[www.reciis.cict.fiocruz.br]
e-ISSN 1981-6278

Artigo original

Uma aplicação de biometria na web voltada para planos de saúde

DOI: 10.3395/reciis.v4i5.333pt

Antonio Idelvane Santana Silva
Instituto Federal de Educação, Ciência e Tecnologia do Piauí (IFPI) e Infoway Tecnologia e Gestão em Saúde Ltda, Teresina, Brasil
idelvane@infoway-pi.com.br

Ney Paranaguá de Carvalho
Instituto Federal de Educação, Ciência e Tecnologia do Piauí (IFPI) e Infoway Tecnologia e Gestão em Saúde Ltda, Teresina, Brasil
ney@infoway-pi.com.br

Pedro de Alcântara dos Santos Neto
Departamento de Informática e Estatística (DIE), Universidade Federal do Piauí (UFPI), Teresina, Brasil
pasn@ufpi.edu.br

Resumo

Biometria cada vez mais vem sendo adotada no reconhecimento de pessoas. É o recurso que possibilita realizar o reconhecimento de uma pessoa por suas características físicas (íris ocular, impressão digital, face) ou por seu comportamento (voz, assinatura). Ela pode ser empregada nos mais diferentes lugares para o reconhecimento de indivíduos, sendo a Web um dos seus grandes focos de atuação atualmente. Criar um sistema biométrico Web é uma tarefa que envolve um estudo detalhado dessa plataforma. Questões de segurança, usabilidade e ambiente do cliente devem ser levadas em consideração desde o início do projeto. O presente trabalho fornece uma visão de como funciona um sistema biométrico Web, abordando aspectos técnicos e operacionais para sua implementação e implantação. Além disso, é apresentado um estudo de caso de uma solução biométrica para um plano de saúde gerenciado pela Web, bem como uma visão geral de como foi realizada essa implantação.

Palavras Chaves

biometria; gestão de planos de saúde; sistema de informação; autenticação; sistema biométrico Web

A popularidade da Internet trouxe cada vez mais abrangência aos serviços ofertados nesta plataforma, o que aumentou cada vez mais a necessidade de se identificar e autorizar o acesso a uma pessoa. Muitas aplicações web necessitam manter seguras suas informações ou serviços. Para isto muitas técnicas são desenvolvidas no intuito de manter seguros tais sistemas. As técnicas clássicas para a autenticação de uma pessoa apresentam alguns problemas, como por exemplo, o uso de senhas está sujeito a interceptação por terceiros, compartilhamento ou esquecimento. Apesar dessa técnica estar amplamente desenvolvida, ela não garante totalmente a assertividade quanto à identidade de uma pessoa, tendo como base a fraquezas do método. Em decorrência desses fatos, está sendo cada vez mais difundido o conceito de biometria utilizada em sistemas web.

A Biometria é o recurso que possibilita identificar pessoas por suas características físicas, como por exemplo, íris dos olhos, impressão digital ou comportamentais, como voz, assinatura, que definem a sua individualidade (COSTA, 2001). A autenticação biométrica ocorre em duas fases: primeiramente é feita a captura da característica biométrica do usuário para que esta possa ser utilizada em sua autenticação. Após a captura é realizada uma conversão desta característica para um modelo matemático, conhecido como *template,* o qual é submetido para autenticação. A segunda fase é a autenticação, na qual o usuário apresenta a característica biométrica para que seja comparada e validada com o modelo armazenado.

A utilização da biometria em sistemas web requer um estudo minucioso das peculiaridades desta plataforma:

- Desempenho – diz respeito à velocidade com que é feita a autenticação da pessoa, considerando-se a transmissão dos dados com informações do indivíduo;
- Facilidade de uso – uma boa interface é fundamental para uma aplicação web que utilize biometria, visto que esta funcionalidade não pode agregar mais complexidade ao sistema. Uma interface concisa e interativa é uma alternativa para este quesito;
- Ambiente do usuário – restrições no ambiente cliente devem ser analisadas. Realizar o levantamento sobre qual sistema operacional e hardware utilizado no cliente para evitar incompatibilidades com o software utilizado no reconhecimento da característica biométrica é de grande valia no processo de implantação do sistema biométrica na aplicação web.

A biometria, no contexto Web, possui vários tipos de aplicações (COSTA, 2007). Neste trabalho será apresentada uma abordagem para um sistema de plano de saúde. Para tanto foi desenvolvida uma aplicação em Java na Web que procura atender aos requisitos desta plataforma, bem como aos anseios do plano de saúde ao qual foi desenvolvida. O trabalho está dividido da seguinte forma: a Seção 2 apresenta os principais conceitos de biometria; na Seção 3 é detalhada uma forma de implementar uma solução biométrica para a plataforma web; na Seção 4 é apresentado um estudo de caso de utilização de biometria em uma aplicação para um plano de saúde na web; a Seção 5 mostra os trabalhos futuros e Seção 6 apresenta a conclusão do trabalho.

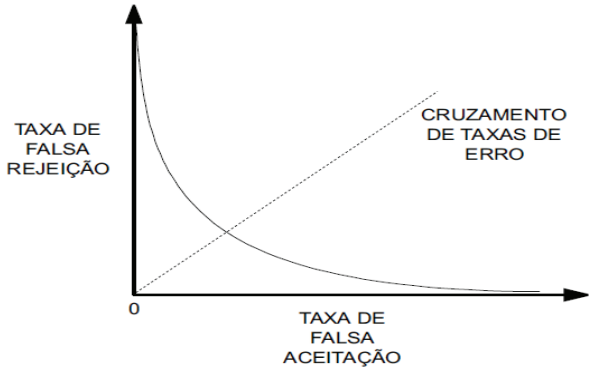
Biometria

A Biometria refere-se ao uso de características de um indivíduo para sua autenticação perante um sistema de informação (LIU *et al.,* 2001) (JAIN *et al.*, 2008). Com a biometria o indivíduo passa a ser seu próprio mecanismo de autenticação. No que diz respeito à biometria, existem duas formas diferentes de se fazer autenticação de uma pessoa:

- Verificação: é o processo biométrico que vai determinar a validade de uma identidade apresentada. Conceitualmente isso pode ser entendido como o processo que compara um a um (1:1) a amostra da característica biométrica apresentada, *template*, com a outra amostra biométrica que foi registrada, para determinar se são do mesmo indivíduo. Por exemplo: é feita a captura da impressão digital do polegar direito de uma pessoa. No processo de verificação, ele apresenta sua digital do polegar direito para comparação com aquele que foi armazenado anteriormente. Como resultado, pode-se haver duas respostas: sim, é a mesma pessoa, ou não, são pessoas distintas;
- Identificação: é o processo biométrico que identifica um indivíduo, por suas características biométricas, dentro de uma base de dados registrada. Esse é um processo de comparação de um para muitos (1:N), onde se apresenta uma amostra da característica biométrica e, busca-se em uma base de *templates* biométricos, qual indivíduo pertence aquela amostra. Como resultado, tem-se uma resposta: um indivíduo validado a partir do *template* fornecido. Esse processo pode ser mais lento que o de verificação, visto que é necessário fazer a comparação com vários *templates* cadastrados.

Existem hoje muitas características utilizadas, isoladamente ou em conjunto, para verificar e/ou autenticar um sujeito. Cada método pode ser avaliado através de vários parâmetros: grau de fiabilidade, nível de conforto, nível de aceitação e custo de implementação. O grau de fiabilidade diz respeito à confiança que o método de autenticação biométrica transmite. Ele pode ser aferido levando em conta a FAR (*False Acceptance Rate* – Taxa de Falsa Aceitação, ou falso positivo), que é o percentual de chance de um intruso acessar o sistema, e o FRR (*False Rejection Rate* – Taxa de Falsa Rejeição, ou falso negativo), que diz respeito ao percentual de um usuário cadastrado não ser reconhecido. Porém, essas variáveis são mutuamente dependentes, não sendo possível reduzir o valor de ambas. Desta forma, procura-se o ponto de equilíbrio chamado de CER (*Crossover Error Rate* – Taxa de Intersecção de Erros) (LIU *et al*., 2001). Quanto mais baixo for o CER, mais preciso o sistema biométrico. A Figura 1 apresenta a relação entre as variáveis responsáveis por definir o grau de fiabilidade de uma tecnologia de autenticação biométrica.

Figura 1 – Taxas de erros associadas a sistemas biométricos.



Fonte: KAZIENKO, 2003.

O nível de conforto é uma medida subjetiva que denota o quão prático é a tecnologia escolhida para autenticação biométrica. O nível de aceitação, também subjetivo, está relacionado ao grau de intrusão da tecnologia. Um sistema biométrico será mais aceito quanto menos intrusivo ele for.

O custo de implementação diz respeito a toda a estrutura

de hardware, software e pessoas (engenheiros de software, pessoal de suporte), envolvidas no processo de implantação da biometria em um determinado sistema (LIU *et al.*, 2001).

Tecnologias de Autenticação Biométrica

Reconhecimento facial

Para reconhecer uma face, os sistemas mapeiam a geometria e as proporções do rosto. Posteriormente, são extraídos e registrados os pontos delimitadores na face, sendo definidas proporções, distâncias e formas de cada elemento do rosto – boca, nariz, olhos, sobrancelhas, etc. Isso permite que seja realizada a comparação (VIGLIAZZI, 2003). As principais medidas analisadas são:

- Distância entre os olhos;
- Distância entre a boca, nariz e olhos;
- Distância entre olhos, queixo, boca e linhas do cabelo.

No reconhecimento facial os problemas são essencialmente ocasionados por diferentes orientações da cabeça da pessoa, visto que a mesma está em posição livre (POH *et al.,* 2001).

Leitura da íris

A íris apresenta diversas características que podem ser utilizadas para realização do reconhecimento biométrico. As principais são o fato de seu tecido ter uma imagem muito complexa e possuir uma forma radial. Essa forma radial proporciona à íris 266 graus livres, número de variações que permitir distinguir íris diferentes (VIGLIAZZI, 2003). O fato de a íris estar protegida atrás da córnea, diminuindo riscos de danos ao tecido e de não está sujeita aos efeitos do envelhecimento, permite um padrão biométrico estável até a morte.

Reconhecimento da voz

A autenticação biométrica pelo reconhecimento da voz é baseada no fato de que as características físicas de indivíduo implicam à sua voz características únicas. O aspecto físico mais relevante é a forma do intervalo vocal, que é composto por todos os órgãos e cavidades que participam da produção da fala (MAGALHAES, 2003).

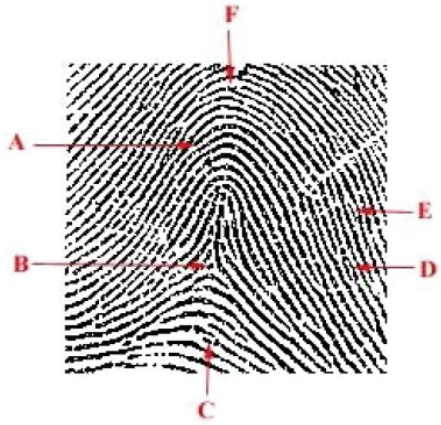
A captura do som se dá através de um microfone. Assim, é necessário que o usuário pronuncie uma frase ao microfone, repetindo-a até que seja extraído um padrão harmônico, que é armazenado. Os padrões da fala em momentos diferentes resultam similaridade, mas com vetores característicos diferentes.

Impressão digital

As impressões digitais, ou simplesmente digitais, são desenhos formados pelas dobras cutâneas das polpas dos dedos das mãos e dos pés. Estão localizadas na derme (tecido que constitui a parte mais profunda da pele, constituindo sua parte fundamental; situada sob a epiderme) e se reproduzem na epiderme (membrana fina e transparente que recobre externamente a derme), gerando diversos formatos (VIOLA, 2006).

O método que permite a identificação de pessoas pela comparação das impressões digitais é chamado de datiloscópico. O termo datiloscopia é formado pelos elementos gregos: *Daktylos* que significa dedos e *Skopein* que significa examinar, sugerindo, portanto, o estudo dos dedos, ou das impressões digitais (VIOLA, 2006). Em relação a sua constituição, as linhas que compõem a impressão digital podem ser ditas paralelas, considerando uma determinada orientação, e se as analisarmos em uma vizinhança local a um dado ponto. Essas linhas possuem perturbações locais, que originam deformações chamadas minúcias (REIS, 2003). Na Figura 2 são mostrados os tipos de minúcias utilizados durante o processo de reconhecimento por impressão digital.

Figura 2 – Tipos de minúcias



A = Terminação, B= Ilha, C= Espora, D= lago, E= crista independente, F= bifurcação.
Fonte: REIS, 2003.

As minúcias servem de parâmetro para a maioria dos algoritmos que comparam impressões digitais e não se alteram ao longo da vida da pessoa, a não ser que o dedo sofra danos que comprometam a integridade da epiderme. As peculiaridades da impressão digital são extraídas por um leitor de impressão digital e armazenadas, podendo haver, dessa maneira, comparação (VIGLIAZZI, 2006). O processo de comparação, ou *matching*, verifica qual é o grau de similaridade entre as características extraídas da amostra do usuário e o perfil armazenado previamente. Esse processo

fornece uma pontuação (*score)* representativa da semelhança entre os dois conjuntos de dados. Caso a similaridade seja superior a certo limite previamente determinado, conhecido como limiar, ou *threshold*, a decisão é autorizar o acesso do usuário, ou seja, a autenticação foi validada. Caso a similaridade seja inferior ao limiar, a decisão é não autorizar o acesso do usuário (REIS, 2003).

O processo de reconhecimento através da impressão digital é o mais amplamente conhecido e utilizado atualmente. As principais razões para a escolha desse método são (COSTA, 2007):

- Confiabilidade: a possibilidade de falha é mínima, visto às características inerentes de cada pessoa;
- Baixo custo: os leitores de impressão digital possuem um dos menores custos em relação aos leitores das outras tecnologias;
- Baixo nível de intrusão: exige apenas que o usuário pressione o leitor de impressão digital (leitor biométrico ou scanner);
- Familiaridade: a impressão digital já vendo sendo colhida há anos para os mais variados fins, isso aumenta o grau de aceitabilidade da autenticação por impressões digitais.

Autenticação em sistemas web

Quando se desenvolve uma aplicação para web, deve ser atentado um pré-requisito muito importante, a segurança. Na tentativa de cumprir com esse pré-requisito foram criados vários mecanismos para este fim. Dentre eles, o mais conhecido é a utilização de senhas e/ou palavras chaves para autenticação das pessoas (COSTA, 2007). Ao informar sua senha e/ou palavra de chave de acesso, o usuário do sistema web é comparado com um registro encontrado no banco de dados e é realizada sua validação. Esse processo de autenticação através de senhas pode ser falho por inúmeros motivos, como por exemplo: roubo de senhas, senhas fracas, mau uso das senhas (uso sem preocupação de interceptação de terceiros).

Outra abordagem é o uso de *smart cards,* que identificam o indivíduo através de um chip que possui um microprocessador. Os *smart cards* possuem instruções que autenticam um usuário através de um PIN (*Personal Identificator Number*) (MAGALHAES, 2003) (FERREIRA *et al*., 2006). O problema com os *smart cards* é que os mesmos podem ser clonados ou roubados, o que pode provocar uma falha de segurança para o processo.

A biometria aplicada a sistemas Web possibilita uma maior segurança que os métodos anteriores quando usada corretamente (COSTA, 2007). Levando em consideração que o custo para falsificação de uma característica física ou comportamental é bastante elevado, a biometria possibilita uma boa alternativa para validação de usuários de um sistema web.

Biometria para sistemas web

Durante o desenvolvimento do sistema biométrico para uma aplicação web, deve-se atentar a questões de desempenho, facilidade de uso da aplicação e condições adversas no ambiente do usuário final. No desenvolvimento web existem duas tecnologias que possibilitam o desenvolvimento de uma aplicação que utilize biometria: *ActiveX* (FARRAR, 2001) e *Applets* Java (DEITEL *et al.*, 2005).

ActiveX é uma especificação desenvolvida pela Microsoft que permite aos programas Windows comuns executar dentro de uma pagina da Web, os programas ActiveX podem se escritos em linguagem como Visual Basic, Visual C++. Ele está presente tanto no lado do servidor quanto do cliente em uma aplicação Web. Os componentes escritos para *ActiveX* são executados no cliente e possuem privilégios de acesso aos recursos de hardware e software do mesmo.

ActiveX permite a criação de páginas web com conteúdo ativo, que interagem com o usuário final. Possuem uma grande variedade de componentes previamente desenvolvidos que podem ser integrados facilmente a outras aplicações web e possuem duas grandes vantagens: 1) o *download* dos componentes *ActiveX* é feito de modo automático, sendo que esse processo ocorre uma única vez; 2) seus componentes possuem acesso aos recursos do sistema operacional Windows que exista no cliente, possibilitando a utilização de vários recursos de software e hardware. O acesso direto aos recursos facilita a integração entre o hardware utilizado para a leitura da característica biométrica e a aplicação web que utiliza *ActiveX.*

Esse acesso direto ao SO do usuário final, constitui, também, uma grande desvantagem ao *ActiveX*, pois possibilita a ação de alguma pessoa má intencionada. Para que isso ocorra, um código malicioso é escrito de forma a ser executado no momento da ação do componente *ActiveX.* Com isso podem ser escritos programas que apagam dados do HD (*hard disk)* do cliente ou até formatar a máquina. Outra desvantagem do *ActiveX* é que ele é particular ao Internet Explorer da Microsoft, portanto dificultando a portabilidade das aplicações desenvolvidas com essas tecnologia.

A outra tecnologia possível para implementação de um sistema web é baseada em *Applets* Java. Um *applet* é um tipo especial de programa que é "baixado" da Internet e executa no navegador do usuário final da aplicação. Ele tipicamente está embutido em uma página Web. Ao contrário dos componentes *ActiveX*, os *applets* não possuem permissão para acessar os recursos da máquina do cliente facilmente, visto que os mesmos são executados de forma separada dos outros processos do navegador através de um mecanismo chamado *sandbox,* cuja tradução é caixa de areia (DEITEL *et al.*, 2005). O *sandbox* refere-se ao conjunto de restrições de segurança impostas sobre o *applet*. Ele existe para prevenir ações de potenciais códigos perigosos que possam ser executados na máquina cliente.

Uma das vantagens de se ter um *applet* como tecnologia empregada para um sistema que usa biometria, é que eles, por serem desenvolvidos em Java, são multiplataforma e possuem um alto nível de segurança, características da linguagem. Porém, os *applets* apresentam algumas desvantagens: 1) possuem grande dificuldade para se adequarem às necessidades das aplicações RIA (*Rich Internet Applications*), devido a, por exemplo, sua baixa performance na inicialização (DEITEL *et al.*, 2005); 2) a cada vez que a página web é carregada, deve ser feito o *download* do *applet* pois eles não permanecem em *cache;* 3) o fato de serem executados no *sandbox* proíbe o *applet* a ter acesso ao sistema de arquivos ou iniciar algum processo no cliente, no entanto pode-se autorizar o acesso a alguns recursos através de sua assinatura com um certificado digital.

Implementação

No desenvolvimento de sistemas biométricos normalmente é utilizado um SDK (*Software Development Kit*), ferramenta para captura e casamento de padrões para determinada tecnologia biométrica. Para o trabalho em questão, foi escolhido o *software* proprietário da empresa Griaule Biometrics, o *Fingerprint* SDK (*Software Development Kit*) 2009 (GRIAULE, 2009).

O *Fingerprint* SDK 2009 é oferecido em duas versões: o *Fingerprint* SDK para *Windows* que suporta várias linguagens de programação Windows via DLL (*Dinamic Link Library*) ou *ActiveX*, e o *Fingerprint* SDK Java que permite o desenvolvimento de programas Java multiplataforma com acesso a dispositivos biométricos. A comunicação com o leitor biométrico ocorre através de bibliotecas que devem ser instaladas na máquina cliente. Tais bibliotecas são facilmente instaladas através da execução de instaladores criados tanto para Windows (Fingerprint_SDK_2009_Installer.exe) quanto para Linux (Fingerprint_SDK_Java_2009_*Installer*.jar) (GRIAULE, 2009).

Outra característica importante do SDK escolhido é que o mesmo proporciona uma comunicação com um número razoável de leitores biométricos, o que possibilita um melhor discurso quanto à preocupação com os custos do cliente.

Existem duas maneiras de se integrar a ferramenta com uma aplicação Web desenvolvida em Java (GRIAULE, 2009):

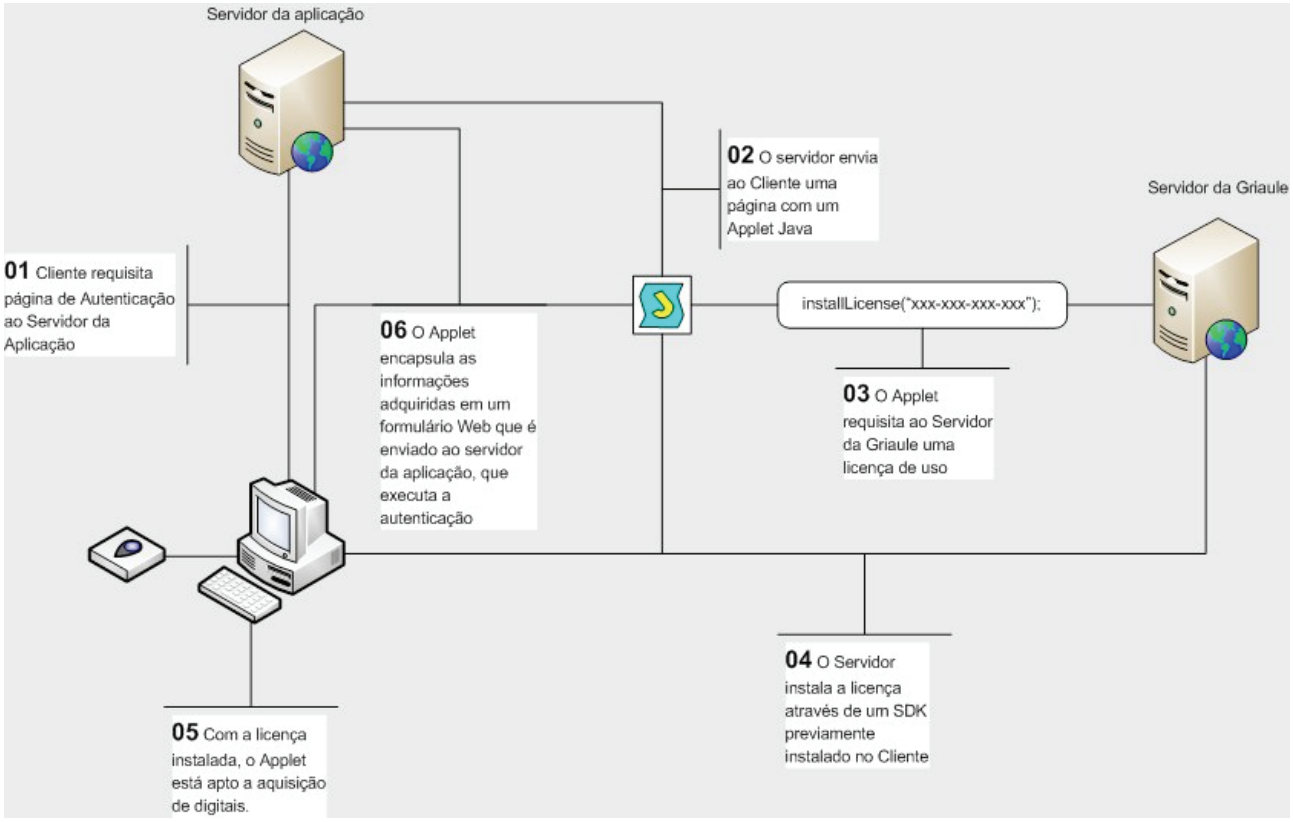
- O cliente envia a imagem da digital convertida em um *array* de bytes, que foi captura pelo *applet*, para o servidor, que possui a aplicação que de fato usa o SDK. Esta aplicação faz o que tem que ser feito com a impressão digital recebida, como por exemplo: armazena em banco de dados, compara com outra armazenada, extrair template (realizar cálculos a partir da imagem da digital), etc.;

- A segunda opção é deixar toda a responsabilidade do processo de reconhecimento no *applet*. Ele será responsável pela captura, extração do template e comparação da digital, acessando somente o banco de dados do servidor. Esse método possui desvantagens, pois o banco de dados precisa ser visível ao cliente e o *applet* precisa possuir permissões de acesso sobre a máquina cliente, enquanto na primeira opção somente o servidor precisa ser visível.

A primeira opção apresentada foi escolhida por oferecer maior segurança (não expõe o servidor) e exigir menos das máquinas clientes. Para que não ocorram problemas durante a execução do *applet*, é necessário que o *jar (Java archive)* contendo as classes do SDK responsável por comunicação com o leitor biométrico esteja "assinado" com um certificado digital, no modelo chave pública e privada, para garantir a sua origem promovendo maior segurança (DEITEL *et al.*, 2005). A assinatura do *jar* pode ser feita através da ferramenta *keytool* que vem inclusa dentro do próprio SDK da *Sun* (DEITEL *et al.*, 2005). Caso a aplicação tenha fins comerciais, faz-se necessário a contratação de uma entidade certificadora para a compra de um certificado para o *applet*.

A Figura 3 demonstra como funciona o processo de autenticação/licenciamento. No momento da carga do *applet* é realizado o licenciamento da máquina do cliente pelo SDK, para tanto é feito o acesso ao servidor Web da *Griaule* para geração do arquivo de licenciamento da máquina cliente. Realizada essa etapa, o *applet* aciona o leitor que captura a digital em forma de um *array* de *bytes*. A digital capturada é submetida ao servidor da aplicação através de um formulário web. De posse da informação capturada, pode-se realizar as operações de armazenamento de *template* em banco de dados ou comparação com um registro existente.

Figura 3 – Processo de autenticação/licenciamento.



Fonte: Elaborado pelos autores.

Implantação

Durante o levantamento bibliográfico não foram encontradas referências que demonstrassem o processo de implantação de um sistema biométrico para plataforma Web. Esse fato denota a importância do trabalho em questão por seu caráter inovador.

Ao se realizar a implantação da aplicação Web que utiliza biometria, os aspectos listados a seguir devem ser observados:

Submeter o template capturado através de postback - o postback é a medida tomada por uma página web interativa onde a página e seu conteúdo são enviados ao servidor da aplicação para o processamento de informações, sendo que a mesma página é retornada como resultado (DEITEL *et al.*, 2005). Esse mecanismo favorece a comunicação do *applet* como servidor sem que haja a interceptação dos dados colhidos. Ele é necessário devido o fato de existirem barreiras criadas nas máquinas clientes para dificultar o envio e/ou recebimento de informações não autorizadas pelo mesmo, um exemplo disso são os *firewalls*.

Tornar a interface interativa – um dos aspectos mais importantes a ser levado em consideração no desenvolvimento de uma aplicação Web é a interação com o usuário. Após a captura da digital, é interessante apresentar ao usuário a imagem da digital capturada, isso comunica o usuário que a digital foi capturada com sucesso, além de um botão que comunique a idéia de envio da imagem.

Adequar parâmetros de comparação – o *threshold*, limiar estabelecido para determinar se a amostra da digital colhida e a recuperada para a comparação são da mesma pessoa, deve ser minuciosamente estudado para que sejam evitados constrangimentos por não reconhecimento do usuário do sistema. O valor estabelecido afeta diretamente as taxas de falso positivo e falso negativo.

Possibilitar o armazenamento da característica biométrica utilizada no processo – a informação sobre qual dedo, olho ou mão foi utilizado no momento da aquisição da característica biométrica a ser utilizada no processo é fundamental para que seja facilitado o manuseio do sistema biométrico. Essa ação fornece um apoio ao operador do sistema no ato da autenticação, pois possibilita ao mesmo informar ao usuário qual dedo, por exemplo, colocar no dispositivo.

Simular o ambiente do cliente – é de fundamental importância testar a aplicação nos mais diferenciados ambientes. Ao realizar este procedimento, será possível estabelecer requisitos mínimos para execução do sistema biométrico no cliente, como por exemplo, qual SO é compatível e qual versão do JRE deve ser utilizada. Outro teste

a ser realizado é o de compatibilidade com outras soluções biométricas, como controle de ponto dos funcionários, que o cliente possa ter.

Dificuldades

Durante o processo descrito na seção anterior algumas dificuldades podem ser encontradas. Tais dificuldades podem ser classificadas de acordo com o local onde ocorrem:

No cliente: dificuldades de instalação de dependências no cliente.

Máquinas desatualizadas e/ou com restrição de execução de aplicativos são empecilhos para processo como um todo. Outro grande problema é a incompatibilidade com softwares de reconhecimento biométrico de outros fornecedores. A fim de solucionar estes problemas deve-se estabelecer uma especificação mínima para máquinas clientes e realizar testes com outros sistemas biométricos que porventura o cliente utilize.

Na aplicação: baixa performance na carga do applet.

Atualmente quando se desenvolve uma página Web que possui um *applet*, tem-se que esperar que o usuário final possua a versão mais atualizada da JRE (*Java Runtime Environment*) ou pelo menos a versão para que o *applet* foi desenvolvido. Este problema constitui uma das principais fontes de frustração no desenvolvimento de um *applet*, pois não importa o quão bem projetado o mesmo seja, sempre ocorrerá o problema da desatualização do JRE do cliente ou até mesmo a falta da JRE. Na maioria das vezes a primeira carga do *applet* é muito demorada, devido à inicialização da JVM (*Java Virtual Machine*). A baixa performance na inicialização da JVM é conhecida como *Java Cold Start,* que provoca uma péssima experiência do usuário quanto ao uso de *applets*. Com intuito de resolver esse problema, foi criado o novo *Java Plug-in* e o *Java Deployment Toolkit* a partir da versão Java SE 6.0 *update* 10 (DEITEL *et al.*, 2005). O *Java Deployment Tookit* consiste de um conjunto de funções *JavaScript* para evitar incompatibilidades com navegadores no cliente e agilizar a instalação da aplicação que contenha um *applet* ou aplicação *Java Web Start* (DEITEL *et al.*, 2005).

Estudo de Caso: Iapep Saúde

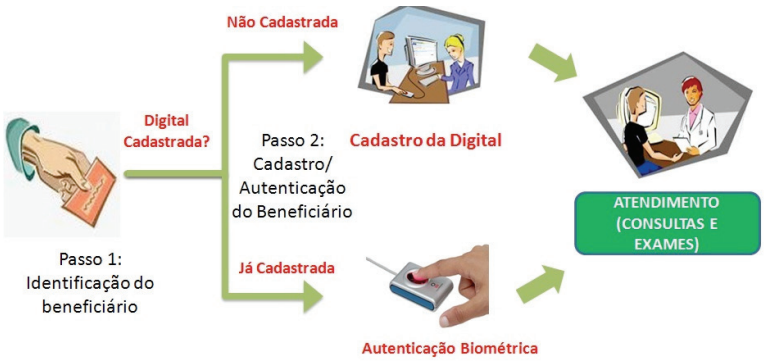
O IAPEP Saúde é o plano de saúde do Instituto de Assistência e Previdência do Estado do Piauí. Criado em janeiro de 1966, com a missão de prestar serviços que visem à proteção à saúde e o bem estar dos servidores do Estado do Piauí. Diante desta premissa, o IAPEP Saúde, hoje, é responsável em garantir qualidade e pontualidade a serviços assistências de saúde a uma população de 171 mil segurados.

A quantidade de atendimentos no IAPEP Saúde é superior aos demais planos de saúde com atuação no Piauí. Por mês, a média de atendimento é de 30 mil consultas e de 70 mil exames em todas as especialidades médicas e odontológicas, inclusive as com tratamento contínuo, como psicologia, fisioterapia, hidroterapia, nutrição, acupuntura e fonoaudiologia.

Biometria no sistema web

Na tentativa de oferecer maiores garantias a respeito da identidade dos segurados do plano e, com isso, combater as fraudes por falsidade ideológica, foi desenvolvido um sistema biométrico que foi integrado ao sistema de informação web do IAPEP. O processo de identificação do segurado foi modificado com a adição do requerimento da digital do segurado. A estratégia definida para captura das digitais dos segurados e sua utilização é ilustrada na Figura 4. A melhor alternativa para efetuar o cadastro das impressões digitais dos segurados foi deixar que fosse realizado diretamente na clínica em que ocorra o atendimento ao segurado. Outra alternativa seria realizar o cadastramento diretamente na sede do plano, porém o número elevado de segurados impossibilita esse cadastramento em um tempo hábil.

Figura 4 – Processo de autenticação Iapep Saúde.



Fonte: Elaborado pelos autores.

Durante o processo de marcação de consultas médicas ou exames, é feita a solicitação da carteira do segurado. Ao informar os dados do segurado é feita uma busca em banco de dados pelo mesmo. Após esta etapa, verifica-se a existência de digital cadastrada. Em caso positivo é requerida a impressão digital do segurado para que seja validada com a do registro recuperado. A Figura 5 apresenta a tela contendo o *applet* de requisição de impressão digital. Para o caso do IAPEP, o método de reconhecimento por verificação biométrica é a melhor escolha, tendo em vista a grande quantidade de segurados. Nesse método é feita a validação se o segurado é quem ele diz ser, ao invés de buscar todos os segurados e comparar com a digital apresentada. Caso o segurado não possua digital cadastrada é feito o direcionamento para tela de cadastro de impressão digital (ver Figura 6).

Figura 5 – Tela de captura de impressão digital.

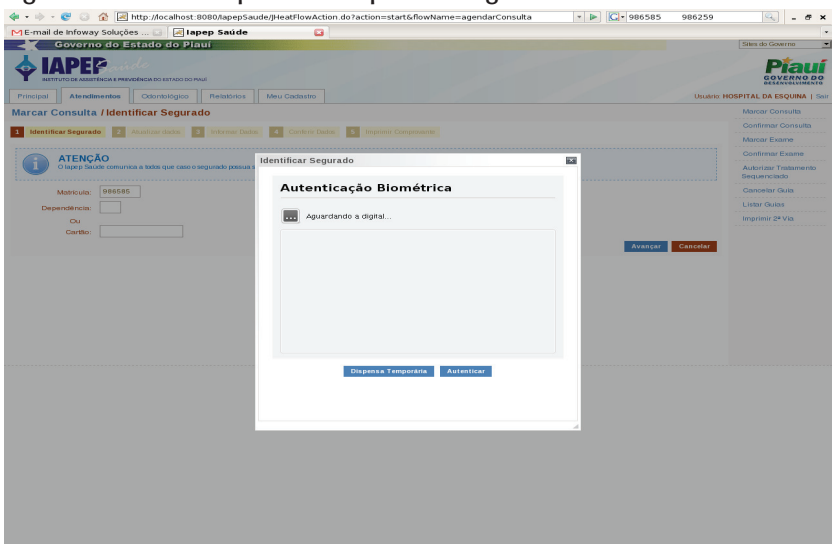
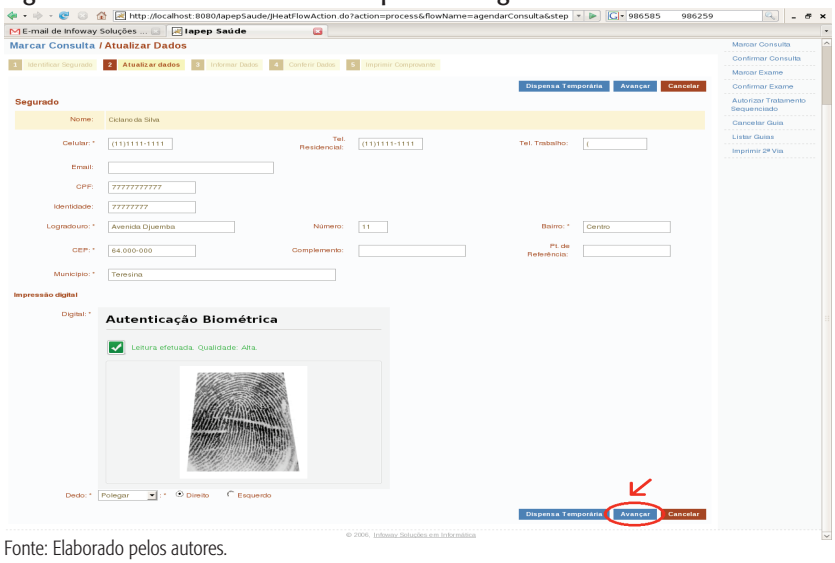


Figura 6 – Tela de cadastro de impressão digital.



Fonte: Elaborado pelos autores.

Dificuldades

Durante o processo de implantação do sistema biométrico do Iapep Saúde, foram encontradas algumas dificuldades o que motivou a escrita do trabalho em questão. As principais dificuldades encontradas decorreram dos seguintes aspectos:

- Falta de testes no ambiente do cliente – de acordo com o item 3.3.5 o ambiente do cliente deve ser testado. Tal medida não foi tomada no início do processo o que acarretou em uma nova estratégia de implantação, consequentemente atrasando o cronograma inicial de instalação.

- Problema de parametrização de variável no SDK – o item 3.3.3 fala da necessidade de adequação do *threshold* da solução biométrica. O fato de não ter sido modificado desde o início gerou um número elevado de falso negativo, não reconhecimento da pessoa cadastrada, problema que foi sanado com a adequação do valor.

• Incompatibilidade com outra solução biométrica – decorre da não observação ao item 3.3.5 do trabalho em questão. Em alguns casos foi necessária a utilização de uma nova máquina pelo cliente, para outros foi estudada uma maneira de tornar compatível a utilização dos sistemas biométricos;

• Necessidade de instalação no cliente – a necessidade dessas dependências provocou a criação de um pacote de instalação a ser utilizado por cada usuário final. Até o momento não foi desenvolvida uma solução para este problema.

Trabalhos Futuros

Para o futuro serão realizadas modificações no código do *applet* a fim de agilizar o processo de carga do mesmo. Serão utilizados os recursos do *Java Deployment Toolkit* e novo *Java Plug-in*, para resolver o problema do Java *Cold start*. Também será refeito todo o código do *applet* para plataforma JavaFX (DEITEL *et al.*, 2005). JavaFX é uma plataforma de software multimídia desenvolvida pela *Sun Microsystems* baseada em Java para a criação e disponibilização de aplicações RIA (*Rich Internet Applications*) que pode ser executada em vários dispositivos diferentes.

O JavaFX está totalmente integrado com o JRE. Para a construção de aplicações em JavaFX os desenvolvedores usam uma linguagem estática tipada chamada JavaFX Script.

Também será estudada a possibilidade de se fazer o download de todas as dependências do SDK da Griaule no cliente, para que não seja preciso a presença de uma equipe de suporte para realizar a instalação manualmente.

Conclusão

A Biometria refere-se ao uso de características físicas (íris dos olhos, impressão digital) ou comportamentais (voz, escrita) de um indivíduo para sua autenticação perante um sistema de informação. Atualmente é utilizada como meio de garantir segurança em diversos tipos de aplicação, inclusive nas aplicações Web. Neste trabalho foi exibido um guia para a implementação e implantação de um sistema biométrico a partir de experiências no desenvolvimento de uma solução para um plano de saúde na Internet. Foram discutidas as preocupações quanto segurança, interação com o usuário final, ambiente operacional que devem ser vistas no decorrer do processo de desenvolvimento e instalação do sistema no ambiente operacional. Este trabalho foi desenvolvido justamente por conta da dificuldade em se implantar a biometria em um sistema de gestão operando pela Web. A intenção do trabalho é tornar essa tarefa mais simples para aqueles que tiverem que executá-la, uma vez que as principais questões envolvidas são citadas, demonstrando possíveis alternativas a serem seguidas, formas de implementação e justificativa para a escolha de uma das opções.

No que diz respeito às aplicações da biometria na web, foi demonstrada sua utilização na identificação de segurados de um plano de saúde no combate a fraudes por falsidade ideológica. Nesse estudo de caso, foram expostos os problemas ocorridos durante a implantação, o que também motivou o desenvolvimento deste trabalho, sendo que as conclusões deste estudo proporcionaram a criação de um modelo genérico, que pode servir como modelo na criação de sistemas biométricos na plataforma Web.

Referências

COSTA, L. **Um modelo para autenticação biométrica para web banking**. Dissertação (Mestrado em Engenharia Elétrica) - Universidade Federal de Santa Catarina. 2007.

COSTA, S.M.F. **Classificação e verificação de impressões digitais.** 2001. 193p. Dissertação (Mestrado em Sistemas Elétricos) – Escola Politécnica da Universidade de São Paulo. Disponível em: <http://www.teses.usp.br/teses/disponiveis/3/3140/tde-18032002-102113/>. Acesso em: 21 jan. 2010.

DEITEL, H. M.; DEITEL, P.J. **Java como programar**. 6. ed. [S.l.]: Prentice-Hall, 2005.

FARRAR, B. **Usando Active X.** [S.l.]: Campus, 2001. 424p.

FERREIRA, C.R.; SANTOS, M.R.; SOUSA, E.F. **Identificação biométrica**. 2006. Disponível em: <http://www.frb.br/ciente/Impressa/Info/Identificacao>. Acesso em: 21 maio 2009.

GRIAULE. **Fingerprint SDK 2009.** Disponível em: http://www.griaulebiometrics.com/page/pt-br/fingerprint_sdk/overview. Acesso em: 19 maio 2009.

JAIN, A.K.; FLYNN, P.; ROSS, A.A. (Eds.). **Handbook of biometrics.** Berlin: Springer, 2008.

LIU, S.; SILVERMAN, M. **A practical guide to biometric security technology.** IT Professional,v.3, n.1, p.27–32, 2001. [doi: http://dx.doi.org/10.1109/6294.899930].

MAGALHAES, P.S. **Biometria e autenticação**. 2003. Disponível em: <https://repositorium.sdum.uminho.pt/bitstream/1822/2184/1/capsi.pdf>. Acesso em: 17 maio 2009.

POH, N.; KORCZAK, J. Hybrid biometric person authentication using face and voice features. In: INTERNATIONAL CONFERENCE, AUDIO AND VIDEO-BASED BIOMETRIC PERSON AUTHENTICATION AVBPA 3., 2001, Halmstad. **Proceedings**... Berlin: Springer-Verlag, 2001. p.348-353.

REIS, C.M.S. dos. **Autenticação com impressão digital.** Disponível em: http://www.deetc.isel.ipl.pt/comunicacoesep/disciplinas/pfc/fingerprint/files/carlos.pdf. Acesso em: 17 maio 2009.

VIGLIAZZI, D. **Biometria: medidas de segurança.** 2 ed. [S.l.]: Visual Books, 2006.

VIOLA, F.M. **Estudo sobre formas de melhorias na identificação de características relevantes em imagem de impressão digital.** 2006. Dissertação (Mestrado) – Universidade Federal Fluminense. 2006. Disponível em: http://www.ic.uff.br/PosGraduacao/Dissertacoes/298.pdf.