基于用户信任评估和属性的零信任物联网访问控制研究

邵全义

摘要：随着物联网的应用范围持续扩大，传统的安全防护体系已无法有效应对不断变化的安全挑战。零信任架构为模糊边界的物联网环境和访问权限管理问题提供了全新的视角，基于该技术的安全体系结构通过实施严格的权限审核和持续的信任评估，为物联网设备创造一个更加安全的操作环境。文章提出了一种基于用户的信任评估和属性的零信任访问控制策略，旨在应对物联网面临的多样化安全挑战。理论分析和研究表明，该访问控制模型不仅增强了安全性，还实现了精细化的动态访问管理，这与现有研究成果形成了有效的对比。

随着物联网技术的迅猛进步，它正在逐步融入人们的日常生活，广泛应用于工业、医疗、城市管理、智能家居等多个领域。在物联网的深入应用过程中，该技术的跨行业融合与协作不仅带来了新的机遇，同时也产生了一系列的挑战。当前迫切需要一种创新的安全模型来有效应对物联网面临的安全威胁。本文旨在探讨通过用户信任评估与属性管理实现的零信任访问控制技术，在物联网实施中的显著优势。

一、架构模型介绍

（一）零信任架构

在物联网环境下，网络系统的规模不断扩大，结构日益复杂。传统的基于边界的网络安全框架已无法满足网络系统快速发展的安全要求。零信任架构的创新之处在于放弃传统的边界安全模型，所有应用皆部署于公共网络，不再区分内外网络。该架构认为网络中潜在的安全威胁是普遍存在的，因此假设网络环境始终处于不安全状态。即使在网络内部，也必须持续进行身份验证，以便授予权限。这种模式允许用户以安全的方式，在任何场所和任意设备上访问系统，从而满足现代远程工作的需求。零信任架构的核心理念是围绕身份展开的动态访问管理[1]，强调对内外部的设备、用户以及网络活动均持不信任态度。

（二）基于属性的访问控制模型

作为保护数据资源的一个重要手段，访问控制在信息安全领域被广泛采用[2]。基于属性的访问控制（ABAC）能够通过将属性引入用户与权限之间作为决策依据，更有效地解决角色基础控制（RBAC）模型中角色数量繁多的问题。ABAC模型通过分析用户的特定属性来分配权限，从而提供了更为细致的权限配置，更加符合大规模复杂系统的要求。这种方法增强了访问控制的灵活性和适应能力，进一步提升了系统的安全性与管理效率。基于属性的访问控制是一种逻辑上的访问管理方法[3]，ABAC的权限授予机制并不单纯依赖于用户的身份，而是通过实体的属性来进行决策，引入了属性作为用户与权限之间判断的依据。ABAC被认为是一个极具适应性的访问控制框架，能够实现细致化与动态的访问控制，因此本研究选择采用ABAC模式以实现零信任环境下的精细化访问管理。

二、基于用户信任评估和属性的零信任物联网访问控制

随着物联网的持续演进，当前的安全防护需求使得传统的边界防护网络架构面临诸多挑战，显得力不从心。一旦入侵者成功突破防线，组织便在假设内部环境完全安全的情况下，遭遇可能极其严重的内部威胁[4]。为了解决这一问题，本文提出了一种结合用户信任评估与属性的零信任访问控制模型。这一模型将零信任架构与基于属性的访问控制相结合，同时引入用户行为和意图的信任评估，以更加全面地反映用户的实际情况。

（一）总体架构

图1展示了基于用户信任评估和属性的零信任物联网访问控制的整体框架，该框架主要通过两个步骤来实现：第一，结合属性基的访问控制在零信任架构的基础上，以达到动态且细致的访问权限管理。第二，在实施访问控制时，增加信任评估机制，以便更准确地反映用户的真实行为和意图。

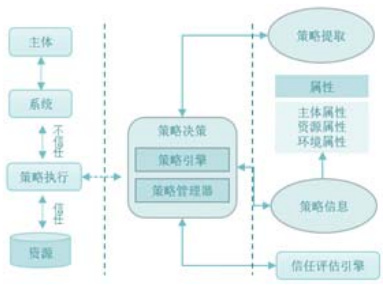

图1基于用户信任评估和属性的零信任物联网访问控制架构

在零信任的架构中，控制层与数据层执行各自不同的功能。控制层作为系统的基础，负责各逻辑组件之间的交流，并指导数据层的设置，以确保所有对受保护资源的访问请求在经过严格的身份验证、授权和细致的访问控制策略处理后才能被执行。应用程序的数据传输由数据平面负责。通过在实现访问控制时引入对信任的评估，该系统能够更准确地捕捉到用户的真实意图。信任评估的结果是利用模糊层次分析法进行计算的，只有当用户的相关特征与访问控制规则匹配，并且信任评估结果超过设定阈值时，用户才被授权访问资源。

（二）用户信任评估方法

对用户的信任进行评估是一个至关重要的过程，该过程采用模糊层次分析法来计算用户的信任评分，通过这种机制，原本模糊且不易确定的用户行为信用评估问题，得以转化为加权求和的形式，从而使得信用证据的分析更加简洁明了。初始用户行为证据可以依靠网络流量监测工具、专门的或根据需求开发的数据采集工具等获得，这些信任证据表示为BE=(aij)nm，m为信任证据的最大项数，当某个证据的项数不够时需要用0补齐，n是将用户行为信任划分的特性个数。获取用户行为证据后还需要将证据进行规范化处理为在区间[0，1]递增的无量纲值，这样可以方便信任评估的计算，经过规范化处理后的信任证据表示为E=(eij)nm。

在访问系统的过程中，通过流量监控程序获取的用户信任数据，其表现形式可以是百分比或具体数值等多样化的形式。为了方便计算信任评分，便需要将信任数据标准化为在区间[0，1]范围内的无量纲值，标准化评估方法如下：1.性能特性中包含平均用户CPU使用率、平均IP包网络带宽占用率；可靠特性中平均用户重传率、平均用户IP丢包率、平均连接建立成功率是百分比表现形式，已经在区间[0，1]内，规范化方法为：eij=aij，其中初始信任证据表示为BE=(aij)nm，经过规范化处理后的信任证据表示为E=(eij)nm。2.对于其他具体数值形式的信任证据，其规范化至[0，1]区间的方法如下：

$$e_{ij}=\frac{a_{ij}-(a_{ij})\min}{(a_{ij})\max-(a_{ij})\min}$$

在此，(aij)max表示可获得的信任证据的最高值，而(aij)min则指信任证据的最低值。

三、研究结果

本节探讨了用户当前的信任评估，并指明了安全特性变更对这一评估的影响。此外，通过研究用户信任指数的时间演变，进一步证明了信任评估的可靠性和有效性。为实现更为细致的访问管理，本文提出了一种新的控制模型，该模型通过结合基于属性的权限管理和信任评价机制，使得权限控制变得更加灵活且准确，从而降低了不必要的权限过度授予的风险。与传统的基于角色的访问控制方法相比[5]，该模型在权限的管理上实现了更细致和灵活的配备，通过零信任框架，在访问控制的过程中采用单独的控制平面进行信息交换，并且无论网络位置如何，都需要进行持续的身份验证与授权，从而显著提升了安全性和可靠性。

四、总结

随着物联网设备的迅猛发展与广泛应用，以及它们之间的紧密互联，网络的边界逐渐模糊，这给访问管理系统带来了巨大的挑战。当前传统的边界导向网络结构已无法满足日益复杂的物联网需求。本文提出的新的访问控制框架和持久性认证方案，建立在零信任的原则之上，具体为用户可信度评估及相关属性的零信任访问控制模型。该系统的架构在零信任模型的基础上，融入了基于特征的访问控制以及信任评估机制。该模型融入了零信任安全理念中的“动态验证、永不信任”这一核心思想，摒弃了传统依赖网络边界区分内部与外部的方式。系统通过对每一次访问请求进行不断的验证和即时的权限授予，确保了其安全性。

参考文献：

[1]Azad A M, Abdullah S , Arshad J, et al.Verify and trust: A multidimensional survey of zero-trust security in the age of IoT[J].Internet of Things, 2024, 27101227-101227.

[2]Zanasi C, Russo S, Colajanni M .Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures [J].Ad Hoc Networks, 2024, 156103414-.

[3]Yang C, Raj S P, Ye Z, et al.Automation and Orchestration of Zero Trust Architecture: Potential Solutions and Challenges[J].Machine Intelligence Research, 2024, 21(2): 294-317.

[4]Hamed A , Ross H , Christian J, et al.XACML2mCRL2: Automatic transformation of XACML policies into mCRL2 specifications[J].Science of Computer Programming, 2024, 232

[5]余波，台宪青，马治杰.云计算环境下基于属性和信任的RBAC模型研究[J].计算机工程与应用，2020，56(9)：9.

【作者系郑州财经学院副教授。本文系2025年河南省重点研发与推广专项（科技攻关）“零信任赋能工业物联网访问控制关键技术研究”（编号：252102210186）】

人工智能在远程银行营销中的创新应用

杭州银行股份有限公司 吕盛蕾

近年来，互联网技术和移动通信的快速发展深刻改变了人们的生活方式和消费习惯，也为银行业务的开展带来新的机遇。传统的线下网点服务模式已无法完全满足客户多元化、个性化的金融需求，越来越多的银行开始重视线上渠道和远程服务。远程银行营销面临着新的挑战，亟须引入先进的技术手段，提高响应速度和服务质量，建立与客户的紧密联系。人工智能作为新一轮科技革命的核心驱动力，在众多领域得到广泛应用，展现出巨大的发展潜力。将人工智能技术与远程银行营销相结合，有望突破传统营销模式的局限，打造智能化、数字化的营销服务体系，实现差异化的竞争优势。

一、人工智能在远程银行营销中的作用

（一）提升营销效率，实现精准获客

传统的远程银行营销往往采用电话、短信、邮件等方式，在对客户信息缺乏充分了解的情况下进行营销触达，效果难以保证。而人工智能技术可以从海量数据中快速识别目标客户、匹配个性化的营销内容，大幅提高获客效率。例如，运用机器学习算法对客户的金融交易、信贷记录等信息进行分析，构建用户画像，预测客户潜在需求，实现“千人千面”的个性化营销。同时，机器学习还可优化营销渠道组合，根据客户的偏好特征和行为习惯，选择最佳的触达时间和方式，提高营销的精准度和转化率。

（二）优化客户体验，提供智能服务

随着客户金融需求日益多样化，传统的远程服务模式难以快速响应，容易引起客户不满。人工智能可充分发挥其感知、认知、决策等优势，为客户带来全新的服务体验。例如，基于自然语言处理技术搭建智能客服系统，7×24小时在线解答客户咨询，无须排队等待；利用知识图谱技术分析客户诉求，对相似问题归类、总结，提炼标准答复，保证服务质量；应用语音识别、情感分析等技术，根据客户语气情绪调整服务策略，提供人性化关怀。智能客服有效缓解了人工坐席的压力，确保客户能随时随地获得专业、高效的金融服务，极大提升了客户满意度。

（三）赋能营销决策，发掘业务机会

远程银行营销涉及海量、高维度的客户交易数据，传统的分析手段难以全面挖掘数据价值。人工智能可充分利用机器学习算法，在复杂数据中快速找出有价值的关联特征和规律，形成新颖、有效的营销策略。深度学习技术可从非结构化数据如客户评论、录音文本等提取关键信息，分析客户情感倾向，预判客户流失风险，为维系客户关系提供决策参考。知识图谱可对客户的金融行为进行多维关联分析，发现交叉营销和向上营销的机会。人工智能处理数据的速度和精度远超人力，能快速响应市场变化，持续优化营销方案，为银行把握业务机遇、创造价值提供强大的数据和技术支持。

二、远程银行营销存在的问题

（一）营销数据利用不足，客户洞察有限

银行积累了大量的客户信息和交易数据，但受制于传统的数据管理方式和分析技术，难以充分挖掘数据价值。客户数据往往分散在各个业务系统中，缺乏统一的整合和管理，数据质量参差不齐，严重影响了数据分析的效果。此外，银行对非结构化数据的利用还十分有限，难以从客户评论、客服记录等非结构化信息中捕捉客户情绪和偏好，对客户需求的洞察比较肤浅。营销决策主要依赖经验和直觉，难以做到以客户为中心，个性化营销方案的适配性和有效性难以保证，容易引起客户反感。

（二）营销渠道不畅，响应速度滞后

当前，远程银行营销仍主要依靠传统的渠道如电话、短信等，营销内容趋于同质化，很难引起客户兴趣。客户习惯于在线上渠道获取金融产品信息并进行对比，但银行在数字化营销渠道的布局还不够完善，触达方式单一，互动性不足。客户在官网、App等渠道的咨询得不到及时有效的答复，问题解决周期长，在线客服接待能力有限，无法满足客户随时随地获得服务的要求，错失营销良机。营销渠道的不畅严重影响了客户服务体验，削弱了营销效果。

（三）营销效果评估滞后，缺乏持续优化

传统的营销效果评估主要关注营销活动的触达率、响应率等表层指标，缺乏对客户全生命周期价值的考量。银行对获客成本、渠道贡献、客户忠诚度等深层次指标重视不够，对不同营销方案的ROI缺乏系统评估，难以科学判断营销资源配置的合理性。营销过程数据的采集和分析还不够及时，存在数据滞后、反馈不畅等问题，营销过程优化和策略调整往往滞后于市场变化。缺乏数据驱动的营销闭环管理机制，营销效果难以持续改进，投入产出难以达到最优。

三、推动人工智能在远程银行营销中应用的对策建议

（一）夯实数据基础，推进数据治理

高质量的数据是人工智能应用的前提。银行要高度重视数据的获取、存储、管理和应用，建立健全数据治理体系，提升数据的规范性、准确性、安全性。一是要推动数据的标准化和集中化管理，建立统一的主数据平台，消除业务条线间的数据壁垒，实现客户信息、产品信息等关键数据的共享；二是加强数据治理工具和平台的建设，运用大数据、云计算等技术，提高数据采集、清洗、存储和计算的效率，保证数据应用的时效性；三是拓展数据采集渠道和数据源，积极探索行外数据与行内数据的融合应用，获取更加全面、立体的客户信息，增强客户洞察；四是重视元数据、主数据的管理，建立统一数据标准和数据字典，确保业务概念一致性，为人工智能的规模化应用奠定坚实的数据基础。

（二）优化营销流程，提升服务质量

银行要以客户需求为中心，优化远程银行营销的组织架构和业务流程，建立敏捷高效的营销服务运作机制。一是成立专门的智能营销团队，加强数据分析、产品经理、营销策划等关键岗位的配置，打破部门间的信息壁垒，强化协同联动；二是借助流程挖掘等技术，系统梳理现有营销服务流程，找出服务瓶颈，优化业务办理路径，减少流程中的等待和循环；三是整合各渠道的客户交互数据，运用语义分析、情感分析等技术，及时了解客户诉求，预判服务风险，提供个性化服务方案；四是完善知识库建设，借助知识图谱技术，系统化管理各类产品、服务和营销信息，为智能客服提供决策支持，提升服务的专业性；五是制定统一的服务标准，明确差异化服务的触发条件和路径，并纳入系统流程，规范服务运作，保证服务质量稳定。

（三）加快场景应用，创新营销模式

银行要把握人工智能应用的最佳切入点，加快在营销关键场景的智能化改造，推动营销模式创新。一是聚焦获客、活客、留客等关键环节，重点布局智能获客、智能服务、智能风控等场景，提高营销资源配置的效率和效果；二是打通线上线下渠道，整合网点、App、微信银行等服务入口，利用人脸识别、语音识别等技术，实现客户身份的无缝识别和服务接续，营造便捷、一致的服务体验；三是发挥人工智能的决策优势，建立数字化的营销闭环，加强营销全流程管理，借助A/B测试等，持续优化营销策略；四是创新营销内容和形式，利用自然语言生成、智能投放等技术，低成本制作和分发个性化营销素材，提升客户的参与度和转化率；五是拓展服务边界，发掘金融场景与生活场景的连接点，嵌入客户的消费旅程，提供智能化、情景化的普惠金融服务。

四、结语

人工智能正在成为数字经济时代的战略性技术，深刻影响着金融业的发展格局和服务模式。将人工智能技术与远程银行营销相结合，能显著提升营销效率，优化客户体验，为银行业创新发展注入新动能。银行要立足自身禀赋，强化科技引领，加快构建线上线下一体、金融场景与生活场景互联的智能化营销服务体系，为客户提供更极致的体验，实现从“以产品为中心”向“以客户为中心”的战略转变。

以中华优秀传统文化赋能思想政治理论课创新

冷凤平

思想政治理论课肩负着传承与发展中华优秀传统文化、培养担当民族复兴大任时代新人的重要任务。中华优秀传统文化蕴含着十分丰富的立德树人资源，拥有丰富的思政课教学素材。要使思政课在立德树人中发挥关键作用，就需要从中华优秀传统文化中汲取养分、寻找根基，实现思想政治理论课与传统文化智慧的深层融合。这既是提升思政课教学效果的重要举措，也是传承中华优秀传统文化的必然要求。

用中华优秀传统文化滋养思想政治理论课教学内容。中华文化源远流长、博大精深，其中包含的优秀传统文化更是灿烂辉煌，蕴含着中华民族在长期历史演进过程中积淀的思想智慧和经验的精华。在思想政治教育过程中，应充分利用多样的中华优秀传统文化滋养教育内容，增加中华优秀传统文化与思想政治理论课在教学内容上的黏合度，将其创新性地融入思想政治教育课堂之中，为思想政治理论课服务。如，思政课教师应自觉地运用中华优秀传统文化的价值理念、核心命题或经典格言等，来解读教材中的基本原理和基本观点；思政课教师还可以充分挖掘《论语》《孟子》等中华传统文化典籍的丰富内涵，启发学生对中华传统文化中的价值观念、道德观念等方面的思考。

用中华优秀传统文化创新思想政治理论课教学形式。思想政治教育过程实际上就是育人的过程，受教育者是思想政治教育实践活动的最主要参与者，在思想政治教育活动中有效提升思政课教学效果，使受教育者由被动接受知识转化为主动学习，有赖于教学形式的创新发展。充分探索中华优秀传统文化蕴含的丰富多样的故事与载体，将其灵活运用到思想政治理论课中，将思政课讲“深”、讲“透”、讲“活”是创新教学形式的重要途径。如，思政课可与本地的优秀传统文化相结合，打造出独具本地特色的精品思政课；思政课教师可借助中华优秀传统文化中具有思辨性的观点，采取辩论赛的形式展开思政课堂；思政课教师还可与中华传统故事相结合，在课堂中编演故事等，进而充分调动受教育者在思政课中发挥主体性作用，提升思政课的趣味性与实效性。

充分借鉴和吸收中华优秀传统文化的教育资源，用中华优秀传统文化滋养教育内容、创新教学形式，以此赋能新时代思想政治理论课的创新发展，使思想政治理论课成为一种更持久、更深沉的力量，实现以理服人、以德养人、以文育人。

（作者单位：湘潭大学马克思主义学院）