智能制造环境下的多因子动态认证框架

陈羽 *，赵国柱，赵欢欢
滁州学院 计算机与信息工程学院，安徽 滁州 239000

摘　　要： 智能制造环境中的用户认证对环境变化高度敏感，传统的认证方式通常依赖于单次认证结果，未能考虑认证过程中对特定环境的觉察，难以实现持续的上下文感知。针对上述问题，本文提出了一种面向智能制造场景的多因子认证方案，该方案能够根据实际需求灵活组合多种动态认证因子，并结合上下文感知机制增强认证过程，从而提高认证的安全性。这一方案解决了传统认证方法忽略的环境特征的不可伪造性、认证过程的持续性以及身份认证的抗攻击性等关键问题。

关 键 词： 智能制造；用户认证；信息安全

A Multi-Modal Dynamic User Authentication Scheme for Smart Manufacturing Environments

Chen Yu*, Zhao Guozhu, Zhao Huanhuan
School of Computer and Information Engineering, Chuzhou University, Chuzhou, Anhui 239000

Abstract: User authentication in intelligent manufacturing environments is highly sensitive to environmental changes. Traditional authentication methods typically rely on a single authentication result, lacking continuous contextual awareness throughout the authentication process. To address this issue, this paper proposes a multi-factor authentication framework for intelligent manufacturing. The framework flexibly integrates multiple authentication factors according to operational requirements and incorporates a real-time sensing mechanism to enhance authentication security, thereby improving authentication security. It effectively addresses key limitations of traditional authentication methods, including the lack of non-replicability in environmental characteristics, the discontinuity of the authentication process, and the robustness of identity authentication against adversarial threats.

Keywords: smart manufacturing; user authentication; information security

引言

随着智能制造的不断发展和普及，制造业正在逐步实现数字化、网络化和智能化转型。这一转型不仅提升了生产效率和产品质量，还促进了产业链的数字化协同，增强了上下游企业的互动与资源共享[7]。然而，随着这种转型的深入，智能制造系统面临日益严峻的安全挑战，尤其是在设备认证方面，其脆弱性愈发凸显。当下的智能制造系统通常由大量互联的设备和智能终端构成，这些设备承担着数据采集、指令执行和远程协作等关键功能，是生产过程中的核心组成部分[5]。由于远程可控和高度互联的特性，关键设备极易成为黑客攻击的目标。一旦被攻击或篡改，可能导致生产中断、设备损坏，甚至造成重大经济损失和安全隐患。

因此，身份认证成为保障智能制造系统安全的核心环节，需要同时验证操作人员的身份及其所处环境的安全性。然而，传统的多因子认证机制通常依赖固定的身份凭据，难以适应动态环境，且在面对攻击者伪造身份信息、利用系统漏洞绕过认证等威胁时，缺乏足够的抗攻击能力[8]。此外，这类方法往往忽略环境特征的不可伪造性，使得认证过程无法持续感知特定环境中的行为模式。

为此，本文针对智能制造场景的认证需求，提出了一种多因子动态认证框架。该框架融合生物特征、环境特征与行为特征的动态信息，构建个性化的安全认证特征空间，实现对操作人员及环境的持续验证。同时，在认证过程中持续检测环境的安全性，提高认证过程的适应性和抗攻击能力。这一方法对确保生产环境的安全稳定有重要的实际意义和参考价值。

一、智能制造情景下的认证技术概述

在智能制造环境中，身份认证是防止未经授权访问设备及敏感应用的关键安全机制，用于验证用户合法性并控制其对特定设备、资源或操作的访问权限。根据认证因子数量的不同，身份认证形式可分为单因子认证（Single-Factor Authentication, SFA）和多因子认证（Multi-Factor Authentication, MFA）[9]。

（一）单因子认证

单因子认证是一种通过单一身份认证因子来验证用户合法性的认证机制，以操作简便为主要优点，广泛应用于各类信息系统

通讯作者：陈羽

及物理访问控制场景。常见的单因子认证方式包括用户名密码认证、单次生物特征认证和单次定位认证。

用户名密码认证是最早且最常用的单因子认证方式，用户通过输入预先设定的用户名和密码来证明其身份。尽管这种方式具有较低的部署成本和较高的用户普适性，但其安全性存在缺陷，包括易受暴力破解、字典攻击，易遗忘和泄露，难以抵御身份冒用的风险等。

基于单次生物特征的认证方式利用人体固有的生理特征，如指纹、人脸、虹膜，来进行身份验证，在一定程度上提升了认证的安全性[1]。然而，该方法无法确保操作人员是否身处受控场所，难以在特定环境之外有效验证其身份，并且易受到如照片、视频或3D面具伪造等攻击方式的威胁。

单次定位认证利用用户或设备的空间位置信息，通过单次环境或位置特征进行身份验证，例如GPS定位、Wi-Fi接入点（APs）信号强度分析[3]或超声波传感检测等。简单的GPS定位软件易受欺骗性攻击或信道干扰，而更为复杂的方法，如基于信标帧特征、RSSI值或超声波检测[4]，虽然能够提升定位精度，但在智能制造环境下往往面临较高的硬件部署成本，并对如信号遮挡、设备移动等环境变化较为敏感。

单因子认证在智能制造环境下难以有效抵御环境伪造、保障认证持续性及提高抗攻击能力，存在认证安全隐患。因此，多因子认证成为提升系统安全性与鲁棒性的关键策略。

（二）多因子认证

多因子认证是一种结合多个身份认证因子进行用户合法性验证的机制，要求用户在获得授权访问前提供至少两种不同类型的验证，通过不同认证方式的综合判断提高系统的抗攻击能力和安全防护水平。这种方法比传统的单因子认证更为安全，因为即便其中一个认证因子被破解，攻击者仍然无法绕过认证流程[2]。

常见的多因子认证有四类，其特征和优缺点如表1所示。认知因子依赖于用户记忆的信息，如密码、PIN 码和安全问题等；生物因子利用用户固有的生理或行为特征，如指纹、虹膜、面部识别和声纹等；行为因子基于用户的操作模式，包括击键节奏、鼠标移动轨迹和典型登录时间等；环境因子通过用户所处环境特征进行身份验证，如设备指纹、网络位置、Wi-Fi 信号和地理位置信息等。

表1 常见认证因子的分类

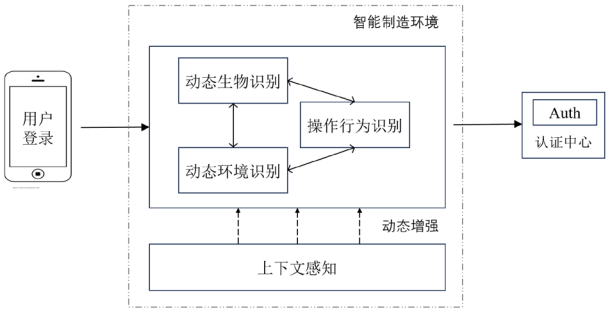
认证因子	特点	优点	缺点
认知因子	基于用户记忆的信息	易于实现，用户熟悉，部署成本低	易遗忘，易受社会工程攻击、暴力破解和泄露风险
生物因子	基于用户的生理特征	唯一性强，难以伪造，适用于无接触式认证	设备成本较高，可能受环境因素影响，存在隐私泄露风险
行为因子	基于用户的操作模式	用户无感知，难以复制，可用于持续身份验证	需要持续监测，误判率可能较高，受用户状态变化影响
环境因子	基于用户的环境特征	适用于动态认证，提高安全性，用户无感知	依赖外部环境，可能存在误判，易受环境变化影响

不同认证因子各具优缺点，相互结合可提升整体安全性。值得注意的是，生物因子、行为因子和环境因子具备持续动态认证的能力，可在感知环境上下文的基础上，对操作的安全性进行实时评估，从而降低被攻击的风险。此外，多因子认证方案可根据不同智能制造工厂的具体需求进行灵活配置，以适应复杂多变的工业环境。

二、基于上下文感知的多因子动态认证框架

智能制造环境下的安全认证需要具备对环境的动态感知能力，以捕获来自多源异构的上下文数据。由于不同智能制造工厂对认证强度的要求存在差异，认证方案应具备适应性和可扩展性。本节提出一种融合多种动态特征的多因子认证框架，能够根据具体环境需求灵活调整认证策略，以实现针对性安全保障，如图1所示。

在操作人员完成基于认知因子的初始登录后，系统结合生物识别、行为识别和环境识别三类动态因子进行认证。这些认证因子相互关联，并依托上下文感知技术获取更加全面的环境信息，从而实现风险环境下认证策略的动态增强。最终，综合认证结果被传输至认证中心实现安全性判断和认证过程的数据记录。该框架具备自适应性，可根据智能制造工厂的安全需求动态调整认证策略，并灵活增减认证因子，以下具体介绍核心认证模块的细节。



> 图1 智能制造环境下的多因子认证框架

（一）动态生物识别

动态生物识别技术利用个体的生理特征进行身份验证，能够根据不同的生物信息对用户进行动态身份确认，本框架采用动态面部特征和动态语音特征两种生物因子。其中，动态面部特征识别通过捕捉用户面部在动态环境中的变化，包括眨眼、摇头等动作，抵御照片或视频伪造攻击。而动态语音特征识别通过分析用户语音的动态变化，包括语调、语速、呼吸等特点，防止录音重放攻击。

（二）操作行为识别

操作行为识别基于用户与设备交互时的个体化操作特征进行身份验证，这些行为特征具有较高的稳定性且难以伪造。本框架采用打字节奏特征和操作流程习惯作为行为因子，实现动态行为认证。其中，打字节奏特征通过分析用户在输入密码时的打字速度、按键间隔等参数，识别异常输入模式，以防范自动化攻击或

凭证泄露。而操作流程习惯则基于用户在登录过程中的常规操作顺序，检测异常行为，如选项点击顺序的变化或异常停顿时间，以提高伪冒攻击的识别能力[4]。

（三）动态环境识别

在智能制造工厂中，动态环境特征能够反映设备所处场景的独特性，为身份认证提供额外支撑。本框架采用环境噪声和地面纹理作为环境因子，实现动态环境认证。其中，环境噪声特征通过分析操作场景的背景噪声模式，包括设备运行声、空间回声等因素，判断用户是否处于预期环境，防范音频伪造或远程操控攻击。而地面纹理特征通过监测地面光照和表面纹理的变化，检测用户所处的物理位置，避免环境伪造。相比静态定位，动态环境识别能够提供持续的场景感知能力，在身份认证过程中实时校验用户的操作环境[6]。

（四）上下文感知的认证增强

在动态认证过程中，认证框架对认证因子的变化趋势进行持续监测与综合评估，并将评估结果划分为三类：认证通过、认证失败及潜在风险。对于认证通过和认证失败的情况，认证系统可迅速终止认证流程；而当检测到潜在风险时，认证框架将触发认证增强机制，引导系统进一步提取更精细的动态特征。该认证框架依托于持久的环境感知能力，持续监测操作人员的生理特征、环境噪声及操作行为的变化，并据此动态调整认证策略。作为具体执行单元，认证系统在框架的指导下，实时感知并分析认证数据，识别异常行为，并主动响应潜在安全威胁，从而确保认证过程的自适应性与安全性[9]。

在智能制造工厂中应用该框架时，需要经历环境考察、系统部署和效果评估三个阶段。初始阶段，需深入分析工厂的生产环境、设备布局及身份认证流程，识别认证环节中的潜在安全风险与优化需求，并收集相关数据以支撑认证因子的合理配置。部署完成后，经过一段时间的运行，需基于实际应用数据对不同认证因子的有效性进行量化评估，并持续优化认证流程。

三、总结

本研究针对智能制造环境中的身份认证问题，提出了一种基于上下文感知的多因子动态认证框架。该框架融合生物识别、操作行为识别和环境识别等多种动态认证因子，并结合上下文感知技术，实现对操作人员身份及其操作环境的持续验证。相比传统的认证方式，本框架能够有效应对智能制造环境中的动态安全威胁，提高身份认证的抗攻击能力及环境适应性。

参考文献

[1]Zulfiqar M, Syed F, Khan M J, et al. Deep face recognition for biometric authentication[C]//2019 international conference on electrical, communication, and computer engineering (ICECCE). IEEE, 2019: 1-6.

[2]许丹丹，李沛谕，张世倩，等.统一身份认证系统中的多因子身份认证方法[J].福州大学学报(自然科学版)，2023，51(05)：616-620.

[3]AlQahtani, Ali Abdullah S., et al. "Leveraging Machine Learning for Wi-Fi-based Environmental Continuous Two-Factor Authentication." IEEE Access (2024).

[4]Zhao G, Zhang P, Shen Y, et al. Passive user authentication utilizing behavioral biometrics for IIoT systems[J]. IEEE Internet of Things Journal, 2021, 9(14): 12783-12798.

[5]永立，贾娟，吴习沫，等.基于密码技术的智能制造网络安全保障体系研究[J].电脑知识与术，2024，20(24)：10-13.DOI：10.14004/j.cnki.ckt.2024.1230.

[6]胡文俊.网络安全视域下的身份认证技术研究[J].科技创新与应用.2022，12(7).

[7]王立岩.高质量发展下智能制造的变革驱动与天津实践[J].城市，2019，(08)：3-11.

[8]曾维恺.面向多因子身份认证协议的形式化验证工具设计与实现[D].北京邮电大学，2024.DOI：10.26969/d.cnki.gbydu.2024.001729.

[9]Ometov A, Bezzateev S, Mäkitalo N, et al. Multi-factor authentication: A survey[J]. Cryptography, 2018, 2(1): 1.