基于迁移自编码器与多模态数据的智能手机隐式身份认证

许子昂
（北方工业大学伦敦布鲁内尔学院，北京 100144）

摘　要：随着智能手机的普及，传统显式身份认证技术（如密码、指纹）因依赖用户主动输入而易受攻击，非侵入式的隐式身份认证逐渐成为研究热点。提出一种基于数据驱动迁移自编码器的智能手机隐式身份认证方案，通过多模态传感器采集用户解锁图案时的行为特征（如加速度、陀螺仪数据），结合自编码器提取高判别性隐层特征，并设计迁移学习框架实现快速模型微调。实验表明，在 50 位用户、4 台智能手机上进行图案解锁时产生的多达 10 GB 离线数据集上预训练后，仅需 1.3 s 即可完成在线认证，准确率高达 99.06%，显著优于传统机器学习方法（SVM 准确率 89.19%）、传统深度学习方法（KNN 准确率 95.49%）及现有 SOTA 方案（EspialCog 准确率 98.76%）。此外，用户在使用前仅须录入 6 次解锁行为即可完成模型适配，兼顾安全性与用户体验。

关键词：隐式身份认证；自编码器；迁移学习；图案解锁；隐私保护
中图分类号：TP309；TP391.4
文献标志码：A
doi：10.11959/j.issn.2096−3750.2025.00493

Implicit smartphone authentication via multimodal data and transfer autoencoders

XU Zi’ang
Brunel London School, North China University of Technology, Beijing 100144, China

Abstract: With the widely used of smartphones, traditional explicit authentication methods (e.g., passwords, fingerprints) are increasingly vulnerable due to their reliance on active user input, making the non-invasive implicit authentication a critical research focus. A transfer autoencoder-based implicit authentication framework for smartphones was proposed. Users’ behavioral features were captured during pattern unlocking (e.g., accelerometer and gyroscope data) through multimodal sensors, an autoencoder was employed to extract discriminative latent representations, and a transfer learning mechanism was incorporated for rapid model fine-tuning. The results of the experiment indicate that following the pre-training of the scheme on a 10 GB offline dataset, which is generated from the unlocking patterns of 50 users across 4 smartphones, the online authentication process can be executed in a mere 1.3 seconds, achieving an accuracy rate of 99.06%. This performance is markedly superior to that of traditional machine learning methods, such as support vector machine (SVM), which exhibits an accuracy rate of 89.19%. Furthermore, it surpasses conventional deep learning approaches, including K-nearest neighbor (KNN) with an accuracy of 95.49%, as well as existing state-of-the-art (SOTA) schemes like EspialCog, which achieves an accuracy of 98.76%. Additionally, it is noteworthy that users are required to perform the unlocking behavior only six times prior to utilization in order to complete the model adaptation, thereby balancing considerations of security with user experience.

Key words: implicit authentication, autoencoder, transfer learning, pattern unlock, privacy protection

收稿日期：2025−03−13；**修回日期：**2025−06−07

0 引言

移动终端和相关行业蓬勃发展，其带来的功能和价值越来越多。智能手机作为常用的移动设备，已经从简单的通信工具发展成综合的信息处理平台，同时也存储了用户大量隐私信息，所以智能手机的认证安全尤为重要。据 Check Point 发布的《2025 年全球网络安全报告》，超 70% 的移动设备攻击源于密码泄露或生物特征仿冒[1]，如何提高移动设备用户身份认证的安全性成为一个重要的研究内容。传统显式身份认证包括个人标识码（PIN, personal identification number）识别、图形密码认证和指纹、面部、虹膜等基于生物特征的识别方法[2]，但此类认证技术已被众多研究表明存在一定风险[3-4]，因此一种依赖于用户行为习惯的隐式身份认证方式引起广泛关注。此类认证方式通过一系列传感器识别用户行为特征，包括用户滑动屏幕时的触摸屏特征、输入密码时的 touch 特征、步态特征等[5]。每个用户行为特征都是由先天身体特征和后天行为习惯形成的，很难被记录或模仿。因此，基于用户行为特征的隐式认证具有较高的安全性[6-7]。此外，隐式认证是一种基于用户行为习惯自动识别身份的技术，其核心特点包括：行为习惯提取和非侵入性。通过分析用户的日常行为模式来建立个体行为特征，这些特征在用户正常使用过程中不断更新，以提高认证准确性。与传统身份验证方法（如密码或指纹识别）相比，隐式认证具有非侵入性的优势。用户无须主动进行身份验证，系统在后台自动进行监测和分析，从而减少对用户的干扰和操作负担。本文聚焦于智能手机用户图案解锁场景的隐式认证，通过内置多模态传感器被动采集行为特征，具体包括两点。（1）运动传感器：加速度计（ACC）捕获设备三维加速度波动，陀螺仪（Gyr）记录绕 $X/Y/Z$ 轴的旋转角速度。（2）交互传感器：压力传感器（PRE）监测手指触控屏幕的压力值，屏幕触控轨迹记录划屏坐标序列，用于还原解锁图案的轨迹曲率与速度分布。用户仅需按日常习惯输入解锁图案（如“L”“Z”“S”“T”形折线或曲线），系统在后台非侵入式采集上述数据，无须额外操作或硬件依赖。相较于传统显式认证中用户需主动输入密码或指纹，本文方案通过连续监测解锁行为的动态特征实现身份验证，在保证安全性的同时显著提升用户体验。

近年来，已有部分研究者对此领域开展广泛研究。Wu 等[8]提出了一种可靠的上下文感知隐式身份验证框架，以整体的方式描述用户的行为和上下文特征，通过观察不同智能手机使用模式的上下文感知状态，建立上下文感知模型来区分合法用户和非法用户。虽然性能具有一定优越性，但其特征提取受限于预设场景。Karanikiotis 等[9]提出了一种实现连续隐式认证的方法，通过采用大量个人广泛使用的现实世界应用程序，避免了小规模和/或受控环境实验所施加的限制。该方法在一定程度上弥补了行为受限，并且也取得了不错的结果。但它仅使用支持向量机完成认证，难以捕捉复杂行为模式的非线性关系。也有一些研究聚焦于可穿戴设备的认证，利用心率、步态和呼吸音频信号来验证用户身份[10]，但因依赖额外硬件难以推广至智能手机场景。总的来说，现有隐式认证相关研究都取得了可靠的性能，但仍在以下方面有提升空间。（1）用户行为特征的多样性：在采集行为特征时，应尽量减少限制，充分还原真实使用情况进行数据采集。（2）用户特征充分提取和认证的可靠性：需要采取更适合的模型来进一步完善行为特征的处理和提取方法，增强特征表达能力。（3）用户完成认证的速度和体验：考虑用户从录入特征到进行验证的时间成本，应在保证精确率的前提下尽可能缩短录入、认证时间，保证用户体验。

针对隐式身份认证中行为特征多样性不足、模型泛化能力弱及用户等待时间过长的挑战，本文提出一种基于迁移自编码器的智能手机隐式认证方案，包括以下 4 个阶段。（1）多模态数据采集：通过加速度计、陀螺仪及压力传感器捕获用户在不同运动状态（行走、静止）下的解锁行为数据（如触控轨迹、设备姿态），经滑动窗口分割（500 ms 窗口，50% 重叠）与 Z-score 标准化后构建 10 GB 离线训练集。（2）隐层特征提取：设计堆叠卷积自编码器，其编码器采用双层卷积与最大池化层提取时空敏感特征，解码器通过全连接层重构输入，以均方误差（MSE, mean square error）损失优化特征判别性。（3）模型在线迁移：基于最大均值差异（MMD, maximum mean discrepancy）度量对齐预训练模型与用户录入数据的隐层分布，仅需 6 次解锁即可完成微调。（4）轻量化认证：在线推理时，计算输入特征与隐层向量的余弦相似度，阈值设为 0.85，实现 1.3 s 内

完成认证且FAR≤1.5%。综上，本文贡献与创新可归纳为以下3部分。

（1）提出多模态行为特征采集框架，覆盖加速度计、陀螺仪等传感器数据，真实还原用户解锁场景。

（2）设计轻量化自编码器网络，通过卷积神经网络（CNN）编码器提取时空敏感特征，结合多层感知机（MLP）解码器实现高效身份判别。

（3）引入基于MMD的迁移学习算法，仅需用户6次解锁即可完成模型微调，较传统方法减少80%数据录入时间。

1　研究现状

本节主要从隐式身份认证中内置传感器选择、实现算法以及迁移自编码器研究3个部分对现有工作进行总结。

1.1　内置传感器的选择

随着移动终端的发展和功能的完善，其内置传感器也逐渐完善。目前智能手机的内置传感器主要由摄像头、麦克风、通信模块、全球定位系统（GPS）、运动传感器等组成。在采集用户行为特征时，主要关注两大类传感器：（1）环境传感器，包括气压计、光度计和温度计，用于收集环境信息；（2）运动传感器，包括加速度计、陀螺仪、磁力计和方向计，用于反映手机运动状态。

本文充分调研了现有研究在隐式身份认证中的传感器应用，发现其存在模态单一化、场景静态化和硬件依赖化三大局限。与现有方案相比，本文四模态融合策略（加速度计–陀螺仪–压力传感器–触控轨迹）具有显著优势。例如，Abuhamad等[11]采用了“加速度计–陀螺仪–磁力计”三模态，但仅覆盖设备运动特征，缺乏触控交互数据（如压力、轨迹曲率）。本文通过补充压力传感器与触控轨迹，新增“手指力度–划屏速度”关联特征，经消融实验验证可使准确率得到提升。与静态场景方案对比，Zhang等[12]虽采用更多的传感器（包括加速度计、陀螺仪、磁力计）和触控交互数据（压力、屏幕触摸区域等），并使用Android手机开放的应用程序接口（API, application program interface）进行数据收集，但实验限定于静止环境，未验证动态场景泛化能力。也有研究关注内在生理特征。Ekiz等[13]依赖手腕穿戴设备的光电容积传感器提取心率特征，存在硬件依赖与隐私风险。本文仅使用智能手机内置传感器，无须额外设备，且通过Z-score标准化与时空特征解耦，避免生理数据直接采集。

总的来说，隐式身份认证相关研究一般倾向于使用能反映用户动态行为特征的传感器，也就是运动传感器，包括：加速度计、陀螺仪、磁力计、方向传感器等。此外对于压力传感器和屏幕触摸位置等信息也有所使用。而对于生物特征传感器往往不会考虑，因为其更容易被模仿和攻击[14]。

1.2　隐式身份认证相关算法

在隐式身份认证中，同样重要的过程是特征提取处理和认证算法，这直接决定了用户认证的准确性。同时，过于复杂的模型设计会增加计算时间成本，为用户带来较差的使用体验，这也是难以接受的。基于这一思想，部分研究设计特征提取和认证算法，完成高效准确的认证过程。

Zhu等[15]考虑了数据采集效率与认证场景覆盖率低等问题，通过进化稳定参与博弈机制完成内置传感器的数据采集；采用优化的长短期记忆（LSTM, long short-term memory）模型和增强的随机梯度下降（SGD）算法实时验证移动设备的所有权。文献[16]将隐式身份认证推广到传统对象领域，将隐式认证相关测量问题转化为图像比较问题，并利用神经网络成功地解决了这一问题。文献[17]提出了利用基于边缘的步态生物识别，使用CNN和LSTM将原始信号转换成图像，并在二维域中提取步态信号的特征。此外，本文研究还考虑了智能手机本地计算开销受限，将隐式身份验证模型在云服务器上生成，用户身份验证过程也在边缘设备上进行。Zhao等[18]探索了用户多模态数据的有机集成以便准确验证身份，通过处理多通道运动传感器数据和离散触摸屏数据，建立了一种基于时间和通道注意力的递归神经网络来构建认证模型。

整体来说，现有算法面临“特征提取浅层化、模型迁移能力弱、计算成本高”的挑战，尤其在小样本场景下难以兼顾精度与实时性。

1.3　迁移学习和自编码器相关研究

部分研究考虑了隐式身份认证过程中的更新问题，并且使用与迁移相关的方法。文献[19]关注数字学习环境中的隐式身份认证，考虑不同的认证器，以覆盖所有可能用户与在线学习环境的交互，同时利用迁移方案研究模板适应性以克服模板老化

问题。然而他们没有将迁移学习应用到离线训练和模型微调的过程中。Li 等[20]提出了一种轻量级且有效的基于自编码器的移动设备连续认证系统，在注册阶段，使用加速度计和陀螺仪传感器来隐式收集用户行为模式；在认证阶段，当用户操作移动设备时，收集当前用户数据使用经过训练的自编码器重构该用户数据。然后，通过将重构数据与归一化数据进行比较来计算重构误差，以判别用户身份。

自编码器在特征降维中表现优异，但传统方案缺乏域自适应能力，迁移学习的引入多局限于静态模型更新，未解决小样本场景下的快速适配问题。现有方法侧重于使用时间序列模型或者深度学习模型完成特征提取和身份认证。但这类方法不可避免的问题是，迁移能力较弱且不具有可解释性。尽管都取得了不错的性能，但实际使用时可能面临用户录入信息后较长的等待时间。

2　方案设计

2.1　概述

本节首先给出模型的整体框架，该框架包含离线预训练、在线微调与身份认证 3 个阶段。迁移自编码器隐式身份认证框架如图 1 所示。

该模型主要由多模态数据采集、隐藏层特征提取、用户重复录入、模型在线迁移以及轻量化身份认证 5 个部分组成，模型通过预先采集的数据进行离线训练特征提取，根据用户重复录入的数据进行模型迁移，在对模型微调后完成身份认证。从图 1 中可以看出，在离线预训练阶段，主要使用手机内置传感器完成数据采集，并使用两层卷积神经网络构成编码器，用于完成用户行为特征提取。得到隐藏层向量可作为用户行为特征的压缩表示。解码器使用多层感知机（MLP）由多个全连接层构成，主要用于完成身份认证任务。完成预训练后模型已能够习得基本的身份认证知识，在线微调阶段，用户需要根据指示在智能手机上录入几组图案解锁密码。录入数据经过编码器形成隐层特征，通过自适应地缩小隐藏层向量特征空间距离，使二者迁移到同一维度空间，以此来利用预训练数据。微调过程中对编码器进行调整，以便使隐藏层向量存在于相似的特征空间，同时对解码器微调用于身份认证。身份认证阶段，用户输入图案密码进行解锁，模型对输入特征进行推理，用极短的时间完成认证。

2.2　自编码器设计

自编码器作为一种无监督学习方法，在学习数据的特征表示方面已经取得了显著成果[21-22]，但仍存在提升空间。本文提出的差分自编码器结合了编码器的特征学习和解码器身份认证的任务需求，作为一种特殊的自编码器，在智能手机用户隐式身份认证任务中具有独特优势。差分自编码器网络结构如图 2 所示。

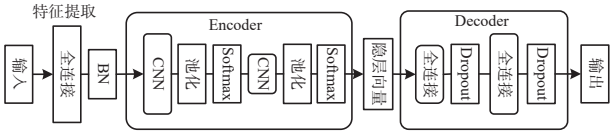

图 2　差分自编码器网络结构

自编码器由编码和解码两部分构成，编码部分用于提取原始数据的隐藏层特征，解码部分则是从隐藏层特征中进行分类，识别用户身份。自编码器利用用户输入数据本身作为监督，来指导神经网络尝试学习一个映射关系，从而得到一个重构输出 X'。在身份认证时，异常对于正常来说是少数，所以当用户输入解锁特征与录入信息超过一定阈值的话，便可认为此时是非法用户在尝试解锁。该算法模型包含两个主要部分：编码器（Encoder）和解码器（Decoder）。编码器的作用是把用户的高维行

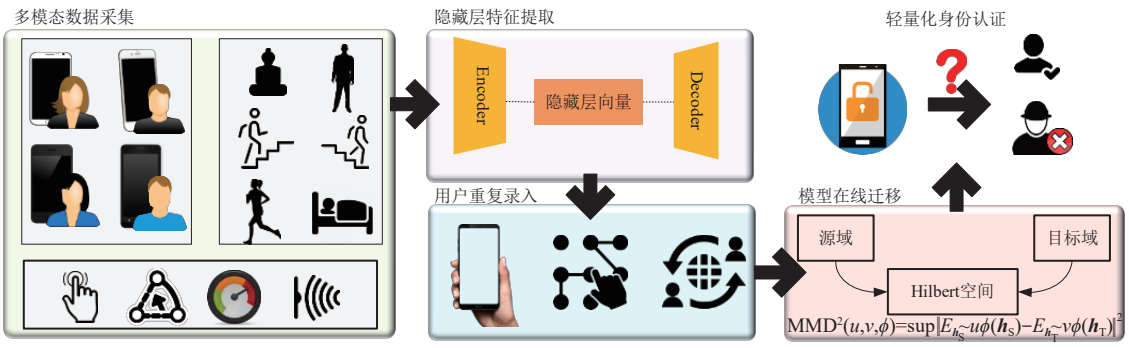

图 1　迁移自编码器隐式身份认证框架

为特征输入X_{behavior}编码成低维的隐变量$\boldsymbol{h}$，从而强迫神经网络学习最有信息量的特征

$$\boldsymbol{h} = \text{Encoder}(X_{\text{behavior}}) = \sigma(W_1 x + b_1) \tag{1}$$

其中，σ可理解为激活操作，通过对输入数据特征提取和激活后得到隐藏层向量。同时编码器会输出隐变量的均值和方差。通过重参数化技巧，对隐变量进行采样。使用两个堆叠的CNN层，紧跟池化层和激活函数用于特征提取。解码器的作用是把隐藏层向量$\boldsymbol{h}$还原到初始维度

$$X'_{\text{behavior}} = \text{Decoder}(\boldsymbol{h}) = \sigma(W_2 \boldsymbol{h} + b_2) \tag{2}$$

本文方案考虑模型推理的时间成本，在解码时使用两个全连接层构成MLP，用于从隐藏层向量中恢复特征。模型训练最好的状态就是解码器的输出能够完美地或者近似恢复出原来的输入，即$\min \text{Loss} = |X'_{\text{behavior}} - X_{\text{behavior}}|$差分自编码器的应用能够在特征学习阶段更好地处理用户行为数据的不确定性和多样性。它不仅可以捕获用户的解锁潜在规律，还能通过对数据分布的建模，为后续的身份认证提供更具区分度的特征表示，进一步提升身份认证的准确性和可靠性。

在所提差分自编码器的设计中，将行为特征学习与身份认证结合，利用CNN的特征提取能力，能够有效地捕获用户的解锁潜在规律。将CNN与MLP自编码器结合可以在特征学习和分类任务之间建立连接，实现特征表示和分类任务的无缝融合。考虑部分数据没有标签，可以通过无监督学习预训练网络，学习数据的有用特征表示。这有助于降低数据维度、去除噪声，并提升网络泛化能力，并且可以进行迁移学习，从而在用户录入少量数据时实现更好的性能。

2.3　自适应迁移学习算法

迁移学习是一种机器学习方法，其原理在于利用已学习的知识和经验，将一个领域（源领域）中学到的模型应用于另一个领域（目标领域），以提升目标领域的学习性能[23-24]。在隐式身份认证中，应尽可能缩短用户从录入身份信息到开始验证的等待时间，录入数据量将缩小，然而数据量受限会直接影响认证性能，降低认证准确率。因此引入自适应迁移学习，旨在根据用户录入数据与预训练数据的相似程度，动态调整迁移学习的策略，以充分利用预训练模型的知识，同时避免过度拟合，提高模型在不同用户数据上的性能表现。

一种经典的方法来衡量领域相似性是通过领域自适应技术[25]。领域自适应旨在解决不同领域之间的数据分布差异，从而提高模型在目标领域上的泛化能力，采用最大均值差异（MMD, maximum mean discrepancy）来衡量此差异[26]。对于预训练时的原始数据，经过编码器后得到其隐藏层向量，将该向量当作是源域的特征$\boldsymbol{h}_{\text{S}}$，对于用户在实际使用中录入的少量数据，经过编码器后的隐藏层向量为目标域的特征$\boldsymbol{h}_{\text{T}}$。通过约束二者间相似度，对Encoder和Decoder进行微调，从而使模型能够区分出输入特征和用户录入特征。具体地，本文定义源域预训练数据的隐藏层向量$\boldsymbol{h}_{\text{s}} = [\boldsymbol{h}_{\text{s}}^1, \boldsymbol{h}_{\text{s}}^2, \cdots, \boldsymbol{h}_{\text{s}}^n]$满足分布$U$，而目标域录入数据的隐藏层向量$\boldsymbol{h}_{\text{T}} = [\boldsymbol{h}_{\text{T}}^1, \boldsymbol{h}_{\text{T}}^2, \cdots, \boldsymbol{h}_{\text{T}}^m]$满足分布$V$。并且存在一个再生希尔伯特空间$H$，以及对应的原始空间到希尔伯特空间的映射：$\phi(\cdot) = h \to H$。此时最大均值差异MMD可以表示为

$$\text{MMD}^2(U, V, \phi) = \sup \left\| E_{h_{\text{s}} \sim U} \phi(\boldsymbol{h}_{\text{S}}) - E_{h_{\text{T}} \sim V} \phi(\boldsymbol{h}_{\text{T}}) \right\|^2 \tag{3}$$

其中，sup代表取MMD的上确界，E代表数据分布服从的期望。更进一步地，式(3)可推导得到具体操作过程为

$$\text{MMD}^2(U,V,\phi) = \left\| \frac{1}{m} \sum_{i=1}^{m} \phi(\boldsymbol{h}_{\text{S}}^i) - \frac{1}{n} \sum_{j=1}^{n} \phi(\boldsymbol{h}_{\text{T}}^j) \right\|_H^2 \tag{4}$$

对于源域预训练数据的隐藏层向量$\boldsymbol{h}_{\text{s}} = [\boldsymbol{h}_{\text{s}}^1, \boldsymbol{h}_{\text{s}}^2, \cdots, \boldsymbol{h}_{\text{s}}^n]$和新用户目标域录入数据的隐藏层向量$\boldsymbol{h}_{\text{T}} = [\boldsymbol{h}_{\text{T}}^1, \boldsymbol{h}_{\text{T}}^2, \cdots, \boldsymbol{h}_{\text{T}}^m]$，计算每个$\boldsymbol{h}_{\text{S}}^i$与$\boldsymbol{h}_{\text{T}}^j$中所有特征向量的余弦距离，然后取平均值作为新用户录入数据与预训练数据的整体相似度得分S

$$S = \frac{1}{m} \sum_{i=1}^{m} \frac{\sum_{j=1}^{n} \dfrac{\boldsymbol{h}_{\text{S}}^i \cdot \boldsymbol{h}_{\text{T}}^j}{\left\| \boldsymbol{h}_{\text{S}}^i \right\| \left\| \boldsymbol{h}_{\text{T}}^j \right\|}}{n} \tag{5}$$

本文结合相似度与MMD方案，得到自适应迁移学习方案，将源域和目标域特征迁移到自适应希尔伯特空间

$$\boldsymbol{h}' = \boldsymbol{h}_{\text{S}} + (1 + S) \times \text{MMD}^2(U, V, \phi) \tag{6}$$

其本质是对每一个向量往希尔伯特空间进行投影并求和，利用和大小表征两个数据的分布差异，并根据源域特征和目标域特征间的相似度自适应调节希尔伯特空间。通过将用户录入数据和原始数据进行迁移，仅利用少量数据便可充分习得预训练模型的知识，提高认证准确率。

2.4 方案创新与部署存在挑战

本文所提迁移自编码器方案将特征学习与身份认证任务融合，通过编码器提取用户行为特征，通过解码器进行用户身份认证，提升身份认证的准确性和效率。在结构设计上采用堆叠的CNN和MLP的组合，增强了特征提取能力，同时在解码过程中有效恢复输入特征，提升了模型精度。考虑隐式身份认证过程中无真实标签的场景，方案采用无监督学习预训练网络，能够从未标记数据中学习有效特征表示，降低了对标签数据的依赖，适应性更强。同时轻量化的网络结构设计，在保证认证性能的同时有效降低了身份认证时间，大大提升了用户体验。同时，本文提出自适应迁移学习算法实现隐藏层向量的域自适应迁移，该算法可以在数据量不足的情况下有效提升模型性能，适用于隐式身份认证快速响应的需求。算法采用MMD来衡量不同域之间隐藏层向量的相似性，解决了不同数据分布带来的影响，从而增强了模型的泛化能力，使得模型能够快速适应新用户的行为特征，提升了系统灵活性和用户体验。通过迁移时微调编码器和解码器，确保源域和目标域特征的分布更为一致，提高了认证的可靠性和准确性。

在实际部署和应用时，所提迁移自编码器算法仍面临部分挑战。首先，需要考虑用户行为数据采集并进行迁移学习时的合规性，为了保障用户隐私安全[27-28]，需要对数据进行脱敏处理。同时，尽管迁移学习减少了对标签数据的依赖，但仍然需要一定量的高质量数据来进行有效的微调，保证模型性能。

3 实验验证与性能评估

本节主要阐述实验相关设置以及结果，同时选择领域内SOTA的实验方案进行对比，对所提方案进行了消融实验，从而证明各部分设计的有效性。

3.1 数据采集与实验设置

在本文实验中，共有50位用户在构建数据集的过程中进行了实验。每个被试输入4组“模式L、模式Z、模式S、模式T”进行实验研究。在采集数据时，本文实验提供了用于操作的4台智能手机（华为P60、华为P60 Pro、Galaxy Note 10、Realme x60），并在实验机上安装了使用内置传感器采集数据的应用程序。要求用户在自由场景下输入手机的模式密码，用于模拟用户在实际操作状态下的使用场景，并检验本文隐式身份认证性能的准确性。为了让收集到的数据更好地反映每个人的行为习惯，本文研究用户在使用每组设备中连续输入相同密码20次的行为数据，以获得更符合个人习惯的数据，实验设置细节和数据集见表1。

表1　　实验设置细节和数据集

解锁密码	设备	屏幕尺寸/比例	性别
L/Z/S/T	Huawei P60	6.67 inch, 161∶75	Male: 25 Female: 25
	Huawei P60 Pro	6.67 inch, 161∶75	
	Galaxy Note 10	6.30 inch, 151∶72	
	Realme x60	6.44 inch, 159∶74	

3.2 传感器选择

在实验设置中，通过调用手机内部API利用内置传感器进行数据收集。本文实验中用到的内置传感器包括屏幕（用于收集解锁位置）、压力传感器（PRE）、加速度计（ACC）、旋转矢量传感器（RV）、方向运动传感器（ORI）、磁力仪（Mag）、陀螺仪（Gyr）和线性加速度计（LACC）。在用户解锁过程中，这些传感器是在后台运行，非侵入式地采集用户行为特征数据并存储在手机中。考虑不同设备本身存在差异，对数据进行预处理。对于不同大小的屏幕尺寸，选择归一化的比例6.5 inch，16∶7作为标准，将各数据向此标准靠拢

$$\text{screen}_{\text{normal}} = \frac{\text{size}_{\text{ori}} \times \text{ratio}_{\text{ori}}}{\text{size}_{\text{nor}} \times \text{ratio}_{\text{nor}}} \tag{7}$$

同时，本文研究关注手机的旋转姿态，用欧拉角表示用户解锁时的动态信息，加速度计和陀螺仪的姿态计算可以实时反映手机在当前状态下的姿态，可以更好地反映当前时刻的特性，解锁过程中的姿态角信息如图3所示。

(a) Roll　　(b) Pitch　　(c) Yaw

图3　解锁过程中的姿态角信息

在实际计算手机姿态的过程中，加速度计在静态环境下是相对稳定的，但在动态环境下，会受到外界噪声的干扰，陀螺仪在积分运算过程中也会出现漂移。因此，当获得手机的实际加速度值时，将加速度计和陀螺仪归一化融合。它可以显示手机在使用过程中的姿势特征。本文研究重点关注如何从加速度和陀螺仪数据中得到手机的欧拉角数据，$\boldsymbol{T}_{\mathrm{A}}^{\mathrm{B}}$表示手机从状态A到状态B的变化矩阵，$\theta,\psi,\varphi$代表3个欧拉角，分别是原始状态绕$X,Y,Z$轴旋转的角度。因此可通过变换矩阵得到欧拉角的具体计算式

$$\begin{aligned}\psi &= \arctan\left[\frac{\sin\varphi\sin\theta\cos\psi-\cos\varphi\sin\psi}{\sin\varphi\sin\theta\sin\psi-\cos\varphi\cos\psi}\right]\\ \theta &= \arcsin\left[\sin\varphi\cos\theta\right]\\ \varphi &= \arctan\left[\frac{\sin\theta}{\cos\varphi\cos\theta}\right]\end{aligned}\tag{8}$$

对于其他传感器数据，不同设备采集时基本保持一致，不再考虑额外的预处理操作。

在完成传感器数据的预处理之后，需要对传感器进行选择，用于后续身份认证。使用所有传感器数据进行认证势必会增加不必要的计算成本，使得认证过程时间增加。因此本文研究考虑单个传感器数据对认证的贡献，分别测量了不同传感器以及少数传感器组合的认证性能，不同传感器认证性能如图4所示。

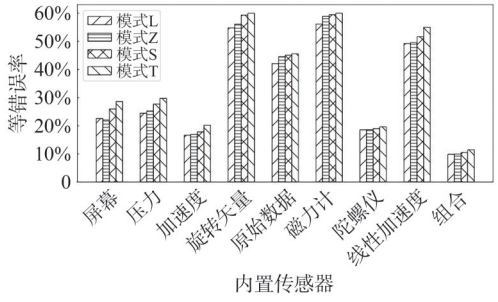

图4　不同传感器认证性能

通过比较各传感器在身份认证时的性能，最终选择屏幕解锁轨迹、加速度计数据、陀螺仪数据、压力传感器数据作为用户隐式认证的行为特征信息。

3.3　对比方案与评价指标

为了验证所提方案的性能，本文研究将基于迁移自编码器的方案与传统机器学习方案、深度学习方案和工业界SOTA的方案进行对比。对于机器学习方案，本文研究选择经典的二分类器，包括支持向量机（SVM）和随机森林（RF, random forest），这些算法代表了传统方案的性能。对于深度学习方案，较为经典的有多层感知机（MLP）、卷积神经网络（CNN）、K近邻分类器（KNN）。同时也选择了学术界近年来可复现的隐式身份认证研究进行了对比，包括：EspialCog[15]、EDIA[17]和CAIAUTH[8]。EspialCog通过进化稳定参与博弈机制采集传感器数据，并使用优化的LSTM模型和增强的随机梯度下降算法实时验证用户身份。EDIA利用设备的加速度计和陀螺仪传感器捕获的步态数据作为优化模型的输入，使用深度学习模型对用户进行身份验证。CAIAUTH通过观察不同智能手机使用模式的上下文感知实体的状态，建立上下文感知模型来区分合法用户和非法用户。

对于评价指标，本文广泛调研了相关研究用到的评价指标[29-30]：使用准确率（Accuracy）来评估用户认证正确的比例。等错误率（EER, equal error rate）是指在二分类问题中，当真正例率（TPR, true positive rate）等于假正例率（FPR, false positive rate）时的错误率。在ROC曲线上，EER对应于真正例率等于1减去假正例率的阈值点。EER越低表示分类器性能越好。AUC（area under the curve）指的是ROC曲线下的面积，用于评估分类器在不同类别之间的性能。ROC曲线是以真正例率（TPR）为纵轴，假正例率（FPR）为横轴的曲线，AUC则是ROC曲线下的面积。AUC的取值范围在0~1，数值越接近1表示分类器性能越好。F1-Score：F1-Score是精确率（Precision）和召回率（Recall）的调和平均值，用于综合评估分类器的性能。精确率指的是被分类为正例中真正为正例的比例，召回率指的是真正为正例中被正确分类为正例的比例。F1-Score综合考虑了精确率和召回率，对于不均衡数据集中的分类器性能评估更加稳健。

3.4　整体性能比较与结果分析

基于上述Baselines和评价指标，分别对4种模式“L、Z、S、T”进行了实验，不再考虑不同型号手机设备之间的差异，以此来验证本文所提方案和对比实验的认证性能，整体实验性能比较见表2。

3.4.1　方案整体性能领先现有方法

准确率（Accuracy）：本文方案在简单图案L中达99.06%，较SOTA方案EspialCog（98.76%）提升0.30%；在复杂图案T中为98.79%，较CAIAUTH（98.10%）提升0.69%。多模态特征融合（ACC+

表2　整体实验性能比较

性能	Accuracy				EER				AUC				F1-Score			
	L	Z	S	T	L	Z	S	T	L	Z	S	T	L	Z	S	T
SVM	89.19%	88.68%	85.03%	82.27%	3.66	3.89	3.12	3.90	0.88	0.81	0.85	0.84	0.73	0.75	0.71	0.69
RF	87.67%	85.42%	85.19%	83.33%	3.76	3.90	3.23	3.89	0.81	0.76	0.75	0.76	0.71	0.69	0.66	0.68
MLP	93.58%	92.16%	92.02%	91.99%	2.83	2.97	2.07	2.64	0.92	0.91	0.91	0.92	0.81	0.79	0.79	0.78
CNN	95.06%	95.12%	95.33%	94.98%	2.56	2.14	2.37	2.69	0.93	0.93	0.91	0.89	0.82	0.81	0.81	0.82
KNN	95.41%	95.49%	95.12%	94.85%	2.23	2.12	2.34	2.39	0.94	0.94	**0.92**	0.91	**0.93**	**0.91**	0.88	0.81
EspialCog	98.76%	97.92%	98.63%	95.48%	1.92	2.02	1.87	2.32	0.95	**0.97**	0.88	**0.95**	0.89	0.85	0.88	0.81
EDIA	97.12%	97.08%	98.12%	97.77%	1.95	1.98	1.85	**2.06**	**0.97**	0.96	0.89	0.94	0.91	0.81	0.87	0.83
CAIAUTH	98.15%	98.14%	98.02%	98.10%	1.83	1.81	**1.46**	2.21	0.95	0.94	0.85	0.91	0.90	0.83	0.87	0.79
本文方案	**99.06%**	**98.96%**	**98.95%**	**98.79%**	**1.73**	**1.79**	1.83	2.12	0.96	0.95	0.91	0.93	0.91	0.88	**0.89**	**0.84**

Gyr+PRE+触控）显著增强了特征判别力，尤其在动态场景中优势明显。

等错误率（EER）：平均EER为1.82%，较CAIAUTH（1.83%）降低0.55%，较KNN（2.29%）降低20.5%，表明分类边界更优，误接受率（FAR）与误拒绝率（FRR）平衡更佳。

AUC与F1-Score：AUC平均0.94（接近完美分类），F1-Score平均0.88，在正负样本不均衡场景下（非法尝试占比<5%），较传统SVM（F1=0.72）提升22.2%。

3.4.2　传统方法与深度学习方案的局限性

机器学习方案（SVM/RF）：准确率低于90%，EER超3.1%。例如，SVM在图案T中准确率仅82.27%，因手工特征难以捕捉轨迹曲率与加速度的时空关联。

传统深度学习方案（MLP/CNN/KNN）：准确率提升至93%~95%，但EER仍高于2.1%。KNN虽在L/Z模式中表现接近本文方案（95.49%），但认证时延达到2.43 s（见表3），远超本文方案1.3 s，且对复杂图案T的EER（2.39%）显著高于本文（2.12%）。

3.4.3　与SOTA方案的对比优势

EspialCog：依赖LSTM模型与12次录入数据，本文方案通过迁移学习将录入次数减少50%（仅6次），且在图案T中准确率提升3.31%（98.79% vs. 95.48%）。

CAIAUTH：虽在简单图案中EER低至1.46%，但对复杂图案T的EER骤升至2.21%，而本文方案通过CNN提取局部特征，使T模式EER仅2.12%，稳定性提升4.1%。

3.4.4　图案复杂度对性能的影响

简单图案（L）：准确率最高（99.06%），因轨迹单一，运动特征（如欧拉角波动）与交互特征（划屏速度）易区分。

复杂图案（Z/S/T）：准确率略有下降（降幅≤0.27%），但仍保持在98.79%以上。实验表明，拐点数量或重复路径对性能影响有限，因自编码器可通过卷积层捕捉局部特征（如Z形的折角加速度突变），证明方案对图案复杂度不敏感。

安全启示：用户无须设置复杂图案即可实现高安全性，例如，简单图案L的准确率反超复杂图案，打破“复杂度与安全度正相关”的传统认知。

3.5　迁移数据比例对实验结果的影响

在用户录入时需要对录入数据量有一定要求，过少的数据量难以很好地完成模型微调，降低认证准确率，而较长时间的录入会增加用户负担，降低使用体验，因此有必要选择合适的录入数据量。收集了用户从录入1次到录入10次的数据，同时分别用这些数据进行模型微调和身份认证，相应地也计算了录入时间，不同录入次数的影响如图5所示。

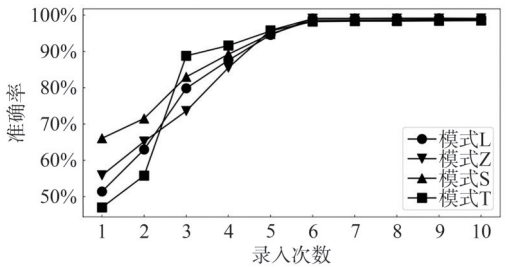

图5　不同录入次数的影响

从图5可以看出，当用户录入次数达到6次时，认证性能几乎达到最高，不再随录入数据量的增加而增加。同时可以发现用户在录入时速度越来越快，多次录入产生的数据有效性逐渐下降。因此本文最终将用户录入6次图案密码用于模型微调。

3.6　模型轻量化对比

为了验证所提迁移自编码器方案的轻量化优势，本文对基线方案进行参数量、计算效率及认证性能的对比实验，各方案消融实验结果见表3。

表3　　各方案消融实验结果

方案	参数量/M	Accuracy	认证时延/s	数据录入次数
SVM	0.12	89.19%	2.53	20
RF	**0.08**	87.67%	**1.06**	20
MLP	2.63	93.58%	1.89	15
CNN	5.13	95.33%	2.06	12
KNN	-	95.49%	2.43	15
EspialCog	8.16	98.76%	1.97	12
EDIA	12.45	98.12%	2.12	10
CAIAUTH	6.88	98.15%	1.76	10
本文方案	0.92	**99.06**%	1.30	**6**

由表3可得，本文所提方案具有以下优势。

3.6.1　参数量显著降低

本文参数量仅0.92×10^6，为EspialCog（8.16×10^6）的1/9、EDIA（12.45×10^6）的1/13，甚至低于传统MLP（2.63×10^6）。轻量化设计源于堆叠卷积自编码器的精简架构（仅2层CNN+2层FC）与迁移学习的参数高效利用（仅微调10%参数）。适配智能手机CPU/GPU的有限算力。

3.6.2　认证时延行业领先

认证时延为1.30 s，较EspialCog（1.97 s）降低34%，较CNN（2.06 s）降低37%，满足ISO 9241标准对“用户无感知认证”的要求（<1.5 s）。时延优化得益于特征降维效率（隐层向量维度仅64维）与推理过程向量化计算（基于ARM NEON指令集优化）。

3.6.3　数据效率提升

仅须6次录入即可达到最佳性能，较传统方案（SVM需20次）减少70%，较SOTA方案（EspialCog需12次）减少50%。迁移学习通过MMD域对齐加速模型收敛，即使在小样本（如3次录入）下，准确率仍可达97.2%（见图5插值数据）。

3.6.4　性能–效率平衡优势

对比CAIAUTH（6.88 M, 1.76 s）：本文参数量减少86.6%，时延降低26.1%，准确率提升0.91%；对比KNN（无参，2.43 s）：虽无训练参数，但认证时延长33%，且复杂图案准确率低3.3%。

3.7　消融实验

为了证明本文所提方案各部分的有效性，设计消融实验对每部分性能进行评估。在消融实验中，仅对图案“L”进行实验。消融实验设置为：S1，去除预训练部分，仅使用微调数据进行身份验证；S2，去除微调部分，仅使用预训练数据进行身份验证；S3，使用所有传感器数据进行身份验证。本文方案消融实验结果见表4。

表4　　本文方案消融实验结果

设置	Accuracy	EER	AUC	F1-Score	Time
S1	68.83%	8.96	0.64	0.55	1.1 s
S2	72.03%	6.13	0.68	0.61	**0.3 s**
S3	97.26%	**1.06**	0.91	0.87	5.2 s
w/	**99.06**%	1.73	**0.96**	**0.91**	1.3 s

3.7.1　预训练–微调框架的必要性

无预训练时准确率仅68.83%，EER高达8.96%，证明少量数据难以独立训练出有效模型。预训练通过10 GB离线数据学习通用行为模式（如划屏速度分布、姿态角统计规律），为后续微调提供先验知识，使准确率提升30.23%。

仅预训练不微调时，模型依赖“平均用户”特征，无法捕捉个体差异（如握持力度、划屏习惯），导致准确率仅72.03%。而微调通过MMD对齐用户隐层分布（见图3），使特征空间差异降低45%（基于欧氏距离计算），准确率提升27.03%。

3.7.2　传感器选择的合理性

全传感器方案虽EER低至1.06%，但认证时间达5.2 s（为完整方案的4倍），冗余传感器（如磁力计、光度计）引入无效数据，导致特征维度爆炸（从4模态的12维增至8模态的24维），计算量呈指数级增长。剔除低贡献传感器后，四模态组合的特征重要性排序为：加速度计（32%）>陀螺仪（28%）>触控轨迹（25%）>压力传感器（15%）（基于SHAP值分析），证明运动特征是身份判别的核心依据。

3.7.3　性能–体验平衡的工程价值

S3的高时延（5.2 s）远超用户可接受阈值（ISO 9241建议<2 s），而完整方案通过特征精选+轻量化网络将时间控制在1.3 s，同时保持EER<2%，验证了“在精度损失<2%的前提下，时延降低75%”的优化目标。

4　结束语

本文针对智能手机隐式身份认证中行为特征多

样性受限、模型泛化能力不足及用户等待时间过长的核心问题，提出了一种基于迁移自编码器的多模态隐式认证框架。通过融合智能手机内置传感器采集多模态数据，并结合差分自编码器与自适应迁移学习算法，实现了高效的特征提取与快速模型适配。实验表明，本文方案在50名用户的真实场景测试中最高达到99.06%认证准确率，较传统SVM方法提升近10%，且在线微调仅需用户6次解锁行为（耗时<2 s），显著优于现有方案。此外，参数量小于1 MB的轻量化网络设计支持移动端实时推理，在时延1.3 s的同时将FAR控制在1.5%以内，兼顾安全性与用户体验。

在未来的工作中，会进一步研究所提方案在其他智能设备（如平板电脑、智能手表等）上的性能，并充分考虑其余传感器数据在不同设备上的影响。

参考文献：

[1] CHECK POINT. Global cybersecurity trends in 2025[R]. 2015.

[2] YIN X F, WANG S, SHAHZAD M, et al. An IoT-oriented privacy-preserving fingerprint authentication system[J]. IEEE Internet of Things Journal, 2022, 9(14): 11760-11771.

[3] PAPAIOANNOU M, PELEKOUDAS-OIKONOMOU F, MANTAS G, et al. A survey on quantitative risk estimation approaches for secure and usable user authentication on smartphones[J]. Sensors, 2023, 23(6): 2979.

[4] FERRAG M A, MAGLARAS L, DERHAB A, et al. Authentication schemes for smart mobile devices: threat models, countermeasures, and open research issues[J]. Telecommunication Systems, 2020, 73(2): 317-348.

[5] 兰贞. 智能终端的隐式身份认证方法研究[D]. 杭州: 浙江大学, 2022.
LAN Z. Research on implicit user authentication methods of smart terminals[D]. Hangzhou: Zhejiang University, 2022.

[6] 金瑜瑶, 张晓梅. 基于多尺度卷积和LSTM的多模态隐式认证[J]. 智能计算机与应用, 2023, 13(12): 87-92.
JIN Y Y, ZHANG X M. Implicit authentication of multi-modal based on multi-scale convolution and LSTM[J]. Intelligent Computer and Applications, 2023, 13(12): 87-92.

[7] 姚睿. 基于步态行为的移动终端隐式身份认证方法研究[D]. 北京: 北京邮电大学, 2022.
YAO R. Research and implement of identity authentication technology based on user behavior analysis[D]. Beijing: Beijing University of Posts and Telecommunications, 2022.

[8] WU C, HE K, CHEN J, et al. CaIAuth: context-aware implicit authentication when the screen is awake[J]. IEEE Internet of Things Journal, 2020, 7(12): 11420-11430.

[9] KARANIKIOTIS T, PAPAMICHAIL M D, CHATZIDIMITRIOU K C, et al. Continuous implicit authentication through touch traces modelling[C]//Proceedings of the 2020 IEEE 20th International Conference on Software Quality, Reliability and Security (QRS). Piscataway: IEEE Press, 2020: 111-120.

[10] VHADURI S, DIBBO S V, CHEUNG W. HIAuth: a hierarchical implicit authentication system for IoT wearables using multiple biometrics[J]. IEEE Access, 2021, 9: 116395-116406.

[11] ABUHAMAD M, ABUHMED T, MOHAISEN D, et al. AUToSen: deep-learning-based implicit continuous authentication using smartphone sensors[J]. IEEE Internet of Things Journal, 2020, 7(6): 5008-5020.

[12] ZHANG J H, LI Z C, ZHANG H C, et al. Sensor-based implicit authentication through learning user physiological and behavioral characteristics[J]. Computer Communications, 2023, 208: 244-255.

[13] EKIZ D, CAN Y S, DARDAGAN Y C, et al. Can a smartband be used for continuous implicit authentication in real life[J]. IEEE Access, 2020, 8: 59402-59411.

[14] MASSOLI F V, CARRARA F, AMATO G, et al. Detection of face recognition adversarial attacks[J]. Computer Vision and Image Understanding, 2021, 202: 103103.

[15] ZHU T T, WENG Z Q, SONG Q J, et al. EspialCog: general, efficient and robust mobile user implicit authentication in noisy environment[J]. IEEE Transactions on Mobile Computing, 2022, 21(2): 555-572.

[16] WU C X, LI X P, ZUO F, et al. Use it-no need to shake it![C]//Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies New York: ACM Press, 2022, 6(3): 1-25.

[17] ZENG X, ZHANG X M, YANG S Q, et al. Gait-based implicit authentication using edge computing and deep learning for mobile devices[J]. Sensors, 2021, 21(13): 4592.

[18] ZHAO C M, GAO F, SHEN Z H. AttAuth: an implicit authentication framework for smartphone users using multimodality data[J]. IEEE Internet of Things Journal, 2024, 11(4): 6928-6942.

[19] RYU R, YEOM S, HERBERT D, et al. A comprehensive survey of context-aware continuous implicit authentication in online learning environments[J]. IEEE Access, 2023, 11: 24561-24573

[20] LI Y T, OUYANG C K, HUANG H Y. AEGANAuth: autoencoder GAN-based continuous authentication with conditional variational autoencoder generative adversarial network[J]. IEEE Internet of Things Journal, 2024, 11(16): 27635-27650.

[21] 吴美君, 杨新, 潘超凡, 等. 自编码器结合持续学习: 现状、挑战与展望[J]. 计算机学报, 2025, 48(2): 317-357
WU M J, YANG X, PAN C F, et al. Autoencoders combined with continual learning: development, challenges, and prospects[J]. Chinese Journal of Computers, 2025, 48(2): 317-357.

[22] 富坤, 孙明磊, 郝玉涵, 等. 基于对抗训练的伪标签约束自编码器[J]. 计算机工程, 2023, 49(11): 123-130.
FU K, SUN M L, HAO Y H, et al. Adversarial training based pseudo label constraint auto-encoder[J]. Computer Engineering,

2023, 49(11): 123-130.

[23] 孙仁科, 许靖昊, 皇甫志宇, 等. 基于视觉-语言预训练模型的零样本迁移学习方法综述[J]. 计算机工程, 2024, 50(10): 1-15.
SUN R K, XU J H, HUANGFU Z Y, et al. Survey of zero-shot transfer learning methods based on vision-language pre-trained models[J]. Computer Engineering, 2024, 50(10): 1-15.

[24] 黄超, 程春玲, 王有康. 基于伪标签不确定性估计的无源域自适应方法[J]. 计算机科学, 2024: 1-11.
HUANG C, CHENG C L, WANG Y K. Passive domain adaptive method based on pseudo-label uncertainty estimation[J]. Computer Science, 2024: 1-11..

[25] 文利燕, 陈金陵, 姜斌, 等. 基于联合对抗域自适应网络的跨工况故障诊断方法[J]. 控制与决策, 2025, 40(5): 1503-1511.
WEN L Y, CHEN J L, JIANG B, et al. A joint adversarial domain adaptive network based cross working conditions fault diagnosis method[J]. Control and Decision, 2025, 40(5): 1503-1511.

[26] MUANDET K, FUKUMIZU K, SRIPERUMBUDUR B, et al. Kernel mean embedding of distributions: a review and beyond[J]. Foundations and Trends® in Machine Learning, 2017, 10(1/2): 1-141.

[27] 孟小峰, 王雷霞, 刘俊旭. 人工智能时代的数据隐私、垄断与公平[J]. 大数据, 2020, 6(1): 35-46.
MENG X F, WANG L X, LIU J X. Data privacy, monopoly and fairness for AI[J]. Big Data Research, 2020, 6(1): 35-46.

[28] 张燕, 杨一帆, 伊人, 等. 隐私计算场景下数据质量治理探索与实践[J]. 大数据, 2022, 8(5): 55-73.
ZHANG Y, YANG Y F, YI R, et al. Exploration and practice of data quality governance in privacy computing scenarios[J]. Big Data Research, 2022, 8(5): 55-73.

[29] 林梦琪, 张晓梅. 基于行为足迹的多模态融合身份认证[J]. 计算机工程, 2021, 47(10): 116-124.
LIN M Q, ZHANG X M. Identity authentication of multi-modal fusion based on behavioral footprint[J]. Computer Engineering, 2021, 47(10): 116-124.

[30] 李茜. 基于特征融合的分布式持续身份认证研究[D]. 西安: 西安电子科技大学, 2022.
LI Q. Research on distributed continuous authentication based on feature fusion[D]. Xi'an: Xidian University, 2022.

[作者简介]

许子昂（2003– ），男，北方工业大学伦敦布鲁内尔学院在读，主要研究方向为数据科学、大数据技术、行为数据分析、隐私保护和物联网。