ISBN: 978-989-8533-96-8 © 2019 IADIS

ESTUDO EXPERIMENTAL DA BIOMETRIA COMPORTAMENTAL PARA AUTENTICAÇÃO CONTÍNUA DE USUÁRIOS EM APLICAÇÕES BANCÁRIAS *MOBILE*

Priscila Morais Argôlo Bonfim Estrela, Dino Macedo Amaral, Robson de Oliveira Albuquerque, William Ferreira Giozza, Georges Daniel Amvame-Nze e Alexandre Solon Nery
Universidade de Brasília - Departamento de Engenharia Elétrica, Brasília - DF, Brasil - Zipcode 70910-900

RESUMO

Neste artigo é proposto um *framework* multimodal para autenticação contínua e implícita em aplicações bancárias *mobile*, baseado na biometria comportamental no momento de digitação da senha, em tempo de *login* e na interação via *touchscreen* com a aplicação pós *login*, para geração de alertas de segurança caso um impostor tente se passar por um usuário legítimo na utilização da aplicação. Os resultados demonstram que a abordagem utilizada é promissora. Por exemplo, com o uso do algoritmo *Random Forest* foi possível atingir uma precisão média de 96% com *Equal Error Rate* (EER) de 3,57% para os modelos de digitação da senha, e 99% com EER de 0% para a interação via *touchscreen* com a aplicação pós *login*.

PALAVRAS-CHAVE

Autenticação Contínua, Biometria Comportamental, *Mobile*

1. INTRODUÇÃO

A necessidade de diminuir fraudes em aplicações de meios de pagamento mobile é um problema crescente. E focar apenas na identificação da fraude ao invés da prevenção (L. Peotta *et al*, 2011) é um cenário corrente encontrado em soluções de *Internet Banking*. Neste contexto, a biometria *touch* surge como uma possível solução para esta questão pois, utilizada em conjunto com um outro método de autenticação, via senha por exemplo, pode trazer um maior nível de segurança na autenticação do usuário (P. S. Teh *et al*, 2016). Isso permite tornar a experiência do usuário melhor, bem como reduzir o número de fraudes baseadas no roubo de credenciais, pois, neste cenário, além de roubar as credenciais, seria necessário que o criminoso tivesse um comportamento semelhante ao usuário vítima de fraude na interação com o dispositivo no momento de digitação da senha e na interação com a aplicação.

O *framework* proposto neste trabalho baseia-se em um modelo que une tanto a autenticação contínua estática, quanto a dinâmica, para autenticação do usuário durante todo o momento de interação com a aplicação. A autenticação contínua é baseada nas características do movimento e dos sensores durante a interação com a aplicação por parte do usuário. O foco deste trabalho é voltado para as aplicações bancárias *mobile*. Na fase de desenvolvimento, considera-se um ambiente experimental mais próximo do real, com alguns resultados apontando para uma acurácia entre 96% e 99%, com EER entre 0% e 3,57%, mesmo em um ambiente sem determinação dos dispositivos específicos.

Este artigo está organizado conforme se segue. Na Seção 2 é apresentada uma revisão de conceitos e da literatura. A Seção 3 descreve a modelagem experimental e apresenta e discute os resultados preliminares obtidos com o modelo proposto. Por fim na Seção 4 são apresentadas as conclusões deste trabalho e sugestões para trabalhos futuros.

2. CONCEITOS BÁSICOS E REVISÃO DA LITERATURA

Nesta seção serão apresentados os principais conceitos envolvidos na autenticação contínua em dispositivos móveis, em conjunto com uma revisão da literatura, focada em trabalhos desenvolvidos para aplicações financeiras.

2.1 Conceitos Básicos

A biometria comportamental *touch* refere-se ao processo de medir e avaliar o ritmo do toque humano em dispositivos *touchscreen* mobile (P. S. Teh *et al*, 2016). O comportamento biométrico no uso de um dispositivo *touchscreen*, pode ser obtido a partir das informações coletadas dos vários sensores que compõem os *smartphones* modernos como: acelerômetro, sensor de luz do ambiente, compasso de digitação, giroscópio, GPS, sensor de proximidade, *touchscreen* e WiFi (D.-H. Shih, C.-M. Lu, and M.-H. Shih, 2015). Um conjunto dessas informações coletadas pode ser capturado para construir o padrão biométrico de um indivíduo, de uma forma implícita e não intrusiva.

A autenticação contínua pode ser definida como a contínua verificação da identidade de uma pessoa baseada em aspectos do seu comportamento na interação com um dispositivo computacional (L. Fridman *et al*, 2017), tais como por exemplo a continuidade e a transparência (A. Mahfouz *et al*, 2017). Na autenticação contínua em dispositivos *mobile*, o processo de verificação contínua pode acontecer baseado em um comportamento único, como o padrão de digitação, de forma estática ou pode se dar de forma multimodal, observando um conjunto de vários comportamentos e classificadores para a definição da biometria comportamental do indivíduo de forma dinâmica (L. Fridman *et al*, 2017).

2.2 Trabalhos Relacionados

Em (M. Temper, S. Tjoa, and M. Kaiser, 2015), foi implementado um *framework* para aplicações bancárias *mobile*, baseado na autenticação contínua de usuários. O trabalho envolveu 22 voluntários, que interagiram com uma aplicação prototipada, baseada na interface de uma aplicação original de um banco. Nesse trabalho foram utilizadas 15 características diferentes. Foram colhidos os dados de 30 sessões de cada usuário, sendo que 10 foram utilizadas para treino e as outras 20 para testes. O aparelho utilizado foi um Nexus 4 com Android 4.4.4. A identificação do usuário foi baseada na dinâmica de digitação e na interação com o *touchscreen*. A principal contribuição desse trabalho foi utilizar um classificador baseado na lógica Fuzzy. Apesar do alto EER obtido (11,5%) esse trabalho foi destacado por ter o foco em aplicações bancárias, e sua estrutura conter a captura tanto estática quanto dinâmica da biometria comportamental do indivíduo, o que serve de referência, para a busca por uma melhor precisão.

Em (A. Buriro, S. Gupta, and B. Crispo, 2017) é descrito um experimento com autenticação contínua em aplicações *mobile* com foco em *Internet Banking*, com captura apenas estática, digitação da senha. Para a captura das características foi desenvolvida uma aplicação, bem parecida com uma aplicação original de uma solução de meio de pagamento bem conhecida, que funciona em qualquer dispositivo com Android 4.4.x ou superior. Cada voluntário precisou digitar a senha de 8 dígitos, em 3 sessões durante 3 dias. Foram coletadas 30 amostras de cada um dos 95 usuários, contendo informações do acelerômetro, de orientação, sensor de gravidade, magnetômetro e giroscópio. Com base nessas informações foram geradas 142 características diferentes, para cada indivíduo. O melhor resultado observado durante os experimentos, com uma precisão de 96%, foi utilizando o algoritmo *Random Forest* com 15 amostras para treino.

3. ESTUDO EXPERIMENTAL

O primeiro ponto a ser observado é a contribuição deste estudo para o desenvolvimento de um *framework* que seja capaz de fornecer a autenticação dos usuários durante sua interação com uma aplicação móvel financeira, abrangendo desde os eventos de digitação aos de deslize de tela. Tendo esses aspectos em consideração, a Tabela 1 apresenta um resumo da contribuição deste trabalho em relação a outros trabalhos na revisão da literatura.

Tabela 1. Contribuição deste estudo em relação aos trabalhos correlatos

Trabalhos	Dados Sensores	Autenticação continua estática	Autenticação continua dinâmica	Dispositivos não determinados	Acurácia maior que 95%	Aplicação bancária
(M. Temper, S. Tjoa, and M. Kaiser, 2015)	-	x	x	-	-	x
(A. Buriro, S. Gupta, and B. Crispo, 2017)	x	x	-	x	x	x
Este trabalho	x	x	x	x	x	x

3.1 Modelo de *Framework* para Autenticação Contínua

O modelo de *framework* utilizado para autenticação contínua, ilustrado na Figura 1, permite capturar as características dos usuários na interação com uma aplicação mobile via *touchscreen* tanto de forma estática, no instante de digitação da senha para efetuar o login, denominado Momento 1, quanto de forma dinâmica, na interação com a aplicação após o *login*, movimentos horizontais, verticais e toques, nomeado de Momento 2. Essas capturas são utilizadas para a geração de alertas de segurança caso a precisão de autenticação seja menor que 86% para o Momento 1 e menor que 89% para o Momento 2. Considera-se uma margem de 10% em relação à melhor precisão obtida para cada um dos momentos durante o experimento.

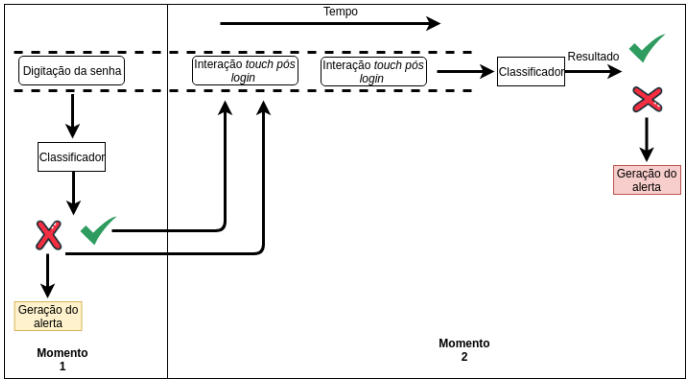

Figura 1. Visão macro do framework de autenticação contínua proposto

3.2 Objetivos do Estudo Experimental

O objetivo deste estudo experimental é investigar, em um ambiente simulado de uma aplicação bancária móvel, mais próxima do real, como as características da interação capturadas nos Momentos 1 e 2, podem ser utilizadas para autenticação contínua de um indivíduo. Para compor este objetivo maior, foram estabelecidas algumas perguntas de interesse:

1. Qual a quantidade mínima de interações necessárias para treino do modelo, tornando possível autenticar um usuário ao digitar uma senha?
2. Qual a quantidade mínima de interações necessárias para treino do modelo, tornando possível autenticar um usuário a partir da interação com uma aplicação após *login*?
3. O padrão de digitação e interação do usuário entre *logins* se mantém consistente?
4. As informações capturadas de sensores são realmente relevantes para a definição de um modelo de autenticação contínua baseada em biometria comportamental?

3.3 Experimento

Para a definição do comportamento biométrico na interação com o *touchscreen*, tanto no Momento 1 quanto no Momento 2, as características são capturadas por meio de uma aplicação Android, utilizando as APIs *MotionEvent* e *SensorEvent* conforme Tabela 2.

Tabela 2. Características coletadas no experimento

Característica	**Método/atributo**	**Sensor**
Tempo	getEventTime(), getDownTime()	—
Ação	getAction()	—
Pressão	getPressure()	—
Tamanho do dedo	getSize()	—
Coordenada x	getX()	—
Coordenada y	getY()	—
Velocidade angular ao redor do eixo x	values[0]	Acelerômetro
Velocidade angular ao redor do eixo y	values[1]	Acelerômetro
Velocidade angular ao redor do eixo z	values[2]	Acelerômetro

Além das características listadas na Tabela 2, o experimento incluiu características derivadas destas, como os intervalos de toques na tela, médias do tempo de pressionamento, média do tamanho do dedo e pressão, compondo ao todo 12 características avaliadas no Momento 1, e 14 para o Momento 2.

Para a captura das características foi desenvolvida uma aplicação *mobile* Android englobando as versões 5.0 a 9.0, considerando versões 21 a 28 da SDK. A aplicação foi composta de um fluxo de cadastro e três fluxos de serviços, cada um com duas telas, além da tela de digitação da senha e menu para a seleção do serviço. Considerou-se um total de 8 telas possíveis para a captura de características da interação *touch*, disponibilizadas comumente por uma aplicação bancária *online*, e em particular no caso deste trabalho, as funções de consulta de saldo, pagamento de boleto e transferência. Para o cadastro foi necessário informar uma senha de 6 a 8 dígitos.

Os usuários foram convidados a interagir com a aplicação durante dois dias, via *Firebase App Distribution*. Nesse período, 16 usuários participaram do experimento de forma anônima, com a aplicação gerando um identificador aleatório para cada um. Apenas 14 usuários forneceram dados suficientes para a geração de modelos. Foram capturados um mínimo de 25 *templates* por usuário, com pelo menos 6 interações com a aplicação. Os *templates* coletados foram armazenados em um *Firebase Realtime Database*.

Os aparelhos utilizados no teste foram: Xiaomi Redmi Pro, Motorola XT1635-02, Samsung GT-I9500, LG F670S, LG-M250, Nexus 6P, Motorola One, Xiami POCOPHONE F1, Xiaomi Pixel, Samsung SM-A305GT, Samsung SM-G530H, Samsung SM-G800H, Samsung SM-G930F, Samsung SM-G950F, Samsung SM-G955U, Samsung SM-G975F, Samsung SM-J500M, Xiaomi XT1925.

3.4 Resultados

Para a criação dos modelos foram avaliados 3 algoritmos de Aprendizado de Máquina diferentes: *Support Vector Machine* (SVM), *Random Forest* (RF) e *K-NearestNeighbors* (KNN), disponíveis na biblioteca *python scikit-learn*. Para cada um dos Momentos foi criado um modelo por usuário. Cada usuário teve um modelo treinado para a digitação da senha e outro para a interação *touchscreen* após *login*. A Tabela 3 mostra os resultados obtidos para autenticação no Momento 1 e para o Momento 2.

Para o Momento 1, foram necessários no mínimo 3 templates para treino do modelo utilizado na autenticação, obtendo-se uma precisão de 96% com o algoritmo RF, e EER de 3,57%. Para o Momento 2, foram necessários no mínimo 5 templates, resultando em uma precisão de 99% com o algoritmo RF e EER de 0%. O experimento se deu entre sessões e entre dias, mostrando que o reconhecimento do padrão de interação com a aplicação se mantém consistente neste período. O algoritmo com o melhor desempenho para ambos os Momentos de autenticação foi o RF. Entre as características consideradas mais importantes para os modelos criados pelo RF, pelo menos 2 das 3 características foram capturadas via acelerômetro, indicando que as

informações coletadas de sensores são determinantes na definição de um modelo de autenticação contínua baseada em biometria comportamental touch.

Tabela 3. Precisão média dos modelos nos 2 momentos avaliados

	Momento 1 – Digitação da senha	**Momento 2 – Interação com aplicação pós *login***
Algoritmos	**Acurácia**	**Acurácia**
SVM	0,8116	0,8211
RF	0,9649	0,9943
KNN	0,9585	0,9592

4. CONCLUSÃO

Os resultados preliminares observados neste estudo experimental, permitiram obter 96% de acurácia média com EER de 3,57% para autenticação contínua estática, baseada no padrão de digitação de senha, e 99% com EER de 0% para autenticação contínua dinâmica, pós *login*. A autenticação contínua de usuários baseado no seu comportamento via interação *touchscreen* no uso de aplicações em *smartphones*, mostra-se promissora. É possível prever seu uso como forma de garantir um método de autenticação não intrusivo, sem custos adicionais de hardware, se aliada a outros métodos tradicionais de autenticação. O estudo ainda prevê a possibilidade de melhorar a experiência do usuário de aplicações financeiras, de uma forma implícita, além de gerar redução de gastos com fraudes baseadas em roubos de credenciais.

Como trabalhos futuros pretende-se incluir no modelo informações de contexto do usuário, incrementar as características com dados de outros sensores disponíveis no aparelho, ampliar o número de usuários, com a disponibilização do *framework* funcional *online* para fins de pesquisa na *Play Store Google Play*.

AGRADECIMENTO

Os autores agradecem o apoio das Agências brasileiras de pesquisa, desenvolvimento e inovação CNPq (Projeto INCT SegCiber 465741/2014-2), CAPES (Projetos FORTE 23038.007604/2014-69 e PROBRAL 88887.144009/2017-00) e FAPDF (Projetos UIoT 0193.001366/2016 e SSDDC 0193. 001365/2016) e ao Programa de educação continuada da Universidade Corporativa Banco do Brasil (UniBB), bem como o suporte do Laboratório LATITUDE/UnB (Projeto SDN 23106. 099441/2016-43), e as cooperações com o Ministério da Economia (TEDs DIPLA 005/2016 e ENAP 083/2016) e o Gabinete de Segurança Institucional da Presidência da República (TED 002/2017).

REFERÊNCIAS

A. Buriro, S. Gupta, and B. Crispo, 2017. Evaluation of motion-based touch-typing biometrics for online banking. In2017 International Conference of the Biometrics Special Interest Group (BIOSIG). IEEE, Darmstadt, Germany, pp 15.

A. Mahfouz *et al*, 2017, A survey on behavioral biometric authentication on smartphones. Elsevier Journal of information security and applications, vol. 37, pp. 28–37.

D.-H. Shih, C.-M. Lu, and M.-H. Shih, 2015. A flick biometric authentication mechanism on mobile devices. in 2015 International Conference on Informative and Cybernetics for Computational Social Systems (ICCSS). IEEE, Chengdu, China, pp. 31–33.

L. Fridman*et al*, 2017. Active authentication on mobile devices via stylometry, application usage, web browsing, and gps location. IEEE Systems Journal, vol. 11, no. 2, pp. 513–521.

L. Peotta *et al*, 2011. A formal classification of internet banking attacks and vulnerabilities. In International Journal of Computer Science & Information Technology, vol. 3, pp 186-197.

M. Temper, S. Tjoa, and M. Kaiser, 2015. Touch to authenticate - continuous biometric authentication on mobile devices. 2015 1st International Conference on Software Security and Assurance (ICSSA). IEEE. Suwon, South Korea, pp. 30-35.

P. S. The *et al*, 2016. A survey on touch dynamics authentication in mobile devices. In Elsevier, Computers &Security, vol. 59, pp 210–235.