

INTEGRAÇÃO DE LEITORES BIOMÉTRICOS COM NAVEGADORES WEB PARA AUTENTICAÇÃO REMOTA DE USUÁRIOS

Abhner Vianna Ignachitti¹; Fernando Eduardo Resende Mattioli^{2,3}; Eduardo Fernandes Saad⁴

^{1,2,4} Faculdade de Talentos Humanos - FACTHUS, Uberaba (MG), Brasil

³Universidade Federal do Triângulo Mineiro - UFTM, Uberaba (MG), Brasil

facul@binehzim.com.br, fernando.mattioli@facthus.edu.br, eduardo.saad@facthus.edu.br

RESUMO: A biometria digital já está presente no dia-a-dia e amplamente utilizada atualmente. Com esta tecnologia pode-se identificar indivíduos de forma rápida e bastante precisa, dispensando o uso de documentos com foto. Este artigo descreve a criação de um software para integrar leitores biométricos com navegadores web utilizando o SDK (*Software Development Kit*, ou kit de desenvolvimento de software) da fabricante do leitor (Nitgen). Esta integração é possível porque o SDK permite a integração com várias linguagens de forma simples. A solução foi implementada em duas etapas sendo a primeira com ActiveX e Ajax/jQuery e a segunda utilizando Java. A solução proposta apresenta o projeto de um software que permite coletar a impressão digital do usuário e depois autenticá-lo através da web, tornando a utilização do sistema mais seguro uma vez que elimina-se a validação manual de dados com a autenticação através da biometria.

PALAVRAS CHAVE: ActiveX, Autenticação biométrica, Java, Navegadores.

INTEGRATION OF BIOMETRIC READERS WITH WEB BROWSERS FOR REMOTE AUTHENTICATION OF USERS

ABSTRACT: *Fingerprint biometrics is already present in our lives and is very common today. This technology can identify people quickly and accurately, eliminating the use of documents with photo. This article describes the creation of a software to communicate biometric readers with web browsers using the SDK provided by Nitgen. This communication is possible because the SDK (Software Development Kit) allows the use of many programming languages. The solution was implemented in two stages: first with ActiveX and Ajax / jQuery and then with Java. The proposed solution presents the design of a software to read fingerprints and then use this information to authenticate the user through the web, making the system more secure and eliminating manual data validation with use of authentication through fingerprints.*

KEYWORDS: *ActiveX, Biometrics authentication, Java, Web browsers.*

INTRODUÇÃO

Segundo Pinheiro (2008), o roubo de identidade em ambientes de rede vem se tornando bastante comum e muitas pessoas sofrem este tipo de ataque. Por esse motivo, a autenticação de usuários é um item fundamental para a segurança. De acordo com Silva (2008), a autenticação garante a identidade de um usuário pois consegue verificar se uma pessoa é realmente quem ela diz ser.

Sendo assim, a utilização da biometria digital para autenticação de usuários se torna uma solução viável já que ela está presente no dia-a-dia e é amplamente utilizada atualmente. As principais razões para a escolha desse método são: confiabilidade, baixo custo a longo prazo, baixo nível de intrusão e familiaridade. Com esta tecnologia pode-se identificar indivíduos de forma rápida e bastante precisa, dispensando o uso de documentos com foto (COSTA, 2001).

O tipo biométrico mais seguro para determinar a identidade de indivíduos, depois do teste de DNA, é a digital. Após a coleta das digitais, é feita uma análise dos

elementos físicos dos dedos, sejam eles os poros ou as linhas papilares. Estas linhas papilares são conhecidas como “minúcias” que formam padrões que podem ser identificados e comparados com padrões coletados, permitindo que a autenticação seja possível caso estes padrões sejam compatíveis (PINHEIRO, 2008).

Em particular, no caso da operadora de planos de saúde considerada neste estudo, quando um beneficiário necessita liberar procedimentos médicos, estas solicitações partem dos próprios consultórios, clínicas ou laboratórios através da web. A identificação deste paciente fica a cargo da atendente que se responsabiliza por verificar a carteirinha e comparar com um documento contendo foto no momento do atendimento. Sendo assim, o processo demanda um tempo considerável além de ser suscetível a erros principalmente quando o local é bastante movimentado (MANUAL, 2010).

Pensando na agilidade deste processo, necessitou-se criar uma solução que identificasse os usuários de forma mais rápida e assertiva. O processo seria mais rápido adotando a biometria como meio de identificação uma vez que a ciência da biometria é capaz de reconhecer atributos

físicos únicos, seja ela a impressão digital, íris, retina, reconhecimento de voz ou facial (COSTA, 2001).

A utilização de leitores biométricos por meio da web já é uma realidade nos navegadores mais novos através da *WebAuthn*, uma API de integração entre a internet, navegadores e dispositivos de segurança já bastante difundida. A *World Wide Web Consortium* (W3C), principal órgão regulamentador de padrões da internet no mundo, junto com a *FIDO Alliance* (consórcio industrial que trabalha com padrões de autenticação entre dispositivos) aprovou este padrão para a Web em 2019, porém ela é focada na autenticação de usuários ao realizar login em sistemas (SEGINFO, 2019).

Já o objetivo da solução proposta é a identificação do usuário que será atendido, ou seja, identificar se quem será atendido é realmente o beneficiário do plano de saúde uma vez que o acesso ao sistema não é feito pelo beneficiário e sim pelos médicos ou atendentes. O presente projeto abordará de forma objetiva o desenvolvimento para integrar navegadores e leitores de biometria digital, permitindo que a operadora de saúde possa identificar remotamente cada um de seus clientes atendidos nos diversos pontos espalhados pela cidade. A solução proposta também pode ser utilizada para a integrar com a web qualquer dispositivo conectado ao computador (como sensores, câmeras para reconhecimento facial, leitores de código de barra etc.) contornando uma limitação existente atualmente. Além de solucionar o problema, espera-se que a integração traga muito mais segurança para a utilização do plano de saúde pois dificultará que outra pessoa utilize o plano indevidamente, evitando fraude e a utilização de dados não autorizada.

REFERENCIAL TEÓRICO

A Biometria. Segundo Santos (2007), a biometria é a ciência que possibilita o reconhecimento e autenticação segura de determinada pessoa utilizando características físicas - como impressão digital - e padrões de comportamento como a escrita. Por meio de softwares e algoritmos que tornam o reconhecimento seguro e rápido, foi possível chegar ao desenvolvimento e aplicação da biometria com a finalidade de autenticar e autorizar usuários em sistemas de informação.

Aplicações Da Biometria. Atualmente, a utilização de biometria está popularizada, sendo a autenticação biométrica aplicada por grandes empresas e até mesmo pelo governo. Um exemplo da popularização da biometria é a utilização da digital para identificar eleitores no Brasil. De acordo com o TSE – Tribunal Superior Eleitoral (2019), já são mais de 119 milhões de pessoas com digitais cadastradas e aptas a utilizá-las na hora de exercer sua cidadania nas eleições, o que demonstra grande aceitação pelas pessoas e a assertividade deste método de identificação. A biometria digital já te dá acesso a telefones

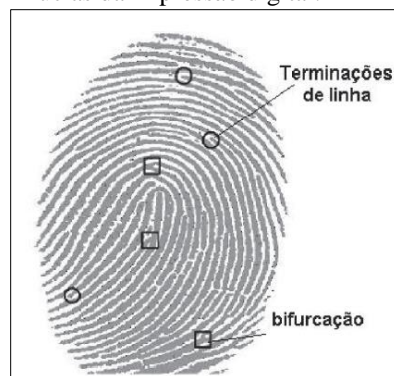
celulares, contas bancárias, fechaduras domésticas e permite identificar pessoas com grande confiabilidade.

Tipos De Biometria. É possível gerar um identificador biométrico com a maioria dos atributos físicos do ser humano. Abaixo lista-se os tipos principais e mais conhecidos de reconhecimento por biometria: impressão digital; íris; retina; reconhecimento de voz e reconhecimento facial

Atualmente, um dos tipos mais difundidos e utilizados é a biometria por digital, que está se tornando cada vez mais popular, uma vez que apresenta grande agilidade, grande nível de acerto e grande aceitação pelos usuários. Segundo Santos (2007), as soluções de reconhecimento biométrico podem ter um custo inicial eventualmente superior aos demais meios, porém, devido ao fato de dispensar mídias de reconhecimento – como chips, crachás etc. – possuem custo de manutenção e utilização menores a longo prazo, o que viabiliza sua utilização.

Biometria Por Digital. As impressões digitais são os padrões encontrados na ponta dos dedos das mãos e dos pés de cada indivíduo e o tipo biométrico mais seguro para determinar a identidade de indivíduos, depois do teste de DNA, é a digital. Finalmente, a biometria digital é muito popular e mais conhecida pela sua utilização no meio forense, onde são analisados os elementos físicos dos dedos, sejam eles os poros ou as linhas papilares. Estas linhas papilares são conhecidas como “minúcias” onde padrões são identificados para que a comparação seja possível, conforme se vê na Fig. 1 (PINHEIRO, 2008).

Figura 1: Minúcias da impressão digital.



Fonte: (PINHEIRO, 2008).

Segundo Pinheiro (2008) e Vigliuzzi (2006), estas minúcias dão a cada indivíduo uma identificação única, já que mesmo em gêmeos - idênticos ou não - essa característica nunca se repetirá. Essas minúcias são utilizadas como parâmetro para grande parte dos algoritmos de comparação de impressões digitais uma vez que elas não sofrem alteração ao longo do tempo, nem mesmo pela idade.

Os padrões da digital são coletados por um leitor e através desta coleta é possível armazená-la ou realizar a comparação de identificação. O processo conhecido como *matching* determina o grau de compatibilidade entre os padrões extraídos da digital do usuário e o padrão

armazenado no banco de dados, fornecendo uma pontuação da compatibilidade das amostras. Caso a compatibilidade seja superior ao limite configurado, a autenticação é válida. Caso a compatibilidade seja inferior, a autenticação não é válida (COSTA, 2001).

De acordo com Costa (2001), em relação à biometria, o processo de autenticação pode ocorrer de duas formas, verificação e autenticação.

Verificação: É quando uma digital é capturada e comparada com um registro já selecionado. Um exemplo é quando identificamos o usuário através do número da sua carteirinha, localiza-se o registro da sua digital armazenada no banco de dados e compara-se com a digital coletada. Este processo é mais rápido pois não é necessário realizar uma busca em todas as digitais armazenadas. **Autenticação:** É quando se colhe uma digital e a compara com uma massa de dados, ou seja, compara-se a digital coletada com cada registro armazenado no banco de dados, a fim de localizar de quem é a biometria colhida. Este processo é mais demorado pois necessita uma pesquisa extensa além de realizar a comparação registro a registro.

Uma das vantagens da biometria por digital é seu custo de manutenção relativamente baixo a longo prazo, além da sua boa aceitação por parte das pessoas. Com isso, se torna uma tecnologia interessante para autenticação de usuários devido à sua confiabilidade. Embora confiável, a autenticação por digital pode apresentar problemas como FRR (*False Rejection Rate*) e FAR (*False Acceptance Rate*) que são, respectivamente, as taxas de rejeição e aceitação falsas. Isso significa que mesmo se tratando do indivíduo correto, existe uma pequena possibilidade de negativas indevidas, assim como uma pequena taxa de aceitação falsa (PINHEIRO, 2008).

Apesar de bastante eficiente, estes falsos resultados se dão devido ao fato que a digital pode apresentar lesões, envelhecimento ou até mesmo desgaste na pele sendo que até pequenos cortes podem interferir na leitura da digital (VIGLIAZZI, 2006).

Apesar do pequeno índice de falhas, a leitura biométrica da digital possui uma vida útil longa e é bastante persistente, além de ser umas das mais eficientes, mais utilizadas e de baixo custo em comparação a outros tipos (PINHEIRO, 2008).

Hipóteses. Para elaboração do presente projeto, e após a identificação do problema, fez-se necessário desenvolver uma solução para integrar leitores de biometria digital com a web, devido ao fato de atualmente existir uma grande limitação para utilização de leitores digitais remotos e integrados com navegadores web. Conforme cita o manual do SDK do fabricante, a integração nativa com o leitor em navegador web é possível somente no *Internet Explorer* utilizando ActiveX e a DLL fornecida pelo SDK, porém, ao usar outros navegadores, surge um problema que é a falta de integração do leitor com navegadores que não possuem ActiveX uma vez que esta linguagem já está descontinuada e é de propriedade da Microsoft. O ActiveX basicamente faz uma adaptação de programas para funcionar online ou direto no navegador. Trata-se de uma ferramenta muito utilizada

antigamente, por exemplo, para visualização de vídeos do *Windows Media Player* diretamente no navegador (FARRAR, 2001).

Sendo assim, a hipótese principal investigada neste trabalho aborda a possibilidade de se desenvolver um software que resolva a questão de integração em diversos navegadores utilizando Java e uma comunicação via HTTP que fará toda a comunicação com o servidor, totalmente isolada e independente dos navegadores, permitindo buscar informações no servidor e confrontá-las com as digitais colhidas no momento do atendimento.

Decidiu-se pela biometria digital para autenticação pois é uma alternativa rápida, viável e de fácil aceitação pelo público em geral uma vez que hoje a digital já é amplamente utilizada no dia-a-dia de muitas pessoas.

MATERIAIS E MÉTODOS

Para a elaboração do projeto, utilizou-se o leitor de digital da marca Nitgen, modelo Hamster 2, que conta com um SDK próprio para captura e validação das digitais. Além disso, o manual e a documentação do leitor possuem vários exemplos de fontes para diversas linguagens, tornando ainda mais fácil o desenvolvimento de integrações com o leitor.

A captura e validação das digitais é feita pelo SDK de forma rápida e fácil. Conforme mostra a Fig. 2, o primeiro passo é escolher de qual dedo será coletada a digital para armazenamento. Esta coleta pode ser configurada para qualquer dedo e como se vê na imagem, foi configurada para coletar os 10 dedos das mãos.

Figura 2: SDK Nitgen para captura da digital.



Fonte: Os autores, 2020.

Após selecionar o dedo, a segunda etapa é a coleta da digital. São realizadas duas capturas do mesmo dedo para que seja feita uma primeira validação de compatibilidade entre as duas amostras coletas. Isso garante que a coleta foi realizada no mesmo dedo. Em caso negativo, um aviso informa que as digitais não coincidem e o processo é interrompido, conforme vemos na Fig. 3.

Em casos positivos, o SDK retorna à tela inicial para escolha de um novo dedo e destaca os dedos já coletados, conforme vemos na Fig. 4.

Após a finalização do processo de captura, o SDK gera uma chave de autenticação única de todos os dedos coletados. Esta é a chave utilizada para validação das digitais e que será gravada no banco de dados para análise posterior.

Figura 3: Exemplo de comparação com falha ao capturar digital pelo SDK Nitgen.



Fonte: Os autores, 2020.

Figura 4: Exemplo de coleta válida de biometria digital feito pelo SDK Nitgen.



Fonte: Os autores, 2020.

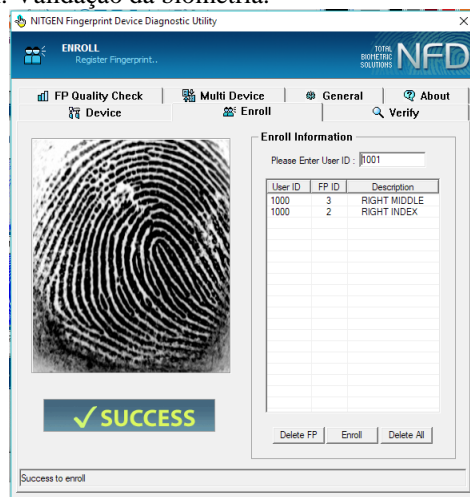
O SDK também possui um software para testes e validações do leitor e das coletas. Conforme se vê na Fig. 5, é possível gravar temporariamente a chave gerada para validação da biometria para fins de teste.

Também é possível testar e configurar o leitor como se vê na Fig. 6. Nestas configurações é possível, inclusive, definir a qualidade da captura e o grau de compatibilidade ao realizar a comparação das digitais o que torna o SDK do

fabricante extremamente versátil pois é facilmente configurável e se integra com diversas linguagens como C++, Delphi, Java, ActiveX e .NET tornando sua utilização prática e rápida (GRIAULE, 2009).

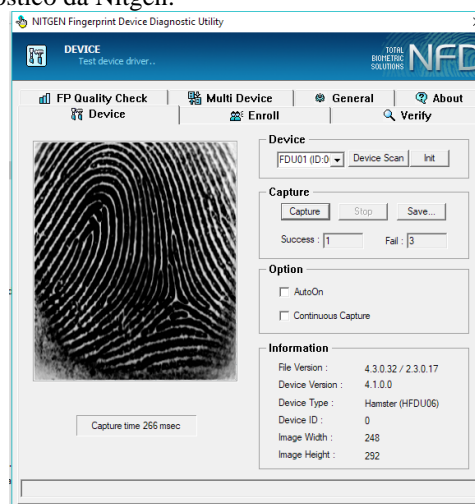
Inicialmente, para o projeto piloto e análise dos impactos da implantação, a validação da biometria foi desenvolvida com a solução nativa em ActiveX e Ajax/jQuery, utilizando os drivers de captura e validação fornecidos pelo SDK do fabricante. A opção pelo ActiveX se deu pelo fato do software online da empresa funcionar melhor no navegador Internet Explorer e não seria necessário criar nenhuma estrutura adicional no ambiente para suportar e validar as biometrias digitais do projeto piloto. Além disso, o projeto piloto serviu para verificar a viabilidade da implantação, evitando assim o desperdício de tempo e dinheiro caso a solução proposta não atendesse a necessidade.

Figura 5: Exemplo do software de Teste e Diagnóstico da Nitgen. Validação da biometria.



Fonte: Os autores, 2020.

Figura 6: Exemplo do software de teste, configuração e diagnóstico da Nitgen.



Fonte: Os autores, 2020.

Para o projeto piloto, foram selecionados prestadores de pouco movimento para verificar os impactos gerados pela biometria digital a fim de não interferir no funcionamento geral de todos os outros consultórios e laboratórios. Com o sucesso do projeto piloto, apesar da limitação do uso via ActiveX e Internet Explorer, foi possível determinar que o desenvolvimento de uma solução mais ampla seria uma ótima alternativa uma vez que não foram identificados problemas de validação nem tão pouco resistência por parte dos usuários na utilização do projeto piloto.

Após a conclusão do piloto e constatação da eficácia do novo processo de validação da biometria, definiu-se pelo desenvolvimento de um software próprio em Java. Esta opção se fez necessária devido ao grande volume de dados que seria necessário trafegar quando se fizesse a implantação em toda a rede prestadora. Além disso, esta decisão foi motivada pela limitação existente quanto ao uso do ActiveX, tecnologia descontinuada pela Microsoft após o lançamento do novo navegador *Edge*. A partir deste evento, outros navegadores também não conseguiram utilizar o ActiveX, por ser uma linguagem exclusiva do *Internet Explorer*.

Por fim, para contornar o problema da falsa aceitação positiva, optou-se por utilizar a verificação em duas etapas: verificação do número da carteirinha seguido da verificação da impressão digital. Com esses dois métodos, será possível tornar o sistema mais confiável uma vez que ele validará o número único do cartão, permitindo a fácil localização do registro no banco de dados, juntamente com a impressão digital do seu usuário, reforçando ainda mais a relação de confiança e dispensando a utilização do documento com foto. Já nos problemas de falsa rejeição, foi definido um processo interno de contingência que consiste em desabilitar a validação das digitais – temporariamente ou permanentemente – bastando que o beneficiário se apresente na sede da cooperativa para constatação do problema de leitura.

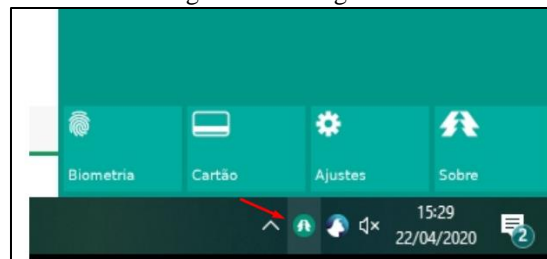
RESULTADOS E DISCUSSÃO

Integração. A integração inicia-se após o médico ou atendente efetuar acesso no sistema online. Antes de iniciar a validação da biometria, é feita uma pré-validação da carteirinha utilizando um leitor de cartões magnéticos.

Na validação do cartão, são verificados dados como data de validade, via do cartão, situação financeira do cliente, situação do plano de saúde e principalmente a validação do número do cartão, que será utilizado para busca das informações no banco de dados e validação da biometria. Uma vez que todos os dados estejam válidos, o site inicia a verificação da digital caso a biometria do usuário já tenha sido coletada. Nos casos em que a biometria não tenha sido coletada, o processo segue o fluxo normal, sem a autenticação da biometria. Também é neste momento que é determinado o tipo de validação que será utilizada, seja pela aplicação Java ou ActiveX.

Java. No momento da validação, o site envia uma comunicação para a máquina local via HTTP para identificar se o aplicativo está instalado. O software de integração roda em segundo plano (oculto) e fica ativo discretamente na barra de tarefas do Windows após instalado e iniciado corretamente, conforme mostra a Fig. 7.

Figura 7: Software em Java responsável pela integração do leitor biométrico Nitgen com navegadores Web.



Fonte: Os autores, 2020.

Caso o ícone esteja verde, significa que existe uma conexão ativa com os servidores e será possível fazer a integração com o navegador. Caso o ícone esteja cinza, significa que a conexão não está ativa e não será possível integrar o leitor com o navegador. Por último, caso o ícone esteja vermelho, significa que o aplicativo Java não identificou o leitor biométrico conectado ou existe alguma falha na instalação do leitor. Internamente, a aplicação Java disponibiliza um servidor HTTP local que recebe requisições *Web* na porta 17501. A escolha desta porta se deu pelo fato de ser uma porta alta e fora dos padrões HTTP, diminuindo a possibilidade de existir um outro serviço rodando na máquina local com a mesma porta. Caso a escolha fosse pelas portas 80 ou 8080, por exemplo, haveria grandes chances de conflito com o aplicativo Java uma vez que essas portas são comumente usadas por diversas aplicações, inviabilizando a instalação do aplicativo Java. O aplicativo disponibiliza dois métodos para validação:

Verificação de STATUS de conexão: retorna 0 caso o integrador não esteja conectado com o servidor ou 1 caso todas as conexões estejam ativas e o leitor esteja conectado na máquina.

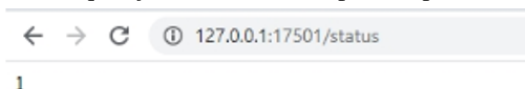
Pedido de ativação e validação do beneficiário: retorna uma ID única responsável pela identificação deste usuário no banco de dados.

Após a validação inicial de elegibilidade, o sistema online envia uma requisição para o cliente Java instalado localmente na máquina do prestador através do IP local, utilizando o endereço <http://127.0.0.1:17501/status>, conforme vemos na Fig. 8. Caso a conexão esteja ativa, o aplicativo Java retorna o identificador '1' permitindo que o sistema continue e possa ser feita uma nova requisição no endereço <http://127.0.0.1:17501/autenticar> que ativa o leitor e inicia a coleta da digital utilizando o SDK da fabricante, conforme mostra a Fig. 9.

Após o leitor ser iniciado e a digital ser coletada, o aplicativo Java recupera as informações de biometria armazenadas no banco de dados utilizando o número da

carteirinha passado na *url* e compara com o registro coletado pelo leitor, utilizando novamente o SDK da fabricante para realizar a validação. Após verificado, é feita uma gravação em uma tabela do banco de dados e retornada uma chave única de autenticação para o site. A partir daí o site passa a buscar as informações no banco de dados com o ID de autenticação retornado pelo aplicativo Java e, caso encontre o registro válido, permite o usuário seguir o processo confirmando que o usuário foi autenticado com sucesso. Toda comunicação com os servidores feita pelo aplicativo Java funciona sobre o protocolo HTTP com certificado SSL, exceto as requisições locais uma vez que essas requisições são feitas na própria máquina e não possuem nenhuma informação sigilosa. A utilização de autenticação SSL torna mais segura toda a comunicação entre os computadores dos prestadores com os servidores da cooperativa. O funcionamento de todo o fluxo destes processos pode ser observado na Fig. 10.

Figura 8: Requisição STATUS feita para o aplicativo.



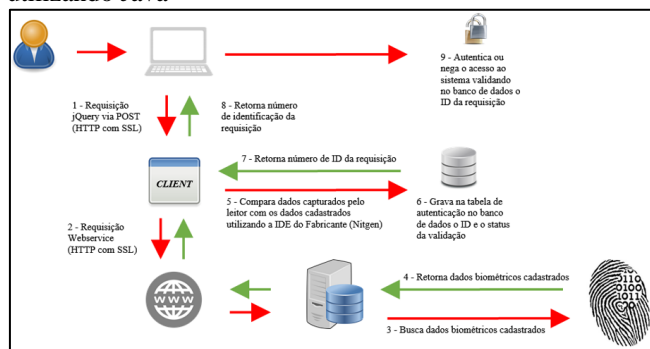
Fonte: Os autores, 2020.

Figura 9: Requisição para iniciar a coleta e validação da biometria para a carteirinha informada



Fonte: Os autores, 2020.

Figura 10: Fluxo da integração do leitor com o navegador utilizando Java

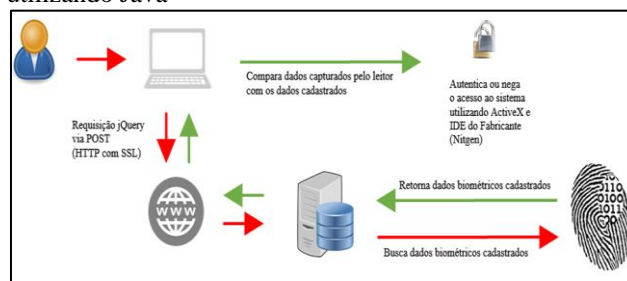


Fonte: Os autores, 2020.

ActiveX. O processo inicial na aplicação web é o mesmo, porém o sistema somente irá utilizar a integração via ActiveX caso o software Java não esteja instalado e o navegador seja o *Internet Explorer*. Isso se dá pelo fato de

ainda existirem máquinas antigas utilizando *Windows XP* ou anterior que não possibilitam a utilização do aplicativo Java. Nestes casos, a única solução é através do ActiveX e *Internet Explorer*. Após as verificações, a ativação do leitor é realizada utilizando Ajax/jQuery que carrega a biblioteca DLL disponibilizada pela fabricante para integração via ActiveX e ativa o leitor para coleta da digital. Após realizada a coleta, inicia-se uma requisição na própria aplicação Web que retorna os registros biométricos da pessoa armazenados no banco de dados. Após recuperados os dados biométricos, o SDK realiza a comparação com os dados coletados pelo leitor de biometria e, caso os dados coletados coincidam com os dados armazenados no banco de dados, o sistema valida e libera o acesso para continuar. Um diagrama do funcionamento deste projeto pode ser visto na Fig. 11.

Figura 11: Fluxo da integração do leitor com o navegador utilizando Java



Fonte: Os autores, 2020.

Em ambos os casos, sempre será utilizada a autenticação pelo modo de verificação uma vez que após a validação da carteirinha o sistema já está posicionado no registro que deverá ser verificado com a amostra recolhida, seja ela pelo Java ou por ActiveX.

CONCLUSÃO

Integrando o navegador com o leitor biométrico, foi possível identificar parte dos beneficiários do plano de saúde que procuram os credenciados para atendimento médico, tornando o processo mais ágil e seguro e evitando o processo manual de identificação da carteirinha com a apresentação de um documento com foto.

Espera-se, com a total implantação do projeto, que pelo menos 80% dos beneficiários atendidos pelo plano sejam identificados remotamente através da biometria digital diretamente pela internet, trazendo mais segurança e controle nas utilizações do plano de saúde. Além disso, espera-se evitar o uso de cartões de forma indevida uma vez que a autenticação biométrica tornará mais difícil que outra pessoa utilize o plano de saúde sem autorização.

Devido a pandemia de 2020, a esterilização de superfícies tornou-se primordial e a limpeza necessária a cada utilização do leitor de impressões digitais cria um pequeno problema para sua utilização uma vez que o leitor necessita ser tocado para que a leitura seja realizada. Um

desenvolvimento futuro bastante interessante, baseado na solução proposta por este projeto, seria realizar a integração de câmeras de vídeo e bibliotecas de reconhecimento facial de código aberto como a OpenCV. Essa integração permitiria que a pessoa continue sendo autenticada por algum meio biométricos, mantendo a segurança do sistema e evitando o contato físico com o leitor de digitais. Utilizando bibliotecas de código aberto também seria possível contornar a limitação do alto custo cobrado pelas soluções corporativas de reconhecimento facial disponíveis no mercado, mantendo o baixo custo e a autenticação por biometria, que foram fatores principais e necessários para a elaboração deste projeto.

REFERÊNCIAS

COSTA, Silvia Maria Farani. **Classificação e verificação de impressões digitais**. 2001. 193p. Dissertação (Mestrado em Sistemas Elétricos) – Escola Politécnica da Universidade de São Paulo. Disponível em: <https://www.teses.usp.br/teses/disponiveis/3/3140/tde-18032002-102113/publico/dissertacao_Silvia.pdf> Acesso em: 21 de janeiro de 2020.

FARRAR, Brian. **Using ActiveX: The most complete reference**. Que, 1996. 382p.

GRIAULE. **Fingerprint SDK 2009**. Disponível em: <<https://pt.scribd.com/doc/111023939/53926349-Fingerprint-Sdk-2009-Manual-English>>. Acesso em: 20 dezembro 2019.

MANUAL interno para autorização de procedimentos e consultas pelos consultórios e prestadores de serviço. **Revisão 008**. Uberaba: Unimed Uberaba, 2010. 20p.

PINHEIRO, José. Biometria nos Sistemas Computacionais: Você é a senha. **Ciência Moderna**, 2008.

SANTOS, Alfredo. Gerenciamento de identidades. Segurança da informação. Rio de Janeiro, **Brasport**, 2007.

SEGINFO. **WebAuthn torna-se um padrão oficial de autenticação da Web**. Disponível em: <<https://seginfo.com.br/2019/03/15/webauthn-torna-se-um-padrao-oficial-de-autenticacao-da-web-confira/>>. Acesso em: 01 de jan. de 2020.

SILVA, Luis Gustavo Cordeiro. Certificação Digital - Conceitos e Aplicações. **Editora Ciência Moderna**, 2008.

TSE, Tribunal Superior Eleitoral. **Biometria atual por UF**. Disponível em: <<http://www.tse.jus.br/eleitor/biometria/biometria-atual-uf>> Acesso em: 11 de junho de 2020.

VIGLIAZZI, Douglas. Biometria: medidas de segurança. 2ª Ed. **Visual Books**, 2006.