2022 年国际万物人工智能会议(AIE) | 978-1-6654-7400-9/22/$31.00 ©2022 IEEE | DOI: 10.1109 / AIE57029.2022.00091

边缘计算安全的人工智能: 一项调查显示

Francxa Tagne Waguie
理学院
信息系统工程系，
近东大学
frank.waguie@yahoo.fr

Fadi Al-Turjman
尼科西亚，梅尔辛 10 近东大学人工智能与机器人研究所人工智能工程系，土耳其凯里尼亚大学工程学院人工智能与物联网研究中心，凯里尼亚，梅尔辛 10，土耳其
Fadi.alturjman@neu.edu.tr

摘要:**边缘计算是扩展云计算潜力的一个前瞻性概念。为了继续使用计算机服务，保持一个没有任何形式的安全和破坏的良好氛围是至关重要的。由于围绕该区域的安全问题，围绕边缘计算环境的安全问题受到了阻碍。许多研究人员都研究了边缘计算的安全问题，然而，并不是所有人都对需求进行了彻底的研究。安全需求是指定系统为消除各种安全缺陷而执行的流程的功能和操作的目标。本研究的目的是全面概述目前用于边缘计算安全的许多不同的人工智能技术，旨在帮助未来的研究定位研究潜力。本文分析了最新的研究，并阐明了以下主题:用于对抗安全威胁的最先进技术，该方法使用的技术趋势，用于评估技术能力的指标，以及用于边缘计算安全的人工智能领域未来研究人员的研究机会。**

关键词:人工智能，边缘计算，安全，文献综述。

I. 介绍

随着传感器在现实世界中的部署不断增长，越来越多的物理事物通过传感器连接到物联网(IoT)。智慧城市、智能家居、环境感知和可穿戴医疗设备都是物联网技术大规模分布的领域[1][2]。在传统的物联网服务中，与物联网相连的传感器和设备必须将数据上传到云服务器以执行计算任务。处理后的数据将在任务执行后发送回物联网设备。 虽然由于云计算，传感器和设备的处理负担减轻了，但庞大的数据传输开销大得不方便，必须加以考虑。2018 年，全球有 112 亿台联网物联网设备，预计到 2020 年这一数字将增至 200 亿台[3]，导致数据快速增长。然而，目前网络容量的增长速度远远低于数据的增长速度

978-1-6654-7400-9/22/$31.00 ©2022 ieee 446

DOI 10.1109 / AIE57029.2022.00091

通信网络的复杂性使得降低延迟变得困难。网络带宽已经成为实现普通物联网服务之前必须克服的重要障碍。为了克服上述挑战，最近创建了一种称为边缘计算(EC)的新计算方法，并迅速在业界获得了吸引力。将计算任务转移到网络边缘的系统被称为“EC”。它的缩写是“边缘计算”。[4],[5]。与云计算相比，EC 提供了许多好处，包括保护终端用户隐私、最小化数据传输期间的延迟、减少网络带宽负载以及降低数据中心能源使用。边缘计算(EC)消除了物联网设备将原始信息提交到中央云服务的需要，而是允许它在边缘节点(ENs)上进行处理、存储和传输，从而减少了延迟。需要快速响应时间的物联网和移动计算应用将受益于 EC 的增强支持。另一方面，欧共体并不是万灵药。ec 支持的物联网设备在计算卸载、精确定位和实时处理等多个领域都有了重大改进。这部分是由于终端用户数据处理接近低延迟的来源。另一方面，EC 引入了新的安全问题，扩大了系统的攻击环境[6]。

II. 文献综述

A. 异构环境& &;分布式布局

移动数据收集、传感器网络、网格计算和无线传感器网络都属于广泛的范畴。在电子商务中使用的技术。在这样一个异构环境中，跨多个安全域建立统一的安全规则和机制是很困难的。

网络边缘设备(ENs)很难集成以进行集中控制[7]，因为它们分布在网络外围之外。攻击者可以将被劫持的节点作为跳板，通过关注已知存在安全漏洞的 ENs 来渗透整个系统。

边缘计算安全背景。因为搜索将只查看已建议的四个在线电子数据库，因此只会找到与计划审查相关的一小部分文献。

为了限制审查工作的范围，搜索仅限于计算机科学和信息、计算机科学和理论以及工程主题领域。在第一次搜索中，我们只考虑了 2015 年 1 月至 2019 年 11 月期间在会议上发表或在同行评议期刊上发表的论文。这些文章是通过以下搜索提示找到的: {“人工智能”与“边缘计算”与“安全”或“边缘计算”与“安全”与“人工智能”或“安全”与“边缘计算”}。入选标准包括: 在 2015 年 1 月至 2019 年 1 月期间发表的具有较高意义的期刊或会议论文，以英文撰

B. 有限的计算源

云计算和 EN 计算功能由于其物理结构而受到限制。因此，分布式拒绝服务(DDoS)攻击会对网络产生重大影响。因为 en 不支持重量级安全机制。

已经开发了许多安全策略和算法来补偿边缘计算特征所带来的危险[8]。算法和模型遵循入侵检测、数据机密性或访问控制的相同设计，在当今的大部分安全系统中使用。随着攻击手段和方法的不断升级，传统的防御措施往往被抛弃。然而，令人着迷的是，人工智能(AI)正在为隐私和安全问题提供新的解决方案。

III. 方法

为了保证数据的搜索和检索是准确和客观的，这种审查工作适用于系统审查。在开始文献和数据提取搜索过程之前，已经制定了一份审查方案，其中详细说明了搜索策略，在选择要考虑或丢弃的论文时建立纳入/排除的具体标准，以及评估被选中进行审查的文章的计划。在部署之前，其中一位作者对协议进行了授权。**图 1** 描述了评审任务方法中涉及的过程。

A.搜索策略

对所有作品进行了全面的搜索，包括审查和技术，集中于人工智能在边缘计算中解决安全问题的应用。Web of Science、Scopus、IEEE-Explore、Wiley、Springer 和 Science Direct 都被用来进行搜索。这是因为它们包括了来自著名期刊和会议记录的论文，提供了一个有代表性的样本，说明了我们对人工智能的理解

写;排除标准包括:如果论文没有关注人工智能在边缘计算安全方面的应用，如果论文没有完全可访问。

Scopus 发表论文 273 篇， Web of Science 271 篇， IEEE-Explore 1328 篇， Science Direct 354 篇， Springer 371 篇，Wiley 405 篇。总共发现了 3002 件物品。扫描所搜索项目的标题和摘要。扫描后，发现 2730 件物品

外

图 1: 已实现评审的体系结构。

该图显示了这一审查所涉及的不同步骤。箭头表示连续的步骤，右边的正方形表示前一步的结果。

对符合纳入标准的数据进行了彻底的抽象，以获得符合研究目标的相关数据。记录了以下细节: 作者,

IV. 结果

几家期刊的出版物，涵盖了广泛的主题。大部分论文来自 IEEE explore Magazine(70%) 和 ACM Digital Library 期刊 (20%)，Science Direct 占了剩余的 10%。在保留的每篇文章中，我们提取了研究的描述(研究目的和研究目的)，用于攻击检测的方法，用于性能分析的方法，该方法的优点及其局限性(表 1)。

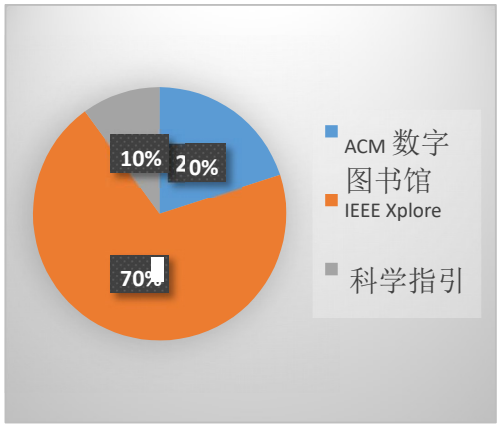


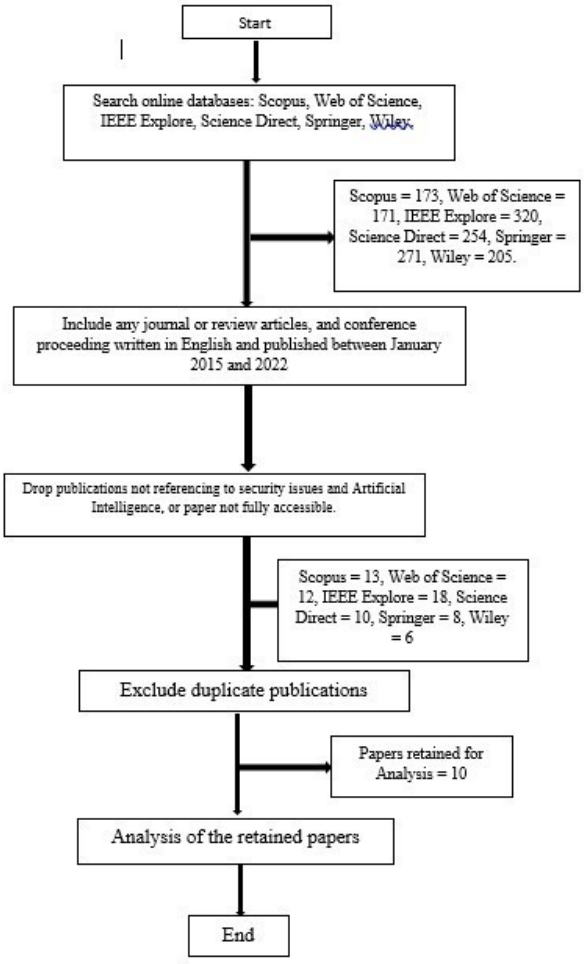
图 2: 根据各自的期刊分发文章。

V. 讨论

尽管过去的审查研究为理解边缘计算安全和隐私挑战提供了值得注意的基础，但评估之间的范围在提供安全和隐私需求的完整评估方面受到限制。此外，使用部署的技术手段来确保满足规范的方法没有得到充分的检查。这篇综述使用了一种系统的方法来提供关于边缘计算系统中的安全和隐私的全面知识。

根据研究结果，从分析的论文中提供了十种边缘计算安全策略，所有策略都以攻击检测为目标。这些技术包括 SDN 架构框架、MAB 架构框架、博弈论算法、贪心算法、聚类算

该评论研究了来自不同期刊和会议记录的四个独立电子数据库中的 10 份出版物。**图** 2 描述了的分布



法、机器学习、新颖方法(D2D 通信)、新颖方法(混合特征分析)、新颖方法(GPS)、新颖方法(ANDROIDS)。的

还研究了用于评估方法有效性的绩效指标。可以看出，策略使用指定的度量来评估其在每一类标准下的有效性，确认期望的目标。表 11 强调了使用特定标准评估策略的目标。这将有助于未来的学者理解为什么每个测量都以特定的方式使用。

这项研究旨在尽可能快地完成审查。然而，各种情况可能会影响得出的结论，降低结果的质量。以下是一些促成因素:

- 由于只有一位作者搜索了原始研究论文，数据收集过程被扭曲了。
- 因此，为了收集数据，只审查了四个电子数据库。因此，来自其他相关数据库的研究可能会被排除在外。结果，审查工作的广度受到限制。

VII. 结论

边缘计算范式有很大的希望，旨在消除云计算的几乎所有缺点。接受该条约的主要障碍之一是安全问题。因此，弄清楚如何处理这些问题至关重要。结果表明，在边缘计算安全和人工智能方面的综合文献综述是第一次。它的目标是提供对顶级安全的当前流程的完整和周到的掌握，以及方法所使用的尖端技术方法。鉴于此，总共有 10 篇论文使用正常的系统文献综述过程进行了广泛的检查。这些发现表明了对检索数据进行全面审查后得出的重要结论。根据这项研究的结果，在边缘计算的隐私和安全方面，有八个不同类别的标准需要考虑。其次，研究表明，除了完整性、不可否认性和可靠性之外，每个需求都有自己的一套专门为其构建的方法，这些方法都在四个单独的方案中进行了评估。最后，为了确定趋势，研究结果将发现的程序按其相关的技术方式进行分类。第四，综述工作发现了每种方法的局限性，为未来学者的研究前景奠定了基础。此外，还发现，在某种需要下的每一类程序都有不同的衡量其有效性的标准，以便实现特定的目标。最后，为了对使用人工智能研究边缘计算安全性感兴趣的学者的优势，提到了未来研究的开放性问题。

- 只考虑在学术期刊上发表的作品和在会议上发表的作品，作为补充信息的来源，专利、期刊和专题讨论会被省略。

VI. 开放性研究问题

在研究的大部分论文中，在引入方法之前，特别是身份验证和隐私保护措施，攻击没有得到充分的研究或以任何有意义的方式处理。 这些攻击对处于交互边缘的小工具的机密性构成严重威胁，因为它们可能泄露敏感信息。

入侵检测系统(IDS)用于识别和缓解多种类型的网络入侵。另一方面，当涉及到边缘计算时，入侵检测系统必须在边缘网络的每个层面(边缘节点、最终用户和云)上实现。如果 IDS 仅应用于一个或两个级别，则可能无法阻止恶意攻击在整个边缘网络中传播。

VIII. 鸣谢

我们想了解人工智能和物联网研究中心，人工智能和机器人研究所，近东大学和格雷斯之门有限责任公司。

IX. 参考文献

[1] C. Livadas, R. Walsh, D. Lapsley 和 W. T. Strayer，“使用机器学习技术识别僵尸网络流量”，Proc。*——相依。当地的第一版。《网络》，LCN, 967-974 页，2006,doi:* 10.1109 / LCN.2006.322210。

[2] F. X. Ming, R. A. Ariyaluran Habeeb, F. H. B. Md Nasaruddin, A. Bin Gani，“基于物联网的实时二氧化碳监测&;云技术”，ACM Int。相依。 *爵士。，vol. Part F147956, pp.* 517-521, 2019, doi: 10.1145/3316615.3316622。

[3] 肖彦，贾彦，刘春春，程晓霞，余健，吕伟，“边缘计算安全:《最新技术与挑战》，诉讼程序。*IEEE, 2019,* doi: 10.1109 / JPROC.2019.2918437。

[4] 陈峰，夏霞，陈峰，何琪，金宏，“基于边缘计算的应用程序数据分布”，电子工程学*报。Distrib 平行。系统。，第 32 卷*，第 2 期。1, pp. 31-44, january 2021, doi: 10.1109 / TPDS.2020.3010521。

[5] 史伟和 S. Dustdar，“边缘计算的前景”，计算机(长)。*海滩。加州)。，第 49 卷*，no。5, pp. 78-81, 2016 年 5 月，doi: 10.1109 / MC.2016.145。

[6] P. K. Manadhata 和 J. M. Wing，“系统攻击面的形式化模型”，HP 实验室。*技术。没有代*表。115, pp. 1-28, 2011, doi: 10.1007 / 978-1-4614 - 0977 - 9 - _1。

[7] P. *Lai* et al.，“可变大小向量装箱边缘计算的最优边缘用户分配”，选。*指出第一版。科学。(包括潜艇。收。 Artif 指出。智能。收。《生物信息学》，vol. 11236 LNCS, pp. 230-245,* 2018, doi: 10.1007 / 978 - 3 - 030 - 03596 - 9 - _15。

[8] 林俊，余伟，张宁，杨晓霞，张宏，赵伟，“物联网研究综述”架构、使能技术、安全和隐私与应

用，”IEEE 物联网学报，第 4 卷，第 1 期。5, *pp. 1125-1142, 2017, doi:* 10.1109 / JIOT.2017.2683200。