Autenticação Contínua Usando Sensores Inerciais dos Smartphones e Aprendizagem Profunda

Ismael J V Paz, Hendrio L S Bragança, Eduardo Souto

[1] Instituto de Computação (ICOMP) – Universidade Federal do Amazonas

{ismael.vidal, hendrio.luis, esouto}@icomp.ufam.edu.br

Abstract. *Smartphones are part of our daily lives and can help perform various tasks, from measuring physical activities to banking operations. To ensure the data security of this device, most systems employ static authentication solutions, such as password, pattern, PIN or fingerprint. However, in a scenario where an imposter user has access to the passwords or gains physical access to the unlocked device, all sensitive data ends up being exposed. To deal with this problem, this work proposes a continuous authentication method for mobile devices using data from inertial sensors. The process of identifying the genuine or imposter user is performed through an authentication model defined from a deep network architecture based on convolutional neural networks with recurrent layers. Furthermore, this work employs a trust model to avoid blocking genuine users and preventing an imposter from being undetected for a long time. Tests using data from 30 users show that the proposed model can detect imposter users in up to 61 seconds.*

Resumo. *Muitos usuários têm optado pelo uso de dispositivos móveis como smartphones para a realização de tarefas do dia a dia. Para garantir a segurança desses dados, a maioria dos sistemas emprega soluções de autenticação estática, tais como senha, padrão em grade, chave de segurança ou sensor de impressão digital. Entretanto, em um cenário onde um usuário impostor tem acesso às senhas ou obtém acesso físico ao dispositivo desbloqueado, todos os dados acabam sendo expostos. Para lidar com esse problema, este trabalho propõe o desenvolvimento de um método de autenticação contínua para dispositivos móveis utilizando os dados de sensores inerciais. O processo de identificação do usuário genuíno ou impostor é realizado por meio de um modelo de autenticação definido a partir de uma arquitetura de rede profunda baseada em redes neurais convolucionais com camadas recorrentes. Além disso, este trabalho emprega um modelo de confiança visando evitar o bloqueio de usuários genuínos e impedir que um impostor fique muito tempo agindo sem ser detectado. Testes utilizando dados de 30 usuários mostram que o modelo proposto consegue detectar os usuários impostores em até 61 segundos.*

1. Introdução

Os smartphones têm substituído cada vez mais o uso de computadores na realização de tarefas cotidianas como envio de e-mails, pagamento de contas e outras transações bancárias. Entretanto, agregar muitas informações em um único dispositivo implica em um custo associado à segurança e privacidade das informações do usuário. As

informações armazenadas em smartphones podem apresentar conteúdos sensíveis como dados pessoais, credenciais de autenticação de aplicações (por exemplo, *login* e senha de aplicações bancárias), números de cartão de crédito, mensagens privadas, informações do trabalho, dentre outros.

Para minimizar os problemas de segurança e privacidade do usuário, a maioria dos smartphones emprega uma abordagem de autenticação baseada em credenciais de conta (e.g. login e senha, padrões e PIN - *Personal Identification Number*) para verificar a identidade do usuário. Esse processo é chamado de autenticação estática *(Static Authentication - SA)*, visto que ocorre somente uma vez, quando o usuário acessa o dispositivo ou uma aplicação em específico (Mahfouz, Mahmoud, & Eldin, 2017).

Um problema com essa abordagem é que o usuário pode deixar de bloquear o smartphone em diversas situações, o que permite que um intruso acesse o dispositivo. Além disso, existem inúmeras formas de burlar o acesso, permitindo que o invasor tenha acesso às informações sensíveis disponíveis no dispositivo. Por exemplo, Javed, Beg, Asim, Baker, and Al-Bayatti (2020) descrevem ataques (*side-channel attacks*), em que a senha pode ser inferida a partir de entradas do teclado virtual com precisão usando dados de sensores dos smartphones. Aviv, Gibson, Mossop, Blaze, and Smith (2010) demonstram que é possível identificar senhas a partir dos rastros de manchas na tela, esse ataque é conhecido como *smudge attack*. Ataques que observam o conteúdo exibido na tela do dispositivo sem o consentimento dos usuários, também conhecidos como *Shoulder Surfing*, demonstram ter sério impacto na privacidade e na segurança dos usuários (Marques, Guerreiro, Carriço, Beschastnikh, & Beznosov, 2019). Na tentativa de minimizar esses problemas, os fabricantes de smartphones têm incorporado mecanismos de autenticação baseado em informações biométricas como impressões digitais ou imagens de rosto. Entretanto, tais mecanismos também são sujeitos a ataques *smudge* (Aviv et al., 2010) e (Nguyen, Sae-Bae, & Memon, 2017) e ataques de captura de vídeo (Mahbub, Patel, Chandra, Barbello, & Chellappa, 2016).

Uma maneira de superar as limitações deixadas pela abordagem de autenticação estática é adotar o uso da autenticação contínua (*Continuous Authentication* - CA) como uma camada de segurança adicional, verificando a autenticidade do usuário continuamente durante o uso do dispositivo. Na literatura existem diferentes mecanismos que fornecem a autenticação contínua do usuário com base nos padrões de toque na tela (Patel, Chellappa, Chandra, & Barbello, 2016) ou de marchar do usuário (Muaaz & Mayrhofer, 2017). O reconhecimento do usuário por meio do toque na tela é ineficiente devido à necessidade constante de forçar o usuário a realizar o processo de autenticação (M. P. Centeno, Moorsel, & Castruccio, 2017). Por outro lado, a autenticação baseada no caminhar do usuário também possui limitações, pois nem sempre o usuário está caminhando enquanto utiliza o dispositivo (Muaaz & Mayrhofer, 2017).

Uma alternativa para resolver esses problemas é a adoção da biometria comportamental baseada em dados coletados pelos diversos sensores existentes nos smartphones. A proposta de usar um método de biometria comportamental no processo de autenticação do usuário é promissora porque os dados coletados podem ser obtidos de forma silenciosa, transparente, sem incomodar o usuário genuíno e sem alertar o impostor sob avaliação (Büch, 2019).

Para tratar limitações apresentadas, este trabalho propõe o desenvolvimento de um método de autenticação contínua para dispositivos móveis utilizando os dados de sensores inerciais: acelerômetro, giroscópio e magnetômetro. O método de autenticação proposto utiliza uma rede neural profunda com uma arquitetura de redes neurais convolucionais (*Convolutional Neural Networks* - CNN) e camadas recorrentes (*Long Short-Term Memory* - LSTM). As camadas de convolução são usadas no processo de extração automática de características e as camadas de recorrência são responsáveis pela modelagem de características temporais dos dados processados pelas camadas convolucionais. A principal vantagem de utilizar aprendizagem profunda é a sua capacidade de criar modelos capazes de analisar e aprender o comportamento humano para a autenticação do usuário.

Além disso, este trabalho emprega um modelo de confiança proposto por Mondal and Bours (2015a) para evitar o bloqueio de usuários genuínos e impedir que um impostor fique muito tempo agindo sem ser detectado. Os resultados experimentais com dados de 30 usuários mostram que o modelo proposto consegue detectar um usuário impostor em até 61 segundos. Esses resultados são promissores e comprovam a viabilidade do uso de dados de sensores inerciais na definição de modelos de autenticação contínua.

O restante deste trabalho está organizado da seguinte forma: a Seção 2 descreve alguns trabalhos relacionados no contexto de CA. A Seção 3 apresenta o método de CA proposto. A Seção 4 detalha os experimentos e apresenta os resultados. Por fim, a Seção 5 apresenta as considerações finais.

2. Trabalhos Relacionados

Os sistemas de reconhecimento de autenticação contínua para smartphones podem ser desenvolvidos a partir de dados extraídos das interações do usuário com a tela (Mondal & Bours, 2015b) (Dee, Richardson, & Tyagi, 2019) e teclado (Gao et al., 2021) (Darabseh & Siami Namin, 2015) ou a partir de dados dos sensores (M. P. Centeno et al., 2017) (Büch, 2019). Informações comportamentais como padrão de marcha do usuário (Santos et al., 2017) (Bhattarai & Siraj, 2018) e de localização do usuário (dados do GPS) (Jin, Tomoishi, & Matsuura, 2017) também têm sido empregadas para desenvolver autenticadores biométricos. Nesta seção, nós descrevemos alguns trabalhos que propõem a utilização de dados dos sensores inerciais presentes nos smartphones para construção de modelos de autenticação contínua.

Lee and Lee (2016) propõem um sistema de autenticação, denominado de *iAuth*, que combina dados de sensores de dispositivos vestíveis (smartwatch e smartphone). O *iAuth* inclui um módulo de autenticação na nuvem que permite que o conjunto de dados de treinamento (dados dos sensores: acelerômetro, giroscópio e magnetômetro) seja usado para gerar modelos eficientes. Resultados experimentais usando o algoritmo KRR (*Kernel Ridge Regression*) mostram que o *iAuth* pode alcançar taxas de acurácia de até 92.1% com consumo de bateria inferior a 2%.

Shen, Chen, and Guan (2018) desenvolvem um mecanismo de autenticação contínua usando sensores inerciais (acelerômetro e giroscópio) dos smartphones. Os autores extraem características no domínio do tempo e da frequência a partir dos dados dos sensores e investigam a melhor combinação de características para caracterizar os padrões de movimento dos usuários. Os resultados experimentais avaliando diferentes cenários apresentam taxas de erros (ERR) que variam entre 2.21% à 28.22%.

M. P. Centeno et al. (2017) propõem um sistema de autenticação biométrica contínua que se baseia em padrões de movimento do usuário enquanto interage com o smartphone. O modelo de autenticação é baseado em uma arquitetura de rede neural autocodificadora. Os resultados experimentais mostram que o sistema proposto alcança 2,2% (EER) nos cenários testados do mundo real.Em um outro trabalho, M. P. n. Centeno, Guan, and van Moorsel (2018) propõem a utilização de dados dos sensores inerciais para realizar a autenticação do usuário usando uma rede neural convolucional siamesa. A extração de características é realizada pela rede neural convolucional e a classificação (usuário legítimo e intruso) é obtida usando o classificador OCSVM (*One-Class Support Vector Machine*). Os resultados experimentais apresentam taxas de acurácia de 97,8% e ERR de 3%. Entretanto, Büch (2019) estende o trabalho de Centeno, Guan e Moorsel propondo uma análise da rede convolucional siamesa em diferentes cenários reais. Os resultados mostram que as taxas de acurácia são inferiores às apresentadas em seus trabalhos anteriores se condições mais próximas do cenários do mundo real forem aplicadas.

Diferentemente das abordagens apresentadas, o modelo de autenticação contínua proposto neste trabalho utiliza uma arquitetura de rede profunda híbrida baseada em camadas de convolução e de recorrência para gerar modelos de autenticação a partir da combinação de dados extraídos do acelerômetro, giroscópio e magnetômetro. Outra questão importante discutida neste artigo é sobre as métricas de desempenho utilizadas na CA. A maioria dos artigos, como os citados acima, avalia seus resultados usando taxas de falso positivo (FAR), falso negativo (FRR), erro igual (EER) e acurácia (ACC). Além dessas métricas, nós acreditamos que é importante para um sistema de CA detectar quando uma intrusão está acontecendo. Isso nos permite saber quanto tempo os impostores conseguiram interagir com o sistema antes da detecção. Por essa razão, nós também usamos outras métricas de avaliação adotadas no trabalho de Mondal and Bours (2015a): o Número Médio de Ações de Impostor (ANIA) e o Número Médio de Ações Genuínas (ANGA).

3. Autenticação Contínua Usando Sensores Inerciais

Esta seção detalha o método autenticação baseada nos dados dos sensores inerciais proposto. Uma visão geral da arquitetura é apresentada na Figura 1 e consiste de quatro etapas: aquisição de dados, pré-processamento dos dados, construção do modelo de classificação e aplicação do modelo de confiança. Estas etapas são detalhadas nas seções seguintes.

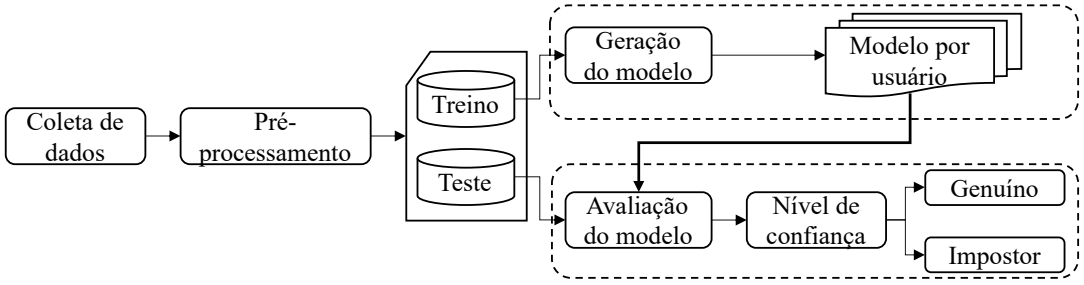

Figura 1. Visão geral do método de autenticação contínua proposto.

3.1. Aquisição e Pré-processamento dos Dados

Em geral, os dados coletados de sensores inerciais de smartphones são organizados cronologicamente na forma de uma série temporal. Os dados do acelerômetro, por exemplo, são representados por um conjunto de três vetores $acc_i = (x_i, y_i, z_i)$, onde $i = (1, 2, 3, ..., n)$. Nós avaliamos a construção de modelos de classificação utilizando a combinação de dados do acelerômetro, giroscópio e magnetômetro. Um exemplo para o sensor de acelerômetro para diferentes usuários pode ser visto na Tabela 1.

Tabela 1. Representação tabular dos dados brutos do acelerômetro.

index	acc_x	acc_y	acc_z	user_id
1	-0,0197	-0,6146	0,7356	u5
2	0,5587	-0,8722	0,8313	u5
...	...	...	...	...
25885	-1,0832	0,6966	0,0148	u12
25886	-1,0832	0,6966	0,0148	u12

Os dados brutos coletados são pré-processados sendo divididos em blocos menores, chamados de segmentos, utilizando uma técnica de janela deslizante (Banos, Galvez, Damas, Pomares, & Rojas, 2014). Dessa forma, o particionamento dos dados é realizado a uma taxa de amostragem com sobreposição de 50%. Um dos motivos para a adoção da janela deslizante é baseado na sua simplicidade em termos de implementação e processamento, o que a torna ideal para aplicações em tempo real (Bragança et al., 2019).

Cada segmento contém uma quantidade limitada de amostras que é definida pelo seu tamanho **bragancca2019reconhecimento**. Um segmento de dados $w_i = (t_i, t_f)$ possui um tempo inicial t_i e um tempo final t_f. Logo, a segmentação consiste em obter um conjunto de segmentos $W = (w_1, ..., w_m)$. Esse processo é realizado considerando também as múltiplas séries disponíveis na base de dados.

3.2. Modelo de Autenticação: Arquitetura de Rede Neural DeepConvLSTM

O processo de extração de atributos a partir de dados de sensores inerciais que modelam uma assinatura comportamental de um usuário requer conhecimento especializado. Por essa razão, este trabalho usa uma arquitetura de rede neural profunda proposta por Ordóñez and Roggen (2016), denominada de DeepConvLSTM, conforme mostra a Figura 2. A arquitetura combina camadas convolucionais, que atuam como extratores de características (neste caso, correlações entre dados dos sensores inerciais) e fornecem representações abstratas dos sinais dos sensores. O modelo proposto possui três camadas convolucionais. Cada camada possui 32 filtros e um tamanho de kernel igual a 4, possui taxa de regularização de 0,01, função de ativação *relu* e *BatchNormalization* entre as camadas de convolução.

O modelo possui duas camadas recorrentes LSTM (*Long Short-Term Memory*) após as camadas de convolução, pois as dependências internas entre os dados dos sensores podem trazer informações de contexto significativas ou padrões desconhecidos que podem ser úteis para identificar comportamentos como uma correlação entre os diferentes sensores. As unidades de um LSTM são usadas como unidades de construção e, neste

caso, cada camada recorrente é composta por 64 unidades. A saída da rede é obtida através de uma camada densa de uma unidade com a função de ativação *sigmoid*, que contém a probabilidade da amostra pertencer ao usuário genuíno ou impostor.

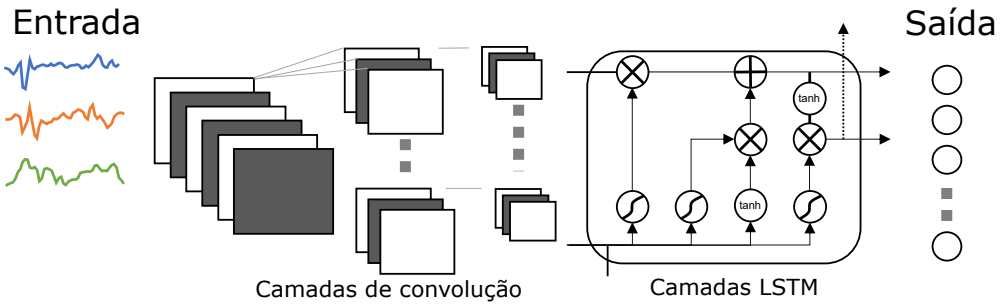

Figura 2. Arquitetura para autenticação contínua em smartphones baseada na rede neural DeepConvLSTM. Os dados dos sensores inerciais são processados por três camadas convolucionais. Duas camadas recorrentes produzem o resultado da classificação com uma camada de saída. Uma camada densa de 1 unidade com a função de ativação sigmoidal contém a probabilidade de que a amostra pertença ao usuário genuíno ou impostor.

3.3. Modelo de Confiança e as Métricas ANGA e ANIA

No modelo de confiança proposto por Bours (2012), as ações realizadas por um usuário em avaliação são continuamente comparadas com o modelo que expressa as ações realizadas pelo usuário genuíno. Assim, se uma ação específica for executada de acordo com a forma como o usuário genuíno realizaria a tarefa (modelo de usuário genuíno), a confiança do sistema nesse usuário aumenta. Tal procedimento é chamado de recompensa. Por outro lado, se houver um desvio entre os comportamentos do usuário genuíno e do usuário que está sendo avaliado, a confiança do sistema nesse usuário diminui, causando uma penalidade de confiança.

Penalidades sucessivas podem fazer com que o nível de confiança exceda um limite mínimo de confiança estabelecido, o que faz com que o sistema seja bloqueado até que uma nova autenticação seja realizada (por exemplo, autenticação por senha). Espera-se que o usuário genuíno gere mais recompensas sucessivas durante um período de teste quando comparado a um usuário impostor.

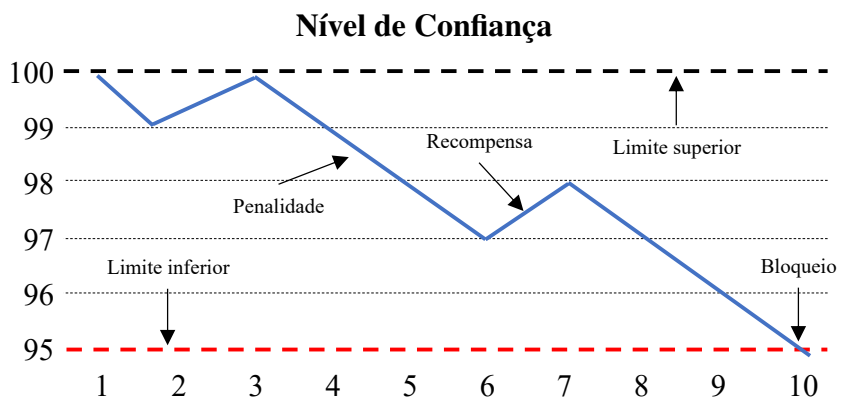

Figura 3. Cenário de um usuário bloqueado.

A Figura 3 exemplifica o comportamento do modelo de confiança durante um período de tempo de utilização do smartphone por um usuário não-autorizado. Nesse cenário foi levado em consideração um limiar de confiança de 95 pontos. O usuário impostor tenta utilizar o dispositivo. No instante 2 e 7, por exemplo, o usuário impostor apresenta comportamento semelhante ao do usuário genuíno. Entretanto, quando um intruso simula um comportamento genuíno, precisa manter o padrão autêntico por um período de tempo, caso contrário, será bloqueado e será necessária uma nova autenticação biométrica. Esse recurso permite que nosso modelo de autenticação detecte ataques de falsificação em tempo rápido com alta precisão, conforme demonstrado em nossos resultados. Para atingir esse objetivo é necessário medir o desempenho com base no número médio de ações impostoras (ANIA) e no número médio de ações genuínas (ANGA).

A função de cálculo de ANGA é dada por:

$$ANGA = \frac{1}{n}\sum_{i=1}^{n}\frac{agen}{bgen} \tag{1}$$

onde *n* é o número usuários, *ag* é o número de ações genuínas de cada usuário e *bg* é o número de vezes que o usuário genuíno é bloqueado indevidamente (bloqueio genuíno).

A função de cálculo de ANIA é dada por:

$$ANIA = \frac{1}{n}\sum_{i=1}^{n}\frac{aimp}{bimp} \tag{2}$$

onde *n* é o número usuários, *aimp* é o número de ações impostoras de cada usuário e *bimp* é o número de bloqueios impostores. O desejável é que haja um número reduzido de bloqueios genuínos (*bgen*) e um elevado número de bloqueio impostor (*bimp*). Quando não há bloqueios genuínos, *bgen* é zero e ANGA tende ao infinito.

Em resumo, o ANIA deve ser o mais baixo possível, para que os usuários do ANIA possam ser identificados mais rapidamente e realizar menos operações ilegais. O ANGA deve ser o mais alto possível para que os usuários legítimos possam utilizar o dispositivo sem interrupção.

4. Experimentos e Resultados

Para validar o modelo proposto foram realizados três conjuntos de experimentos:

(i) Avaliação do impacto da utilização de diferentes combinações de sensores inerciais na acurácia do autenticador proposto. Foram realizados três rodadas de avaliações com as seguintes combinações: somente acelerômetro, acelerômetro com giroscópio, acelerômetro com giroscópio e magnetômetro.

(ii) Comparação dos resultados do modelo proposto com os modelos propostos por (M. P. n. Centeno et al., 2018) e (Büch, 2019). Estes trabalhos foram escolhidos por implementarem CA baseados em sensores inerciais.

(iii) Avaliação do modelo de confiança. Esse trabalho realiza uma comparação com o trabalho proposto por (Mondal & Bours, 2015b) que utiliza modelo confiança para autenticação contínua de usuários baseado em dados de toques na tela. Não foram encontrados trabalhos que implementam o modelo de confiança para a autenticação contínua baseada em sensores de smartphones.

Todos os experimentos foram realizados em um servidor Intel Core i7-7700, 3.60GHz, 64GB RAM com o sistema operacional Linux Mint 19 64 bits. Este servidor possui uma placa GeForce GTX 1080 Ti utilizando o CUDA 10.1. O modelo foi implementado usando a linguagem Python 3.6 e bibliotecas públicas de aprendizagem de máquina.

As seções seguintes descrevem a base de dados utilizada, detalha as metodologias de separação de dados e os processos de verificação do nível de confiança, além de apresentar os parâmetros que serão empregados nos algoritmos. Por fim, serão discutidos os resultados encontrados.

4.1. Base de dados

O conjunto de dados HMOG (*Hand Movement, Orientation, and Grasp dataset*) (Sitová et al., 2016) é comumente utilizado em diversos trabalhos de autenticação contínua para dispositivos móveis (M. P. n. Centeno et al., 2018), (M. P. Centeno et al., 2017) e (Büch, 2019). A base de dados possui registros de 100 usuários de smartphones com o sistema operacional Android. Para cada usuário, os dados são coletados em 24 sessões diferentes, no intervalo de 5 a 15 minutos. Essas sessões incluem leitura, escrita e navegação em mapa em duas condições diferentes de movimento corporal (andar e sentar). Cada usuário gerou cerca de 5 horas de dados e possui dados de acelerômetro, giroscópio, magnetômetro e evento de toque, sendo que os sensores inerciais foram coletados a uma taxa de 100Hz. Para nossa proposta foram selecionados 30 usuários, escolhidos aleatoriamente. Os usuários cujo $id = (733162, 526319, 796581, 207696)$ foram removidos da base de dados, pois estavam sem informação ou com informação incompleta.

4.2. Separação dos Dados

Para treinamento do modelo de autenticação por usuário, o conjunto de dados HMOG foi separado em dois subconjuntos: treino e teste. A rede DEEPCONVLSTM foi treinada com dados do usuário genuíno e impostor. Para cada usuário, o treinamento ocorre com 50% dos dados do usuário genuíno e os outros 50% formado pelos dados dos *N* usuários impostores. Essa abordagem foi adotada para evitar o desbalanceamento da base, evitando que o resultado esteja enviesado para o genuíno ou para o impostor.

Para testar o modelo de autenticação por usuário, o conjunto de teste é composto por dados que não foram utilizados durante a fase de treinamento, ou seja, 50% dos dados restantes do usuário genuíno e 50% dos dados dos usuários impostores, seguindo a mesma lógica de formação dos dados de treinamento, evitando assim o desbalanceamento do modelo.

4.3. Nível de Confiança

O nível de confiança trata a sensibilidade do sistema em bloquear ou não o usuário, evitando que usuários genuínos sejam bloqueados, logo reduzindo o FRR. A Tabela 2 mostra os limiares para realizar a penalização ou de recompensa. As funções de recompensa serão utilizadas no caso de $T_{\mathrm{c}} > 0.5$, o segundo limiar de recompensa serve para decidir qual função de recompensa será utilizada.

A primeira função de recompensa ${f^1}_{\text{recompensa}} x_{\mathrm{i}} = x_{\mathrm{i}}$ fornece os valores da acurácia da rede neural no intervalo de $0.5 < x < 0.9$, sendo assim mais moderada. No caso do

Tabela 2. Parâmetros utilizados no nível de confiança

Limiar de recompensa/penalidade	$T_{\text{c}} = 0.5$
Segundo limiar de recompensa	$T_{\text{cr}} = 0.9$
Segundo limiar de penalidade	$T_{\text{cp}} = 0.4$
Funções de recompensa	${f^1}_{\text{recompensa}} x_{\text{i}} = x_{\text{i}}, {f^2}_{\text{recompensa}} x_{\text{i}} = 1$
Funções de penalidade	${f^1}_{\text{penalidade}} x_{\text{i}} = 1 - x_{\text{i}}, {f^2}_{\text{penalidade}} x_{\text{i}} = 1$

resultado da rede neural estiver entre os valores $0.9 < x < 1$ é utilizado a segunda função de recompensa ${f^2}_{\text{recompensa}} x_{\text{i}} = 1$ atribuindo 1 ao resultado. Isso permite recompensas maiores para resultados mais precisos.

Em relação as funções de penalidade a primeira ${f^1}_{\text{penalidade}} x_{\text{i}} = 1 - x_{\text{i}}$ é utilizada quando x estiver no intervalo de $0.4 < x < 0.5$, caso x a rede neural retorne um valor $x < 0.4$ é atribuída a segunda função, penalizando o usuário de maneira mais drástica dado a maior probabilidade de um usuário impostor.

4.4. Métricas de Avaliação

Para avaliação do método proposto foi utilizado a acurácia da rede neural, o FAR e o FRR que são métricas relacionadas aos usuários impostores aceitos e impostores negados de acessar sistema de autenticação, respectivamente. Além dessas métricas o ANIA e o ANGA, introduzidos pelo trabalho de (Mondal & Bours, 2015a), permitem entender a eficiência do sistema. A Tabela 3 faz uma sumarização das métricas utilizadas nessa pesquisa.

Tabela 3. Métricas utilizadas no Método Proposto

Metrica	Fórmula	Descrição
FAR	$FAR = \frac{False\ Acceptances}{Correct\ Rejects}$	elementos classificados erroneamente como genuíno mas que pertenciam ao impostor.
FRR	$FRR = \frac{False\ Rejects}{Correct\ Acceptances}$	elementos classificados erroneamente como impostor mas que eram genuínos.
EER	$EER = \frac{FFR + FRR}{2}$	essa métrica é a composição da FRR com a EER.
ANIA	$ANIA = \frac{1}{n} \sum_{i=1}^{n} \frac{aimp}{bimp}$	quantidade média de iterações até bloquear o usuário impostor.
ANGA	$ANGA = \frac{1}{n} \sum_{i=1}^{n} \frac{agen}{bgen}$	quantidade de bloqueios do usuário genuíno durante o uso do dispositivo.

4.5. Resultados

Nesta seção são apresentados os resultados obtidos pelo método de autenticação contínua proposto. O primeiro conjunto de experimentos teve como objetivo validar quais conjuntos de sensores inerciais produzem os melhores resultados. Foram avaliadas as seguintes combinações de sensores: somente os dados acelerômetro (acc), acelerômetro e giroscópio (acc+gyr), e por último o acelerômetro em conjunto com o giroscópio e magnetômetro (acc+gyr+mag).

A Tabela 4 mostra que as taxas de acurácia são próximas para os três conjuntos de sensores avaliados, sendo o melhor resultado de 99,81% de acurácia e a menor taxa de erro médio de 0.17% para o modelo gerado a partir da combinação dos sensores acelerômetro, giroscópio e magnetômetro.

Tabela 4. Resultado de acurácia, FAR, FRR e ERR para modelo proposto a partir da combinação de sensores inerciais.

Sensores	Acurácia	FAR	FRR	EER
acc	98.67%	1.05%	1.32%	1.71%
acc+gyr	98.76%	1.03%	1.23%	1.65%
acc+gyr+mag	99.81%	0.15%	0.18%	0.17%

É importante destacar que devido as taxas de acurácia serem muito próximas, a utilização somente do acelerômetro pode ser considerada uma boa alternativa para a implementação em massa do autenticador proposto nesse trabalho. A maioria dos smartphones existentes no mercado dispõe desse sensor.

No segundo conjunto de experimentos foi realizado um comparativo com outros trabalhos baseados em sensores inerciais. A Tabela 5 mostra que o sistema de CA proposto apresenta a melhor acurácia (99.81%) e menor taxa de erro (0.17%). O melhor resultado do método proposto pode ser explicado pela melhor capacidade de extração de característica pelas camadas de convolução do modelo de autenticação. Essa comparação não é perfeitamente justa com o trabalho de (Büch, 2019) devido ao emprego de uma metodologia de particionamento de dados diferente.

Tabela 5. Resultados alcançados pelos trabalhos de Autenticação Contínua utilizando sensores inerciais.

Sensores	Acurácia	EER
Método Proposto	99.81%	0.17%
Centeno et al. (2018)	97.80%	3%
H. Buech (2019)	65.30%	36.8%

No último experimento é avaliado o modelo de confiança. A Tabela 6 apresenta os valores de ANGA e ANIA obtidos pelo método proposto juntamente com as porcentagens de usuários impostores detectados e a comparação com o trabalho de Mondal. Os resultados mostram que o modelo de autenticação proposto conseguiu, em todos os cenários de avaliação, autenticar 100% dos usuários genuínos. Além disso, a redução dos valores da ANIA (número de ações impostoras) é notável em todas as avaliações quando comparado aos resultados obtidos por (Mondal & Bours, 2015a), indicando que o modelo proposto foi capaz de reconhecer um usuário impostor mais rapidamente. (Mondal & Bours, 2015a) conseguem identificar o usuário em até 1326 ações enquanto este trabalho consegue autenticar em até 61 ações, o que representa uma redução de até 95.39% das ações necessárias para bloquear usuários impostores.

Tabela 6. Comparativo do modelo de confiança.

Trabalho	Usuário	Genuíno	Impostor
Mondal	Genuíno	100%	1.27%
		ANGA: ∞	ANIA: 1326
	Impostor	-	98.63%
		ANGA: -	ANIA: 84
Método Proposto	Genuíno	100%	0
		ANGA: ∞	ANIA: 61
	Impostor	-	100%
		ANGA: -	ANIA: 2

5. Conclusões e Trabalhos Futuros

Os recentes avanços nas tecnologias de sensoriamento tornaram os smartphones um dos dispositivos mais promissores para o monitoramento em tempo real de diversas atividades realizadas pelos seus usuários. Utilizamos os sensores inerciais para desenvolver um método de autenticação contínua para reautenticar passivamente usuários autênticos enquanto utilizam o dispositivo. Por outro lado, nosso método também é capaz de bloquear o dispositivo automaticamente quando detecta comportamentos anômalos. Essa maneira de superar as limitações deixadas pela abordagem de autenticação estática por meio da autenticação contínua nos permitiu implementar uma camada de segurança adicional, verificando a autenticidade do usuário continuamente durante o uso do dispositivo.

Usamos uma arquitetura de rede profunda baseada em redes neurais convolucionais (CNN) com camadas recorrentes (LSTM) para criar modelos de autenticação por usuário. Avaliamos nosso método de autenticação em três cenários. O modelo de confiança adotado se mostrou eficaz para minimizar bloqueios desnecessários de usuários genuínos, uma vez que eventuais desvios na conduta de uso dispositivo implicariam em situações de bloqueios indevidos e constantes. Em cenários em que um usuário não autorizado tenta burlar o sistema de autenticação, precisa manter o padrão de usuário genuíno, caso contrário, será bloqueado e será necessária uma nova autenticação biométrica. Isso permite que nosso método detecte ataques em tempo rápido com alta precisão.

Os resultados mostraram que nosso sistema de autenticação contínua é eficaz na detecção de usuários genuínos sem bloqueá-los injustamente, sendo capaz de detectar e bloquear usuários impostores mais rapidamente quando comparado a outras pesquisas. O modelo proposto pode ser facilmente incorporado em dispositivos como um serviço de autenticação contínua, permitindo que eles sejam constantemente autenticados com base em seus padrões de uso, em vez de depender apenas de outras formas de credenciais, ou seja, nome de usuário e senha.

Referências

Aviv, A. J., Gibson, K., Mossop, E., Blaze, M., & Smith, J. M. (2010). Smudge attacks on smartphone touch screens. In *Proceedings of the 4th usenix conference on offensive*

technologies (p. 1–7). USA: USENIX Association.

Banos, O., Galvez, J.-M., Damas, M., Pomares, H., & Rojas, I. (2014). Window size impact in human activity recognition. *Sensors*, *14*(4), 6474–6499. Retrieved from https://www.mdpi.com/1424-8220/14/4/6474 doi: 10.3390/s140406474

Bhattarai, A., & Siraj, A. (2018). Increasing accuracy of hand-motion based continuous authentication systems. In *2018 9th ieee annual ubiquitous computing, electronics mobile communication conference (uemcon)* (p. 70-76). doi: 10.1109/UEMCON.2018.8796725

Bours, P. (2012). Continuous keystroke dynamics: A different perspective towards biometric evaluation. *Information Security Technical Report*, *17*(1), 36-43. Retrieved from https://www.sciencedirect.com/science/article/pii/S1363412712000027 (Human Factors and Bio-metrics) doi: https://doi.org/10.1016/j.istr.2012.02.001

Bragança, H. L. d. S., et al. (2019). *Reconhecimento de atividades humanas usando medidas estatísticas dos sensores inerciais dos smartphones* (mastersthesis). Universidade Federal do Amazonas.

Büch, H. (2019). *Continuous Authentication using Inertial-Sensors of Smartphones and Deep Learning* (mastersthesis, Hochschule der Medien, Stuttgart). Retrieved from https://hdms.bsz-bw.de/frontdoor/index/index/docId/6506

Centeno, M. P., Moorsel, A. v., & Castruccio, S. (2017). Smartphone continuous authentication using deep learning autoencoders. In *2017 15th annual conference on privacy, security and trust (pst)* (p. 147-1478). doi: 10.1109/PST.2017.00026

Centeno, M. P. n., Guan, Y., & van Moorsel, A. (2018). Mobile based continuous authentication using deep features. In *Proceedings of the 2nd international workshop on embedded and mobile deep learning* (p. 19–24). New York, NY, USA: Association for Computing Machinery. Retrieved from https://doi.org/10.1145/3212725.3212732 doi: 10.1145/3212725.3212732

Darabseh, A., & Siami Namin, A. (2015). Keystroke active authentications based on most frequently used words. In *Proceedings of the 2015 acm international workshop on international workshop on security and privacy analytics* (p. 49–54). New York, NY, USA: Association for Computing Machinery. Retrieved from https://doi.org/10.1145/2713579.2713589 doi: 10.1145/2713579.2713589

Dee, T., Richardson, I., & Tyagi, A. (2019). Continuous transparent mobile device touchscreen soft keyboard biometric authentication. In *2019 32nd international conference on vlsi design and 2019 18th international conference on embedded systems (vlsid)* (p. 539-540). doi: 10.1109/VLSID.2019.00125

Gao, Z., Diao, W., Huang, Y., Xu, R., Lu, H., & Zhang, J. (2021). Identity authentication based on keystroke dynamics for mobile device users. *Pattern Recognition Letters*, *148*, 61-67. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167865521001586 doi: https://doi.org/10.1016/j.patrec.2021.04.019

Javed, A. R., Beg, M. O., Asim, M., Baker, T., & Al-Bayatti, A. H. (2020). Alphalogger: Detecting motion-based side-channel attack using smartphone keystrokes. *Journal of Ambient Intelligence and Humanized Computing*, 1–14.

Jin, Y., Tomoishi, M., & Matsuura, S. (2017). An in-depth concealed file system with gps authentication adaptable for multiple locations. In *2017 ieee 41st annual computer software and applications conference (compsac)* (Vol. 1, p. 608-613). doi: 10.1109/COMPSAC.2017.56

Lee, W.-H., & Lee, R. (2016). Implicit sensor-based authentication of smartphone users with smartwatch. In *Proceedings of the hardware and architectural support for security and privacy 2016*. New York, NY, USA: Association for Computing Machinery. Retrieved from https://doi.org/10.1145/2948618.2948627 doi: 10.1145/2948618.2948627

Mahbub, U., Patel, V. M., Chandra, D., Barbello, B., & Chellappa, R. (2016). Partial face detection for continuous authentication. In *2016 ieee international conference on image processing (icip)* (p. 2991-2995). doi: 10.1109/ICIP.2016.7532908

Mahfouz, A., Mahmoud, T. M., & Eldin, A. S. (2017). A survey on behavioral biometric authentication on smartphones. *Journal of Information Security and Applications*, *37*, 28-37. Retrieved from https://www.sciencedirect.com/science/article/pii/S2214212617302417 doi: https://doi.org/10.1016/j.jisa.2017.10.002

Marques, D., Guerreiro, T., Carriço, L., Beschastnikh, I., & Beznosov, K. (2019). Vulnerability amp; blame: Making sense of unauthorized access to smartphones. In *Proceedings of the 2019 chi conference on human factors in computing systems* (p. 1–13). New York, NY, USA: Association for Computing Machinery. Retrieved from https://doi.org/10.1145/3290605.3300819 doi: 10.1145/3290605.3300819

Mondal, S., & Bours, P. (2015a). A computational approach to the continuous authentication biometric system. *Information Sciences*, *304*, 28-53. Retrieved from https://www.sciencedirect.com/science/article/pii/S0020025514011979 doi: https://doi.org/10.1016/j.ins.2014.12.045

Mondal, S., & Bours, P. (2015b). Swipe gesture based continuous authentication for mobile devices. In *2015 international conference on biometrics (icb)* (p. 458-465). doi: 10.1109/ICB.2015.7139110

Muaaz, M., & Mayrhofer, R. (2017). Smartphone-based gait recognition: From authentication to imitation. *IEEE Transactions on Mobile Computing*, *16*(11), 3209-3221. doi: 10.1109/TMC.2017.2686855

Nguyen, T. V., Sae-Bae, N., & Memon, N. (2017). Draw-a-pin: Authentication using finger-drawn pin on touch devices. *Computers Security*, *66*, 115-128. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167404817300123 doi: https://doi.org/10.1016/j.cose.2017.01.008

Ordóñez, F. J., & Roggen, D. (2016). Deep convolutional and lstm recurrent neural networks for multimodal wearable activity recognition. *Sensors*, *16*(1). Retrieved from https://www.mdpi.com/1424-8220/16/1/115 doi: 10.3390/s16010115

Patel, V. M., Chellappa, R., Chandra, D., & Barbello, B. (2016). Continuous user authentication on mobile devices: Recent progress and remaining challenges. *IEEE Signal Processing Magazine*, *33*(4), 49-61. doi: 10.1109/MSP.2016.2555335

Santos, G., et al. (2017). Técnicas para autenticação contínua em dispositivos móveis a partir do modo de caminhar.

Shen, C., Chen, Y., & Guan, X. (2018). Performance evaluation of implicit smartphones authentication via sensor-behavior analysis. *Information Sciences*, *430-431*, 538-553. Retrieved from https://www.sciencedirect.com/science/article/pii/S0020025517311209 doi: https://doi.org/10.1016/j.ins.2017.11.058

Sitová, Z., Šeděnka, J., Yang, Q., Peng, G., Zhou, G., Gasti, P., & Balagani, K. S. (2016). Hmog: New behavioral biometric features for continuous authentication of smartphone users. *IEEE Transactions on Information Forensics and Security*, *11*(5), 877-892. doi: 10.1109/TIFS.2015.2506542