UNIVERSIDADE FEDERAL DO AMAZONAS - UFAM

INSTITUTO DE COMPUTAÇÃO- ICOMP

PROGRAMA PÓS-GRADUAÇÃO EM INFORMÁTICA - PPGI

AUTENTICAÇÃO CONTÍNUA USANDO SENSORES INERCIAIS DOS SMARTPHONES E APRENDIZAGEM PROFUNDA

Ismael Junior Vidal Paz

Manaus - AM

Abril de 2022

Ismael Junior Vidal Paz

AUTENTICAÇÃO CONTÍNUA USANDO SENSORES INERCIAIS DOS SMARTPHONES E APRENDIZAGEM PROFUNDA

Dissertação apresentada ao Programa de Pós-Graduação em Informática do Instituto de Computação da Universidade Federal do Amazonas como requisito para a obtenção do grau de Mestre em informática.

Orientador

Eduardo J.P. Souto, Dr.

Universidade Federal do Amazonas - UFAM

Instituto de Computação- IComp

Manaus - AM

Abril de 2022

Ficha Catalográfica

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

Paz, Ismael Junior Vidal
P348a Autenticação contínua usando sensores inerciais dos smartphones e aprendizagem profunda / Ismael Junior Vidal Paz . 2022
60 f.: il. color; 31 cm.

Orientador: Eduardo James Pereira Souto
Dissertação (Mestrado em Informática) - Universidade Federal do Amazonas.

1. Autenticação contínua. 2. Sensores Inerciais. 3. Redes Neurais Profundas. 4. Redes DeepConvLSTM. I. Souto, Eduardo James Pereira. II. Universidade Federal do Amazonas III. Título

FOLHA DE APROVAÇÃO

"AUTENTICAÇÃO CONTÍNUA USANDO SENSORES INERCIAIS DOS SMARTPHONES E APRENDIZAGEM PROFUNDA"

ISMAEL JÚNIOR VIDAL PAZ

Dissertação de Mestrado defendida e aprovada pela banca examinadora constituída pelos Professores:

Prof. Eduardo James Pereira Souto - PRESIDENTE

Prof. Eduardo Luzeiro Feitosa - MEMBRO INTERNO

Dr. Thiago de Souza Rocha - MEMBRO EXTERNO

Manaus, 08 de Abril de 2022

Ao meu pai Sebastião,

dedico.

Agradecimentos

A presente dissertação de mestrado não poderia chegar até esse ponto sem o precioso apoio de várias pessoas. Em primeiro lugar, não posso deixar de agradecer ao meu orientador, Professor Doutor Eduardo J.P. Souto, por toda a paciência, empenho e sentido prático com que vem me orientando neste trabalho. Muito obrigado por me ter corrigido quando necessário, sem nunca me desmotivar. Ao César Goersch, Ada e Ronem por todo suporte dado no trabalho e desejo igualmente agradecer a todos os meus colegas do laboratório ETSS, especialmente ao Kevin, Hendrio, Paulo que deram um suporte nos momentos difíceis do trabalho. Gostaria ainda de lembrar o grupo de estudos DDI, composto pelos amigos André, Joethe, Marcos e Mauro cujo apoio e amizade estiveram presentes em todos os momentos. Por último, mas não menos importante, quero agradecer à minha família e amigos pelo apoio incondicional que me deram, especialmente a minha esposa Emanuelle e aos meus filhos Luís Guilherme e Gustavo, por estarem me apoiando durante essa jornada.

Nem tão longe que eu não possa ver

Nem tão perto que eu possa tocar.

Engenheiros do Hawaii

Resumo

Muitos usuários têm optado pelo uso de dispositivos móveis como smartphones para a realização de tarefas do dia a dia como o envio de *e-mail*, interação com redes sociais, pagamento de contas e outras transações bancárias. Essas tarefas se tornaram mais simples de serem realizadas. Por outro lado, um grande volume de informações sensíveis e sigilosas são armazenadas e acessadas a partir desses dispositivos como, por exemplo, fotos, *logins* e senhas de bancos, dados pessoais, dentre outras. Ao buscar facilidade e usabilidade pelo uso dos smartphones, o usuário pode negligenciar a segurança e a privacidade de dados sensíveis. Atualmente, para garantir a segurança desses dados, a maioria dos sistemas emprega soluções de autenticação estática, em que o usuário desbloqueia o dispositivo uma única vez, por meio de um mecanismo de autenticação 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 sensíveis 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. Esses resultados promissores comprovam a viabilidade do uso de dados de sensores inerciais na definição de modelos de autenticação contínua.

Palavras-chave: Autenticação contínua, Sensores Inerciais, Redes Neurais Profundas, Redes DeepConvLSTM.

Abstract

Many users have chosen to use mobile devices such as smartphones to perform day-to-day tasks such as sending emails, interacting with social networks, paying bills, and other banking transactions. Whilst such tasks have become simpler to perform, however, a large volume of sensitive and confidential information is stored and accessed from these devices, such as photos, bank logins and passwords, personal data, and electronic messages. When prioritizing the ease and usability of smartphones, the user can unknowingly neglect the security and privacy of sensitive data. To ensure the security of this data, most systems currently employ static authentication solutions. This is where the user unlocks the device once through an authentication mechanism such as password, grid pattern, security key, PIN (Personal Identification Number) or fingerprint sensor. However this security measure is vulnerable: in a scenario where an imposter user has access to passwords or gets physical access to the unlocked device, the entire amount of data will be exposed. To deal with this problem, this work proposes the development of 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 Long Short-Term Memory (LSTM). In addition, 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. These promising results prove the feasibility of using data from inertial sensors to define continuous authentication models.

Keywords: Continuous authentication, Inertial Sensors, Deep Neural Networks, DeepConvLSTM Networks.

Lista de figuras

Lista de tabelas

Sumário

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 (HAQ et al., 2018). Entretanto, agregar muitas informações em um único dispositivo implica em um custo associado à segurança e privacidade das informações do usuário. Portanto, apesar desses dispositivos terem se tornado uma saída popular, a segurança e a privacidade ainda são um problema a ser resolvido, pois 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), número de cartão de crédito, mensagens privadas, informações do trabalho, dentre outros.

Para minimizar esse problema, 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. O 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). O problema dessa abordagem é que o usuário pode deixar o smartphone sem bloquear o acesso, permitindo 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, Spreitzer et al. (2017) descrevem ataques (side-channel attacks), em que a senha ou PIN podem ser obtidos por leitura de dados eletromagnéticos, utilizando equipamentos especiais. Há também os *smudge attacks* (AVIV et al., 2010) que ocorre quando o padrão de desbloqueio é roubado utilizando iluminação e câmeras adequadas. Por último, Wakabayashi, Kuriyama e Kanai (2017) apresentam um ataque chamado *shoulder-surfing attack* caracterizado pelo roubo de senha, PIN ou padrão utilizando técnicas de engenharia social.

Na tentativa de minimizar os problemas de autenticação enfrentados pelos usuários quando utilizam métodos tradicionais (senha, padrões e PIN), os fabricantes de smartphones têm incorporado o leitor biométrico para utilizar a digital do usuário e realizar o desbloqueio do smartphone. Entretanto, já é possível burlar esse mecanismo de autenticação por meio da criação de uma cópia das digitais (NGUYEN; SAE-BAE; MEMON, 2017).

O problema dos métodos de autenticação estáticos descritos é que a identificação do usuário ocorre somente na entrada do sistema, possibilitando acessos indevidos caso o impostor encontre o dispositivo desbloqueado ou consiga burlar a autenticação biométrica (NETO; FIGUEIREDO, 2019).

Uma maneira de superar as limitações deixadas pela autenticação estática é adotar o uso da autenticação contínua (*Continuous Authentication* - CA) pois, por meio dela, uma segunda camada de segurança é adicionada, verificando a autenticidade do usuário continuamente durante o uso do dispositivo.

Na literatura, existem diferentes mecanismos que fornecem a autenticação contínua do usuário realizadas por meio do toque na tela ou com base na marcha do usuário, conforme caracterizados por (BARBELLO, 2016). 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 (CENTENO; MOORSEL; CASTRUCCIO, 2017). Por outro lado, o processo de autenticação baseado no caminhar do usuário também possui limitações, pois nem sempre o usuário está caminhando enquanto utiliza o dispositivo. 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, 2019a).

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 utiliza uma rede neural profunda com uma arquitetura de redes neurais convolucionais (*Convolutional Neural Networks* - CNN) e camadas recorrentes (*Long Short-Term Memory* - LSTM). 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 e Bours (2015a) para evitar o bloqueio de usuários genuínos ao mesmo tempo que impede que um impostor fique muito tempo agindo sem ser detectado. Para validação do modelo será utilizado uma base de dados pública (SITOVÁ et al., 2016), voltada para autenticação de usuários.

Para comparação do modelo de autenticação contínua proposto com outros trabalhos (ABUHAMAD et al., 2020), foram utilizadas as seguintes métricas: acurácia; taxa de aceitação falsa (*False Acceptance Rate* - FAR), que corresponde ao percentual de entradas inválidas que são incorretamente aceitas, ou seja, o percentual de usuários impostores que utilizaram o sistema sem interrupções; a taxa de rejeição falsa (*False Reject Rate* - FRR), que corresponde ao percentual de entradas válidas que são incorretamente rejeitadas, ou seja, o percentual de usuários genuínos que foram considerados impostores pelo sistema; taxa de erro igual (*Equal Error Rate* - EER), que é calculada a partir das taxas FAR e FRR.

Além dessas métricas, este trabalho também utiliza duas outras métricas que foram propostas pelo trabalho de (MONDAL; BOURS, 2015b) para determinar o número de ações que os impostores conseguiram realizar no sistema antes da detecção. Para isso foram utilizadas o ANGA - (*Average Number of Genuine Actions*) que corresponde ao número médio de ações que um usuário genuíno consegue realizar sem ser bloqueado e o ANIA - (*Average Number of Imposter Actions*) que corresponde ao número médio de ações que um usuário impostor consegue realizar até ser bloqueado.

1.1 Objetivos

Para lidar com os os problemas mencionados acima, esta pesquisa tem como objetivo desenvolver um método de autenticação contínua baseado em dados extraídos, a partir, dos sensores inerciais e demonstrar a eficácia do método proposto na identificação de usuários impostores, identificando padrões comportamentais dos usuários a partir dos efeitos que os atos ou ações voluntárias geram para os sensores inerciais.

Para atingir esse objetivo, pretende-se alcançar os seguintes objetivos específicos:

- Definir um mecanismo de captura de dados dos sensores móveis que servirá de entrada para a criação do modelo de autenticação.
- Definir e implementar uma arquitetura de rede profunda baseada em redes neurais CNN com camadas recorrentes LSTM nas etapas de aprendizado e classificação. 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.
- Integrar um modelo de confiança proposto por (BOURS; BARGHOUTHI, 2009), capaz de efetuar uma avaliação continuada das atividades do usuário com o objetivo de evitar o bloqueio de usuários genuínos e impedir que um impostor fique muito tempo agindo sem ser detectado.

1.2 Organização do Trabalho

O restante deste documento está organizado da seguinte maneira: O Capítulo 2 descreve os conceitos e ferramentas utilizados que são importantes para compreensão do método, destacando a abordagem de autenticação contínua utilizando dados de sensores inerciais. Além disso, é apresentada uma breve descrição dos métodos de avaliação utilizados neste trabalho.

No Capítulo 3 são apresentados os trabalhos na literatura que deram contribuição relevante a esta pesquisa. O Capítulo 4 descreve a arquitetura da solução, o modelo de autenticação baseado em uma rede neural profunda e o modelo de confiança empregado como critério de avaliação.

O Capítulo 5 apresenta o protocolo experimental, a base de dados utilizadas nesta pesquisa, a metodologia de separação dos dados de treino e teste, as métricas de avaliação, e a avaliação dos resultados obtidos.

Finalmente, o Capítulo 6 fornece uma discussão sobre os resultados encontrados na pesquisa e descreve direções de trabalhos futuros.

2 Fundamentação Teórica

Este capítulo aborda os principais conceitos, significados e as técnicas utilizadas para tarefa de autenticação contínua. A Seção 2.1 apresenta os sistemas de autenticação contínua, bem como as métricas utilizadas para verificar a eficiência desses sistemas. A Seção 2.2 introduz os modelos de classificação e as redes neurais profundas, bem como as redes convolucionais que serão utilizadas neste trabalho.

2.1 Sistemas de autenticação contínua em smartphones

A autenticação contínua é o processo de verificar o usuário com base em suas informações fisiológicas e/ou comportamentais (MAHFOUZ; MAHMOUD; ELDIN, 2017). Tais informações podem ser obtidas a partir de sensores como *touchscreen*, giroscópio, acelerômetro, câmera, dentre outros. A Figura 2.1 apresenta uma relação de sensores que podem ser utilizados no processo de autenticação contínua.

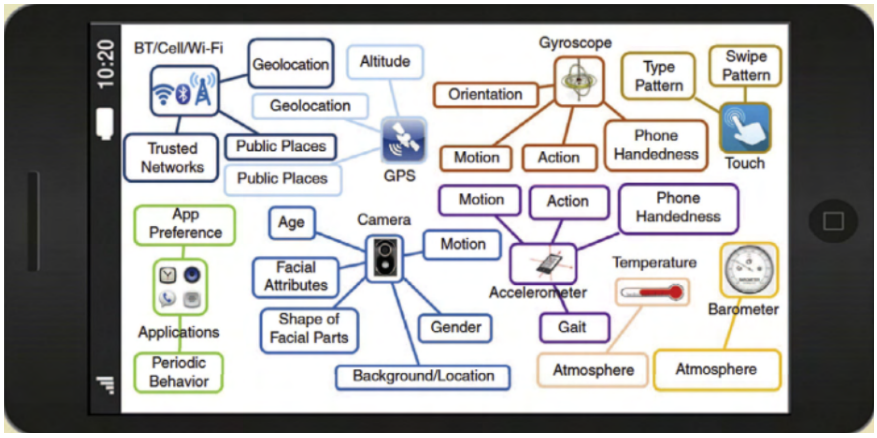


Figura 2.1 – Sensores para Autenticação Contínua. Fonte: Patel et al. (2016)

O principal objetivo deste método de autenticação é impedir que pessoas não autorizadas tenham acesso às informações salvas no smartphone, considerando que na autenticação estática só é realizada a validação do usuário

quando ele acessa o sistema. É importante que seja transparente ao usuário, evitando interrupções e, além disso, o sistema precisa ter continuidade, ou seja, deve se manter presente durante todo o período que o usuário esteja utilizando o dispositivo. Em termos de transparência ao usuário, é importante atentar para a quantidade de interrupções, gerando o mínimo de falso negativo, para o usuário genuíno. Ao mesmo tempo é necessário capturar o usuário impostor rapidamente sem que este tenha acesso aos dados do usuário genuíno.

Neste trabalho serão utilizados os principais sensores inerciais, que são o acelerômetro, o giroscópio e o magnetômetro. Esses sensores estão disponíveis em todos os smartphones e não exigem uma permissão especial, pois não fornecem acesso a dados sensíveis do usuário. As seções seguintes descrevem os dados coletados por esses sensores.

2.1.1 Acelerômetro

O acelerômetro é um sensor presente em todos os smartphones, sendo responsável por monitorar a aceleração dando indicação sobre o movimento do sistema com relação a uma variável do eixo inercial. O princípio básico de funcionamento por trás deste acelerômetro é o sistema de massa e mola (THOMAZINI; ALBUQUERQUE, 2020). As molas, enquanto dentro da sua região linear, são governadas pela lei de Hooke, que diz que o deslocamento da mola é proporcional à força aplicada(F), ou seja, $F = kx$, onde k é uma constante inerente à mola e x é o valor da deformação da mola.

Este sensor é responsável por detectar uma mudança repentina de direção. Isso pode ser causado por frenagem brusca, impacto de colisão ou até mesmo movimentos cotidianos do usuário como, por exemplo, atender o telefone ou enviar uma mensagem de texto.

Matematicamente, os dados podem ser visualizados em um plano tridimensional ao longo dos eixos x, y e z, conforme ilustrado na Figura 2.2. Dessa forma, os dados brutos do acelerômetro são representados por um conjunto

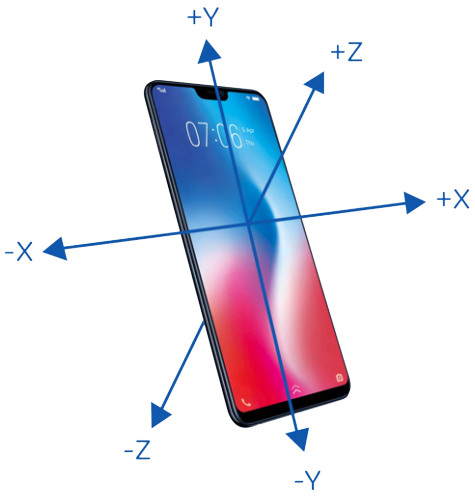


Figura 2.2 – Eixos do Acelerômetro. Fonte: Autor

de três vetores $acc_{\mathrm{i}} = x_{\mathrm{i}}, y_{\mathrm{i}}, z_{\mathrm{i}}$, onde i =(1,2,3,. . . ,n). A frequência da coleta de dados é medida em *Hertz*(Hz), ou seja, a quantidade de amostras que o sensor gera no intervalo de 1 segundo. Por exemplo, se o sensor gerar 50 amostras por segundo, então a frequência da coleta dos dados é 50Hz. Nos smartphones, a frequência pode variar entre 1Hz e 200Hz (LIMA et al., 2019).

2.1.2 Giroscópio

O giroscópio é caracterizado por medir a direção do dispositivo por meio da taxa de rotação medida em rad/s (radianos por segundo). Nos smartphones modernos, três giroscópios vibratórios são combinados em um único dispositivo para realizar a coleta simultânea dos eixos x, y e z (HERING; SCHÖNFELDER, 2018).

Os giroscópios incorporados nos smartphones são geralmente baseados em uma massa vibratória. Essa massa vibra ao longo de um eixo e é defletida pela força de Coriolis quando exposta a um movimento de rotação, conforme Figura 3. A deflexão detectada é usada para calcular a velocidade angular do movimento. Assim como o acelerômetro, os dados também podem ser visualizados em um plano tridimensional ao longo dos eixos x, y e z. Dessa forma, os dados brutos do giroscópio são representados por um conjunto de

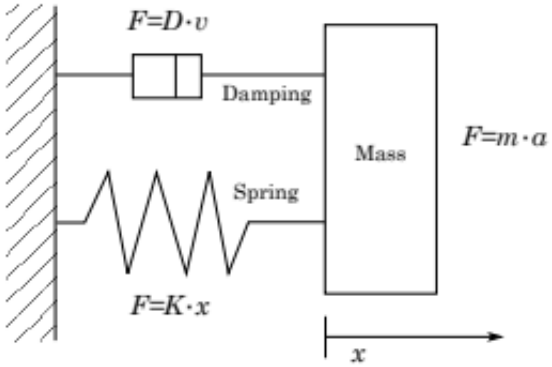


Figura 2.3 – Esquema do Giroscópio. Fonte: (HERING; SCHÖNFELDER, 2018)

vetores $gyr_{\mathrm{i}} = x_{\mathrm{i}}, y_{\mathrm{i}}, z_{\mathrm{i}}$, onde i =(1,2,3,. . . ,n). Nesse sensor, os dados brutos também são coletados em forma de frequência medidas em *Hertz*, similar à coleta de dados do acelerômetro (LIMA et al., 2019). Cada eixo do giroscópio possui os seguintes significados:

- **Eixo x (roll):** mede rotação horizontal do dispositivo, ou seja, mudança na direção do dispositivo (esquerda e direita).
- **Eixo y (pitch):** mede a rotação da inclinação do dispositivo.
- **Eixo z (yaw):** mede a rotação vertical do dispositivo, ou seja, mudança na orientação do dispositivo (retrato e paisagem).

2.1.3 Magnetômetro

O magnetômetro é um sensor capaz de medir as componentes de um campo magnético em três eixos perpendiculares ao longo dos eixos x, y e z. Embora existam diferentes tipos de magnetômetros disponíveis, os tipos mais comuns usados nos smartphones de hoje são baseados em Magnetorresistência Anisotrópica (AMR) ou Magnetorresistência Gigante (GMR). Esses tipos de sensores podem ser miniaturizados, apresentam um baixo consumo de energia, bem como baixos custos de produção. Mas eles ainda fornecem um campo magné-

tico resolução na ordem de $1\tilde{}10nT$ que é boa o suficiente para fins de navegação na Terra (ZHANG et al., 2013).

Os sensores AMR e GMR são efeitos de magnetoresistência (MR), conforme ilustrados na Figura 2.4. Um condutor de um determinado material fica exposto a um campo magnético externo variável sua resistência elétrica sofre mudanças, logo, essa mudança na resistência pode ser medida e usada para inferir a força do campo magnético externo. Ambos AMR e GMR são efeitos que aparecem em ferromagnéticos.

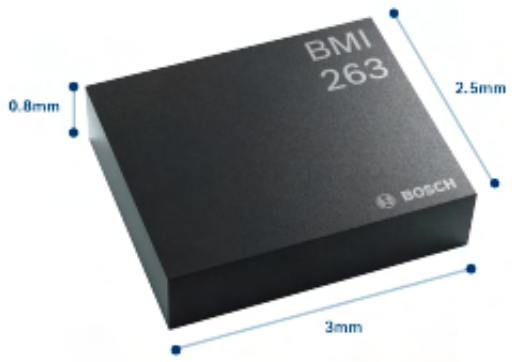


Figura 2.4 – Bosch SensorTech BMI263 IMU. Fonte: (SENSORTEC, 2022)

Os magnetômetros baseados em AMR são mais baratos de produzir do que os baseados em GMR magnetômetros que, por outro lado, são menores, mais precisos e têm um menor consumo de energia (HERING; SCHÖNFELDER, 2018).

Semelhante ao acelerômetro e giroscópio, um magnetômetro em um smartphone precisa medir a força do campo magnético em todos os três eixos para lidar com diferentes possíveis orientações do telefone (VČELÁK; RIPKA; ZIKMUND, 2015). Para determinar a direção em que o dispositivo está apontando, o vetor de gravidade, detectado pelo acelerômetro e, opcionalmente, giroscópio, é necessário. Dessa forma, os dados brutos do giroscópio são representados por um conjunto de vetores $mag_{\mathrm{i}} = x_{\mathrm{i}}, y_{\mathrm{i}}, z_{\mathrm{i}}$, onde i =(1,2,3,. . . ,n) (LIMA et al., 2019).

2.1.4 Métricas de Avaliação de Sistemas de Autenticação

Os trabalhos comparam a eficiência dos sistemas de autenticação contínuas baseado na acurácia do método (ACC), FAR, FRR e EER (Equal Error Rate). O FAR reflete a capacidade de um usuário não autorizado de acessar o sistema, seja por meio de tentativas de acesso sem esforço ou falsificação deliberada ou qualquer outro método de evasão. Quanto mais baixo essa métrica, mais seguro pode um sistema ser considerado (LI et al., 2018). Ela é representada pela proporção entre os usuários impostores aceitos e os usuários impostores rejeitados corretamente:

$$FAR = \frac{False\ Acceptances}{Correct\ Rejects}$$

O FRR é o oposto de FAR e está relacionado a usuário genuínos que foram rejeitados incorretamente pelo sistema. Um sistema de autenticação com alto FRR pode refletir em dificuldade para o usuário genuíno utilizar o sistema (LI et al., 2018). Um FRR mais baixo indica melhor conveniência para o usuário porque o sistema é menos propenso a negar acesso legítimo.Essa métrica corresponde a razão entre o número total de tentativas de autenticação do usuário genuíno rejeitadas para o número total de tentativas autorizadas de usuários legítimos:

$$FRR = \frac{False\ Rejects}{Correct\ Acceptances}$$

Como a diminuição do FAR geralmente resulta em um FRR mais alto e vice-versa, um *trade-off* tem que ser escolhido entre essas métricas, dependendo das circunstâncias do uso planejado caso (LI et al., 2018). Um menor EER indica um sistema mais confiável. Essa métrica, pode ser calculada, a partir da seguinte fórmula:

$$EER = \frac{FFR + FRR}{2}$$

No trabalho de Mondal e Bours (2015b) são adicionadas duas métricas: a quantidade de ações que o usuário impostor consegue realizar ANIA e a

quantidade de usuários genuínos que são bloqueados pelo sistema - ANGA . Essas duas métricas facilitam verificar como o sistema de autenticação se comporta ao longo do tempo.

O cálculo do ANGA é realizado pela seguinte fórmula:

$$ANGA = \frac{1}{n} \sum_{i=1}^{n} \frac{ag}{bg}$$

Onde, n é o número de usuário, ag é o número de ações do usuário genuíno e bg é o número de bloqueio do usuário genuíno. Quando não há bloqueio de usuário genuíno ANGA tende ao infinito. Para o cálculo do ANIA a seguinte fórmula é utilizada:

$$ANIA = \frac{1}{n} \sum_{i=1}^{n} \frac{ai}{bi}$$

O ai é o número de ações do usuário impostor e bi é o número de bloqueio do usuário impostor. Em um sistema de autenticação contínua é esperado que o usuário impostor seja bloqueado rapidamente sendo esperado um resultado alto para essa métrica.

Com a implementação do modelo de confiança ao invés de utilizar a saída da rede neural é adicionada uma nova camada para o usuário evitando bloqueio desnecessário do usuário genuíno e tentando bloquear rapidamente o usuário impostor. Essas métricas são importantes para mensurar a usabilidade do sistema de autenticação.

2.2 Modelos de Classificação

O processo de autenticação contínua dos usuários é similar a um sistema de reconhecimento de padrões de propósito geral. As metodologias utilizadas possuem etapas bem definidas que abrangem à coleta dos dados, pré-processamento dos dados (ex.: segmentação, aplicação de filtros), extração de características e treinamento de modelos de autenticação (ANDRADE et al., 2021).

Estudos de autenticação contínua, em sua maioria, têm utilizado técnicas de classificação baseadas em aprendizado raso, seguido de classificadores baseados em distância. Essas técnicas exigem a extração manual de características dos dados de origem (do inglês, *handcraft features - HF*) como empregado nos trabalhos de Mondal e Bours (2015b) e Shen, Chen e Guan (2018).

As desvantagens das abordagens manuais de extração de características são que os atributos extraídos são específicos do domínio e por isso exigem conhecimento especializado. Além disso, há um custo de tempo a ser considerado (RONAO; CHO, 2016).

Neste trabalho, serão utilizados as redes CNN com o objetivo de extrair as características mais relevantes e que mais contribuem para o processo de classificação de forma automática e as redes LSTM, para modelagem temporal das características . A seguir estas duas arquiteturas serão descritas.

2.2.1 Convolutional Neural Network - CNN

As redes neurais convolucionais foram desenvolvidas tomando por base o cortex visual, que é composto por milhões de agrupamentos celulares complexos, sensíveis a pequenas sub-regiões do campo visual, chamadas de campos receptivos (HUBEL; WIESEL, 1968) esses modelos tem sido largamente empregados em problemas de visão computacional, sendo capazes de realizar o reconhecimento de formas bi-dimensionais e invariantes a distorções como translações e escala.

A CNN é iniciada por uma camada convolucional que podem ser seguidas por camadas convolucionais adicionais ou camadas de *pooling*, a camada totalmente conectada é a camada final. Filtros que deslizam ao longo dos dados de entrada e são aplicados às suas sub-regiões, conforme pode ser visualizado na Figura 2.5. A cada camada, a CNN aumenta em sua complexidade. As camadas anteriores se concentram em recursos simples de padrões do sinal.

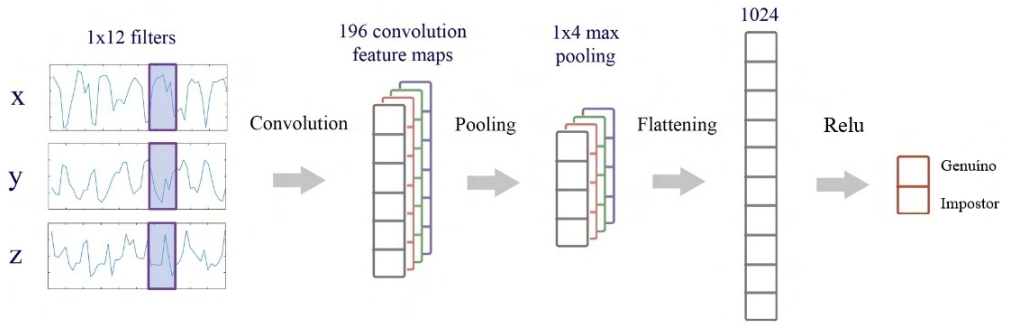


Figura 2.5 – Camadas da Rede Neural CNN. Fonte: Autor

2.2.1.1 Camada convolucional

Essa camada é uma operação matemática que consiste no deslizamento de uma função sobre a outra calculando a integral da soma do produto de ambas a partir da sobreposição gerada pelo deslizamento (IGNATOV, 2018). Nessa camada o filtro atua como uma janela deslizante que irá percorrer os dados de entrada da esquerda para a direita e de cima para baixo, realizando a multiplicação entre a sua matriz e o contexto atual em que a janela se encontra, somando os valores da multiplicação resultante.

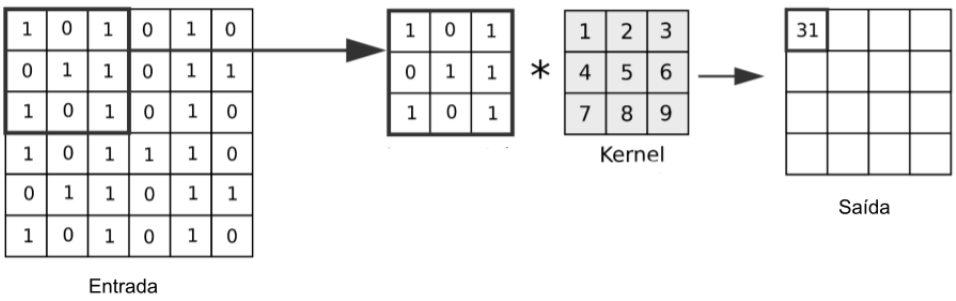


Figura 2.6 – Camada Convolucional. Fonte: Autor

O filtro é uma matriz utilizada para uma operação de multiplicação de matrizes e o seu tamanho varia de acordo com o valor do parâmetro escolhido (ANDRADE et al., 2021). Esta operação é aplicada diversas vezes em diferentes regiões da imagem. A cada aplicação, a região é alterada por um parâmetro conhecido como *stride*. Um exemplo dessa transformação é ilustrado na Figura 2.6, onde é possível notar que a matriz resultante desse exemplo possui uma

dimensionalidade menor que a matriz de origem.

2.2.1.2 Camada de *pooling*

É um processo simples de redução da dimensionalidade. Essa transformação é responsável pela redução do tamanho da matriz. A principal motivação dessa operação no modelo, é de diminuir sua variância a pequenas alterações e também de reduzir a quantidade de parâmetros treinados pela rede.

Essa camada geralmente segue uma camada convolucional e seu objetivo é reduzir e resumir a representação obtida. Existem operações diferentes de *Pooling*, mas todas seguem o mesmo princípio e só se diferem na forma como calculam o valor final. A mais utilizada nos dias de hoje é a *MaxPooling*.

A operação de *MaxPooling* retira o maior elemento de determinada região da matrix (considerando o tamanho do *pool* aplicado). Posteriormente, é feito um deslizamento considerando um parâmetro de *stride* (similar a a operação de convolução) para aplicação de uma nova operação.

2.2.1.3 Camada totalmente conectada

Após várias camadas convolucionais e de *pooling*, a saída dessas camadas é achatada em um vetor unidimensional e usada para a classificação, conforme ilustrado na Figura 2.6. Nesta fase, recursos adicionais podem ser empilhados junto com esse vetor. Para aprender dependências não lineares, a CNN possui uma ou mais camadas totalmente conectadas que executam a classificação.

Para aprender limites de decisão não lineares, a camada convencional normalmente é seguida pela função de ativação não linear aplicada de maneira pontual às suas saídas. Três funções de ativação comumente usadas são sigmoidal, tangente hiperbólica e ReLU. Por fim, a saída da última camada é passada para uma camada máxima suave que calcula a distribuição de probabilidade nas classes previstas.

Todas as camadas mencionadas são empilhadas e formam uma CNN, que pode ser treinada como um todo. Uma maneira comum de fazer isso é usar um algoritmo de propagação reversa e otimizar os parâmetros de treinamento com descida estocástica do gradiente. Neste trabalho a rede CNN compõe o modelo de rede neural proposto para o autenticador biométrico, e terá responsabilidade de extrair características dos dados dos sensores móveis.

2.2.2 Long Short Term Memory (LSTM)

As redes de memória de longo prazo - geralmente chamadas apenas de LSTM são um tipo especial de *Recurrent Neural Network* - RNN, capaz de aprender usando dados sequenciais ou dados de séries temporais. Eles foram introduzidos por Hochreiter e Schmidhuber (1997), e funcionam muito bem em uma grande variedade de problemas, principalmente na predição de séries temporais. Para problemas ordinais ou temporais, como tradução de idiomas, processamento de linguagem natural (NLP) do inglês *Natural Language Processing*, reconhecimento de fala e em sinais de sensores inerciais (YAN et al., 2018).

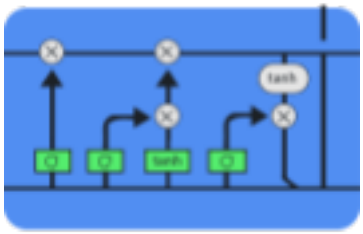


Figura 2.7 – Arquitetura da Rede Neural LSTM. Fonte: Autor

As redes LSTMs são projetados explicitamente para evitar o problema de dependência de longo prazo. Todas as redes neurais recorrentes têm a forma de uma cadeia de módulos repetidos de rede neural, conforme pode ser visualizado na Figura 2.7.

Eles se distinguem por sua "memória", pois obtêm informações de entradas anteriores para influenciar a entrada e a saída atuais. Enquanto as

redes neurais profundas tradicionais assumem que as entradas e saídas são independentes umas das outras, a saída das redes neurais recorrentes depende dos elementos anteriores dentro da sequência.

2.3 Considerações Finais

Este capítulo apresentou os conceitos teóricos relacionados aos sensores inerciais que serão utilizados para o trabalho. Vale ressaltar que o acesso a esses sensores não requer permissões especiais do sistema operacional Android. As métricas de avaliação dos sistemas de autenticação contínua foram apresentadas na Seção 2.1.4 e servirão de apoio para o próximo capítulo de trabalhos relacionados. Por último, os modelos de classificação são apresentados bem como as redes neurais que serão utilizadas.

3 Trabalhos Relacionados

Neste capítulo serão apresentados os principais trabalhos relacionados à autenticação contínua. As seções a seguir apresentam os principais trabalhos relacionados. Dentre esses métodos, na Seção 3.1 os trabalhos que tratam do reconhecimento durante a marcha. Na Seção 3.2, são apresentados trabalhos cujos sistemas de autenticação contínua são baseados no toque na tela. A Seção 3.3 apresentas os sistemas baseados em teclado, e a Seção 3.4 apresenta os que autenticam o usuário baseado em sensores inerciais. Uma sumarização dos trabalhos relacionados é apresentada na Seção 3.5.

3.1 Autenticação Baseada em Marcha Humana

Essa autenticação baseia-se no fato da atividade de caminhar acontecer em ciclos que correspondem ao momento em que levanta o pé e retorna para a mesma posição. Cada pessoa tem sua maneira própria de caminhar (NIXON; TAN; CHELLAPPA, 2010). Essa autenticação pode ser realizada através de visão computacional e/ou dados de sensores vestíveis(DERAWI et al., 2010). As abordagens de visão computacional para o reconhecimento da marcha incluem segmentar as imagens do indivíduo enquanto caminha e capturar as características que permitem o reconhecimento (WANG et al., 2004). Na segunda abordagem os dados de sensores inerciais, são extraídas características relacionadas à marcha que são utilizadas pelo modelo de aprendizagem de máquina para autenticar o usuário (GAFUROV; SNEKKENES, 2009), (QIAN; ZHANG; KIDANÉ, 2008). Nesse trabalho será discutido somente a autenticação baseada em dados de sensores, que realiza a autenticação enquanto utiliza o dispositivo ao contrário da autenticação baseada em visão computacional é realizada somente em um ambiente controlado.

Santos et al. (2017) apresenta um estudo detalhado da autenticação

baseada em marcha humana. Para implementação do trabalho foram utilizados dados do acelerômetro, magnetômetro e giroscópio. Para a etapa de pré-processamento foi projetado um classificador de marcha humana de forma a garantir que não existissem dados de reconhecimento que fossem de outras atividades atividades humanas. Os autores propõem um novo sistema de coordenadas centrado no usuário, a partir da posição do dispositivo e à direção de marcha do usuário. Para validação da técnica, foi implementada uma base de dados com 50 usuários [1] . Para o modelo de autenticação foram utilizados algoritmos clássicos de aprendizagem de máquina, como o *Suport Vector Machine - SVM* e *Random Forests - RF*, conseguiram resultados de 72.1% de acurácia para RF e 82% de acurácia para SVM.

O trabalho de (NICKEL; BUSCH, 2013) utiliza os dados de acelerômetro para autenticar o usuário com o modelo estatístico de chamado modelo oculto de markov *Hidden Markov Model (HMM)*. A taxa de erro médio foi de 6.15% segundo o autor a abordagem proposta realizou testes mais realísticos já que a base de dados leva em um ambiente mais realístico, pois os dados foram coletados em mais de um dia e em um ambiente não plano.

No trabalho de Mantyjarvi et al. (2005) é utilizado o método de correlação de sinais nos dados brutos do acelerômetro com os coeficientes da transformada rápida de fourrier *Fast Fourier Transform (FFT)* e o histograma. A partir, desses dados coletados é realizado uma análise estatística tendo como melhor resultado para a métricas EER de 7% e acurácia de 88%. A abordagem proposta foi testada em uma base privada de 36 usuários.

Thang et al. (2012) utilizaram dados do acelerômetro em abordagens no domínio do tempo e no domínio da frequência. Para o domínio do tempo foi utilizado o *Dynamic Time Warping (DTW)* no padrão da marcha para avaliar a pontuação de similaridade. Para o domínio da frequência foi utilizado o SVM. Foram obtidos 79,1% de acurácia no domínio do tempo e 92,7% de acurácia no domínio da frequência. A abordagem proposta foi testada em uma base privada

[1] RECOD Lab. *RECODGait Dataset*. 2019. Disponível em: <https://recodbr.wordpress.com/code-n-data/#recodgait>.

de 11 usuários.

Apesar dos resultados e as contribuições dos trabalhos apresentados, a utilização deste método de autenticação restringe o uso somente ao caminhar. Existem várias ações que são realizadas durante o dia com o dispositivo móvel, portanto, é esperado que um método de autenticação contínua seja universal durante o uso do dispositivo e não somente durante uma determinada ação.

A autenticação baseada em marcha poderia ser classificada na autenticação baseada em sensores inerciais, todavia devido a grande quantidade de *surveys* (BARBELLO, 2016) (STYLIOS et al., 2016) (MAHFOUZ; MAHMOUD; ELDIN, 2017) este trabalho optou por uma descrição à parte.

3.2 Autenticação Baseado em Toque na Tela

A análise da interação do usuário com o dispositivo por meio do toque na tela também tem sido usada com um método autenticação contínua. Dados de toque de usuários que interagem com um smartphone usando manobras básicas de navegação como rolagem de cima para baixo e da esquerda para a direita foram coletados.

Frank et al. (2012) propõem um classificador para autenticar usuários com base na maneira como eles interagem com a tela sensível ao toque de um smartphone. Os autores identificaram 30 características que podem ser extraídas dos logs de toque na tela sensível. O artigo apresentou uma EER de 0% para autenticação intra-sessão e de 2%-3% para autenticação entre sessões utilizando o SVM.

No trabalho de (MONDAL; BOURS, 2015b) são extraídos dados 15 atributos relacionados aos toque na tela, tais como: duração do toque, coordenada de início e coordenada de término. A acurácia do trabalho se aproximou de 98%, e o FAR e FRR de 0% e o usuário impostor foi detectado em até 84 ações. Apesar de utilizar sensores diferentes esse trabalho foi utilizado para realizar um comparativo com o método proposto em relação ao modelo de confiança, por

ser o único trabalho em autenticação contínua de smartphones a implementar o modelo de confiança.

3.3 Autenticação Baseada em Teclado

Esse sistema de autenticação é baseada em dados que os usuários digitam no dispositivo. São geradas métricas com base na velocidade do pressionamento dos caracteres, bem como a quantidade de caracteres digitados. Para implementação desse sistema de autenticação é necessária a customização de um teclado, que substitua o teclado padrão do Android (KIM; LEE; KIM, 2006), que forneça as informações necessárias para implementação do método. Uma crítica a esse modelo se dá ao fato que, quando o usuário impostor não estiver digitando e só visualizando as informações do dispositivos, não é possível identificá-lo.

3.4 Autenticação Baseada em Sensores Inerciais

Nesse modelo os dados dos sensores inerciais, tais como acelerômetro, giroscópio e magnetômetro são utilizados para autenticação do usuário (CENTENO; MOORSEL; CASTRUCCIO, 2017). O acesso aos dados dos sensores inerciais não requer permissões especiais do Sistema Operacional Android facilitando a adoção desse método.

O iAuth é um sistema de autenticação contínua que foi implementado por Lee e Lee (2016) e utiliza o acelerômetro, giroscópio e magnetômetro para garantir a autenticidade do usuário. Visando melhorar o resultado é proposta a combinação com um *smartwatch*. Vale ressaltar que o trabalho dos autores tem uma preocupação com a energia consumida, o que é um ponto importante a ser considerado por se tratar de um dispositivo móvel. Após a extração de características os autores utilizam algoritmo *support vector machine* (SVM) para classificar e obtiveram uma acurácia de 82.3%, com o FAR de 13.4% e FRR

de 22.30% para a adoção somente do sensores inerciais. Com a combinação do *smartwatch* os resultados foram de 92.1% de acurácia, com um FAR de 7.5% e FRR de 8.3%. Essa melhoria de resultados com a adição do *smartwatch* era esperada devido a quantidade maior de características adicionadas à rede neural.

Shen, Chen e Guan (2018) utilizam dados do acelerômetro e do giroscópio. O autor extrai características no domínio do tempo e da frequência. Em seguida o usuário é identificado através desses sensores nos seguintes cenários: caminhando, andando, subindo escada, descendo escada e pulando. Para classificação utilizou algoritmos clássicos: *K-Nearest Neighbor* (KNN) e árvore de decisão. Os melhores resultados reportados foram de 2.21% para o EER.

Centeno, Moorsel e Castruccio (2017) utilizam uma base de dados pública (YANG et al., 2014). Para classificação, foi utilizada uma arquitetura de rede neural com autoencoder para extração de características e um limiar de decisão para verificar se é impostor ou genuíno. Durante a etapa de treino, o dispositivo envia informações de sensores para um servidor que hospeda um sistema que tem a responsabilidade de realizar de desenvolver o modelo. A extração de características é realizada pela própria rede neural. Como resultado, teve 2% para o EER.

Centeno, Guan e Moorsel (2018) são utilizados os dados dos sensores inerciais da mesma base de dados do trabalho anterior para realizar a autenticação do usuário em uma rede neural artificial com arquitetura siamesa. A extração de características é realizada pela própria rede neural. Como resultado o trabalho teve para EER 3% e uma acurácia de 97,3%. Büch (2019b) utiliza redes neurais siamesa e propõe uma adaptação a normalização proposta pelo trabalho anterior, mas mesmo com essa modificação a acurácia alcançada foi de 65.3%. Esses dois trabalhos foram utilizados para comparar com o método proposto, em relação a eficiência da rede neural.

Essa seção trouxe os principais trabalhos que apresentam soluções

baseadas no comportamento do usuário. Dentre os trabalhos apresentados, há implementações utilizando algoritmos clássicos, tais como SVM e KNN, e redes neurais profundas com implementação de redes com *autoencoders* e redes siamesas. Também foi realizado uma análise sobre a viabilidade do método ser utilizado no mundo real.

3.5 Discussões e Considerações Finais

Neste capítulo foram apresentados os principais trabalhos de autenticação contínua categorizados em 4 tipos de autenticação contínua. A Tabela 3.1 apresenta uma sumarização dos trabalhos relacionados, considerando as seguintes métricas: Acurácia, FAR, FRR e EER.

Tabela 3.1 – Sumarização dos trabalhos relacionados.

Trabalho	Modelo	Sensores	Tipo	Acurácia	FAR	FRR	EER	Dataset
Santos et al. (2017)	SVM	Acelerômetro Giroscópio Magnetômetro	Marcha	82%	-	-	-	Recod Lab
Nickel e Busch (2013)	HMM	Acelerômetro	Marcha	-	-	-	6.15%	privado
Mantyjarvi et al. (2005)	Correlação FFT Histograma	Acelerômetro	Marcha	88%	-	-	7%	privado
Thang et al. (2012)	SVM	Acelerômetro	Marcha	92.7%	-	-	-	privado
Frank et al. (2012)	SVM	Touchscreen	Toque na Tela	-	-	-	0 - 4%	privado
Mondal e Bours (2015b)	SVM	Touchscreen	Toque na Tela	98.63%	0%	0%	-	privado
Lee e Lee (2016)	SVM	Acelerômetro Giroscópio Magnetômetro	Sensores Inerciais	82.30%	13.40%	22.30%	-	privado
Lee e Lee (2016)	SVM	Acelerômetro Giroscópio Magnetômetro + Smartwatch	Sensores Inerciais	92.10%	7.50%	8.30%	-	privado
Centeno, Moorsel e Castruccio (2017)	Autoencoder	Acelerômetro Giroscópio Magnetômetro	Sensores Inerciais	-	-	-	2.20%	HMOG
Centeno, Guan e Moorsel (2018)	Redes Siamesas	Acelerômetro Giroscópio Magnetômetro	Sensores Inerciais	97.30%	-	-	3%	HMOG
Büch (2019b)	Redes Siamesas	Acelerômetro Giroscópio	Sensores Inerciais	65.40%	-	-	36.90%	HMOG
Shen, Chen e Guan (2018)	KNN	Acelerômetro Giroscópio	Sensores Inerciais	-	-	-	2.21%	privado
Método Proposto	DeepConvLSTM	Acelerômetro Giroscópio Magnetômetro	Sensores Inerciais	99.8%	0.15%	0.18%	0.17%	HMOG

Dentre os trabalhos apresentados alguns ainda utilizam modelos de aprendizagem de máquina rasos e trabalhos com aprendizagem profunda, essa última abordagem dispensa a necessidade de extração de características manual, pois essa etapa é realizada pela rede neural. Não há uma padronização

entre os trabalhos no que diz respeito as métricas de avaliação, entretanto, alguns trabalhos optaram por demonstrar a métrica EER que é a composição das métricas FAR e FRR, apesar dessas métricas não serem apresentadas em alguns trabalhos.

A maioria dos trabalhos optou por realizar a coleta dos dados para validar o modelo, entretanto as bases de dados geradas não foram compartilhadas. Este trabalho optou por utilizar uma base pública (SITOVÁ et al., 2016) que é amplamente utilizada por trabalhos de autenticação contínua.

O diferencial deste trabalho em relação aos apresentados é que, além de desenvolver um método de autenticação contínua baseado em dados extraídos a partir dos sensores inerciais, identificando padrões comportamentais dos usuários, ele também projeta uma arquitetura de rede profunda baseada em CNN com camadas recorrentes que são usadas no processo de extração automática de características. Adicionalmente, este trabalho utiliza um modelo de confiança, que trata o resultado da rede neural evitando bloqueios desnecessários do usuário genuíno.

4 Método Proposto

Este capítulo descreve a abordagem proposta e empregada neste trabalho, iniciando na Seção 4.1 onde é apresentada uma visão geral da abordagem proposta. Na Seção 4.2 é detalhado o processo de coleta dos dados. A Seção 4.3 descreve a fase de segmentação dos dados. A Seção 4.4 detalha a separação dos dados bem como a arquitetura da rede neural profunda DeepConvLSTM utilizada no trabalho. A Seção 4.5 apresenta o modelo de confiança que é responsável por autenticar o usuário. Por último, na Seção 4.6 é apresentado as considerações finais.

4.1 Visão Geral

O método de autenticação de usuários de smartphones implementado, baseia-se em informações de sensores inerciais que estão disponíveis em tempo real nos dispositivos com sistema operacional Android. Para isso é utilizada uma abordagem de aprendizado de máquina supervisionada. A Figura 4.1 fornece uma visão geral do método de autenticação que está dividida em quatro etapas.

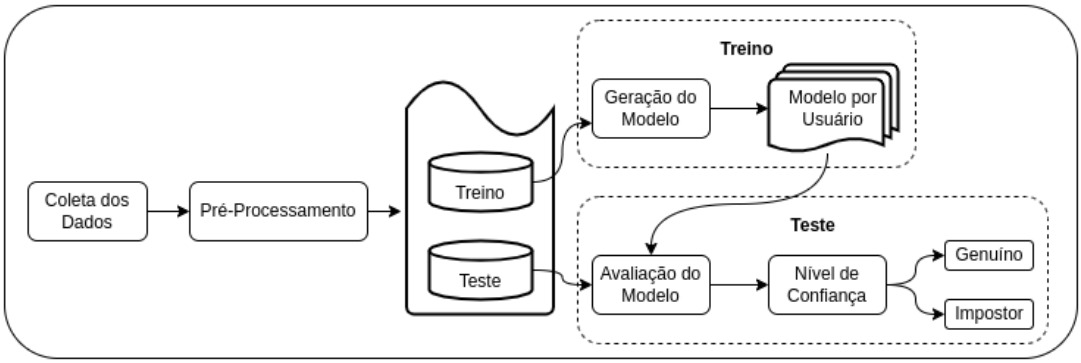


Figura 4.1 – Visão geral da proposta. Fonte: Autor

- **Coleta** - Nessa etapa, os dados são coletados em tempo real pelo sistema operacional, logo, a coleta dos dados se inicia a partir do momento que o usuário desbloqueia o dispositivo.

- **Pré-Processamento** - Como a captura dos dados na etapa anterior foi feita de maneira contínua, é necessário segmentar os dados em tamanhos fixos e menores para envio à rede neural.
- **Treinamento** - Nesta etapa, primeiramente, é realizado um treinamento com os dados do usuário. É criado um modelo para cada usuário.
- **Modelo de Confiança** - Após o treinamento, o modelo de gerado na etapa anterior será utilizado para verificar a autenticidade do usuário, a partir de um nível de confiança a ser detalhado.

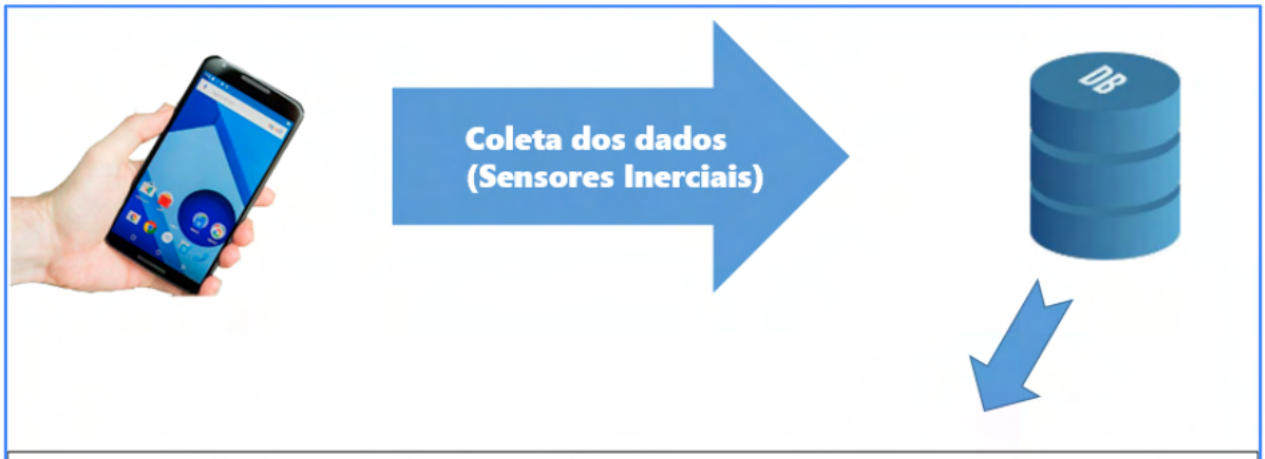
A seções seguintes detalham cada uma das etapas da solução proposta.

4.2 Coleta dos Dados

Como mencionado na Seção 2.1, os dispositivos móveis com o sistema operacional Android são dotados de sensores, ditos inerciais e, que permitem capturar o movimento do usuário. Esses sensores são a base para o método proposto. Vale ressaltar, que não há necessidade de permissão adicional para acessar os dados desses sensores.

Os dados serão coletados do *smartphone* em tempo real a partir de um aplicativo Android que irá funcionar em modo serviço (GOOGLE, 2021), executando em segundo plano para coletar as informações dos sensores enquanto o dispositivo estiver desbloqueado. A Figura 4.2 apresenta os dados brutos provenientes de uma coleta do acelerômetro, giroscópio e magnetômetro. Para cada sensor há valores no eixo X, Y e Z.

As amostras de cada sensor são compostas por três direções ou coordenadas: eixo-x, eixo-y e eixo-z distribuindo as informações em nove colunas. Esses valores estão disponíveis em tempo real no sistema operacional Android em diferentes taxas de amostragem.



x_acc	y_acc	z_acc	x_gyr	y_gyr	z_gyr	x_mag	y_mag	z_mag
-0.260369	8.054890	4.279635	-0.106290	0.154243	-0.121562	-1.3175	1.7483	-2.7316
-0.304662	8.157045	4.599675	0.707993	0.154243	0.585820	-1.4212	1.7483	-2.7316
-0.393846	8.259995	4.156746	0.549473	-0.696997	0.398895	-1.5858	1.7483	-2.7316
-0.638653	8.386888	4.207211	-1.124297	-0.618806	-1.247387	-1.6284	1.7483	-2.7316
-0.793678	8.432977	4.148553	-0.124311	0.995405	-0.499688	-1.6284	1.7483	-2.7316

Figura 4.2 – Dados brutos de Sensores Inerciais. Fonte: Autor

4.3 Pré-processamento

Durante esta etapa, conforme ilustrado na Figura 4.2, os dados brutos coletados do smartphone serão analisados e preparados para o modelo de predição. Os dados das séries temporais são divididos em blocos menores, chamados de segmentos ou janela de tempo.

Com os dados sendo capturados constantemente pelo dispositivo, é importante que eles sejam segmentados utilizando janela deslizante (BANOS et al., 2014) , que é o particionamento dos dados a uma taxa de amostragem com sobreposição de 50%. Um dos motivos para a adotá-la está em 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 (QUISPE et al., 2018). Um segmento de dados `wi = (ti, tf)` possui um tempo inicial ti e um tempo final tf . Logo, a segmentação

consiste em obter um conjunto de segmentos `W = w1, ..., wm`. Esse processo é realizado considerando também as múltiplas séries temporais disponíveis na base de dados.

4.4 Treinamento

Durante esta etapa os dados que são divididos em treino e teste, possibilitando a validação do modelo. Para a fase de treino é necessário que os dados estejam preparados para serem apresentados a um classificador binário (ANDRADE et al., 2021). Assim os dados são rotulados como "genuíno"ou "impostor".

Os dados de cada usuário são divididos em 50% para o treino do usuário genuíno e os outros 50% foram utilizados para geração do usuário impostor. Com o propósito de evitar o desbalanceamento da base, foi utilizado a mesma quantidade de dados do usuário genuíno e do usuário impostor. Em seguida os dados são enviados para a rede DeepConvLSTM.

Em um ambiente real a coleta dos dados é realizada para geração de um modelo único para o usuário genuíno. Vale ressaltar, que durante a fase de treinamento o dispositivo não pode ser utilizado por outro usuário, que não o usuário genuíno, pois isso comprometeria o modelo, consequentemente, reduzindo sua acurácia.

4.4.1 Rede Neural DeepConvLSTM

Para extração da assinatura biométrica é utilizado uma rede neural profunda denominada DEEPCONVLSTM, proposta no artigo de Ordóñez e Roggen (2016). A escolha dessa rede se deu devidos aos excelentes resultados obtidos em Andrade et al. (2021) de autenticação contínua para computadores pessoais. Arquitetura proposta possui camadas convolucionais, que são responsáveis pela extração de características dos dados dos sensores inerciais. Em seguida, camadas de recorrência, que são responsáveis por capturar características dos

dados processados nas camadas de convolução.

Segundo Palaz, Collobert et al. (2015), aplicar aos dados brutos técnicas de extração de características, na maioria das vezes, leva a um desempenho superior do classificador. Deste modo, foram empregadas as redes neurais recorrentes que podem receber como entrada os dados brutos (IGNATOV, 2018) coletados pelo acelerômetro e giroscópio, dispensando a normalização dos dados. Além disso, a descoberta manual de características requer conhecimento especializado, e a escala dos dados brutos produzidos pelos sensores inerciais são um fator limitador. Por essa razão, as redes convolucionais podem ser utilizadas para tratar estes desafios por conta da capacidade de extrair características de sensores inerciais (XU; YANG; HAUPTMANN, 2015).

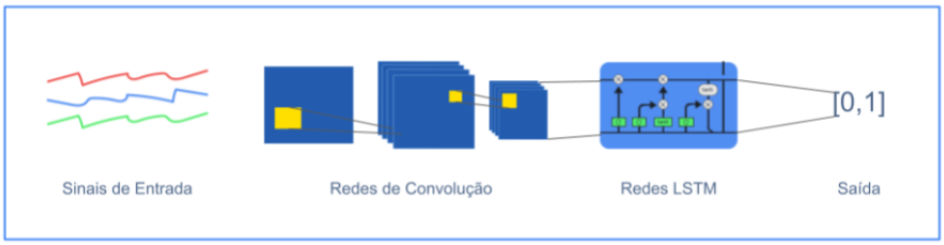


Figura 4.3 – Arquitetura da rede neural proposta. Fonte: Autor

Os dados resultantes das camadas de convolução são passados para as camadas densas recorrentes. As unidades de um LSTM são usadas como unidades de construção e, neste caso, cada camada recorrente é composta por 128 unidades, com saída de tamanho 20. 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.

O resultado dessa etapa é um modelo único para cada usuário. Este modelo será utilizado na autenticação contínua do usuário, pois a cada segmento de dados terá como resultado impostor ou genuíno, possibilitando o modelo de confiança penalizar ou recompensar o usuário.

4.5 Modelo de Confiança

O modelo de confiança implementado foi baseado no trabalho de (BOURS, 2012), essa abordagem que consiste em validar o usuário genuíno evitando interrupções desnecessárias e bloqueando o acesso ao impostor mais rapidamente. O principal objetivo no uso dessa abordagem é reduzir os falsos positivos e falsos negativos.

Em um sistema de autenticação contínua é importante evitar o bloqueio do usuário genuíno, sem reduzir a confiabilidade do sistema. Por esse motivo a importância do modelo de confiança, que é responsável por elevar os níveis de usabilidade e segurança.

Cada segmento da base de teste de usuário genuíno e impostor é verificado pelo autenticador biométrico a cada segmento de código que o modelo informa como genuíno é gerada uma recompensa. Caso o modelo identifique como usuário impostor uma penalidade é aplicada. Chegando ao limite mínimo o usuário é bloqueado.

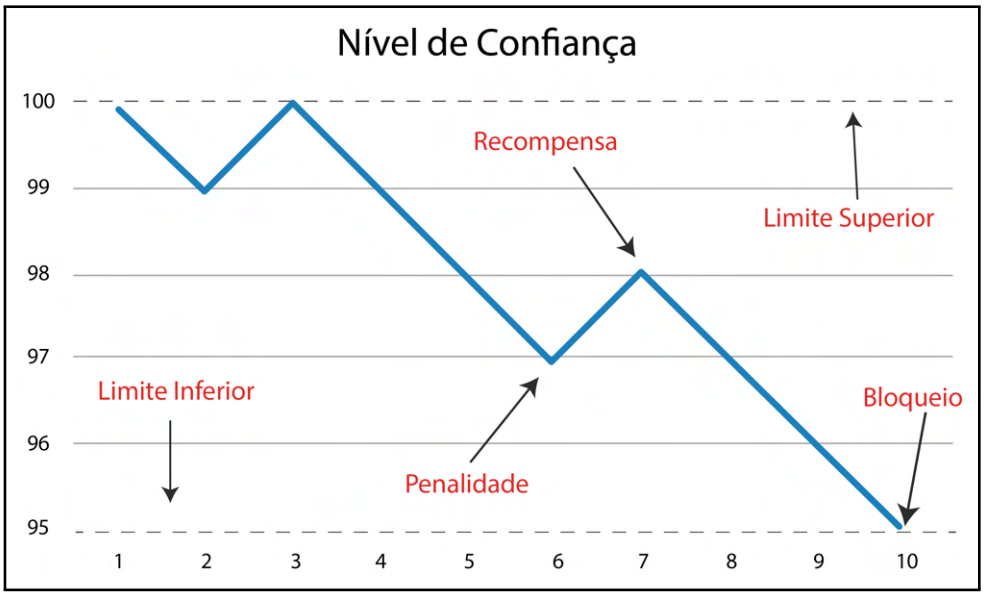


Figura 4.4 – Cenário de um usuário bloqueado. Fonte: Autor

Na Figura 4.4 é possível visualizar o cenário, em que o usuário impostor tenta utilizar o dispositivo e foi identificado pelo modelo de confiança. Nesse cenário foi levado em consideração um limite de inferior de 95, conforme pode ser visualizado na Figura 4.4. Posteriormente, esse limiar será reavaliado,

para inferir qual o melhor taxa para bloquear o usuário. É possível notar pela imagem que no instante 2 e 7 o modelo chegou a considerar o usuário como genuíno, mas a partir do momento 7, o usuário impostor foi penalizado e até chegar ao limite inferior de 95 e ser direcionado para a tela de login.

4.5.1 Nível de Confiança: Obtenção de ANGA e ANIA

O processo de avaliação do nível de confiança e da quantificação de ANGA e ANIA é realizado durante a etapa de teste em momentos distintos. Para obtenção de ANGA de um usuário, a parcela genuína dos dados de teste deste usuário é apresentada ao seu modelo previamente treinado na rede DEEPCONVLSTM, e para cada instância da referida base de dados, é obtida uma probabilidade de esta instância pertencer ao usuário em análise.

Para a obtenção de ANIA, a parcela impostora dos dados de teste deste usuário também é apresentada ao seu modelo previamente treinado na rede DEEPCONVLSTM, sendo que cada usuário que compõe a parte impostora dos dados de teste é avaliado separadamente, e para cada instância, é obtida uma probabilidade desta instância pertencer ao usuário em análise.

O índice de nível de confiança é obtido da avaliação da sequência destas probabilidades ao longo do tempo usando o algoritmo de nível de confiança. Entretanto, o conceito de ANGA e ANIA está relacionado ao número de ações executadas pelo usuário genuíno e impostor, respectivamente.

Essas ações nos estudos de (MONDAL; BOURS, 2015a) são geradas a partir de atos voluntários do usuário na interação com o mouse. Entretanto no estudo de sensores de dados inerciais o processo de coleta é periódico, divergindo portanto da ideia de ação voluntária o que não invalida a metodologia, visto que podemos abstrair o conceito de “ações” como sendo “observações” obtidas em intervalos de tempo (ANDRADE et al., 2021). Logo, cada ação no método proposto equivale a uma unidade 1 segundo dado que a captura dos sinais inerciais ocorre nesse intervalo.

4.6 Considerações Finais

Este capítulo apresentou os principais componentes do método de autenticação proposto. A utilização do do modelo de confiança possibilita uma melhor usabilidade no sistema evitando bloqueios desnecessários. No próximo capítulo será apresentado o protocolo experimental utilizado, bem como os resultados obtidos neste trabalho. As discussões sobre os motivos da utilização do método e configuração dos parâmetros também serão abordados.

5 Experimentos e Resultados

Este Capítulo descreve os experimentos realizados e os resultados obtidos. O capítulo inicia descrevendo o protocolo experimental (Seção 5.1), incluindo a base de dados utilizada nos experimentos, o processo de separação de dados para gerar o modelo, parâmetros utilizados para medir o nível de confiança do autenticador proposto, bem como as particularidades de cada experimento realizado. Na Seção 5.3 são apresentados os resultados e discussões. Por fim, a Seção 5.5 fornece algumas considerações finais.

5.1 Protocolo Experimental

O conjunto de experimentos foram escolhidos de forma a facilitar a comparação com outros trabalhos de autenticação contínua e mostrar a viabilidade do modelo.

5.1.1 Experimentos

Para validar o modelo proposto foram realizados três conjuntos de experimentos. O primeiro conjunto de experimentos tem como objetivo avaliar o impacto da utilização de diferentes combinações de sensores inerciais na acurácia do autenticador proposto. Foram realizados três rodadas de avaliações com as seguintes combinações:

- Acelerômetro.
- Acelerômetro + Giroscópio.
- Acelerômetro + Giroscópio + Magnetômetro.

No segundo conjunto de experimentos, nós comparamos os resultados do modelo proposto com os modelos propostos por (CENTENO; GUAN; MOORSEL,

2018) e (BÜCH, 2019b). Estes trabalhos foram escolhidos por implementarem autenticação contínua baseados em sensores inerciais.

Por fim, no terceiro conjunto de experimentos, foi avaliado o modelo de confiança. Como não há trabalhos que implementaram o modelo de confiança para a autenticação contínua baseada em sensores, esse trabalho realizou a comparação com o trabalho de Mondal e Bours (2015b) que utiliza dados do toque na tela para autenticar o usuário.

Foram utilizados 30 usuários da base de dados, escolhidos aleatoriamente. Excluindo os usuários detalhados na Seção 5.1.2 que estavam com problemas. 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.

5.1.2 Base de Dados

Para treino, validação e teste do modelo proposto foi utilizada o conjunto de dados HMOG (Hand Movement, Orientation, and Grasp dataset) proposto em (SITOVÁ et al., 2016). Este dataset é comumente utilizado em diversos trabalhos de autenticação contínua para dispositivos móveis, conforme por exemplo: (CENTENO; GUAN; MOORSEL, 2018), (CENTENO; MOORSEL; CASTRUCCIO, 2017) e (BÜCH, 2019b).

O dataset HMOG corresponde a dados coletados de 100 usuários de smartphones com o sistema operacional Android. Para cada usuário, os dados são coletados em 24 sessões diferentes. Cada sessão é realizada no intervalo de 5 a 15 minutos. Essas sessões incluem duas condições diferentes de movimento corporal (andar e sentar) e três cenários de atividade: 1) leitura de documentos, 2) produção de textos e 3) navegação em um mapa para localizar um destino.

Em média, cada usuário gerou cerca de 5 horas de dados. O conjunto

de dados original contém dados coletados das seguintes categorias comportamentais: acelerômetro, giroscópio, magnetômetro, evento de toque bruto, toque gesto, gesto de escala, gesto de rolagem e gesto de arremesso. Vale ressaltar, que os dados dos sensores inerciais foram coletados a uma taxa de 100Hz. Neste trabalho usaremos somente dados coletados pelos sensores de inerciais para geração do sistema de autenticação proposto.

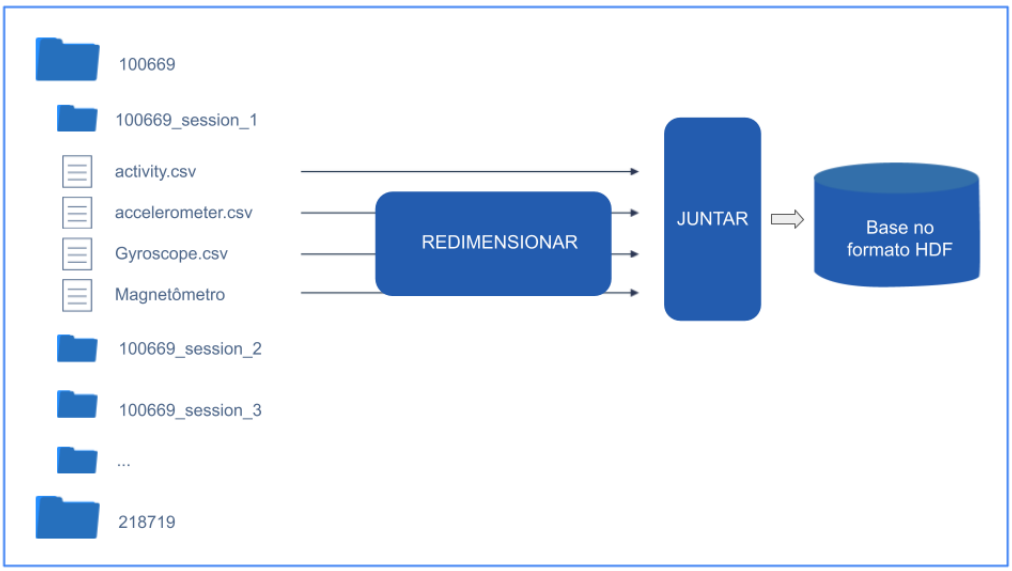


Figura 5.1 – Dados brutos do acelerômetro e giroscópio. Fonte: Autor

Na base de dados, os dados de cada usuário são organizados em pastas que contém os dados por sessão. Dentro de cada sessão é possível encontrar os arquivos referentes a acelerômetro, giroscópio e magnetômetro, como mostrado na Figura 5.1.

Após o pre-processamento da base de dados foram encontrados problemas em quatro usuários, descritos a seguir:

- As sessões de 9 a 14 de acelerômetro do usuário 733162 estavam sem informação.
- Os usuários 526319 e 796581 tinham somente 23 sessões ao invés de 24 sessões.
- O usuário 207696 estava com o nome da pasta trocado para 207969, causando uma inconsistência.

	acc_x	acc_y	acc_z	gyr_x	gyr_y	gyr_z	User
0	-0.110383	5.869652	5.864763	-0.109627	-0.057689	-0.022877	u527796
1	-0.318279	6.200583	6.870062	-0.153548	-0.003016	0.042363	u527796
2	-0.526176	6.531515	7.875361	-0.197470	0.051656	0.107604	u527796
3	-0.624631	6.753711	8.708956	-0.241391	0.106329	0.172844	u527796
4	-0.285317	6.540959	8.855733	-0.285312	0.161001	0.238085	u527796
...	...	...	...	...	...	...	...
18445	4.474648	0.710575	7.692952	0.228177	-0.326434	0.141770	u876011
18446	4.379492	0.808228	7.662184	0.076797	-0.212736	0.097177	u876011
18447	4.284335	0.905881	7.631416	-0.076774	-0.093252	0.043665	u876011
18448	4.179264	0.996195	7.582407	-0.088210	0.027829	0.055583	u876011
18449	3.977446	1.000824	7.342577	-0.014363	0.149866	0.106760	u876011

[9056748 rows x 7 columns]

Figura 5.2 – Visualização dos dados de sensores inerciais no formato HDF. Fonte: Autor

O resultado do pre-processamento dos dados (remoção de atributos e inconsistências) foi salvo no formato de dados hierárquicos (HDF), o qual é considerado mais eficiente para realizar a leitura do que o acesso a dados estruturados (COLLETTE, 2013). Na Figura 5.2 é possível visualizar os dados brutos dos acelerômetro e giroscópio nas três direções: X, Y e Z.

5.2 Separação dos Dados

A rede foi treinada com dados do usuário genuíno e impostor. O treinamento ocorre com 50% dos dados do usuário genuíno e os outros 50% formado pelos dados dos N usuários impostores que formam a base. A parte dos dados do impostor é composta com, aproximadamente, a mesma quantidade do usuário genuíno. Essa abordagem foi adotada para evitar o desbalanceamento da base, evitando que o resultado esteja enviesado para o genuíno ou para o impostor.

A base de teste é feita com todos os dados que não foram usados para treinamento, sendo um conjunto de dados genuíno e $(N - 1)$ conjunto de dados impostores, seguindo a mesma lógica de formação dos dados de treinamento, evitando assim o desbalanceamento do modelo. A Figura 5.3 mostra a separação para o usuário 1.

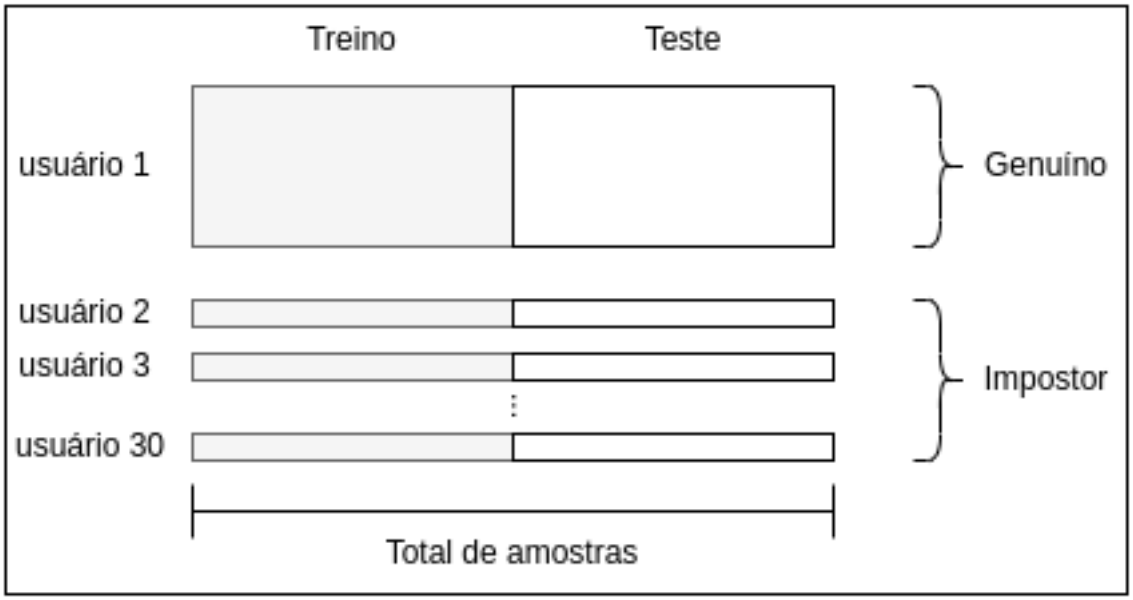


Figura 5.3 – Separação dos dados para o usuário 1– Fonte: Autor

5.3 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 5.1 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.

Tabela 5.1 – Parâmetros utilizados no nível de confiança

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

A primeira função de recompensa ${f^1}_{\mathrm{recompensa}} x_{\mathrm{i}} = x_{\mathrm{i}}$ fornece os valores da acurácia da rede neural no intervalo de $0.5 < x < 0.9$, sendo assim mais moderada. No caso do resultado da rede neural vir entre $0.9 < x < 1$ é utilizado a segunda função de recompensa ${f^2}_{\mathrm{recompensa}} x_{\mathrm{i}} = 1$ 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.

Os limiares e funções de recompensa e penalidade utilizados nesse trabalho se justificam pelos resultados encontrados no trabalho de (ANDRADE et al., 2021), que trata autenticação contínua utilizando contadores de desempenho do sistema operacional.

5.4 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. A Tabela 5.2 faz uma sumarização dessas métricas.

Tabela 5.2 – Métricas utilizadas no Método Proposto

Acurácia	medida de desempenho global que avalia a proporção de classificações corretas, tanto para os casos positivos quanto negativos.
FRR	quantifica os elementos que foram classificados erroneamente como impostor mas que eram genuínos.
FAR	quantifica os elementos que foram classificados erroneamente como genuíno mas que pertenciam ao impostor.
EER	métrica não extraída diretamente do método mas é uma composição da FRR com a EER.
ANIA	quantidade média de iterações até bloquear o usuário impostor.
ANGA	quantidade de bloqueios do usuário genuíno durante o uso do dispositivo.

Este trabalho utilizou da pesquisa do (MONDAL; BOURS, 2015a) e implementou um autenticador biométrico. Este autenticador introduz duas novas métricas. O ANIA que trata da quantidade de iterações até bloquear o usuário impostor e o ANGA que é a quantidade de bloqueios do usuário

genuíno durante o uso do dispositivo. A Seção 2.1.4 apresenta essas métricas detalhadamente.

5.5 Resultados

Nesta seção serão apresentados os resultados obtidos dos experimentos pelo método proposto.

5.5.1 Experimentos

O experimento 1 teve como objetivo validar quais conjuntos de sensores inerciais produzem 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 5.3 mostra que as taxas de acurácia são próximas para os três conjuntos de sensores avaliados, sendo o melhor resultado de 99,81% de acurácia para o modelo gerado a partir da combinação dos sensores acelerômetro, giroscópio e magnetômetro. Além disso, por fornecer mais informações no treino, essa combinação de sensores também apresentou a menor taxa de erro médio de 0,24

Tabela 5.3 – 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 experimento 2 foi realizado um comparativo com outros trabalhos baseados em sensores inerciais. O método proposto obteve 99.81%, que é uma ligeira melhoria em relação ao trabalho do (CENTENO; GUAN; MOORSEL, 2018), que obteve uma acurácia 97.8%. isso mostra a eficácia da rede DeepConvLSTM na autenticação contínua é bastante satisfatório para este experimento, demonstrando a capacidade da rede CNN de capturar padrões dos usuários e da rede LSTM de com dados temporais.

No trabalho de (BÜCH, 2019b) teve uma acurácia de 65.3%, segundo o autor isso se deve a escolha da normalização utilizada. No método proposto foram enviados dados brutos para a rede CNN o que trouxe excelentes resultados para a rede neural dado a capacidade da CNN de realizar a normalização dos dados durante o treinamento, conforme pode ser visualizado na Tabela 5.4.

Tabela 5.4 – Resultados alcançados pelos trabalhos de Autênticação Contínua utilizando sensores inerciais. Fonte: Autor

Sensores	**Acurácia**	**EER**
Método Proposto	99.80%	0.17%
Centeno et al. (2018)	97.80%	3%
H. Buech (2019)	65.30%	36.8%

No experimento 3 é avaliado o modelo de confiança, que é introduzido nesse trabalho como um item adicional na autenticação em dispositivos móveis com sensores inerciais, visando reduzir evitar o bloqueio do usuário genuíno e bloquear rapidamente o usuário impostor. Esse experimento foi realizado com a melhor combinação de sensores apresentados no experimento 1 (acc+gyr+mag).

Como não há trabalhos que implementaram o modelo de confiança para a autenticação contínua baseada em sensores, esse trabalho realizou a comparação com o trabalho de (MONDAL; BOURS, 2015b) que utiliza dados do toque na tela para autenticar o usuário. Que apesar de ter dados de entradas diferentes servirá de comparação com o método proposto.

Tabela 5.5 – 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

Quando utilizado o modelo de confiança o método proposto foi superior em todos os cenários. A Tabela 5.4 mostra que o usuário genuíno conseguiu utilizar o sistema sem interrupções. Além disso os resultados de ANIA e ANGA comparados com o Mondal and Bours indica que o trabalho proposto consegue identificar o usuário impostor rapidamente. Sendo que Mondal and Bours consegue 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%. Cada ação representa 1 segundo coletado pelo sensor, logo o usuário impostor é identificado em 1 minuto.

5.5.2 Considerações Finais

Os resultados apresentados demonstram a viabilidade do método, principalmente do modelo de confiança, que evita evita interrupções desnecessárias, melhorando a usabilidade do sistema. A utilização de dados de sensores inerciais, facilita o desenvolvimento e a adoção de um sistema de autenticação contínua, pois não exige permissões especiais do Sistema Operacional Android e não necessita de acesso a informações sensíveis do usuário. Este capítulo demonstrou a melhor combinação de sensores a serem utilizados.

6 Conclusões e Trabalhos Futuros

Este trabalho demonstrou a viabilidade da autenticação contínua em dispositivos móveis utilizando dados de sensores inerciais. Nos resultados apresentados, nenhum usuário genuíno foi bloqueado indevidamente e todos os impostores foram detectados com até 61 segundos. Abaixo serão listados algumas considerações em relação ao trabalho.

1. **Utilização do modelo de confiança**

   A utilização do protocolo experimental proposto por (MONDAL; BOURS, 2015b) permitiu adicionar o nível de confiança, que é uma contribuição desse trabalho, aumentando a robustez do modelo e diminuindo a interferência na utilização por parte do usuário genuíno sem perder a eficiência em capturar o usuário impostor. Isso refletiu em um melhor processo de avaliação, e comparando com outros estudos que avaliam a taxa de falso positivo e de falso negativo.

   O uso somente das métricas EER, FAR e FRR para o trabalho de autenticação contínua não garante ter uma visão real de como o sistema está se comportando em relação aos usuários genuínos e impostores, pois mesmo que as taxas de falso positivo e taxas de falso negativo baixas, a ausência de um modelo de confiança vai gerar bloqueios indesejados para o usuário genuíno. Sendo assim a adoção das métricas ANGA e ANIA permitem ter uma ideia de como o sistema esta se comportando em relação ao bloqueio dos usuários genuíno e impostor, respectivamente.

2. **Usabilidade do sistema de autenticação**

   Na era da tecnologia onde à informação está cada vez mais acessível e segurança é um item de extrema importância, sendo necessário adicionar camadas de segurança que evitem o acesso à informação por parte de um possível invasor. Esse *trade-off* entre segurança e usabilidade que devem ser satisfeitos, isto é, o sistema deve continuamente prevenir usos não

autorizados enquanto proporciona níveis satisfatórios de experiência de usuário.

Foi observado que a utilização desse autenticador agrega ao estudo uma robustez e estabilidade. Uma vez que um mesmo usuário pode, eventualmente, fugir de seu padrão de comportamento, caso a avaliação ocorresse somente com os métodos tradicionais, certamente estes desvios implicariam em situação de falso negativo.

3. **Modelo de Autenticação Contínua**

   A DEEPCONVLSTM, proposta por (ORDÓÑEZ; ROGGEN, 2016), já havia recebido bons resultado em processamento de sinais devido sua extração dos dados pela rede CNN em conjunto com a rede de recorrência LSTM. Entretanto, essa rede não havia sido empregadas para estudo de autenticação contínua usando dados de sensores inerciais.

6.1 Contribuições

As principais contribuições deste trabalho são:

1. Adaptação do modelo de confiança proposto por (MONDAL; BOURS, 2015b), que havia sido desenvolvido para estudo autenticação contínua baseada na dinâmica de mouse, e que já foi adaptado para autenticação em contadores de desempenho de sistema operacional (ANDRADE et al., 2021) para o estudo de sensores inerciais em dispositivos móveis.

2. Implementação de uma arquitetura de rede profunda baseada em camadas de convolução e de recorrência. Os dados dos sensores inerciais são coletados em períodos sucessivos de tempo e, portanto, são caracterizados como uma série temporal.

6.2 Direções futuras

Como trabalhos futuros ou variações deste trabalho podem ser elencados:

- A implementação de um protótipo em Android possibilitará a validação do sistema em mundo real, permitindo validar as técnicas implementadas. Além disso, seria importante ter uma avaliação do impacto do consumo de energia nos dispositivos causados pelo emprego do mecanismo de autenticação proposto neste trabalho.

- Como a obtenção de dados para treinamento do modelo é difícil e custoso, nós pretendemos no futuro empregar técnicas de aumento de dados *(data augmentation)* visando melhorar ainda mais a precisão do autenticador proposto. É esperado ainda, que a adoção dessa técnica reduza o período de coleta de dados do usuário genuíno para geração do modelo, permitindo o usuário ter o sistema de autenticação em um menor período de tempo.

- Realizar alguns experimentos em conjunto o reconhecimento de atividade humana pode melhorar a precisão da rede em um cenário com menos sensores disponíveis.

- Utilizar função logarítmica na penalização e recompensa pode detectar o usuário impostor mais rapidamente, reduzindo o número de ações até ser bloqueado.

Referências

ABUHAMAD, M. et al. Sensor-based continuous authentication of smartphones' users using behavioral biometrics: A contemporary survey. *IEEE Internet of Things Journal*, IEEE, v. 8, n. 1, p. 65–84, 2020. 14

ANDRADE, C. H. G. et al. Autenticação contínua de usuários utilizando contadores de desempenho do sistema operacional. Universidade Federal do Amazonas, 2021. 23, 25, 39, 42, 49, 54

AVIV, A. J. et al. Smudge attacks on smartphone touch screens. *Woot*, v. 10, p. 1–7, 2010. 12

BANOS, O. et al. Window size impact in human activity recognition. *Sensors*, Multidisciplinary Digital Publishing Institute, v. 14, n. 4, p. 6474–6499, 2014. 38

BARBELLO, B. Continuous user authentication on mobile devices: Recent progress and remaining challenges. 2016. 13, 31

BOURS, P. Continuous keystroke dynamics: A different perspective towards biometric evaluation. *Information Security Technical Report*, Elsevier, v. 17, n. 1-2, p. 36–43, 2012. 41

BOURS, P.; BARGHOUTHI, H. Continuous authentication using biometric keystroke dynamics. In: *The Norwegian Information Security Conference (NISK)*. [S.l.: s.n.], 2009. v. 2009. 15

BRAGANÇA, H. L. d. S. et al. Reconhecimento de atividades humanas usando medidas estatísticas dos sensores inerciais dos smartphones. Universidade Federal do Amazonas, 2019. 38

BÜCH, H. *ContinAuth*. GitHub, 2019. Disponível em: <https://github.com/dynobo/ContinAuth>. 13

BÜCH, H. *Continuous Authentication using Inertial-Sensors of Smartphones and Deep Learning*. Dissertação (mastersthesis) — Hochschule der Medien, Stuttgart, 6 2019. Disponível em: <https://hdms.bsz-bw.de/frontdoor/index/index/docId/6506>. 33, 34, 45, 51

CENTENO, M. P.; GUAN, Y.; MOORSEL, A. van. Mobile based continuous authentication using deep features. 2018. 33, 34, 45, 51

CENTENO, M. P.; MOORSEL, A. van; CASTRUCCIO, S. Smartphone continuous authentication using deep learning autoencoders. 2017. 13, 32, 33, 34, 45

COLLETTE, A. *Python and HDF5: unlocking scientific data*. [S.l.]: "O'Reilly Media, Inc.", 2013. 47

DERAWI, M. O. et al. Unobtrusive user-authentication on mobile phones using biometric gait recognition. In: IEEE. *2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. [S.l.], 2010. p. 306–311. 29

FRANK, M. et al. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE transactions on information forensics and security*, IEEE, v. 8, n. 1, p. 136–148, 2012. 31, 34

GAFUROV, D.; SNEKKENES, E. Gait recognition using wearable motion recording sensors. *EURASIP Journal on Advances in Signal Processing*, Springer, v. 2009, p. 1–16, 2009. 29

GOOGLE. *Android Services Overview*. 2021. Accessed: 2021-11-23. Disponível em: <https://developer.android.com/guide/components/services>. 37

HAQ, M. Ehatisham-ul et al. Continuous authentication of smartphone users based on activity pattern recognition using passive mobile sensing. *Journal of Network and Computer Applications*, Elsevier, v. 109, p. 24–35, 2018. 12

HERING, E.; SCHÖNFELDER, G. *Sensoren in Wissenschaft und Technik*. [S.l.]: Springer, 2018. 8, 19, 20, 21

HOCHREITER, S.; SCHMIDHUBER, J. Long short-term memory. *Neural computation*, MIT Press, v. 9, n. 8, p. 1735–1780, 1997. 27

HUBEL, D. H.; WIESEL, T. N. Receptive fields and functional architecture of monkey striate cortex. *The Journal of physiology*, Wiley Online Library, v. 195, n. 1, p. 215–243, 1968. 24

IGNATOV, A. Real-time human activity recognition from accelerometer data using convolutional neural networks. *Applied Soft Computing*, Elsevier, v. 62, p. 915–922, 2018. 25, 40

KIM, J.-M.; LEE, D.-H.; KIM, K.-N. J. The study of response model & mechanism against windows kernel compromises. *Convergence Security Journal*, Korea convergence Security Association, v. 6, n. 3, p. 1–12, 2006. 32

LEE, W.-H.; LEE, R. Implicit sensor-based authentication of smartphone users with smartwatch. In: ACM. *Proceedings of the Hardware and Architectural Support for Security and Privacy 2016*. [S.l.], 2016. p. 9. 32, 34

LI, Y. et al. Sensor-based continuous authentication using cost-effective kernel ridge regression. *IEEE Access*, IEEE, v. 6, p. 32554–32565, 2018. 22

LIMA, W. S. et al. Reconhecimento de atividades humanas baseado na análise de fluxo contínuo de dados simbólicos. Universidade Federal do Amazonas, 2019. 19, 20, 21

MAHFOUZ, A.; MAHMOUD, T. M.; ELDIN, A. S. A survey on behavioral biometric authentication on smartphones. *Journal of Information Security and Applications*, Elsevier, v. 37, p. 28–37, 2017. 12, 17, 31

MANTYJARVI, J. et al. Identifying users of portable devices from gait pattern with accelerometers. In: IEEE. *Proceedings.(ICASSP'05). IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005.* [S.l.], 2005. v. 2, p. ii–973. 30, 34

MONDAL, S.; BOURS, P. A computational approach to the continuous authentication biometric system. *Information Sciences*, Elsevier, v. 304, p. 28–53, 2015. 14, 42, 49

MONDAL, S.; BOURS, P. Swipe gesture based continuous authentication for mobile devices. In: IEEE. *2015 International Conference on Biometrics (ICB).* [S.l.], 2015. p. 458–465. 14, 22, 24, 31, 34, 45, 51, 53, 54

NETO, W.; FIGUEIREDO, C. Detecção de tentativa de invasão por dados sintéticos em aplicações de biometria por voz. In: SBC. *Anais do XI Simposio Brasileiro de Computacao Ubiqua e Pervasiva.* [S.l.], 2019. 13

NGUYEN, T. V.; SAE-BAE, N.; MEMON, N. Draw-a-pin: Authentication using finger-drawn pin on touch devices. *computers & security*, Elsevier, v. 66, p. 115–128, 2017. 13

NICKEL, C.; BUSCH, C. Classifying accelerometer data via hidden markov models to authenticate people by the way they walk. *IEEE Aerospace and Electronic Systems Magazine*, IEEE, v. 28, n. 10, p. 29–35, 2013. 30, 34

NIXON, M. S.; TAN, T.; CHELLAPPA, R. *Human identification based on gait.* [S.l.]: Springer Science & Business Media, 2010. v. 4. 29

ORDÓÑEZ, F. J.; ROGGEN, D. Deep convolutional and lstm recurrent neural networks for multimodal wearable activity recognition. *Sensors*, Multidisciplinary Digital Publishing Institute, v. 16, n. 1, p. 115, 2016. 39, 54

PALAZ, D.; COLLOBERT, R. et al. *Analysis of cnn-based speech recognition system using raw speech as input.* [S.l.], 2015. 40

PATEL, V. M. et al. Continuous user authentication on mobile devices: Recent progress and remaining challenges. *IEEE Signal Processing Magazine*, IEEE, v. 33, n. 4, p. 49–61, 2016. 8, 17

QIAN, G.; ZHANG, J.; KIDANÉ, A. People identification using gait via floor pressure sensing and analysis. In: SPRINGER. *European Conference on Smart Sensing and Context.* [S.l.], 2008. p. 83–98. 29

QUISPE, K. G. M. et al. Representação simbólica de séries temporais para reconhecimento de atividades humanas no smartphone. Universidade Federal do Amazonas, 2018. 38

RECOD Lab. *RECODGait Dataset.* 2019. Disponível em: <https://recodbr.wordpress.com/code-n-data/#recodgait>. 30

RONAO, C. A.; CHO, S.-B. Human activity recognition with smartphone sensors using deep learning neural networks. *Expert systems with applications*, Elsevier, v. 59, p. 235–244, 2016. 24

SANTOS, G. et al. Técnicas para autenticação contínua em dispositivos móveis a partir do modo de caminhar. [sn], 2017. 29, 34

SENSORTEC, B. *Bosch Sensortec*. 2022. <https://www.bosch-sensortec.com/bst/products/all_products/bmi263>. [Online; accessed 22-Fev-2022]. 8, 21

SHEN, C.; CHEN, Y.; GUAN, X. Performance evaluation of implicit smartphones authentication via sensor-behavior analysis. *Information Sciences*, Elsevier, v. 430, p. 538–553, 2018. 24, 33, 34

SITOVÁ, Z. et al. Hmog: New behavioral biometric features for continuous authentication of smartphone users. *IEEE Transactions on Information Forensics and Security*, IEEE, v. 11, n. 5, p. 877–892, 2016. 14, 35, 45

SPREITZER, R. et al. Systematic classification of side-channel attacks: a case study for mobile devices. *IEEE Communications Surveys & Tutorials*, IEEE, v. 20, n. 1, p. 465–488, 2017. 12

STYLIOS, I. C. et al. A review of continuous authentication using behavioral biometrics. In: ACM. *Proceedings of the SouthEast European Design Automation, Computer Engineering, Computer Networks and Social Media Conference*. [S.l.], 2016. p. 72–79. 31

THANG, H. M. et al. Gait identification using accelerometer on mobile phone. In: IEEE. *2012 International Conference on Control, Automation and Information Sciences (ICCAIS)*. [S.l.], 2012. p. 344–348. 30, 34

THOMAZINI, D.; ALBUQUERQUE, P. U. B. de. *Sensores industriais: fundamentos e aplicações*. [S.l.]: Saraiva Educação SA, 2020. 18

VČELÁK, J.; RIPKA, P.; ZIKMUND, A. Precise magnetic sensors for navigation and prospection. *Journal of Superconductivity and Novel Magnetism*, Springer, v. 28, n. 3, p. 1077–1080, 2015. 21

WAKABAYASHI, N.; KURIYAMA, M.; KANAI, A. Personal authentication method against shoulder-surfing attacks for smartphone. In: . [S.l.: s.n.], 2017. p. 153–155. 12

WANG, L. et al. Fusion of static and dynamic body biometrics for gait recognition. *IEEE Transactions on circuits and systems for video technology*, IEEE, v. 14, n. 2, p. 149–158, 2004. 29

XU, Z.; YANG, Y.; HAUPTMANN, A. G. A discriminative cnn video representation for event detection. In: *Proceedings of the IEEE conference on computer vision and pattern recognition*. [S.l.: s.n.], 2015. p. 1798–1807. 40

YAN, J. et al. Towards a user-friendly and secure hand shaking authentication for smartphones. p. 1170–1179, 2018. 27

YANG, Q. et al. A multimodal data set for evaluating continuous authentication performance in smartphones. In: ACM. *Proceedings of the 12th ACM Conference on Embedded Network Sensor Systems*. [S.l.], 2014. p. 358–359. 33

ZHANG, X.-Y. et al. Thermal stresses in the large grain ybacuo superconductors during zero field cooling. *Journal of superconductivity and novel magnetism*, Springer, v. 26, n. 1, p. 87–92, 2013. 21