Beatriz Cardoso Espedito
Thiago Takeshi Takizawa

COMPARATIVO DOS PROCESSOS DE AUTENTICAÇÃO USADOS EM *SMARTPHONES*

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.

Área de concentração: Segurança da Informação

Americana, 29 de junho de 2021.

Banca Examinadora:

Edson Roberto Gaseta (Presidente)
Mestre
Fatec-Americana

José Luiz Zem (Membro)
Doutor
Fatec-Americana

Luciana H. P. de Almeida Guimarães (Membro)
Mestre
Fatec-Americana

Resumo
Este artigo aborda alguns métodos de autenticação que são utilizados em smartphones. Inicialmente o caminho percorrido foi um estudo sobre a funcionalidade e chega até a origem dos métodos de autenticação biométricos popularmente utilizados, que são: impressão digital, pela íris e facial, métodos esses que estão presentes na maioria dos celulares atualmente. Além disso, a autenticação multifator também foi estudada e também pode englobar métodos biométricos, mas possui mais de uma etapa de autenticação. O desafio deste trabalho atribui a tarefa de realizar uma comparação dos métodos escolhidos, de acordo com alguns parâmetros específicos, incluindo a segurança. A comparação segue a adaptação do Modelo Integrado de Maturidade em Capacitação (CMMI), estabelecendo uma escala de 1 a 5 para avaliação. Posteriormente, o artigo navega superficialmente sobre o universo *blockchain* e traz a reflexão da possibilidade de futuramente, o *blockchain* ser uma ótima opção de autenticação a ser utilizada em smartphones, pois pode ser capaz de sanar as fraquezas dos demais métodos.
Palavras-chave: Autenticação. *Blockchain*. Método. Segurança.

Abstract
This article covers some authentication methods. Initially the path followed was a study on the functionality and even the origin of the popularly used biometric verification methods, which are: fingerprint, iris and facial, methods that are presents in most cell phones today. In addition, the multifactor authentication (MFA) has also been studied, it can also encompass biometric methods, but it has more than one authentication step. The challenge of this research was to make a comparison of the chosen methods, according to some specific parameters, including safety. This present research uses the adaptation of the Integrated Maturity in Training Model (CMMI), establishing a scale from 1 to 5 for evaluation. Subsequently, the article browses superficially about the blockchain universe and brings a reflection of the possibility that in the future, blockchain will be a great authentication option to be used on smartphones, as it may be able to remedy as weaknesses of the other methods.
Keywords: Authentication. Blockchain. Method. Security.

Introdução

No começo dos anos 2000, pouco se falava em segurança de dados, pois a quantidade de pessoas com acesso à internet não era como nos tempos atuais. Existem muitos tópicos para serem abordados quando se fala em Segurança da informação e a evolução da tecnologia até os dias de hoje. Com a entrada da LGPD (Lei Geral de Proteção de Dados) e as mudanças na forma de trabalho e estudo que ocorreram devido a COVID-19, houve mudanças no tratamento de dados e vale a pena conhecer e analisar alguns métodos de autenticação que podem ser usados em dispositivos.

As autenticações biométricas estão não só em dispositivos móveis, e seu crescimento é inegável. Marcas populares de dispositivos móveis como *Samsung*, *Apple*, Motorola e *Microsoft*, produzem cada vez mais dispositivos com pelo menos um sensor biométrico para que o usuário tenha a chance de usufruir de mais de um método de autenticação. Embora o método biométrico esteja crescendo ele ainda não é totalmente aceito pois existem usuários que preferem a utilização de outros métodos de autenticação como por exemplo *password*, *pin*, padrões, entre outros e levando em conta o custo mais elevado da tecnologia para leitura biométrica, o que consequentemente encarece o produto (SHAFIQUE *et al.* 2017).

A autenticação descentralizada ficou mais notória quando a bitcoin, que é uma criptomoeda (NAKAMOTO, 2008) ficou conhecida no mundo. Ter a chance de fazer transações mais rápido e com uma moeda digital é realmente fantástico. Mas, se engana quem crê que a tecnologia é utilizada apenas para processamento de pagamentos, gestão de contratos e compras, pois muitas *startups* já estão desenvolvendo aplicações de gerenciamento de identidade. Esse método será abordado sucintamente, apenas para fins de conhecimento.

Sendo assim, quem usa somente um método de autenticação hoje em dia? Para acessar o e-mail, as redes sociais, cadastrar-se em sites ou simplesmente dar manutenção em contas, é necessário autenticar-se mais de uma vez. Portanto, a intenção deste artigo é analisar os métodos de autenticação apresentados de acordo com os pilares da segurança da informação, voltado para uso pessoal.

2. Segurança da informação

A informação tem sido estudada por muitos autores e pode ser definida de diversas formas, inclusive de acordo com o contexto em que se encontra. Segundo De Sordi (2008, p. 10), a informação é: "a

interpretação de um conjunto de dados segundo um propósito relevante e de consenso para o público-alvo (leitor)". E de acordo com esse significado, assegurar o dado, que é relevante para um certo propósito é essencial. De acordo com a definição Dhillon (2004), a segurança da informação, além de englobar a integridade, confidencialidade, disponibilidade, também engloba o fator humano e a ética.

Por exemplo, existem normas como a NBR ISO/IEC 27002:2013 que possuem diretrizes e políticas para assegurar os dados e eliminar vulnerabilidades e ameaças, além de manter planos de contingência para situações de incidentes de risco que muitas vezes podem ser causadas por falha humana intencional ou não intencional, pois segundo Dhillon (2004), não são apenas questões técnicas que devem ser consideradas, e sim questões organizacionais, estruturais e comportamentais.

O Comitê Nacional de Sistemas de Segurança (CNSS) define que a Segurança da Informação (SI) foi criada para proteção das informações existentes dentro de equipamentos e sistemas que as utilizem para guardar ou transmitir essas informações. As informações que devem ser protegidas, abrangem as políticas de SI, computadores, dados e redes. Segundo Whitman e Mattord (2011), a CNSS desenvolveu um modelo a ser seguido para a SI, baseado no C.I.A *(Confiability, Integrity and Availability) triangle* no qual foca em três grandes pilares no tratamento das informações produzidas dentro de qualquer empresa que são: Confidencialidade, Integridade e Disponibilidade.

A confidencialidade é um dos pilares da segurança da informação que possui um conjunto de regras o qual preserva o acesso limitado das informações, apenas às pessoas autorizadas a acessar tal conteúdo (TCHERNYKH *et al*. 2016). Integridade segundo Whitman e Mattord (2011), é um pilar que foca no dado em si, fazendo-o com que ele esteja protegido de forma a não ser alterado sem que haja total autorização por aqueles responsáveis e dessa forma a informação fica impedida de ser corrompida, danificada ou até destruída. O terceiro pilar é a Disponibilidade, onde a informação estará devidamente habilitada para ser acessada onde e quando for necessária pelas pessoas autorizadas anteriormente (MARTIN & KHAZANCHI, 2006).

3. Tipos de autenticação

Os mecanismos de autenticação são divididos em três bases: autenticação baseada em conhecimento, propriedade e característica. Segundo Antunes (2014), a autenticação baseada no conhecimento consiste no que se sabe. É necessário saber previamente alguma informação, como a senha, por exemplo, para autenticar-se. A autenticação baseada na propriedade consiste no que se tem, é necessário possuir algum objeto físico, como um dispositivo que gere um *token* que expira em um período, por exemplo.

Já a autenticação baseada na característica consiste no que você é, segundo Brito (2009), nesse mecanismo os métodos adotados geralmente são os biométricos. Sistemas de reconhecimento fazem a verificação da autenticação biométrica física ou comportamental.

3.1 Autenticação Biométrica

"Biometria (ou identificação biométrica) é a identificação de uma pessoa com base em suas características únicas, sejam físicas ou comportamentais" (BOLLE *et al*., 2013). Alguns exemplos de padrões biométricos fisiológicos são: a análise da geometria da mão, verificação das veias por imagens térmicas do rosto, punho ou outras partes do corpo, identificação dos odores e salinidade corporal, entre outros. Já os padrões biométricos comportamentais existentes são: autenticação pelo ritmo de escrita, autenticação pela voz, verificação de assinatura, porém, o que será abordado neste trabalho serão alguns métodos de biometria fisiológica que já são usados especificamente em celulares.

Na presente pesquisa serão abordados três métodos de autenticação fisiológica: impressão digital, facial e pela íris. A autenticação pela retina também existe e é utilizada em *smartphones*, porém, o método não foi escolhido como objeto de estudo.

Um sistema biométrico é composto por três etapas: captura, extração e comparação. Segundo Coutinho (2018), na captura obtém-se uma amostra biométrica para posteriormente realizar a identificação de um indivíduo. Por exemplo, no caso da impressão digital, isso ocorre na primeira vez em que é registrada, colocando o dedo sobre o sensor do dispositivo algumas vezes. A extração varia de acordo com a confiabilidade e o rigor analítico de cada sistema, que pode armazenar as informações com mais ou menos segurança, porém é realizada a "remoção" de uma amostra de informação biológica única do indivíduo.

Segundo um determinado sistema desenvolvido por Peres e Hemerly (2005), é efetuada a binarização das imagens, análise dos traços minuciosos, reprocessamento e registro no banco de dados. O resultado dessa análise é chamado de *template*. Por último, com base no registro do banco de dados, é realizada a

comparação utilizando o *template* armazenado para concluir a identificação. Os tipos de autenticação biométrica fisiológica que serão abordados nesse trabalho são:

3.1.1 Reconhecimento facial: Coleta informações das características do rosto

Em 1964, o dispositivo *The RAND Tablet*, capaz de fazer o reconhecimento de rostos, desenhados à mão a partir de fotos (Figura 1) e foi criado pelo cientista Woodrow Wilson Bledsoe. O reconhecimento facial é responsável por validar algumas características da face como: formato do rosto, dimensões das sobrancelhas, distância entre os olhos, nariz e boca, assim como sua largura e tamanho.

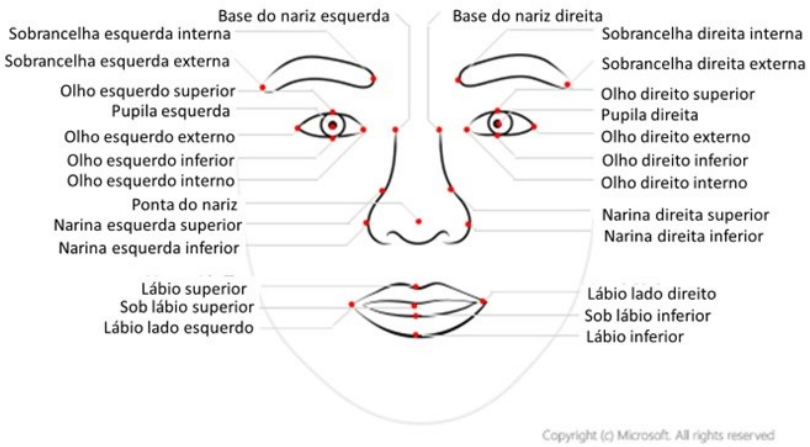
Figura 1. The RAND Tablet

Fonte: medium.com (2018).

Na maioria dos casos, os sensores utilizados são os mesmos das câmeras dos dispositivos ou trabalham com sensores infravermelhos usados para capturar pontos de referência da face. As dicas de referência são um conjunto de pontos fáceis de encontrar em uma face, como as pupilas ou a ponta do nariz. Por padrão, há 27 pontos de referência facial predefinidos. A figura 2 a seguir mostra todos os 27 pontos (MICROSOFT, 2019)

Existem diversos fatores que podem afetar a leitura e o desempenho do sistema, como a iluminação, a resolução das imagens, objetos que cubram parte do rosto do usuário, como óculos escuros, e as mudanças no rosto devido ao envelhecimento (THAKKAR, 2017). Porém, segundo Shafique (2017), o reconhecimento é fácil, por isso é considerado como a melhor maneira de se autenticar dentre todos os outros métodos biométricos, uma vez que as outras opções necessitam que haja um contato ou uma grande aproximação com os aparelhos celulares para que haja a confirmação da identidade enquanto no reconhecimento facial não há essa necessidade. O uso de máscaras aumentou e passou a ser utilizado em praticamente todo mundo, devido à COVID-19. Este é um dos fatores que dificultam a leitura da face na autenticação facial.

Figura 2. Pontos de Referência da Face

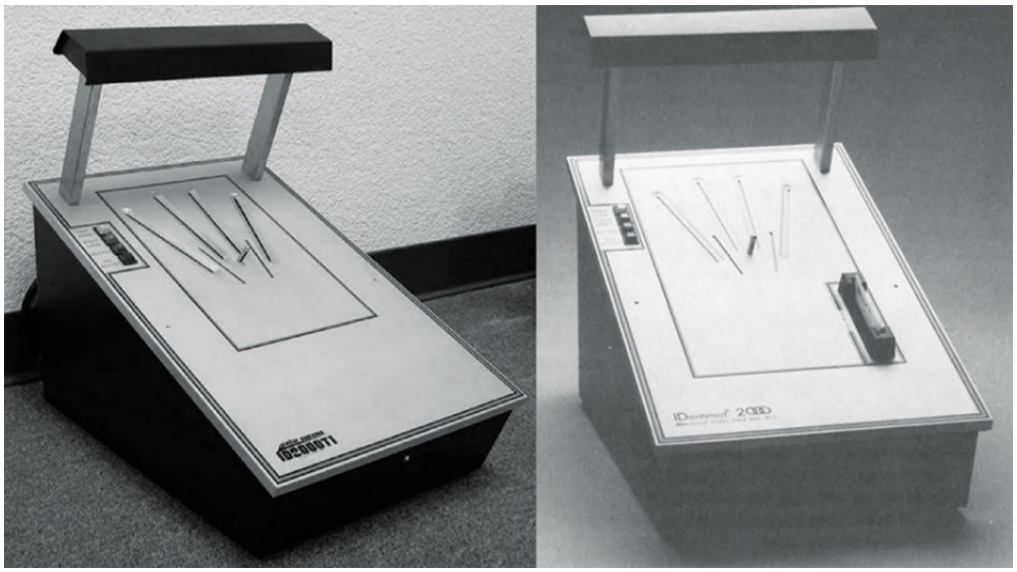


Fonte: Adaptado de Microsoft (2019).

3.1.2 Impressão digital: Captura as impressões digitais e suas características.

Em 1892, Francis Galton inventou o primeiro sistema moderno de impressão digital. Ele foi o primeiro cientista a inventar a biometria, chamando seus projetos de “aplicações de métodos estatísticos para fenômenos biológicos”. Depois disso, a evolução da biometria foi iniciar-se no final de década de 60. Em 1972 surgiu uma máquina eletromecânica chamada Identimat (Figura 3). Era usada na identificação de pessoas por meios de medição da geometria da mão.

Figura 3. Identimat



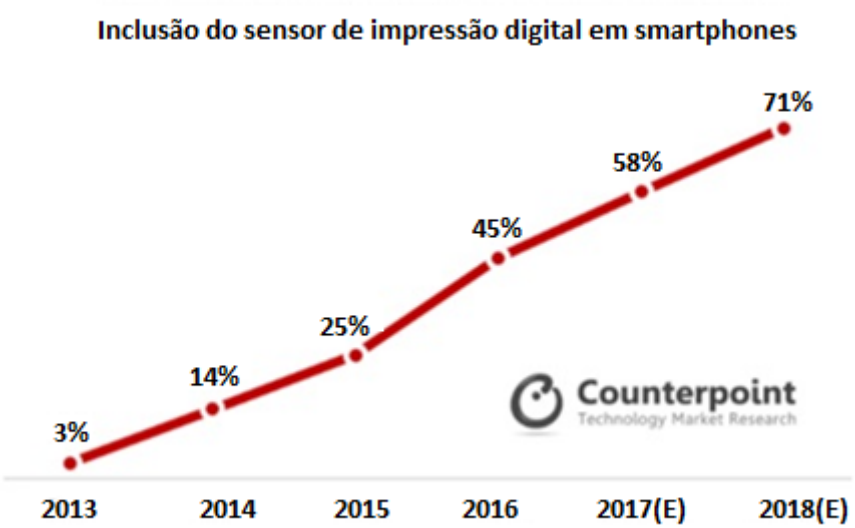
Fonte: thedrive.com (2018).

Para a captura de impressões digitais utiliza-se um *scanner* com diversos tipos de sensores, mas os dois tipos mais utilizados são os óticos, os capacitivos (THAKKAR, 2018), além dos ultrassônicos. *Scanners* ópticos, basicamente utilizam uma luz para iluminar os dedos e uma microcâmera captura a amostra da impressão digital. *Scanners* capacitivos usam um *chip* de silício que identifica baixas correntes elétricas provenientes dos dedos, já os sensores ultrassônicos utilizam um ultrassom para recriar a imagem do dedo. Para Shafique *et. al* (2017), as vantagens da biometria são consideravelmente melhores principalmente para

as impressões digitais, quando comparadas com senhas comuns por diversas características como maior segurança, rápida, confiável e de fácil manuseio pelo usuário.

Hoje em dia, a maioria dos *smartphones* possuem no mínimo o leitor biométrico de impressão digital como opção para o usuário autenticar-se. Segundo Sharma (2017), a previsão para 2018 do envio de *smartphones* com sensores de impressão digital ultrapassaria um bilhão de dispositivos (Figura 4), pois quase três de quatro deles seriam equipados com os sensores. Não diferente de 2020, que apesar de queda na venda de smartphones, o aumento do uso de biometria facial em dispositivos aumentou. Segundo Thakkar (2017), a impressão digital é o tipo de biometria mais utilizado atualmente, para identificar uma pessoa de forma confiável utilizando uma característica física quase universal.

Figura 4. Inclusão do sensor de impressão digital em smartphones



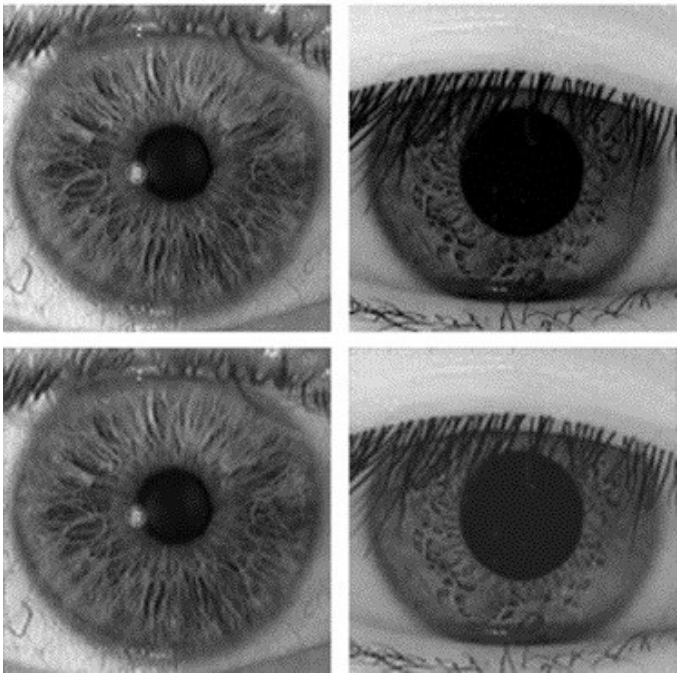
Fonte: Adaptado de *Counterpoint Research* (2017).

3.1.3 Reconhecimento da íris: Faz o reconhecimento da íris.

A tecnologia empregada para o método de autenticação pela íris busca por padrões únicos nos olhos humanos como uma forma de realizar a medição correta da autenticação, o que se torna algo muito vantajoso quando pensamos em fraudes, porém ao mesmo tempo sua tecnologia é tão complexa que encarece o valor do *smartphone*, não se tornando tão difundida (SHAFIQUE et. al, 2017).

O professor e pesquisador John Daughman foi o responsável pelo desenvolvimento do algoritmo *IrisCode* que realiza o reconhecimento da íris. Na Figura 5, é possível visualizar um exemplo de olhos originais e da reprodução proveniente da captura da íris. A estrutura da íris contém padrões intrínsecos que podem ser utilizados para identificação de seres humanos. Os sensores são infravermelhos e usam ondas de luz visíveis. Características como: fibras de colágeno, rugas, sulcos, estrias, sardas e fendas são utilizados com atributos na etapa de classificação desses padrões. (SOUZA; SENZAKO, 2009). “Apesar de algumas doenças alterarem os padrões da íris a chance de fraude é atualmente nula pois alterar seus padrões com finalidade de se passar por outro usuário, é praticamente impossível.” (SOUZA *apud* ROIZENBLATT, 2003).

Figura 5. Análise IrisCode



Fonte: *Information Theory and the IrisCode* (2016).

3.2 Autenticação Multifator

A Autenticação multifator ou MFA (*Multi Factor Authenticator*) consiste em usar mais de uma forma autenticação para comparar a identidade e autenticar-se para acessar algum dado ou plataforma, além da senha tradicional. Também é chamado de 2FA (*Two Factor Authenticator*) ou 3FA (*Three Factor Authenticator*) que dizem respeito à quantidade de métodos requeridos para a autenticação.

> *"One Time Passwords* (OTP) são senhas descartáveis geradas a partir de uma semente previamente compartilhada. O processo de geração de OTPs deve possuir duas entidades: uma geradora e um servidor de verificação. A geradora é um dispositivo de uso pessoal (*smartphone*) com um aplicativo especial." (HALLER, N., METZ, C., NESSER, P., STRAW, M., 1998).

Os métodos mais utilizados para a autenticação multifator são:

● E-mail: Adiciona-se um e-mail de verificação, uma mensagem é enviada para o endereço adicionado, geralmente com um endereço eletrônico para confirmação de acesso.
● Mensagem de texto: Uma mensagem de texto é enviada, com um código ou endereço eletrônico para confirmação. O endereço eletrônico para confirmação deve ser acessado ou o código digitado na plataforma que se deseja acessar.
● Ligação telefônica: Uma chamada é efetuada para o número cadastrado e a confirmação pode ser realizada mediante digitação de algum caractere durante a chamada ou um código é informado para que seja adicionado na plataforma que se deseja acessar.
● Aplicativo: Pode ler um *QR Code* ou gerar um código para ser digitado na plataforma desejada.

Na Figura 6, pode-se ver um exemplo de autenticação multifator, onde o usuário realiza o acesso com login e senha, aprova a solicitação de login por um aplicativo e finaliza a autenticação escaneando sua digital.

Hoje em dia, o MFA é muito utilizado em cenários que necessitem um cuidado maior na segurança do que normalmente é preciso e com o advento de métodos biométricos como forma de autenticação em diversos serviços e principalmente de celulares, melhorou significativamente a segurança ao garantir maiores chances de se conseguir provar a identidade do dono do aparelho ou serviço que esteja utilizando no momento e assim evitando roubo de identidades e fraudes (OMOTOV et. al, 2018)

Figura 6. Simulação de Autenticação Multifator

Fonte: Adaptado de *Secret Double Octopus* (2015).

3.3 *Blockchain*

O *blockchain* é um banco de dados distribuído e surgiu em meados de 2008, ao mesmo tempo que a definição da *bitcoin* por Satoshi Nakamoto, ela vem ganhando espaço no mercado e está sendo implementada em empresas de diversos segmentos. “A tecnologia consiste em ser um ‘livro’ no qual se mantém um registo permanente e a prova de violações devido a sua matemática complexa” (ROUSE, 2016).

Segundo Dittmar (2016), o *blockchain* provê uma solução para uma variedade de preocupações de segurança nos dias de hoje de forma a tornar as nossas autenticações mais simples, necessitando-se de apenas alguns dados para a comprovação, pois, consegue oferecer isso ao descentralizar as identidades dos donos e oferecer um protocolo universal de verificação, utilizando-se dos seus três pilares que são o consenso, a distribuição e a veracidade sendo que a segurança é gerada por um problema matemático denominado de *Proof of Work Problem* (POW), sendo muito utilizada em transações de *bitcoin* por exemplo (DITTMAR, 2016).

Na China, que é uma superpotência com a maior população do mundo, está em constante evolução e portanto, começou-se a ocorrer maiores preocupações em relação ao controle de qualidade dos alimentos produzidos no país, dessa forma eles começaram a utilizar a tecnologia *Blockchain* juntamente com a tecnologia RFID (*Radio-Frequency Identification*), assim sendo o *Blockchain* consegue garantir a informação desde o local de onde o alimento foi produzido e criado, a rota logística em que foi posto e até a distribuição dessa carga para os comerciantes, chegando ao seu comprador final, ou seja a tecnologia consegue funcionar em diferentes esferas da economia de um país e garantir controle de qualidade em cada etapa do processo (TIAN, 2016).

Segundo Bokkem *et. al* (2019) conforme a internet avança, obter informações de pessoas se tornou algo problemático uma vez que os provedores de serviços se tornaram as autoridades centralizadoras o que torna um grande risco ao usuário quando os provedores são atacados. Dessa forma, para melhorar a segurança, a autenticação descentralizada utiliza-se da Identidade Auto Soberana (SSI), uma recente ferramenta com propósito de garantir ao usuário o controle de sua identidade digital.

3.3.1 Identidade Auto Soberana (SSI)

A Identidade Auto Soberana é o conceito que garante a indivíduos e organizações terem total propriedade sobre suas identidades digitais e/ou analógicas. Dessa forma, é possível controlar como seus dados individuais são acessados e utilizados no ambiente digital (ROLIN, 2020).

Hoje em dia, existem países com cenário de identidade digital bem estruturado, já no Brasil as identidades digitais são bem fragmentadas, esse seria um problema a se resolver primeiro antes de trazer a ideia de identidade auto soberana. Segundo Revoredo (2020), no Brasil uma pessoa consegue tirar identidades

físicas diferentes em qualquer Estado. Isto é, uma pessoa má intencionada poderia ter múltiplas identidades físicas, todas com a mesma digital, mas com nome e dados diferentes, devido à falta de integração biométrica entre os Estados.

4. Materiais e métodos

Com base no estudo bibliográfico sobre a área de segurança da informação envolvendo os aspectos da autenticação, como método de segurança implantada em celulares e a partir de artigos científicos, livros da área e sites de referência, para que consigamos aferir os métodos de autenticação e seus aspectos de forma a entendermos suas vantagens, desvantagens e seus pontos discrepantes, fazendo uma análise comparativa adaptada do modelo CMMI (*Capability Maturity Model Integration).*

O Modelo Integrado de Maturidade em Capacitação (CMMI) é uma ferramenta utilizada para o desenvolvimento de softwares de forma a criar cinco níveis de maturação que são: 1 - inicial, 2 - gerenciado, 3 - definido, 4 - gerenciado quantitativamente e 5 - otimizado (GROFFE, 2012). Nesta pesquisa a ferramenta foi adaptada para a avaliação dos métodos de autenticação em celulares, trocando os níveis para: 1 - muito fraco, 2 - fraco, 3 - médio, 4 - forte e 5 - muito forte (Figura 7).

5. Resultados e discussão

Os aspectos utilizados para comparação dos métodos de autenticação foram:

- Praticidade, que foca no quão prático é a sua utilização;
- Segurança, mostrando o nível de confiabilidade e suas possíveis falhas;
- Gerenciabilidade, que aponta a facilidade em sua configuração e manutenção;
- Desempenho, que foca na precisão e estabilidade;
- Acessibilidade, que mostra se o método pode facilitar o uso de pessoas com problemas físicos e
- Aceitabilidade, que define o quão difundido é este método.

Figura 7. Comparação de Métodos de Autenticação

Aspectos / Método	Praticidade	Segurança	Gerenciabilidade	Desempenho	Acessibilidade	Aceitabilidade
Face	5	4	5	4	4	4
Íris	3	5	5	5	4	3
Digital	4	4	4	3	4	5
Multifator	3	5	3	4	4	2

Fonte: Os autores (2021).

De acordo com os resultados acima, podemos verificar que a autenticação facial possui uma boa pontuação em todos os aspectos, uma vez que a verificação pode ocorrer com uma distância física considerável entre o usuário e o celular, mostrando sua praticidade e acessibilidade, boa segurança, porém existem falhas de posicionamento facial e luz de ambiente o que pode acarretar erros de na leitura e consequentemente, no processo de autenticação (THAKKAR, 2017). A autenticação pela íris é uma forte tecnologia de segurança, desempenho e gerenciamento, mas peca pela necessidade de uma aproximação entre o dispositivo e o usuário, além de não ser muito difundida (SHAFIQUE et. al, 2017).

Na autenticação pela impressão digital foi verificado que o método é amplamente aceito e utilizado pelo público em geral, existindo em mais *smartphones* do que outros métodos biométricos, porém o desempenho em comparação com outros métodos é menor uma vez que dependendo da umidade e estado dos dedos, a leitura da digital pode facilmente resultar em falhas de autenticação (PAILANG, 2018). Segundo Marigny (*apud* Diário Digital Lusitano, 2014), as técnicas de biometria foram defendidas pelos europeus como a forma mais segura e exata de conhecer pessoas, segundo um inquérito realizado em setes países europeus.

Já a autenticação multifator apresenta mais fatores de segurança em seu método uma vez que ele combina mais de um tipo de método de segurança existente o que pode dificultar uma fraude ou que o sistema em si seja burlado, porém voltamos ao problema de sua utilização (*user-friendly*), pela demanda maior de tempo provoca uma diminuição em sua aceitação pelo público (SHAFIQUE *et. al*, 2017).

Dentre todos os métodos citados e utilizados nesta pesquisa, a tecnologia *blockchain* está ficando conhecida como um método seguro e de fácil utilização. A estrutura descentralizada garante que, segundo Carvalho (2018) *apud* Stalling (2015), os pilares de segurança da informação sejam seguidos: integridade, confidencialidade e disponibilidade. Também é sabido que esta tecnologia possui uma grande praticidade, uma vez que não é exigido outros intermediadores para validar a operação. Em termos de gerenciabilidade, a estrutura do *blockchain* é imutável, ou seja, não existe a possibilidade de edição ou exclusão do bloco e com a adição de um histórico cronológico de suas ações.

Além dessas características, soma-se a inviolabilidade dos registros que garantem segurança para aplicações da indústria e do mercado. A identidade auto soberana (SSI), segundo Carvalho (2018) *apud* Braga (2017), implementada na tecnologia faz com que apenas os dados essenciais necessitem serem compartilhados somando-se a isso, a SSI facilita em um curto espaço de tempo.

O *blockchain* não entrou na comparação pois até hoje não foi identificada alguma tecnologia específica para a autenticação em smartphones com fins de acesso ao dispositivo ou plataformas e aplicativos. Porém, futuramente, se a tecnologia *blockchain* for utilizada em *smartphones*, poderia compensar os pontos fracos vistos nos métodos estudados gerando um método de autenticação mais robusto, seguro e prático.

6. Considerações finais

Atualmente o mundo se encontra cada vez mais interligado pela internet e conforme a tecnologia avança a segurança dos equipamentos também necessita de inovação. Os celulares estão em uma constante evolução para facilitar o dia a dia do usuário e ao mesmo tempo trabalhando de forma segura com as diferentes formas de autenticações biométricas.

A presente pesquisa concluiu que existem diversas formas existentes de realizar uma autenticação, principalmente com métodos biométricos que afetam diretamente o quesito integridade por tratar de aspectos físicos, porém, dificilmente é possível encontrar métodos totalmente seguro considerando múltiplos fatores e considerando a evolução tecnológica que ocorre exponencialmente conforme o tempo passa. Atualmente, em todos os métodos existentes que foram estudados, existem pontos fortes, assim como falhas, que mesmo esporádicas ou dependentes de algum fator extrínseco, podem ocorrer. Porém, mesmo assim, são as opções mais fortes do mercado em comparação com métodos não biométricos.

O *blockchain* é uma tecnologia que começou a se popularizar principalmente com a utilização de transações financeiras e criptomoedas e que se encontra com novas vertentes para seu uso, com todas as suas ferramentas ela se torna uma tecnologia cada vez mais atrativa e segura para as grandes corporações, abrindo possibilidades para que futuramente a sua utilização como um método de autenticação para celulares exista.

A presente pesquisa pode ser continuada comparando outros métodos de autenticação biométricos que já existem e não foram abordados, assim como métodos que surgirão, sejam eles biométricos ou não, inclusive a b*lockchain,* como possivelmente uma nova forma mais segura e acessível aos usuários, podendo sobrepor os pontos negativos de cada uma das autenticações citadas, fortalecer aquelas já utilizadas hoje ou impulsionar o método multifator, caso seja necessário.

7. Referências

ANTUNES, Bruno. **Conheça os três tipos de métodos de autenticação.** 2014. Disponível em: http://segurancaemsimplesatos.com.br/blog/conheca-os-3-tipos-de-metodos-de-autenticacao/. Acesso em: 03 abr. 2021.

BOKKEM, V, D. et al. “**Self-sovereign identity solutions: The necessity of blockchain technology”**. arXiv, p. 1–8, 2019.

BOLLE, R. M. *et al.* **Guide to biometrics.** New York: Springer Science & Business Media, 2013.

BRITO, Amilton. **Entendendo a Autenticação com Token.** 2009. Disponivel em: https://administradores.com.br/noticias/entendendo-a-autenticacao-com-tokens#:~:text=Autentica%C3%A7%C3%A3o%20baseada%20na%20propriedade%20(o,possui%3A%20Smartcard%20ou%20um%20Token.&text=%C3%89%20comum%20utilizar%20autentica%C3%A7%C3%A3o%20com,conhece%20(Senha%2FPIN). Acesso em 03 abr. 2021.

CARVALHO, Leonardo Rodrigues. **Tecnologia Blockchain e as suas possíveis aplicações no processo**

de comunicação científica. 2018. 95 f. Monografia (Graduação) - Curso de Graduação em Biblioteconomia, Universidade de Brasília, Brasília, 2018. Disponível em: https://bdm.unb.br/bitstream/10483/20896/1/2018_LeonardoRodriguesCarvalho_tcc.pdf. Acesso em: 02 mai. 2021.

COUTINHO, D. **O que é e como funciona a biometria?** 2018. Disponível em: https://ada.vc/2018/05/21/o que-e-biometria/. Acesso em: 24 out. 2020.

DE SORDI, J. O. **Administração da Informação: fundamentos e práticas para uma nova gestão do conhecimento.** São Paulo: Saraiva, 2008.

DHILLON, G. (2004). **Realizing benefits on an information security program.** Business Process Management Journal, 10 (3), 260-261.

DITTMAR, C. B. **"Application of the Blockchain For Authentication and Verification of Identity"**, 2016. Disponível em: http://www.cs.tufts.edu/comp/116/archive/fall2016/bcresitellodittmar.pdf. Acesso em: 24 out. 2020.

GROFFE, Renato José. **CMMI: uma visão geral.** Dev media. Disponível em: https://www.devmedia.com.br/cmmi-uma-visao-geral/25425. Acesso em: 20 mar. 2020.

HALLER, N., METZ, C., NESSER, P., STARW, M (1998). **A One-Time Password System.** RFC 2289. IETF, 1998.

MARTIN, A. P.; KHAZANCHI, D. **Information availability and security policy.** Association for Information Systems - 12th Americas Conference On Information Systems, AMCIS 2006, v. 2, p. 1247–1258, 2006.

MICROSOFT. **Detecção de faces e atributos.** 2019. Disponível em: https://docs.microsoft.com/pt-br/azure/cognitive-services/face/concepts/face-detection

NAKAMOTO, Satoshi. Bitcoin: **A Peer-to-Peer Electronic Cash System.** 2008. 9 p. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em 03 abr 2021.

OMOTOV, A., BEZZATEEV, S. et. al **Multi-Factor Authentication: A Survey.** MDPI: *cryptography*, 2018.

PAILANG. **"The principle and application of semiconductor fingerprint sensor".** 2017. Disponível em: https://gdfingerprint.com/the-capacitive-sensor. Acesso em: 21 mar. 2021.

PERES, T. Morello.; HERMERLY, Elder Moreira. **EXTRAÇÃO DE CARACTERÍSTICAS DE IMPRESSÕES DIGITAIS.** XI ENCONTRO DE INICIAÇÃO CIENTÍFICA E PÓS-GRADUAÇÃO DO ITA, 11., 2005, São José dos Campos. São José dos Campos: CNPQ, p. 155-160 2005. Disponível em: http://www.bibl.ita.br/xiencita/Artigos/ELE05.pdf. Acesso em: 24 out. 2020.

REVOREDO, Tatiana. **Identidade Digital Auto-Soberana.** 2020. Disponível em: https://medium.com/global blockchain-strategy/identidade-digital-auto-soberana-32f3ea297089. Acesso em: 24 abr. 2021.

ROLIN, Gerson. **Você sabe o que é Identidade Digital Auto Soberana?** 2020. Disponível em: https://www.camara-e.net/2020/07/20/voce-sabe-o-que-e-identidade-digital-auto-soberana. Acesso em: 24 abr. 2021.

ROUSE, M. **What is Blockchain?** 2016. Disponível em: https://searchcio.techtarget.com/definition/blockchain. Acesso em: 26 out. 2020.

SENZAKO, Edna Yoshiko. **SSÍRIS - Sistema de segurança baseado em íris: A segurança em seus olhos.** INFOIP: Revista Online de Informática, Inovação e Pesquisa (FATEC, Rio Preto), 2009.

SHAFIQUE. U, KHAN. H, *et. al.* **"Modern Authentication Techniques in Smart Phones: Security and Usability Perspective"**. IJACSA, Vol.8, No.1, 2017.

SHARMA, P. **More Than One Billion Smartphones with Fingerprint Sensors Will Be Shipped In 2018.** 2017. Disponível em: https://www.counterpointresearch.com/more-than-one-billion-smartphones-with-fingerprint-sensors-will-be-shipped-in-2018/. Acesso em: 07 nov. 2020.

SOUZA, J. M. de. **Métodos para Reconhecimento de Íris em Ambiente Não Cooperativo.** Monografia (Pós Graduação em Ciência da Computação). São Carlos. Universidade Federal de São Carlos, 2012. Disponível em: https://repositorio.ufscar.br/bitstream/handle/ufscar/499/4427.pdf?sequence=1&isAllowed=y. Acesso em: 14 nov. 2020.

TCHERNYKH, A. *et al*. **Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability.** Journal of Computational Science, v. 36, 2016.

THAKKAR, D. **Top five biometrics: face, fingerprint, iris, palm and voice.** Bayometric, 2017. Disponível em: https://www.bayometric.com/biometrics-face-finger-iris-palm-voice/. Acesso em: 24 de outubro de 2020.

TIEN, F. **An Agri-food Supply Chain Traceability System for China Based on RFID & Blockchain Technology**. 2016.

WHITMAN, M. E., & MATTORD, H. J. **Introduction to Information Security.** Principles of Information Security. EUA: Cengage, p. 1–38, 2011.