessa forma, todo acesso será monitorado pelo protocolo previamente adicionado ao navegador.

Observou-se, com a fundamentação teórica, a existência de inúmeros protocolos, inclusive alguns semelhantes a esse com relação a garantir a segurança dos dados.

A título de comparação, citamos, por exemplo, os protocolos *Secure Sockets Layer* (SSL) e *Transport Layer Security* (TLS). Para Joshi (2008),

Recebido em 08-12-2017 • Aceito em 27-02-2018

ambos os protocolos visam proteger as informações, mas desconhecem o seu conteúdo, ou seja, tanto o SSL quanto o TLS fazem a autenticação das partes envolvidas em uma troca de informações e cifram os dados a serem transmitidos, sem saber que dados são e muito menos quem foi o responsável.

Segundo Oranje (2008), enquanto o SSL autentica de maneira simples os clientes em um servidor, o protocolo proposto faz isso de maneira mais completa, aumentando a segurança. Já o TLS, que tem a característica de prevenir o acesso indevido de intermediários, pode ser combinado a esse protocolo, oferecendo as informações cifradas, tanto na origem quanto no destino.

O algoritmo desses protocolos citados exige que a comunicação seja criptografada e somente possa ser lida pelo destinatário correto, ideia semelhante à do PR1. Porém, o PR1 acrescenta em seu cabeçalho informações sobre como, quem e onde se deu o acesso, além de outros dados relacionados ao paciente.

Conforme Bella (2007), existem ainda outros protocolos de segurança, tais como *Hyper Text Transfer Protocol Secure* - protocolo de transferência de hipertexto seguro (HTTPS), *Virtual Private Network* (VPN) ou Rede Privada Virtual e o *Secure Shell* (SSH), que é um protocolo de rede criptográfico, mas com características e objetivos diferentes que não oferecem elementos de comparação com esse protocolo.

O protocolo de rastreabilidade desenvolvido é capaz de oferecer o acesso às informações de pacientes de uma instituição de forma controlada e remota, através de dispositivos locais ou móveis, tais como os smartphones ou *tablets* independente se a instituição já possui outro sistema interno. Atua na camada de aplicação e destina-se a instituições que desejam oferecer o acesso aos dados de pacientes internamente ou fora dos limites de sua rede local.

Para o uso do protocolo de maneira correta se faz necessário a aquisição de um arquivo de configuração. Uma vez instalado o protocolo na rede escolhida, o mesmo necessita ser configurado especificamente para a instituição disponibilizar seus dados de forma segura. Isso inclui um conjunto de informações cadastrais que permitirão o acesso e o monitoramento dos dados, as quais listamos:

- Nome da instituição
- Endereço (Código de Endereçamento Postal (CEP) + geolocalização)
- Responsável pela área de Tecnologia da Informação (usuário/administrador)
- Senha de acesso às configurações
- *Internet Protocol* (IP) do servidor de banco de dados
- Tipo de dados (texto, mdb, etc....)
- Tempo de visualização - *timeout* (padrão 2 minutos)

Recebido em 08-12-2017 • Aceito em 27-02-2018

Além dos dados básicos citados, a instituição precisa cadastrar os usuários que terão acesso aos dados (médicos e/ou profissionais da saúde), porém, estes devem também solicitar o acesso via dispositivo. Por exemplo, no caso de um médico querer acessar, via *smartphone* ou *tablet*, os dados de seus pacientes em um hospital, o mesmo deve estar previamente cadastrado no hospital e somente definir sua senha de acesso e os locais típicos de onde o mesmo presta seus atendimentos e aguardar aprovação do hospital para começar seus acessos. Cabe à instituição regularmente acompanhar as solicitações dos profissionais para que, no caso de pedidos de alterações de locais de acesso, esses não sejam ignorados.

A instituição deve disponibilizar uma tabela em seu banco de dados contendo essas informações, ou seja, um cadastro contendo os dados do médico ou profissionais, tais como o número do Conselho Regional de Medicina (CRM), Nome, *E-mail* e seus típicos locais de acesso, conforme listados na **Tabela 1**:

**Tabela 1** – *Layout* da tabela de acesso médico sugerida

| CRM | Nome | *E-mail* | Senha | CEP-Local |
|---|---|---|---|---|

Desta forma, fica claro que a conta de usuário do sistema é de responsabilidade da instituição e não deste protocolo. Isso implica que a instituição pode adaptar seu cadastro como quiser, desde que possa informar ao protocolo os dados necessários para o acesso seguro.

## 2.2 Autenticação

Após a instituição prover em seu sistema o cadastro dos médicos ou profissionais da saúde, para que os mesmos possam acessar os dados que lhe interessam, o protocolo de rastreabilidade irá solicitar as informações do responsável por acessar os dados estatísticos do protocolo ilustrado na **Tabela 1**. Sendo assim, a instituição poderá recuperar as informações sobre os acessos ocorridos em seu banco de dados e se necessário responsabilizar o médico ou o profissional no caso de ações indevidas.

Já na autenticação do médico/profissional, o protocolo irá solicitar suas credenciais de acesso, contendo seu *e-mail* e senha, sendo que as mesmas devem ser informadas via caixas de texto, no aplicativo do dispositivo móvel. Caso uma das informações não corresponda ao cadastrado

Recebido em 08-12-2017 • Aceito em 27-02-2018

pela instituição, o acesso não será liberado, mas caso seja encontrado, o protocolo irá verificar o local atual do acesso. Essa informação irá considerar os locais que o médico informou no momento do cadastro da solicitação de acesso. Os locais são marcados por latitude e longitude e sua localização será aferida no protocolo, considerando a proximidade do local de acesso, não havendo a necessidade de o médico estar exatamente no local cadastrado.

### 2.3 Localização e *Token*

Conforme Saravanakumar e Arun (2014), o Sistema de Geolocalização (GPS), presente na maioria dos equipamentos provedores de acesso móvel (*mobile*), disponibiliza a informação da localização atual do usuário para qualquer sistema solicitante. Essa informação nos equipamentos de procedência é confiável, porém pode ser fraudada através de programas com interesses maliciosos, a fim de mascarar o posicionamento de um usuário, o que é conhecido como *GPS FAKE*.

Existem inúmeros aplicativos com essa finalidade e, dessa forma, procurou-se evitar esse tipo de ação por meio do uso de um algoritmo denominado *token*. Conhecido também como autenticação de dois níveis, a ideia do algoritmo de *token* para o protocolo de rastreabilidade é autenticar sua localização a cada período de tempo.

Utilizou-se uma configuração que, após 30 segundos de conexão o protocolo irá disparar uma checagem via SMS para o usuário confirmar seu acesso. Isso irá se repetir por um período de tempo pré-estabelecido pela instituição, ou seja, pode-se configurar o *token* para enviar outros códigos de confirmação.

Existe ainda a possibilidade de a instituição gerar seus próprios *tokens* para cada médico ou profissional antecipadamente, e enviar aos mesmos via *e-mail*.

O tempo para essa confirmação poderia então ser estipulado pela instituição no intuito de não atrasar um atendimento, considerando que a norma HIPAA indica que um atendimento ao paciente não pode ser obstruído por um sistema de informação.

### 2.4 Definição dos dados

Após a instalação e o cadastro da instituição e dos profissionais que irão acessar os dados, o protocolo começa então a liberar as consultas

Recebido em 08-12-2017 • Aceito em 27-02-2018

e relatórios. As informações para responsabilidade do acesso devem minimamente respeitar um conjunto de dados que irá facilitar a identificação do usuário, bem como os motivos do acesso, locais e ações realizadas.

O conjunto de dados básicos são indicados de acordo com o seguinte *layout* da **Tabela 2:**

**Tabela 2** – *Layout* do cabeçalho do protocolo de rastreabilidade

| ID | Usuário | Data/Hora | Local | Longitude | Latitude | Solicitante | Ação | Paciente | Contador |
|---|---|---|---|---|---|---|---|---|---|

Sendo:

a) Ponto de Acesso de Rede (ID)

Descrição: trata-se de um identificador para o ponto de acesso de rede do dispositivo do usuário. Esta informação é fundamental para identificar o dispositivo do usuário no momento do acesso, porém não é obrigatório, haja vista que o IP, a máquina ou o número do telefone podem mudar de acordo com a rede de onde parte o acesso.

Formato e valores: O campo pode ser do tipo texto e dividido em duas partes, a identificação IP; e o tipo do acesso que pode ser:
I) Para acesso via endereço de rede local
II) Para acesso via endereço de rede de telefonia

Motivo: Este dado identifica o ponto de rede do usuário e pode servir para filtrar os dados de um mesmo grupo de usuários de uma rede. É um dado não obrigatório devido à possibilidade de um endereço se repetir para redes diferentes.

Exemplos:
Ponto de Acesso de Rede ID: 192.168.0.2
Tipo: 1 = Endereço IP
Ponto de Acesso de Rede ID: 19-9991-1212
Tipo: 2 = Número de telefone

b) Usuário

Descrição: Trata-se do nome do usuário previamente cadastrado

Recebido em 08-12-2017 • Aceito em 27-02-2018

pela instituição. Essa informação é obrigatória e serve para responsabilizar o mesmo pelos acessos realizados.

Formato e valores: O campo deve ser do tipo texto e deve aceitar apenas um nome único do usuário, sem espaços e símbolos.

Motivo: Esse dado é fundamental para identificar quem solicitou o acesso e será atrelado à senha do usuário, ou seja, servirá para identificar o profissional e autenticá-lo no protocolo. Com essa informação a instituição pode filtrar os acessos realizados e emitir relatórios de acesso do médico/profissional, caso necessite.

c) Data/Hora

Descrição: Data e horário do acesso à informação. Essa data deve ser sincronizada com o servidor da rede ou da *Cloud* e deverá desconsiderar fusos horários caso ocorra usando o sistema Tempo Universal Coordenado (UTC).

Formatos e valores: O campo deve ser do tipo data/hora e se possível com máscara de entrada padrão, formatada de acordo com a norma ISO/DIS 8601-1[2] (2016).

Motivo: As informações de data e hora são fundamentais para saber os momentos em que o profissional está acessando os dados. É um campo obrigatório e sabe-se que o dispositivo pode estar com essa informação errada, mas como sua captação será automática, o usuário não precisará se preocupar.

d) Local de acesso

Descrição: Localização de onde partiu a solicitação de acesso aos dados definidos pela geolocalização (longitude e latitude).

Formatos e valores: Trata-se de dois campos preenchidos automaticamente pelo sistema de geolocalização do aparelho.

Motivo: Complementar a segurança da informação, sendo que os dados só serão disponibilizados para usuários de locais pré-estabelecidos. Informação obrigatória e, caso não coincida com o cadastro de locais, o acesso não será concedido.

[2] ISO/DIS 8601-1 - norma internacional para representação de data e hora emitida pela Organização Internacional para Padronização

Recebido em 08-12-2017 • Aceito em 27-02-2018

Exemplo:
Longitude do acesso: -22.667885
Latitude do acesso: -99,567991

e) Solicitante

Descrição: Indica se quem solicitou os dados a serem acessados foi o próprio usuário ou outro médico/profissional:

Formato e valores: Campo de formato *booleano* (verdadeiro ou falso) onde o valor padrão é verdadeiro (*true*).

Motivo: Esse valor pode excluir a responsabilidade do usuário atual, passando para outro médico/profissional no caso de acesso compartilhado da informação. É um dado apenas informativo para que a instituição saiba a respeito de quem solicitou o acesso.

f) Ação realizada (transações)

Descrição: Identifica qual ação foi executada no banco de dados disponibilizado pela instituição.

Formato e valores: Trata-se de um campo numérico que indica as possíveis transações realizadas sob o monitoramento do protocolo, sendo que seu significado deve obedecer à **Tabela 3** a seguir:

**Tabela 3** – Possíveis transações realizadas via protocolo

| Valor | Significado |
|---|---|
| 1 | Consulta a dados |
| 2 | Copiar dados de paciente |
| 3 | Copiar imagens de paciente |
| 4 | Relatório de informações cadastrais |
| 5 | Exportar dados |

Motivo: Saber se a ação realizada pode ajudar a instituição a atender às políticas impostas pela HIPAA (2015), bem como prover a privacidade e a segurança da informação.

g) Paciente envolvido

Recebido em 08-12-2017 • Aceito em 27-02-2018

Descrição: Identifica o paciente participante das possíveis transações oferecidas pela instituição.

Formato e valores: Campo "texto", de tamanho variável, dependendo do sistema da instituição, normalmente tratado como código do paciente.

Motivo: Identificar o paciente envolvido na ação solicitada pelo médico. Essa informação é obrigatória e fornecida pelo usuário (médico/ profissional) enquanto utiliza a aplicação móvel.

h) Êxito no acesso (contador)

Descrição: Trata-se de um indicador a respeito de que se houve sucesso no acesso aos dados, por exemplo, no caso das tentativas de *login* (acesso via senha). Essa informação é obrigatória, haja vista que as tentativas de acesso podem ser restringidas a um número máximo e caso esse número seja ultrapassado, pode caracterizar uma tentativa de invasão.

Formato e valores: Dado do tipo numérico, usado como contador das tentativas de acesso.

Motivo: Controlar a quantidade de tentativas de acesso, procurando evitar que exceda uma quantidade pré-definida pela instituição.

**2.5 Consultas e Relatórios**

Em tempo real, o protocolo pode gerar alguns tipos de consultas que podem ser acessadas pelo usuário/administrador da instituição a qualquer momento. Esse recurso permite aos responsáveis o monitoramento sobre quais dados estão sendo manipulados e por quais profissionais.

As consultas geradas por sua vez, podem ser impressas em forma de relatório, possibilitando à instituição localizar e notificar os envolvidos, no caso de um acesso indevido, bem como coletar assinaturas dos mesmos (médicos/ profissionais) por período.

Segundo as normas HIPAA (2015), os usuários de sistemas informatizados da área da saúde que fizerem o mal-uso de informações dos pacientes podem ser processados e responderem judicialmente pela ação, principalmente se esses dados tiverem ligados a problemas de saúde ou *marketing* direcionado.

Esses dados podem ser filtrados por usuário, que são os médicos ou profissionais autorizados ao acesso, por data e hora do acesso, ou ainda, por período de data sendo que o usuário administrador pode escolher a data inicial e a data final.

Recebido em 08-12-2017 • Aceito em 27-02-2018

A consulta gerada pode ser transformada em relatório para impressão para que seja arquivada ou utilizada em caso de acessos indevidos citados anteriormente. Para que essa ação seja efetuada, basta ao usuário/administrador pressionar o botão relacionado a imprimir e o assistente irá exibir as configurações possíveis.

Para maiores detalhes das ações realizadas pelos usuários do protocolo, sugerimos ainda que seja implementado pela instituição um controle de monitoramento de acessos indevidos, desta forma, quando um acesso desse tipo ocorrer, a instituição pode tomar algumas atitudes rapidamente. Como o banco de informações de acesso via protocolo é liberado para quem tem o cadastro, o usuário/administrador pode ainda realizar suas consultas diretamente pelo seu sistema, apenas conectando a rede utilizada.

É possível gerar uma consulta/relatório das tentativas de acesso aos dados. Isso implica que se o médico ou profissional efetuar tentativas de acesso com uma senha errada ou de locais não autorizados, o protocolo armazena esses dados de forma a oferecer à instituição uma forma de controlar e, possivelmente, autorizar o acesso remotamente ao solicitante.

O próprio usuário (médico ou profissional) informa no momento do cadastro os locais de onde pretende realizar os acessos, conforme explicado anteriormente. Porém, em casos de acesso com urgência de outros locais, o mesmo será liberado via SMS e a instituição deve estar ciente disso. O relatório terá um *layout* sugerido conforme a **Tabela 4**:

**Tabela 4** – *Layout* de relatório de tentativas de acesso

| ID | Usuário | Data/Hora | Local |
|---|---|---|---|

## 2.6 Gerando SMS

Para que o protocolo possa liberar o acesso aos médicos ou aos profissionais cadastrados a partir de locais não pré-estabelecidos, o mesmo necessita de um mecanismo para gerar e confrontar um código que será enviado ao usuário. Esse código, conforme explicado anteriormente, terá a função de liberar o acesso, e trata-se de um conjunto de números inteiros sendo enviados através de um serviço de envio e entrega de dados.

Recebido em 08-12-2017 • Aceito em 27-02-2018

Esse serviço normalmente tem um baixo custo de envio que pode ainda ser oferecido gratuitamente por prestadoras de serviços de telefonia, e sua função é exclusivamente a entrega de mensagens de uma origem para um destino.

O uso do SMS no protocolo de rastreabilidade será para o envio de um código de cinco posições, por exemplo: 99999, que será enviado ao dispositivo solicitante via conexão de telefonia.

Durante a geração desse código, o mesmo será armazenado na tabela de acesso temporariamente até que o solicitante digite o mesmo em seu equipamento para liberação. Caso o usuário desista da operação ou ultrapasse o tempo limite de uma hora, o código será removido, devendo o médico ou profissional realizar um novo pedido.

Esse tipo de configuração poderá ser alterado pelo usuário/administrador, bem como o tamanho e o formato do código e seu tempo de validade. Pode ainda ser desabilitada a fim de reduzir os custos com telefonia. Dessa forma, a instituição pode gerar os códigos ou *tokens* de acesso como explicado anteriormente e informar os códigos gerados ao médico ou profissional, antecipadamente.

O usuário, por sua vez, deve administrar esses códigos para usá-los em momentos onde a localização for diferente das informadas na liberação de seu acesso.

O serviço de SMS é criptografado e estará atrelado à identificação do usuário. Isso significa que, caso seja interceptado por alguém mal-intencionado, o mesmo será inútil sem os demais dados de acesso.

Para que o protocolo faça uso de envio de mensagens SMS, é necessária a utilização de uma API onde deve ser informado qual a prestadora do serviço bem como o endereço do *Webservice* ou *Gateway* responsável pelo plano de entrega das mensagens e isso pode ser acoplado no protocolo através da interface de configuração.

## 2.7 JSON - Notação de Objetos JAVASCRIPT

Nesse subitem apresentamos a estrutura do arquivo de transição dos dados entre o cliente *mobile* e o servidor na rede. Na **Figura 1**, ilustramos um exemplo do *Parse*[3] a ser utilizado em cada comunicação.

[3] Parse – fragmento textual para analisador sintático

Recebido em 08-12-2017 • Aceito em 27-02-2018

**Figura 1** – Arquivo JSON

```
{"Envio":[
{"ID": 1,
"Usuário": "Dr. House",
"Date": "10/02/2016",
"Local": "Instituição",
"Longitude": "25,67",
"Latitude": "48,99",
"Solicitante": "Dr. House",
"Ação": "Consulta Imagem",
"Paciente": "Fulano de tal",
"Contador": 1}
] }
```

O JSON foi escolhido por possuir um formato de arquivo considerado mais leve para o tráfego de dados, ou seja, utiliza menos *bytes* na comunicação e isso faz muita diferença quando podemos ter inúmeros usuários utilizando uma mesma aplicação.

O JSON é bastante flexível e permite sua leitura por qualquer uma das linguagens atuais de programação. Isso significa que, independente do sistema utilizado, a captura e o retorno dos dados serão possíveis de serem efetuados. Esse formato possui ainda a possibilidade de trabalhar com os dados cifrados, tanto na origem quanto no destino, e por se tratar de uma estrutura simples não afeta o desempenho do protocolo.

O arquivo ilustrado anteriormente na **Figura 1** mostra a facilidade de entendimento desse tipo de arquivo, onde os campos são separados por dois pontos de seus conteúdos e esses, por sua vez, apenas separados por vírgula. Caso seja necessária a inclusão de um novo campo, basta inclui-lo entre as vírgulas ou no final do arquivo, apenas colocando um nome que ainda não foi usado, isso facilita muito na manutenção. O protocolo foi feito com base na arquitetura REST[4] que permite o uso do JSON[5] como forma de transmissão e recebimento dos dados trafegados.

[4] REST - *Representational State Transfer* (REST), em português Transferência de Estado Representacional

[5] JSON - um formato leve para intercâmbio de dados computacionais

Recebido em 08-12-2017 • Aceito em 27-02-2018

### 2.8 Investimento

Sabe-se que as instituições de saúde estão sempre precisando de recursos para conseguir atender à demanda do atendimento de seus pacientes, isso em qualquer lugar do mundo. No Brasil, este cenário é ainda pior, centenas de pessoas sofrem em filas enormes nas unidades de saúde em busca de um médico ou profissional da área para resolver seus problemas. Este artigo levantou todos esses problemas para que o protocolo de rastreabilidade pudesse ser criado, no intuito de auxiliar e justificar sua necessidade frente a todas as dificuldades apontadas.

É sabido também que os recursos destinados a ferramentas geradoras de informação são poucos e que os investimentos em segurança das informações são menores ainda. Como citado no inicio desse artigo, o objetivo desse protocolo é oferecer uma forma de colaborar com a segurança dos dados dos pacientes, utilizando dispositivos móveis do próprio interessado pelas informações. Isso significa que o custo na utilização do protocolo não acarretará custos à instituição no âmbito de equipamentos, ou seja, a mesma não irá ter que gastar com os equipamentos de acesso além da sua infraestrutura, ficando esse custo a cargo dos médicos ou profissionais da saúde através de seus dispositivos *mobile*.

Na introdução, afirmamos que o acesso a partir de equipamentos moveis oferecido pelas instituições não atende em termos de segurança da informação e fica muito claro que o acesso do PR1 foi criado também para smartphones ou *tablets*, que são dispositivos móveis e que a maioria das pessoas já possuem e que dessa forma, a instituição apenas investe nesse tipo de equipamento se quiser oferecer como um incentivo ao uso, mas não se torna um investimento obrigatório.

## 3. RESULTADOS E DISCUSSÃO

Existem inúmeras justificativas para se investir nas soluções em nuvem e, com a implementação desse protocolo, pode-se perceber alguns fatores que merecem destaque. Uma solução local exige investimentos em servidores de armazenamento, infraestrutura de rede, enquanto que numa aplicação disponibilizada em nuvem fica-se livre desse ônus, sem mencionar o custo envolvido na manutenção dos ativos ao longo do tempo.

A facilidade em gerenciar todas as informações de um único lugar e a não necessidade de licenças de *software* para cada usuário em seus dispositivos móveis também se mostrou um diferencial muito importante, ou

Recebido em 08-12-2017 • Aceito em 27-02-2018

seja, o fato dos dados do protocolo estarem centralizados e disponibilizados para acesso em qualquer lugar permite o uso das tecnologias móveis para os mais variados serviços.

Um usuário pode ser adicionado pela instituição com muita facilidade, apenas criando uma nova conta e configurando as permissões adequadas e o acesso do mesmo pode ser garantido através de qualquer dispositivo, mediante acesso à *Internet*, *smartphones* ou *tablets*, por exemplo, e o pessoal de TI não precisa se preocupar com atualizações de *software* ou elementos de segurança local, tais como antivírus e *firewall*.

Problemas de segurança local que poderiam afetar a empresa inteira são descartados, a aplicação disponibilizada pode conter algoritmos para tal.

O algoritmo de localização implementado no protocolo permitiu que os acessos partissem dos locais certos, previamente informados, garantindo que era mesmo o médico ou um profissional autorizado quem acessava os dados de seu paciente.

O protocolo criado se mostrou muito importante, principalmente quando o acesso é remoto, ou seja, o usuário busca informações do sistema na nuvem (*cloud)* e o protocolo checa se o mesmo é autêntico e, ao mesmo tempo, grava suas informações de acesso, bem como as ações realizadas.

Este protocolo não é o único na área da segurança da informação, mas sem dúvidas acrescenta quando combinamos monitoramento de acessos médicos usando a *Cloud* como base.

Sendo assim, considera-se o início de um novo ciclo de confiança da área da saúde ao disponibilizar seus dados usando a *Internet* como base de conexão, algo que dificilmente era realizado desta forma até então. Os métodos empregados para realizar a implementação do PR1 foram escolhidos pensando ao mesmo tempo em utilizar tecnologias de ponta e recursos simples e acessíveis a qualquer desenvolvedor.

As ferramentas utilizadas para implementação são facilmente encontradas de forma gratuita na *Internet*, por exemplo, o *Android*, JSON, Linguagem Java, entre outras. A ideia é que o desenvolvedor implemente sua própria solução com base nesse protocolo.

Durante o desenvolvimento foram encontrados alguns problemas, por exemplo na escolha do melhor e mais acessível formato para o pacote de tráfego do protocolo proposto. Nesse caso, havia a necessidade de as informações serem de um formato universal, ou seja, que qualquer desenvolvedor pudesse criar uma ferramenta de *software* e pudesse ler esse conteúdo. A escolha foi o formato JSON, considerando que o mesmo oferece essa universalidade fundamental para o sucesso do protocolo.

Recebido em 08-12-2017 • Aceito em 27-02-2018

Alguns testes com o protocolo foram realizados e seus resultados foram considerados satisfatórios. Percebeu-se que durante esses acessos o mesmo efetuou as gravações de acesso e localização de forma correta, comprovando sua capacidade em um cenário de 56 acessos simultâneos, o que implica mais de 50 profissionais ou médicos acessando o protocolo simultaneamente, o que equivale aos profissionais de uma cidade de pequeno porte. O resultado dessa ação é que possibilitou a execução efetiva do protocolo e a percepção de seu funcionamento. Porém, os dados obtidos na fase de testes não podem ser aqui apresentados pela sigilosidade exigida pela própria norma HIPAA.

O protocolo mostrou-se estável na nuvem, apesar de terem sido realizados poucos acessos se comparado a um ambiente real de uma instituição.

A seguir, apontam-se algumas vantagens que foram constatadas na utilização deste protocolo:

- Identificar os usuários das informações, bem como as ações realizadas por eles;
- Oferecer os dados dos pacientes da forma mais atualizada possível;
- Saber a localização dos acessos realizados;
- Baixo custo de utilização do serviço, haja vista que o protocolo ocupa pouco espaço;
- Compatibilidade com dispositivos móveis;
- Atender às normas HIPAA.

Pretende-se, com esse protocolo, aumentar os níveis de segurança durante o acesso aos dados de pacientes e ainda oferecer a algumas instituições a possibilidade do uso das tecnologias *mobile* em seu benefício. Como foi dito anteriormente na introdução deste documento, é muito difícil para a administração de uma instituição confiar suas informações disponibilizadas na *Internet*. Sendo assim, esse protocolo visa também possibilitar esse acesso de forma um pouco mais segura, afinal, sabe-se que a total segurança não é possível de ser garantida.

## CONSIDERAÇÕES FINAIS

É determinante que os avanços tecnológicos interferem em nosso cotidiano e aproveitar desses recursos é primordial quando o assunto é o bem comum.

Com o uso do protocolo de rastreabilidade PR1, percebeu-se que é perfeitamente possível para uma instituição da área da saúde investir seus

Recebido em 08-12-2017 • Aceito em 27-02-2018

recursos em *Cloud Computing*, afinal a confiabilidade atrelada ao algoritmo ultrapassa os níveis de uma rede local. A disponibilidade da aplicação em algo parecido com a *Internet*, fomentando o uso de dispositivos móveis, colabora significativamente com os processos na busca dos diagnósticos corretos. A ideia de que um médico possa acessar os dados de um paciente de qualquer lugar agiliza o tratamento pois se antecipa o acesso à informação.

O fato de o trabalho indicar boas práticas com relação ao manuseio da informação também colabora com a comunidade de desenvolvedores, de forma a entender como é importante agir a fim de garantir a confiabilidade das instituições da área de saúde. O motivo é o desconforto que a área de saúde tem em saber que suas informações estão disponibilizadas em provedores de *Internet*. Portanto, garantir que as informações estão seguras em uma *Cloud* é um desafio que pretende-se desmistificar em trabalhos desse tipo. Para futuras pesquisas, deixamos inúmeras lacunas, principalmente frente aos avanços tecnológicos que podem surgir a partir desse advento. A *Cloud Computing* ainda tem muito a evoluir, assim como é o caso do protocolo de rastreabilidade, que pode ser ampliado e melhorado ao longo do tempo.

Há uma percepção na área da saúde de que as medidas de segurança nos sistemas não podem inibir a efetiva atenção ao paciente. É importante ainda destacar que jamais foi a intenção desse protocolo impedir que um paciente seja atendido.

**REFERÊNCIAS**

BELLA, G.. **Formal Correctness of Security Protocols**; Information Security and Cryptography. Berlin: Springer, 2007.

HAUCK, M. *et al*.. **Challenges and opportunities of cloud computing.** Karlsruhe Reports in Informatics 19, Karlsruhe Institute of Technology - Faculty of Informatics, 2010.

HE, Y.; JOHNSON, C.W.. Generic security cases for information system security in healthcare systems, in System Safety, incorporating the Cyber Security Conference 2012, **7th IET International Conference on**, vol., no., pp.1-6, 15-- doi: 10.1049/cp.2012.1507, 18 Oct. 2012.

HIPAA. **Health Insurance Portability Accountability Act.** Disponível em: <http://tn.gov/health/topic/hipaa >. Acesso em setembro 2015.

ISO/DIS 8601-1 . **Data elements and interchange formats**, Information interchange, Representation of dates and times, 2016.

JADEJA, K. M.. **Cloud computing -** concepts, architecture and challenges in International Conference on Computing, Electronics and Electrical Technologies [ICCEET], 2012.

Recebido em 08-12-2017 • Aceito em 27-02-2018

JOSHI, J.. **Network Security:** Know it all: Know it all**.** Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2008.

KAMALAKANNAN, E.; ARVIND, K. S.. .Privacy conserving and secure distribution of personal health information using cloud, in Information Communication and Embedded Systems (ICICES), 2014, **International Conference on**, vol., no., pp.1-4, 27-28 Feb. 2014.

MAISIE, W. *et al.* Personal health information management system and its application in referral management, in **Information Technology in Biomedicine,** IEEE Transactions on, vol.8, no.3, pp.287-297, Sept. 2004.

OMOGBADEGUN, Z. O.. Security in Healthcare Information Systems, in Information & Communications Technology, 2006. ICICT '06. ITI **4th International Conference on**, vol., no., pp.1-2, - doi: 10.1109/ITICT.2006.358263, 10-12 Dec. 2006.

ORANJE, V. *et al.*. **The Future of the Internet Economy:** a Discussion Paper on Critical Issues, Constantijn (Rand Europe), prepared for The Netherlands Ministry of Economic Affairs, Cambridge, UK, 12 February 2008.

RYAN, W. M.; LOEFFLER, C. M.. Insights into cloud computing. Intellectual. **Property & Technology Law Journal**, *22*(11),22-28. - 2010.

SARAVANAKUMAR, C.; ARUN, C.. Survey on interoperability, security, trust, privacy standardization of cloud computing. In: Contemporary Computing and Informatics (IC3I), 2014 **International Conference on. IEEE**, 2014. p. 977-982.

SELVAKUMAR, K.; SENDHILKUMAR, S.. Challenges and recent trends in personalized Web search: A survey. In: Advanced Computing (ICoAC), 2011 **Third International Conference on. IEEE**, 2011. p. 333-339.

SOBHY, D.; EL-SONBATY, Y.; ELNASR, M. A. . MedCloud: healthcare cloud computing system. In: Internet Technology And Secured Transactions**, 2012 International Conference for. IEEE**, 2012. p. 161-166.

USD (United States Department) of Health and H. Services, **Summary of Hipaa Privacy Rule**, Office for Civil Rights, 200 Independence Avenue, S.W. Washington, D.C. 20201, May 2003.

XUE, Y. . Research on privacy preservation of patient as main body in personal health information system. In: **Intelligent Human-Machine Systems and Cybernetics (IHMSC), 2014 Sixth International Conference on. IEEE**, 2014. p. 226-229.

ZANDIEH, S. O.; KAHYUN, Y. F.; KUPERMAN, G. J. *et al.*. **Challenges to EHR implementation in electronic versus paper-based office practices.** J Gen Intern Med. 2008.

Recebido em 08-12-2017 • Aceito em 27-02-2018