面向网络安全的联邦学习与面向物联网的联邦学习的网络安全研究进展

Bimal Ghimire, IEEE 研究生会员，*Danda B. Rawat, IEEE 高级会员*

***摘要*:近年来，网络安全和新兴物联网机器学习(ML)领域的去中心化范式受到了政府、学术界和工业界的广泛关注。联邦网络安全(FC)被认为是一个革命性的概念，使物联网在未来更安全、更高效。这一新兴概念具有检测安全威胁，采取对策，并有效限制威胁在物联网网络系统中的传播的潜力。网络安全的目标是通过在各种参与者之上形成学习和共享模型的联盟来实现的。联邦学习(FL)被认为是一种隐私感知的 ML 模型，对于保护脆弱的物联网环境特别有用。 在本文中，我们首先介绍了集中式学习、分布式现场学习和 FL 的背景和比较，然后调查了 FL 在物联网网络安全中的应用。本调查主要关注安全方面，但也讨论了几种解决与 FL 相关的性能问题(例如，准确性、延迟、资源约束等)的方法，这些问题可能会影响物联网的安全性和整体性能。为了预测这种新范式的未来演变，我们讨论了该领域正在进行的主要研究工作、挑战和研究趋势。通过本文，读者可以更深入地了解 FL 的网络安全，以及 FL 的网络安全，不同的安全攻击和对策。**

***索引术语*:网络安全，数据卸载，联邦网络安全(FC)，联邦学习(FL)，机器学习(ML)。**

I. 介绍

W随着个人数字助理(pda)、物联网等互联设备的爆炸式增长
(物联网)、可穿戴医疗设备等，每时每刻都在生成前所未有的数据量。巨大的数据量为机器学习(ML)模型和深度学习(DL)在许多领域的应用提供了更好的机会[1]。今天，ML 已经做了它甚至进入了我们的日常生活。从小型手持设备、物联网传感器和网络物理系统(cps)到 Facebook、谷歌、亚马逊等大公司，netflix 一直在将机器学习应用于他们的应用和服务。 Amazon Web Services 、 Google Cloud 和 Microsoft Azure 等都是一些流行的机器学习服务[2]，其中模型可以大规模部署和使用。机器学习不仅可以改善用户体验和业务建模，还可以检测和预防网络威胁和网络攻击。当今世界严重依赖于数据，维护数据的完整性和隐私是重中之重与个人、组织和政府有关的敏感数据需要通过通信链路从一个点传输到另一个点。传统的应对网络安全问题的方法大多是在发生特定类型的攻击后才保护设备。然而，当今网络空间的攻击类型和模式已经发生了巨大变化。利用多态病毒的攻击不断改变其特征，难以检测和预测。因此，检测和预测网络空间中的威胁、异常或任何类型的安全漏洞并采取相应对策的机器学习方法近年来备受关注。通过共享局部训练数据形成集中式学习模型已经被证明可以提高学习模型的性能[3]。

在实践中，基于 ml 的网络安全有多种模型，每种模型都有其优点和缺点，即集中式、分散式和联邦式[1]。网络安全的联邦学习(FL)模型是这些模型中最近增加的。我们将在后续章节中讨论所有这些模型。此外，人们还探索了 FL 在多个领域的适用性，如智慧城市[4]、医疗保健[5]、推荐系统[6]、无线通信[7]、边缘网络[8]、电网[9]、车载自组织网络[10]等。FL 框架固有地支持安全性和隐私性(与集中式学习框架相比)，因为在终端设备中生成的数据不会离开设备。本地使用有用的设备数据，以分布式的方式训练在设备上运行的学习模型。终端设备与云服务器之间只交换更新后的参数。 然而，这种方法仍然暴露了一些安全威胁。因此，本次调查主要集中在 FL 应用的安全方面。 FL 框架为提高安全性和隐私性提供了有希望的潜力，但对于它的成功，阻碍它的问题

2021 年 10 月 25 日收稿;2022 年 1 月 11 日修订;接受 2022 年 2 月 6 日。发布日期:2022 年 2 月 10 日;当前版本日期 2022 年 5 月 23 日。 这项工作部分得到了霍华德大学国防部人工智能和机器学习卓越中心(CoE-AIML)与美国陆军研究实验室签订的合同 W911NF-20-2-0277 的支持;部分由美国国家科学基金会(NSF)拨款 CNS/SaTC 2039583 和拨款 1828811;部分由国家核安全局(NNSA)资助。*(通讯作者: 丹达·b·拉瓦特)*

作者来自霍华德大学电气与计算机科学系，华盛顿特区 20059 美国(e-mail: bimal.ghimire@howard.edu;danda.rawat@howard.edu)。

数字对象标识符 10.1109/JIOT.2022.3150363

必须解决 FL 的性能问题。在这方面，我们还讨论了解决 FL 模型准确性、通信延迟、数据分布和分布式设备资源约束等问题的现有工作。

由于软件和通信接口的日益复杂，物联网和网络物理设备更容易受到各种攻击。此类系统的网络安全漏洞可能会引发一些隐私和安全问题。应对任何威胁或攻击，必须采取适当的安全措施和有效而强大的网络安全解决方案。下面，我们概述了与 IoT 和 CPS 相关的一些常见安全风险，其中 ML 算法依赖于从此类 IoT/CPS 系统收集的数据。

针对 IoT/CPS 设备的攻击: 黑客可以通过暴力攻击轻易破解设备的密码，并操纵这些设备的蓝牙连接，从而泄露私人信息、操纵数据和/或获得控制权。

对云网络的攻击: 物联网和 cps 需要频繁处理存储在云中的大量数据。这些设备使用不同的通信媒介，如 Wi-Fi、蜂窝网络等，向云发送和接收数据。这些通信媒介容易受到攻击者的攻击，中间的攻击者可能会拦截和伪造正在交换的数据。

恶意软件: 像任何其他连接设备一样，物联网和网络物理设备也容易受到恶意软件的攻击。

脆弱的传感器: 物联网和 CPS 设备配备了各种传感器来监控和支持系统。这些传感器是脆弱的，足以受到攻击者的攻击，造成安全和安全威胁。即使是主要的传感器，如全球定位系统(GPS)信号、光探测和测距(LiDAR)信号、惯性测量单元(IMU)数据等也可能被泄露，对设备造成严重威胁。

网络攻击: 物联网和 cps 中的每个设备或端点都是网络攻击面的一部分。 攻击者可以以网络端点为目标，通过访问网络来控制和危害整个系统。诸如 WiFi、蓝牙和 GSM 等协议允许外部设备与各种传感器连接和通信。这些协议包含错误，很容易被攻击者利用。*固件攻击:* 在这种形式的攻击中，攻击者向他/她使用的设备提供恶意固件更新可以直接访问整个系统。

已经有几个调查(例如，[1]和[11]-[15])回顾了 FL，并强调了其分类、方法、进展、应用、挑战等。 然而，我们的工作与其他人不同，因为它提出了关于网络安全的 FL 和 CPS/IoT 环境中 FL 的网络安全的研究。在物联网环境中成功采用 FL 在很大程度上取决于几个性能指标，本文也对这些指标进行了回顾和介绍。为了应对各种网络威胁我们必须建立入侵检测系统和入侵防御系统。这些系统必须了解全球现有的网络威胁，甚至需要主动检测和预测新的和正在出现的威胁。 外语的协作学习框架很适合这种任务。评估安全解决方案，二十多年来一直在努力创建真实的数据集

本调查还突出了这些作品，并讨论了本调查中提出的研究使用的大多数数据集。我们还讨论了联邦设置中常用的一些数据集来评估联邦模型的性能。这种新的学习架构的转变引入了一些新的攻击，例如中毒和逆向工程，我们还讨论了解决这些攻击的研究工作。在本次调查中，除了讨论了最近在 FL 领域的一些研究工作外，我们还介绍了这些工作所应用的 ML 算法和技术。这项调查的目的是帮助读者选择一个特定的研究方向与整体信息。具体来说，本文的主要贡献包括以下几点。

1) 我们对机器学习和网络安全的联邦模型进行了详细的研究，将它们分为两部分。第一部分讨论了 FL 及其在网络安全中的应用，第二部分讨论了 FL 的网络安全。我们的研究主要集中在 IoT/CPS 环境上。
2) 由于在物联网环境中成功采用联邦模型在很大程度上取决于几个性能指标，因此我们还在本文中介绍了这些指标、与之相关的挑战以及潜在的解决方案。
3) 我们还提出并讨论了被调查文章用来评估其模型性能的数据集。
4) 我们还介绍了网络攻击，例如 FL 中的参数中毒和逆向工程。
5) 我们以表格形式总结了物联网网络联邦模型中的安全攻击和对策以及解决的性能问题，以便进行并排比较。
6) 我们讨论了研究的挑战、开放的问题，并对联邦模型提出了建议，这些建议需要得到解决，以充分发挥其潜力。

本文的其余部分组织如下。在第二节中，我们讨论并比较了不同类型的机器学习模型。现有的近期工作与使用 FL 作为保护物联网环境的工具以及与使 FL 框架安全相关的工作将在第三节中讨论。在第四节中介绍了一些研究工作，以解决影响 FL 性能的问题。在第五节中，我们重点介绍了机器学习算法、技术和框架，在第六节中，我们分别讨论了被调查研究使用的数据集。第七部分介绍了物联网领域中 FL 的一些开放挑战和未来研究方向。最后，我们在第八节结束我们的调查工作。 各种缩略语的全称见表 1。

II. 联邦学习概述和联邦网络安全模型

在本节中，我们首先简要概述了不同类型的学习模型，然后详细介绍了 FL 及其挑战。最后，我们提出了一个

表我
缩写和完整形式

Symbol	Full Form
CNN	Convolution Neural Network
GRU	Gated Recurrent Unit
SAE	Stacked Autoencoders
AWID	Aegean Wi-Fi Intrusion Dataset
MNIST	Modified National Institute of Standards and Tech
Cifar10	Canadian Institute For Advanced Research dataset
LSTM	Long Short-Term Memory Networks
SVM	Support Vector Machine
VGGT	Visual Geometry Group
KWS	keyword spotting
NS3	Network simulator 3
DNN	Deep Neural Networks
DRL	Double Deep Q Learning
EV	Electric Vehicle
MLP	Multilayer Perceptron
KNN	K-Nearest Neighbor
SOHO	Small Office or Home Office
ADS	Anomaly Detection System
BC	Blockchain
RF	Random Forest
ECC	Elliptic Curve Cryptographic
IDS	Intrusion Detection System
SDN	Software Defined Network
NFV	Network Function Virtualization
WAN	Wide Area Network
DTN	Delay Tolerant Networking
IIoT	Industrial Internet of Things

联邦网络安全(FC)模型有助于保护 FL 框架。

A. 学习模式的典型类型

应对网络安全问题的方法一直在随着需求不断变化。To cope with the unprecedented growth of heterogeneous connected devices and a tremendous volume of data and traffic generated by them and the development of sophisticated tools to create poly- morphic malware and other threats, ML has been an integral part of cyber defense mechanism in recent times. 本节讨论三种不同的支持 ml 的模型及其优缺点。

1) 集中式学习模式: 该模型使用以云为中心的架构(例如[16]-[19]),其中从终端设备发送的数据在云中集中存储和处理。在云中，对数据进行分析，提取特征，然后在存储数据的基础上建立模型。 模型由通过 API 发送请求的终端设备访问。这种方法具有显著的优势，但也存在一些严重的问题。这种方法的一大优点是，云提供了一个巨大的存储库，因此存储所有客户端发送的大量数据不会有问题。另一个优点是，云大多配备了高性能的服务器。这些好处有助于建立训练有素的模型。此外，云服务最好由服务提供商保护，以防止任何安全漏洞或攻击。这种方法提供了如此巨大的优势，但也有严重的隐私、安全性和延迟问题。所有数据都需要通过不安全的通信链路传输到云端这使得数据很容易被对手攻击。所有的

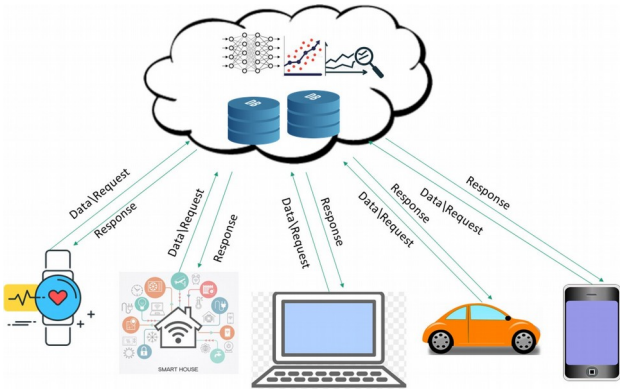


图 1 所示。物联网集中式学习模型。

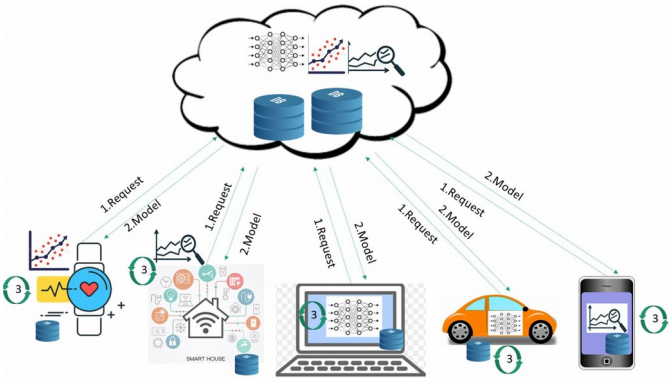


图 2 所示。物联网分布式现场学习模型。

这些设备产生的私人数据存储在云端，这引发了很大的隐私问题。此外，中央机构或云服务提供商拥有对模型和数据的所有控制权。此外，由于数据需要在云中来回传输，如果设备和云之间的通信距离很远，延迟和带宽成本可能会成为大问题。集中学习的工作模型如图 1 所示。

2) 分布式现场学习模式: 在这种学习模型的方法中，一个通用的或预先训练好的模型由服务器预先分发到所有的设备或客户端。在此之后，每个设备通过本地数据的训练和测试来个性化模型，并学习数据生成过程。 这样的学习模型可以从设备生成的实时流数据中进行预测和推断[1]。这里最大的优势是设备生成的数据保存在本地，从而消除了安全、隐私和延迟问题。这种方法的主要缺点是物联网设备相对来说是异构的——在内存、计算和电池电量方面是脆弱的。这些设备不适合使用模型时所需的密集计算[20]。 此外，本地运行的模型缺乏全局更新或关于新出现的安全威胁的知识。分布式现场学习的工作模型如图 2 所示。

3) 联邦学习模型: 它是一种分布式模型，但具有从所有分布式客户端收集全局知识的便利。与分布式设置相同，一般或预训练的模型最初分发给客户端。

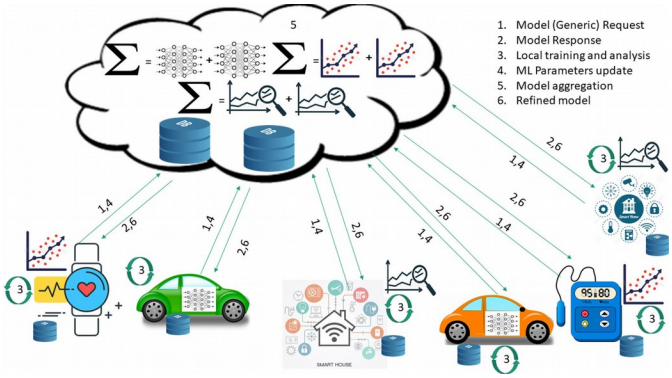


图 3 所示。物联网的 FL 模型。

所有客户端都使用本地原始数据在本地对模型进行个性化客户端在本地执行机器学习任务，并将其参数发送给服务器。然后，服务器汇总从客户端接收到的所有更新并执行 ML 任务，最后将更新后的模型分发给客户端[11]。这是一个持续的过程，通过这个过程，客户可以不断地获得所有新兴的全球知识。FL 的工作模型如图 3 所示。该学习模型首先由[21]提出如下:

$$F(w) = \sum_{k=1}^{K} \frac{n_k}{n} F_k(w) \quad \text{其中} \quad F_k(w) = \frac{1}{n_k} \sum_{i \in P_k} f_i(w)。 \tag{1}$$

在(1)中，$f_i(w)$表示输入预测的损失函数 x_i to an expected output y_i with weight vectors w. K 为当前学习轮的参与者数，Fk(w)为第 K 个参与者的局部目标函数。

对于样本总数 n, nk 是第 k 个参与者局部存在的样本数。同样，Pk 与 nk Pk 是分配给整个数据集 P 中第 k 个参与者的分区。

在典型的 FL 设置中，当设备首先从服务器下载当前模型参数(权重)时，它使用下载的参数初始化本地模型，然后使用本地数据集来训练模型。采用随机梯度下降(SGD)最小化局部目标函数来优化参数。所有这些设备的优化参数被发送到服务器，在那里它们使用 FederatedAveraging 算法进行聚合[21]。通过这种方式，可以更新全局模型并进行学习。由于原始数据驻留在设备本地，只有 ML 参数被发送到服务器，因此 FL 确保了客户端原始数据的隐私性，并符合隐私政策和/或法规，例如欧洲数据保护法规通用数据保护法规(GDPR)[22]。此外，FL 框架还丰富了隐私保护技术，如差分隐私[23]、安全多方计算(SMC)[24]和同形加密(HE)[25]，以安全地将 ML 参数从客户端发送到服务器。尽管具有良好的潜力，但在与物联网应用时 FL 带来了一些挑战。

在这里，我们强调了与物联网 FL 相关的一些主要挑战。

1) *设备内存有限:* 物联网设备在运行过程中不断产生数据。由于它们的内存有限，当数据的批处理大小增加时，在本地训练联邦模型是不可行的。在 FL 场景中，这些设备可能会被丢弃，或者在训练阶段被迫使用一个简单的模型来处理小批量的数据[1]。
2) *电池电量有限:* 如果学习模型复杂，训练数据量巨大物联网设备可能会在训练阶段耗尽电池电量。
3) *有限的计算能力:* 特别是物联网设备，受计算能力的限制。由于这种约束，通过这种设备局部训练模型可能不是一种可行的方法。
4) *弱点:* 近年来，我们看到了各种物联网设备的前所未有的增长。某些类别的物联网设备很容易受到黑客的攻击。这样的设备可能会产生恶意数据，当这些数据用于训练模型时，它甚至可能影响全局或联邦模型。
5) *不可靠和有限的可用性:* 在佛罗里达，客户可以随时退出。 客户机可能会因为几个因素而被放弃，比如不可靠的网络连接、有限的存储、计算能力等等。此外，客户的可用性取决于时间和位置。与夜间相比，白天可能有更多的客户端可用。白天和晚上也一样
地理位置不同。
6) *无状态:* 客户机的可用性取决于几个因素，因此客户机不能保证重复计算。
7) *匿名和中毒:* FL 中的客户端是匿名的，这使得很难区分真正的或恶意的客户端。因此，联邦模型可能会因为恶意客户机的参与而受到损害。
8) *非独立和非同分布(Non- IID)数据:* 设备上本地数据的性质取决于其独特的行为和使用模式，因此客户端和数据的分布是不一致的。同一台设备的数据可能会因为地点、时间和用户的变化而有所不同。
9) *当地的培训:* 每个客户端仅限于其本地数据。设备上没有足够的数据可能无法训练并产生一个好的模型。
10) *准确性:* 由于 FL 的非 iid 数据、无状态、局部训练和资源约束等特点，聚合的全局模型可能不如集中式学习准确。非 ac 精确的全球模式反过来又会影响局部模式，作为连锁反应，全球模式再次受到更大的影响。
11) *通信开销:* 客户机与服务器的通信频率不仅取决于本地数据的特性、大小和质量等因素，还可能受到其他客户机的严重影响。经常与服务器保持沟通

与全局模型一致的本地模型增加了通信开销。

自[21]中首次提出 FL 以来，已经有几项研究解决了 FL 中存在的挑战。例如，提出只有当全局模型的权重与经验选择的某个阈值不同时，才通过聚合全局模型来减少通信开销[26]。针对类似问题，文献[27]提出了一种寻找全局聚合频率的控制算法。为了减轻非 iid 数据的影响并提高准确性，提出了一种局部和全局模型聚合的特征融合方法[28]。为了解决类似的问题，Sattler 等人。[29]设计了一种联邦多任务学习(federated multitask learning, FMTL)框架，基于 FL 曲面的几何特性形成客户端簇，数据分布可联合训练。[20]中的工作使用基于深度强化学习代理的数据卸载决策来解决资源约束问题和其他挑战，并使 FL 操作高效。[30]提出了在分布式学习过程中从客户端更新的多样性中检测基于 sybil 的参数中毒并采取纠正措施。一些作品[31]-[33]已经提出了 FL 设置中的 ids，可以从威胁的全局知识中学习并检测新的和正在出现的网络威胁。在第三部分中，我们讨论了最近几项解决 FL 中存在的挑战和问题的工作。

B. 网络安全模型的典型类型

安全是当今数字世界的基本要求。易受攻击的异构物联网设备呈指数级增长，此外，通过无线媒介进行通信，大大扩大了攻击面。无线通信网络的标准和协议与有线通信网络不同，但更容易受到攻击。物联网设备的移动和分布式特性进一步加剧了安全挑战。因此，为有线网络设计的安全解决方案不能直接应用于无线网络。与学习模型类似物联网环境的网络安全模型可以分为隔离设备级网络安全模型、分布式网络安全模型和 FC 模型三种类型(如图 4 所示)。我们可以把这些看作是提供不同级别安全服务的网络安全模型。采用一种特定类型的安全模型是不够的，因此有效的网络防御机制可能需要这些模型的组合。

1) 隔离设备级网络安全模型: 这种网络安全模型在最低级别工作，并关注为终端设备提供安全服务。由于物联网设备的异构性，每一类设备可能都有特定的漏洞和安全要求。因此，设备级网络安全模型需要负责保护设备免受任何恶意活动的侵害。 从密码设置、有效性认证、访问控制等基本安全措施出发，对每一个连接请求进行验证，建立与外界的安全通信。 设备级安全还旨在验证及时的软件更新，并确保更新过程完全安全。此外，它还旨在保护设备免受恶意软件攻击。虽然

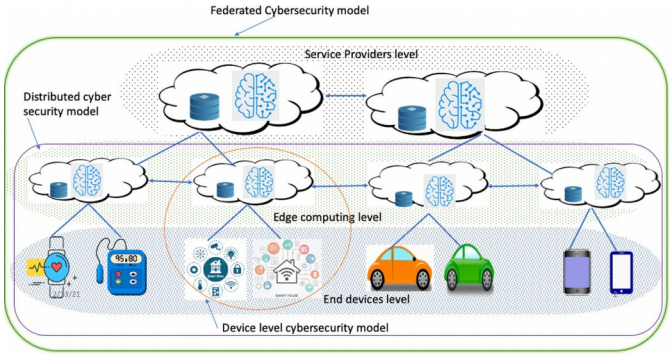


图 4 所示。物联网中 FL 的 FC 模型。

设备级网络安全模型旨在提供所有必要的安全措施，它不足以完全保护系统。攻击者使用复杂的工具和代码来生成新的多态恶意软件来攻击连接的系统。因此，需要机器学习模型来支持设备级安全性，以便根据动态场景进行学习和适应。它应该能够在任何攻击或异常情况下采取防御机制，并允许设备顺利运行。然而，大多数物联网设备都受到资源限制，这使得它们无法运行 ML 模型。 为了解决这个问题，在物联网网络中，通常采用网关节点或边缘节点来运行 ml 支持的网络安全模型，并为网络中连接的所有终端设备提供必要的安全性。

2) 分布式网络安全模型: 每天都有大量新的网络威胁出现。从一个物联网网络的网络攻击/威胁中学习是不够的。在分布式网络中，边缘节点地理位置分散，离终端设备或用户最近。 因此，分布式网络安全模型旨在使地理上分布的边缘节点之间的协作和合作能够提供更好的安全服务基于底层物联网网络的特征，边缘节点之间可能因其提供的特定安全服务而与众不同。如果任何边缘节点不能向附近的设备或用户提供预期的服务，它将与同级别的其他节点协作来完成这项工作。这种合作有助于提供适当的安全解决方案，以应对实时场景中出现的网络威胁/攻击。

3) 联邦网络安全模型: 如图 4 所示的网络安全模型，基于底层/设备层(如[34]和[35])的反馈，从联邦模型的顶层提供安全和其他服务。物联网服务提供商参与这一层面，为各自的用户或设备提供必要的服务。每个用户都可以从其服务提供者访问相应的服务。特定物联网网络上的边缘节点在中间发挥作用，以确保向其最终用户或设备提供必要的安全和服务。 每个服务提供商负责通过边缘节点向其所有分布式设备传播必要的安全服务。 在此安全模型中，每个服务提供者从其所有设备中学习，并相应地更新安全模型。此外，这些独立的服务提供商还相互协作，制定动态防御策略/解决方案来进行对抗

可能的攻击和威胁。在直接的较低级别，如果边缘协作不能实时提供安全解决方案，则特定的边缘节点会向其服务提供商伸出援手。然后，服务提供者提供必要的安全解决方案，或与其他提供者合作完成此工作。

4) 联邦学习和联邦网络安全: FC 模型的现有方法通过根据需要在不同级别进行通信和协作，为物联网应用提供安全解决方案。然而，在同一级别内和/或不同级别之间交换数据/信息的传统方式可能会引起隐私和安全问题。FL 已经成为一种以安全和隐私保护的方式交换数据/信息的解决方案。 伴随 FL 的 FC 模型在任何级别进行协作和交换任何信息，为使物联网网络安全提供了巨大的潜力利用 FL 作为网络防御机制的大多数 FC 方法主要侧重于保护物联网网络，考虑到单一服务提供商提供的单一全局模型。然而，这种方法可以很容易地扩展到涉及由不同服务提供者维护的多个全局模型的协作场景。只有少数研究致力于利用多个全局模型创建一种联邦安全模型。在下一节中，我们将对使用 FL 为物联网网络创建 FC 模型的几个研究工作进行调查。

III. 网络安全和网络安全联合学习的最新进展对于联邦学习

这项工作的重点是调查自 2015 年以来针对网络安全(特别是物联网环境)的几项现有工作。 表二给出了这些工作所处理的问题以及它们被实现或测试的环境。近年来，解决物联网网络安全问题的大量研究工作已转向应用 FL。FL 的框架本质上支持隐私、一定程度上的安全性和延迟，因为只需要传输更新，但这些在集中式学习中实现成本更高。分布式学习解决了这些问题，但缺乏协作学习的全局知识。在物联网网络中，FL 也有一些缺点，比如设备的异构性、资源约束、非 iid 数据、准确性等。主要是，大多数 FL 调查的作品都解决了安全和隐私问题，但也有一些作品解决了延迟[26]，[36]-[41]，资源约束[20]，[27]，[42]-[45]，准确性[28]，[41]，[46]和非 iid[28]，[29]，[39]等问题。所有这些问题在某种程度上都是相互依存的，改善一个问题不应该影响到其他问题。有些作品考虑了所有这些问题，而另一些作品只解决了其中的一部分。我们将讨论为缓解 FL 中存在的此类问题所做的一些贡献。虽然物联网环境中的 FL 是我们研究的主要焦点，但我们最近研究的一些工作是在分布式学习环境中提出和测试的。我们还提到了这些工作，考虑到它们对安全物联网环境的有用性，并且很容易扩展到 FL 设置。

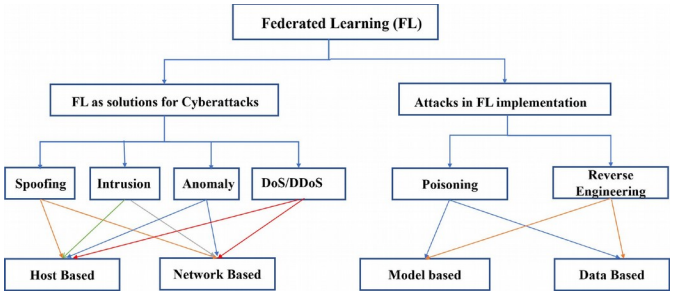


图 5 所示。FL 作为一种针对 FL 中出现的各种攻击和新型攻击的安全解决方案。

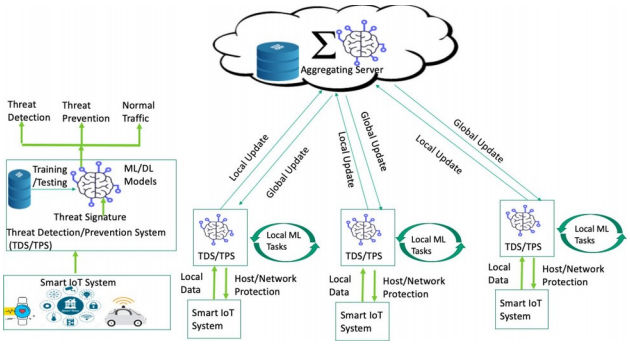


图 6 所示。FL 作为缓解物联网网络中可能存在的威胁的解决方案。

我们把调查过的作品归纳为两类。在一组中，我们讨论了与 FL 作为网络安全工具相关的现有工作，在下一组中，我们介绍了基于 FL 网络安全需求的工作。图 5 突出显示了 FL 作为不同类型攻击的解决方案，以及 FL 作为不同潜在网络攻击的目标。识别和学习不同类型攻击的协作方法可以非常有效地减轻令人生畏的威胁，例如入侵、Dos/DDos、异常等。另一方面，在将 FL 用于实际应用之前，需要解决 FL 典型的新出现的攻击。

A. 面向网络安全的联邦学习

在网络空间的背景下，安全、隐私和信任在文献中得到了广泛的研究。然而，这项调查特别关注的是 FL 环境中物联网环境的网络安全。物联网环境更容易受到不同类型的网络攻击，因此只有通过共享模型更新的 FL 协作学习框架才能有效地增强安全性和隐私性。及时了解和共享不同类型的网络攻击，如欺骗、入侵、异常、DoS/DDoS 等，有助于建立和完善网络防御模型和机制。因此，FL 在设备和网络层面上都有巨大的潜力来有效地保护网络空间。FL 作为缓解可能威胁的解决方案的应用如图 6 所示。

近年来，由于异构传感器设备的空前增长，网络空间变得更加脆弱。由 ML 支持的 IDS 和异常检测器已经成为检测和打击入侵和攻击的强制性工具

表二世
通过调查工程解决问题

Addressed Issues	References	FL	Domain
Security,IDS, IPS	[47]	✗	Smart home
Security, DDoS Resiliency	[48]	✗	IoTs environment
Security, IDS	[5]	✓	IoT network
Malware classification	[49]	✓	Edge devices
Security, IDS	[50]	✓	Network environment
Security	[51]	✗	IoTs environment
Security	[52]	✗	IoTs environment
Security, IDS dataset	[53]	✗	IoT and IIoT
Security,IDS dataset	[54]	✗	-
Security	[55]	✗	IoTs environment
Security, IDS	[56]	✗	VANET
Security, IDS	[57]	✗	Network
Security, IDS	[58]	✗	Network environment
Privacy, Security, IDS	[32]	✓	CPSs
Security, ADS	[59]	✓	SOHO IoTs
Security, ADS	[33]	✗	Smart city IoT
Cyberattacks	[60]	✗	IoTs, CPSs
Cognitive cybersecurity	[61]	✗	CPS-IoT Enabled Healthcare
Privacy, Integrity	[62]	✓	Edge devices
Security, Sybil based poisoning attack	[30]	✓	Edge network
IoT Mirai botnet attack	[63]	✗	IoTs devices
Reliability, Security	[64]	✗	IoTs network
Security, Audit	[65]	✓	Edge network
Security, Trust	[66]	✗	IoTs network
Security	[67]	✗	IoTs network
FL operation, Security	[68]	✓	Overall FL framework (IoTs, Edge cloud, Regional Cloud, Core Cloud)
Privacy, Security, Latency	[36]	✓	IoT edge computing (Connected vehicles)
Jamming attack detection and defense	[69]	✓	UAV
Security, Privacy Throughput, Latency	[37]	✗	IoT network
Privacy, Security, Communication overhead, computational cost	[38]	✗	Fog-based IoT
Gradient sparsification, Accuracy	[70]	✓	IoT edge computing
Security, Intrusion, Privacy, IDS	[31]	✓	IoT devices
Privacy, IDS	[71]	✓	Edge devices
Privacy, Latency, Non-iid	[39]	✓	IoT network
Latency	[40]	✓	IoT network
Learning speed, Accuracy	[46]	✓	Edge devices
Increased accuracy, Convergence process	[28]	✓	Edge devices
Communication, Accuracy	[41]	✓	IoT environment
Efficient communication and training	[26]	✓	IoT environment
Resource constraint, Global aggregation frequency	[27]	✓	IoT environment
Security, Resource constraint	[42]	✗	IoTs environment
Resource constraint	[20]	✓	IoT edge computing
Resource constraint	[43]	✓	WAN
Resource constraint	[44]	✓	IoT edge computing
Privacy, Latency	[72]	✓	Edge network
Non-iid, Accuracy	[29]	✓	Edge network
Resource demand, Scarcity of relevant data, Security, Latency	[73]	✓	IoT Edge network
Privacy, Security	[74]	✓	IIoT
Privacy, Security, IDS, Accuracy	[75]	✓	IoT environment
Security, Data collaboration	[76]	✓	IoT environment
Privacy, Security, Reliability	[77]	✓	IIoT environment
Safety, Resiliency Accuracy, Privacy, Latency	[78]	✓	IIoT environment
Security, IDS, Communication	[79]	✓	IIoT environment

在今天庞大的网络空间中出现的反常现象。在文献中，使用各种 ML 算法(如卷积神经网络(CNN)、非线性自回归(NAR)和 q 学习)的不同方法(如[32]、[58]和[59])被用于设计 idssips，并针对几个基准数据集对其性能进行了测试。大多数致力于设计基于 fl 的安全解决方案的工作主要集中在安全模型的准确性上没有考虑其他重要的性能指标。我们将在下一节中介绍解决性能问题的 FL 工作。

Rahman 等人。[31]提出了一种基于 fl 的自学习 IDS 来保护物联网环境。首先在物联网设备上分布由正常流量和几种攻击类型组成的基准数据集(NSL- KDD)，然后在本地训练和测试基于 ML 的 IDS 模型。该模型

在常规 FL 操作之后发送和汇总更新。该系统达到了接近集中式学习方法的精度。FL 方法成功地创建了一个自学习 IDS，通过该 IDS，终端设备成功地检测到未在其本地数据集中呈现的攻击。这种基于 fl 的 IDS 的优势在于，在实际应用场景中，IDS 能够检测到以前不是由其自身流量生成的入侵。所提出的方法的缺点是，它是在一个非常小的物联网网络环境中进行实验的，除了准确性之外，没有考虑其他性能指标。

在[78]中，通过部署在每个子网的物联网网关上，将协作 IDS (CIDS)开发为智能“过滤器”。每个过滤器的深度神经网络使用位于子网中的本地数据库进行训练，并且从过滤器中学习到的模型被收集并聚合在中央服务器中。在全局知识的补充下，每个过滤器都能够检测和防止实时网络攻击。该模型的性能在多个基准数据集上进行了测试，在检测准确率、网络流量、隐私和学习速度方面，它在 FL 和集中式学习设置中优于几个基线 ML 模型。尽管在几个方面提高了性能，但这种方法只适用于已知的攻击。

[79] 设想了一个使用生成模型的鲁棒的基于 fl 的 IDS。FED-IIoT 是一种用于检测恶意软件的基于 fl 的架构，在参与者端使用生成对抗网络 (GAN) 和联邦 GAN (FedGAN)算法来生成对抗数据并将其注入每个 IIoT 应用程序的数据集中。在服务器端，通过结合防御机制来检测和避免聚合时的异常，确保了训练模型的健壮协作。与现有解决方案相比，所提出的模型显示出更高的准确性，并允许工业物联网环境中参与者之间的安全参与和有效通信。

基于类似的目标，work[32]设计了一个基于 ml 的 IDS 模型来检测工业 cps 环境中的威胁。设计的 IDS 模型被进一步扩展为 FL 框架，以允许多个工业 cps 协作构建一个全面的 IDS。作者通过在实际工业 CPS 数据集上进行广泛的实验，比较了所提出模型与最先进方案的有效性。为了确保联邦模型参数的安全性和保密性，作者为联邦 IDS 引入了基于 Paillier 密码系统的安全通信协议。这项工作的优点是，它使 FL 安全对抗中间人类型的攻击。

为了识别智能家居环境中最关键的网络攻击，[47]首先突出了攻击面，并准备了三个测试用例(测试机密性、身份验证和访问控制)，以发起不同类型的基于网络安全的攻击。然后针对相同的攻击设计和测试 IPS，以验证受影响系统的弹性。

为了在更大的物联网网络中检测网络攻击，一种基于机器学习的网络 IDS (NIDS)能够在分布式雾层中监控智慧城市的所有物联网流量[33]提出。该模型能够很好地检测分布式雾节点上被攻击的物联网设备，并相应地向管理员发出警报。针对 UNSW-NB15 数据集[80]对 NIDS 模型进行了评估，模型的分类准确率达到 99.34%。作者声称他们的方法是独特的，NIDS 模型可以学习正常的流量，并且可以在未来检测到恶意行为。

Sun 等人对传统的 FL 模型进行了扩展。[3]提出了一种分段 FL 框架，用于大规模网络局域网的入侵检测。这种方法不同于传统的基于单一全局模型的协作学习的 FL 模型。该方法保留了多个全局模型，其中每个参与者片段分别进行协作学习，并动态地重新安排参与者的分割。此外这些模型之间相互作用，根据不同参与者的局域网更新参数。作者采用了三种基于知识的方法来标记网络事件并使用数据集训练 CNN。利用 20 个参与者局域网络 2 个月的流量数据集对模型进行了训练和测试，获得了较高的验证精度。与使用单一全局模型的传统 FL 方法相比，分段 FL 框架的优点是能够更好地检测局域网中的入侵。

[56] 提出了一种检测整个 VANET 网络异常行为的 CIDS。CIDS 使用 DL 和 SDN 控制器方法来训练一个可以在 IID 和非 IID 情况下工作的全局 IDS。采用多个 SDN 控制器为整个网络联合训练全局 IDS，而不是直接交换子网流。利用 KDD99 和 NSL-KDD 数据集建立模型并进行测试，以验证 CIDS 对 VANETS 的效率和有效性。该方法的主要突出特点是 CIDS 能够有效地检测整个 VANET 中的入侵，而不像其他方法那样仅局限于局部子网。

为了减轻 Wi-Fi 网络隐私问题，建立了一个联邦 DL 模型[71]，并使用爱琴海 Wi-Fi 入侵数据集(AWID)进行了测试。提出的模型使用一种称为堆叠自编码器(SAEs)的专用深度学习神经网络来捕获异常观测的压缩表示。为了识别新的威胁，联邦模型从新的观察中学习，并更新本地和全局模型。将得到的结果与经典的深度学习模型进行了比较结果表明 FL 模型在分类精度、计算成本和通信成本方面都更有效。这项工作与其他使用专门的深度神经网络的工作不同，它有助于压缩模型参数，这主要有利于减少通信延迟。

为了应对新出现的复杂多态威胁，安全解决方案需要主动识别不可预见和不可预测的网络攻击。为了设计这样一个解决方案，Rege 等人。 [58]扩展了 IDS 以提供对抗性运动的时间预测。该方法采用了四种预测模型，即 NAR 神经网络、外源输入的 NAR 神经网络

(NARX)、用于多步提前预测的 NAR 神经网络和自回归综合移动平均(ARIMA)，并比较了在不同地点收集的两个数据集的结果。该研究确定了五种高级持续威胁的趋势——将会有更多的攻击、更多的混淆、持续的错误归因、从基于机会的攻击到更有针对性的攻击的更大转变，以及从数据操纵到数据加密或删除的更大损害。

出于类似的需求，Vinayakumar 等人。[57]提出了几种实验方法，以确定设计动态 IDS 的最佳算法，该算法可以在主机级别和网络级别有效地检测和预测入侵。作者首先通过选择 dnn 的最优网络参数和网络拓扑，针对公开可用的基准恶意软件数据集(KDDCup 99)对各种 dnn 进行了实验。然后使用其他恶意软件数据集 NSL-KDD、UNSW-NB15、Kyoto、WSN-DS 和 CICIDS 2017 对表现良好的 dnn 进行测试，以设置基准。采用类似的方法来识别性能良好的经典 ML 分类器，并将其性能与 dnn 进行比较。性能评估表明，dnn 优于经典 ML 分类器，最后，作者利用性能更好的 dnn 设计了一个高度可扩展的混合 dnn 框架，称为 scale-hybrid-IDS-AlertNet。所提出的入侵检测系统不仅能够有效监控实时网络流量和主机级事件，而且能够主动预警可能的网络攻击。

文献[59]提出了一种联邦自学习异常检测和预防系统，能够检测和预防物联网网络中出现的和未知的攻击(DÏoT)。在没有人为干预的情况下，DÏoT 构建特定于设备类型的通信配置文件，最终用于检测设备通信行为中的异常。安全网关采用这样一种方式，即每个网关被分配监视一种特定设备类型的流量。 然后使用收集到的流量数据来训练每个网关的本地模型，并将训练的模型参数发送到物联网安全服务进行聚合。物联网安全服务被用作特定于设备类型的异常检测模型的存储库，在后期还用于聚合从安全网关接收的所有更新。

Pang 等人。[50]提出了一种基于学习代理的联邦网络流量分析引擎(FNTAE)，用于实时检测网络入侵。为了检测新攻击导致的异常流量，该模型利用增量学习代理驱动的分析引擎实时捕获攻击特征。与集中式分析系统相比，FNTAE 系统表现得很好，但是，它只适用于对抗已知的攻击。

为了确保物联网环境的安全，一些工作也采用了其他方法。[51]中提出的工作提出了中间人物联网计算工具(MIMIC)，该工具利用中间人攻击概念将 MIMIC 部署为物联网网络的雾计算代理。 MIMIC 部署在物联网网络的边缘节点，能够嗅探、捕获和重放来自物联网的所有传入数据包设备。MIMIC 然后创建一个虚拟层，用于保存所有传感设备的虚拟化，并且允许远程用户仅在虚拟空间上进行查询，从而禁用对物理设备的直接访问。 Zarca 等人。[52]提出了一种利用 SDN 和 NFV 部署物联网蜜网的新方法，以分散网络攻击者并使物联网系统安全。物联网系统的管理员可以通过 SDN 控制器定义的高级安全策略和 NFV 管理和网络编排，将物联网物理架构复制到虚拟环境中作为 vnf，将物联网网络作为服务部署。该模型在 H2020 欧盟项目前提下的测试平台上进行了实验，成功地对网络流量进行了动态过滤、丢弃和分流，并根据新部署的 vIoTHoneyNets(虚拟物联网蜜网)需求调整了网络行为。

还有其他重要的研究来研究网络攻击并建立相应的网络防御机制，这些机制使用不同的方法，利用各种数据库、API、平台、框架和 ML 算法。例如，在[49]中开发了一个恶意软件分类原型，并使用 FL 模型方法进行分散的数据收集和共享。利用虚拟 api 获取的 10 907 个恶意软件数据集对模型进行训练和测试。作者在联邦设置中使用 SVM 和 LSTM ML 算法，在恶意软件分类上取得了较好的结果。在[48]中，通过集成其他框架和工具，开发了一个名为 DRAFT 的框架，以提高端到端物联网平台抵御网络攻击的弹性。所提出的模型被集成到物联网平台中，并使用 Fed4FIRE+联合测试平台对五种已知的模拟网络攻击进行了测试，并证明了所测试的物联网平台的网络攻击弹性有所提高。[69]提出了一种自适应联邦强化学习方法来对抗无人机的干扰攻击。该模型利用无模型 q 学习和 CRAWDAD 数据集，在新探索的环境中学习干扰防御策略。论文[60]研究了大数据物联网和 CPS 背景下的网络安全问题。调查和分析了与 CPS 相关的网络安全问题和漏洞，以查明可能的网络攻击。作者还提出了减轻这些攻击的技术方法。Abie[61]提出了一种认知网络安全的四层架构，以对抗智能 CPS-IoT 医疗环境中的动态和自适应攻击。提出的概念架构旨在模仿人类的认知行为，以预测和应对智能医疗领域中新兴的网络威胁。在另一项为物联网设备提供网络安全的工作中[42]，作者提出了一种方法，将[81]中开发的可信网络边缘设备(NED)作为物联网通信的代理服务。为了保护物联网设备，用户可以通过 NED 一次为多个物联网网关和终端设备轻松高效地设置安全解决方案和策略。建议的方法在 VTT 奥卢场地的公司场景中进行了实验。[67]中提出的一项工作强调了文献中采用的几种硬件辅助技术，这些技术可用于增加另一层保护以对抗物联网领域的网络攻击。 本文还探讨了

硬件解决方案在成本、性能、安全性和实际场景中采用的挑战方面。

为了提高物联网环境中的安全性和可靠性，文献[64]提出了一种可靠高效的集群技术(REACT)。在 REACT 中，提出了一种有效的簇头选择算法和能量均衡路由算法，并针对现有协议 HEED 和 LEACH 进行了估计参数的仿真，比较了吞吐量、网络寿命、剩余能量和可靠性。本文还提出了一种选择攻击点的网络黑客技术策略，以改进网络安全设计。为了促进有效入侵检测系统的设计并对其进行适当的评估，一些工作致力于填补基准入侵数据集可用性的空白，以测试支持入侵检测系统的物联网系统。[53]中提出的工作提出了一个新的数据驱动的物联网/工业物联网(TON_IoT)数据集，其中包含物联网/工业物联网服务的遥测数据、操作系统日志和物联网网络流量，这些数据集从澳大利亚新南威尔士州堪培拉大学网络范围和物联网实验室的中等规模网络的实际表示中收集。TON_IoT 还包含标签和类型特征，表明适合 IoT/IIoT 应用的多分类问题的多个类和子类。将该数据集的特征与其他现有数据集进行比较，以显示其优越性。在另一个例子中，Sharafaldin 等人。[54]产生了最流行的入侵数据集之一，名为 CICIDS2017，它包含了一组重要的特征，符合现实世界的标准。生成的数据集被完全标记为包含 80 多个网络流量特征，并满足所有要求的标准，包括常见的更新攻击，如拒绝服务(DoS)， DDoS，暴力破解，XSS, SQL 注入，渗透，端口扫描和僵尸网络。

在本节中，我们讨论了几种现有的设计网络安全模型的方法，特别是针对物联网环境和 FL 设置。探索了许多 ML 算法、区块链、网络虚拟化、SDN、集群方法等，旨在设计一种有效的网络防御机制，以检测和预防不同类型和规模的物联网网络中的入侵、异常、Dos/DDoS 和其他攻击。

B. 面向联邦学习的网络安全

我们介绍了几个工作，讨论 FL 作为不同类型的安全和隐私问题的有效解决方案。然而，这种新的学习架构引发了一些新颖的攻击。在 FL 设置中，虽然数据驻留在终端设备本地，客户端和服务器之间仅交换 ML 参数，但仍然容易受到各种攻击。我们首先讨论了针对 FL 的不同类型的攻击，然后介绍了研究中提出的缓解策略。

参数中毒(或模型中毒)和逆向工程 ML 攻击是 FL 中的一些严重威胁，也是一个活跃的研究领域(例如[30]，[82]-[84]和[74])。FL 中的典型攻击可以是基于数据的攻击，也可以是基于模型的攻击(如图 5 所示)，可以通过锻造本地来实现

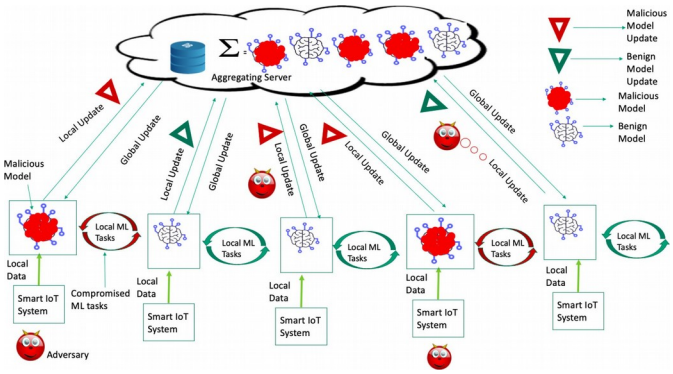


图 7 所示。FL 中的攻击场景。

终端设备数据或客户端或服务器端的模型参数。攻击者如何在 FL 中执行不同的攻击如图 7 所示。 如上所述，攻击者可以控制物联网设备/网络来破坏本地数据和/或本地 ML 任务以生成有毒模型。在其他情况下，攻击者可能会执行中间人攻击来伪造传输中的模型更新，或者只是偷听通信以泄露用户的隐私。

FL 中的攻击不仅会降低学习模型的质量，还会暴露用户的隐私。对手可以通过欺骗用户设备发送的模型更新来泄露用户的隐私。此外，如果对手获得了聚合服务器的控制权，他/她可以全面了解设备更新参数的历史和全局模型的结构。 有了这些信息，攻击者可以通过逆向工程揭示设备的隐私。

随着对模型更新的访问，一些作品展示了使用 GAN 生成看起来与训练图像相似的图像(例如，[85]和[86])。将私有信息的泄漏扩展到下一个层次，Zhu 和 Han[87]证明攻击者可以在几次迭代中从共享模型更新中完全窃取私有训练数据。为了实现这一目标，作者首先生成了一对虚拟输入和标签，并用于根据共同的训练过程生成虚拟梯度。他们没有优化权重，而是优化虚拟输入和标签，使虚拟梯度和真实梯度之间的距离最小，成功地揭示了训练数据的完整。此外，由于中央服务器的完全控制，攻击者可能伪造全局模型，从而可能影响终端设备的本地模型。实际上，汇总这些模型的局部更新可能会显著降低全局模型的质量

即使攻击者无法控制终端设备或服务器，在客户端和服务器之间的传输过程中，模型参数仍然可能被伪造。

另一方面，FL 也容易受到通过终端设备执行的数据中毒和模型中毒攻击。如果攻击者获得对终端设备的控制，他/她可能会在本地模型训练过程中伪造本地数据和/或伪造模型更新，目的是创建一个有偏见的模型。偏置模型的参数反过来可能会影响全局模型的质量。这个问题

在拜占庭问题[88]和 Sybil 攻击[89]的情况下变得更糟。[14]中提出的一项调查对 FL 的威胁进行了分类和讨论，并提出了创建稳健 FL 框架的未来研究方向。

标签翻转攻击是一种最常见的数据中毒攻击，它将一类训练样本的标签更改为另一类(保持样本的特征不变)，以迫使模型预测错误的标签。Fung 等人。 [30]演示了标签翻转攻击，将训练数据集中的标签 1 s 翻转为标签 7s，使模型错误地将 1 s 分类为 7s。在另一种形式的数据中毒攻击中，攻击者可能会改变原始训练数据集的单个特征，从而在模型中植入后门[14]。后门攻击背后的一般方法是将全局模型替换为攻击者的模型，并迫使其对特定子任务进行错误预测，例如，强迫图像分类器将绿色汽车错误地分类为青蛙[90]。 一旦感知到全局模型状态的估计，攻击者就可以用一个简单的权重重新缩放操作来替换模型[91]。Bagdasaryan 等人。[90]通过在数据中注入一定的模式，并改变目标的标签，从而误导全局模型，展示了后门攻击。攻击场景由一个或多个恶意参与者组成，这些参与者在后门数据上进行训练，然后将模型更新共享给服务器进行聚合。

数据中毒最终会毒害模型更新，然而，攻击者可以直接操纵训练过程而不毒害训练数据，需要注意的是，这种形式的模型中毒被认为比数据中毒更有效。Bhagoji 等人。[82]证明了使用模型中毒攻击，考虑一个单一的、非串通的恶意代理，其对抗目标是导致 FL 模型以高置信度对一组选择的输入进行错误分类。为了使目标误分类有效，作者采用了恶意代理的更新提升和交替最小化策略来交替优化训练损失和对抗目标。在另一个例子中，Blanchard 等人。[92]考虑到全知攻击(对手意识到梯度的良好估计)，表现出模型中毒，对手通过乘以负常数发送相反的更新向量来逆转梯度下降的方向，从而降低模型性能。此外，Baruch 等人。[93]证明了在非知识攻击场景中，通过引入即使是很小但精心设计的梯度变化，拜占庭攻击的模型投弹仍然是可能的。

分布式环境中的拜占庭容忍学习已经在一些作品中得到了解决(例如，[86]和[94]-[97])，其中大多数假设参与者的数据是 id 的，未修改的，均匀分布的。然而，在 FL 中，数据分布不同，解决方案并不完全适用。Bagdasaryan 等人。 [90]利用了[86]、[95]和[97]中提出的解决方案，能够部分减轻攻击，但这也以牺牲全局模型的准确性为代价为了解决模型中毒问题，Fung 等人。 [30]首先通过实验证明了 FL 对基于 sybil 的中毒攻击的脆弱性，并提出了一个 FL 模型 FoolsGold，该模型基于分布式学习过程中客户端更新的多样性来识别这种攻击。这个模型甚至有效防止 Sybils 损害诚实用户。与之前的方法相比，该系统的优点是它不受攻击者预期数量的限制，它不需要学习过程之外的额外信息，并且它对客户端及其数据的假设更少。然而，对抗单个客户机对手和改进模型以对抗知情攻击是该模型的一些局限性。

Blanchard 等人。[92]首先证实了联邦平均老化(FedAvg)不抵抗拜占庭攻击，然后提出了一种拜占庭容忍聚合规则 krum 来解决模型中毒攻击。考虑到在一轮通信中 n 个参与*者*中有 f 个拜占庭攻击者，krum 首*先*计算最接近模型更新 δi 的 n-f -2 更新*的*两*两*欧几里德距离，然后计算 δi 与*其*$_{最}$*近*的 n-f -2 更新之间的距离平方和。最后，算法通过最小和的模型更新来更新全局参数。 这背后的想法是选择一个向量，以某种方式最接*近* n 个工人，并保证收敛，无论 f 个*拜*占庭攻击者。

[98]中的一项工作提出了一种不考虑拜占庭工人数量限制的聚合规则，但仍然表现出更好的收敛性。该方法使用随机一阶预言器计算每个工人的分数以确定其可信度。服务器根据估计的损失函数下降和大小对每个候选梯度估计器进行排序。然后计算得分最高的几个候选点的平均梯度服务器将梯度的真实值与平均梯度进行比较，以确定更新是否有害。

Sun 等人。[99]研究了 FL 在数据投毒攻击中的漏洞，设计了一个自适应任意选择目标节点和源攻击节点的双层优化框架来计算最优投毒攻击。利用数据收集过程，攻击者可以直接向所有目标节点注入有毒数据。在无法直接攻击的情况下，作者还考虑了利用通信协议间接将数据投毒到目标节点的方法。这项工作突出了与 FL 相关的挑战，攻击者可以利用通信协议为午餐数据中毒攻击打开后门。为了采用 FL 作为可能的网络安全解决方案，应该建立一个网络安全机制来对抗 FL 中可能存在的威胁。因此，我们还讨论了一些研究工作，提出了针对 FL 中存在的潜在威胁的网络安全解决方案。

为了解决[100]中的后门攻击，作者提出了使用规范裁剪和差分隐私的防御方法。规范裁剪被认为是对抗增强攻击，这可能会产生大规范的更新。该方法通过忽略范数高于某个阈值范数的更新来为梯度更新的灵敏度设置一个界限。此外，作者还使用差分隐私通过在更新中添加高斯噪声来补充范数裁剪，以减轻对手在范数裁剪之外的影响。

在 FL 中，如果攻击者无法控制客户端，仍然很有可能“中间人”

攻击。他/她可以偷听模型更新以揭示客户端的隐私，甚至可以在传输过程中伪造模型更新。为了解决这种攻击场景，差分隐私[77]、同态加密[101]、[102]、安全函数评估或多方计算[103]等技术也被应用于 FL 之上。由于在共享模型更新中添加了噪声，差分隐私可以有效地保护客户端的隐私，因此，miti 门逆向工程攻击，而其他方法甚至可以减少在传输过程中操纵模型更新的任何机会。然而，与差分隐私方法相比，这些方法增加了计算和通信负担。Geyer 等人。[104]提出了一种客户端差分隐私保护联邦优化算法。结果表明，当有足够的客户参与时，可以隐藏客户的参与，但代价是模型性能的轻微损失。Zhang 等。[105]也使用差分隐私方法来保护患者隐私免受可能的逆向工程攻击。

Zhu 和 Han[87]首先演示了逆向工程攻击，然后提出了一些防御策略。实验了在共享前在梯度上添加噪声、梯度压缩和稀疏化等方法，以观察其对信息泄漏的性能。al - marri 等人通过保护终端用户的隐私来解决逆向工程攻击。[75]采用模仿学习方法[106]在 FL 场景中工作。模仿学习采用了学生和老师两种学习模式。 学生模型使用公共数据集进行训练，而教师模型使用敏感用户数据进行训练。然后，使用教师模型对公共数据集进行标记，然后使用公共数据集创建学生模型，并将其发送到集中式服务器以生成新的全局模型。在不泄露任何敏感信息的情况下，将知识从教师模型转移到学生模型，以保护学生模型免受逆向工程攻击。

为了通过保护客户端和聚合服务器之间的参数交换来加强隐私，[同]态加密是可以直接对加密参数执行聚合的技术之一。这种方法允许在不暴露模型更新的情况下进行聚合从而保护 FL 免受任何类型的欺骗或模型更新的操纵。考虑到这种方法的计算和通信开销，Zhang 等。[101]提出了一种高效的同态解决方案 BatchCrypt。为了应用这一解决方案，首先，开发了新的量子化和编码方案以及梯度裁剪技术。在此之后，不再对单个梯度应用同态加密，而是使用 BatchCrypt 对一批编码的量化梯度进行加密。BatchCrypt 在训练和减少通信开销(与加密每个梯度相比)方面表现出显著的加速，而准确性的损失可以忽略不计。

同态加密是一种特殊的加密形式，它允许在不需要解密密钥的情况下直接对加密数据进行特定类型的操作。解密时的加密结果确认了对明文执行操作的结果[107]。

此外，近年来，区块链技术(BC2)因[其]去中心化、可审计、安全和隐私保护等特点，被广泛应用于许多应用领域。因此，一些研究工作(例如[76]和[77])也将区块链纳入了 FL 设置。 为了减轻共享梯度时泄露敏感信息的影响以及恶意服务器伪造聚合梯度的可能性，[74]提出了可验证的梯度(VFL)。该方法采用拉格朗日插值和设置插值点来验证聚合梯度的完整性。 VFL 的主要优点是它使每个参与者能够验证聚合参数。此外，无论参与者的数量如何，验证开销也保持不变。考虑到操作和安全，赵等。[68]通过添加安全域和加密基础设施来设计 FL 平台的通用框架，以在联邦通信方之间建立可信连接和交互。对于类似的目标 Ma 等。[109]强调了 FL 中最常见的问题，如收敛、数据存储、缩放、安全模型聚合和隐私视角，并通过仿真结果提出了潜在的解决方案。

加密方法已被广泛采用为交换信息和认证的方法，以提供安全性和信任。为了在欧盟网络安全法之后促进网络安全认证信息的可信共享，[55]中的工作提出了一个通用的区块链平台，丰富了智能合约，作为权威设备信息的注册表。智能合约存储信息，如制造商名称、联系信息、身份证书、设备类型、设备 id、最新固件版本和哈希/指纹，以及描述典型网络交互的制造商使用描述(MUD)文件，该文件发布在链下数据库和其他数据库中。拟议的区块链为任何电子产品、服务或流程提供可信的网络安全认证信息交换。作者通过展示一个案例研究来验证所提议的工作，他们使用 SDN 控制器从设备注册表智能合约中检索 MUD 文件。为了确保物联网设备与边缘节点之间的通信和数据传输安全，Gyamfi 等。[45]提出了基于椭圆曲线加密(ECC)的轻量级加密方案，嵌入物联网和边缘设备。所提出的方法由三层组成，包括传感器和执行器(第 1 层)、物联网边缘(第 2 层)和云(第 2 层)，其中包括密钥生成在内的大部分计算都发生在第 2 层，以减少物联网边缘的计算开销。IoT 边缘层提取服务器发送的公钥，并在需要时更新到 IoT 设备。通过配置 IoT 边缘和 docker 对所提出的方法进行了模拟，观察结果表明，加密的运行时间缩短了，资源需求也减少了。VerifyNet[62]利用 a

2 区块链技术是一个去中心化的分布式网络，它使用公钥加密、分布式数字账本和共识算法作为核心组件，用于创建一个安全、透明和可审计的网络，允许人们/设备在不存在任何中介的情况下以不可信的方式进行通信[108]。

密钥共享策略和加密，保护工作流中用户局部梯度的隐私

此外，该模型使用 CNN 网络与修改后的美国国家标准与技术研究所(MNIST)数据库来测试模型的分类精度。模型对服务器返回的结果的正确性进行分类。此外，它还允许用户在培训过程中离线。

在当今世界，基于云服务的体系结构是必要的，也是占主导地位的计算服务。与服务提供者相关联的操作和通信必须是安全可靠的。为了评估基于云服务的物联网架构的安全性和声誉，Li 等人。[66]提出了一种新的信任评估框架。该框架集成了安全和基于声誉的信任评估方法，对云服务的信任进行评估。将客户对云服务可信度或云服务质量的反馈评级纳入框架。在性能评估方面，构建了基于安全性的测试评估(SeTA)和基于声誉的测试评估(ReTA)两部分的评估框架并进行了测试。SeTA 使用封装安全指标的合成数据集进行测试，而 ReTA 使用 WSDream 数据集进行测试;结果表明，该框架能够高效地评估云服务的可信度，优于其他信任评估方法。

[76]中提出了一个由私有数据中心、公共数据中心和物联网环境区块链技术组成的安全数据协作框架(FDC)。私有数据中心的作用是处理数据治理、数据注册和数据管理而公共数据中心的作用是促进多方安全计算。区块链技术用于提供可审计的多方交互。该框架在 FL 设置中实现，以解决诸如安全和机密存储、安全共享和有效管理、数据行为的可追溯性和审计、有效授权等问题。在另一个例子中，PriModChain[77]结合了支持差分隐私的 FL、区块链和智能合约，以确保 IIoT 环境中的隐私、安全性、可靠性、安全性和弹性。

为了充分保护终端用户的隐私，安全多方计算(MPC)[3]方法[也]被用于 FL。Fereidooni 等人。[111]使用 MPC 执行安全 FL 聚合，其中聚合服务器不能访问客户端的模型更新以及任何中间全局模型。为了安全地交换模型更新，客户端使用多方加密方案来加密它们的更新。此外，为了访问全局模型，客户端使用其密钥共享解密全局更新。培训后客户端对本地更新进行加密，并将其发送到服务器进行聚合。

尽管有几项研究努力使 FL 免受攻击者控制终端设备和/或在网络中行动

安全多方计算是一种加密协议，它使互不信任的各方能够交互并计算一个联合函数，其中任何一方都不能看到其他方的数据[110]。

中间，FL 仍然容易受到集中式服务器故障的影响。 攻击者可能危及聚合服务器或服务器本身可能采取恶意行动有偏见的服务器可能会操纵聚合过程并偏袒某些客户端。考虑到这些可能性，一些研究(如[112]和[113])建议使用区块链技术，将所有 FL 操作委托给终端设备，以消除集中式服务器。通过这种方法，充当区块链网络矿工的终端设备收集模型更新，验证它，最后执行聚合。这种方法解决了几个安全问题，但仍然无法解决客户机本身可能是恶意的情况。此外，区块链方法涉及高计算和通信要求，因此如果终端设备资源受限，它可能不适用。

充分保护 FL 是一个巨大的挑战，它仍然是一个开放的研究课题。加密方法在安全交换模型更新和保护隐私方面非常有用，但是，如果客户端的隐私被完全保护(即使是对聚合服务器)，则很难检测恶意模型更新并采取适当的措施来对抗串通攻击。 一种方法不足以解决与 FL 相关的所有安全问题。探索上述不同方法的组合可能是解决 FL 中存在的安全问题的潜在解决方案。

IV. 资源约束、沟通延迟和模型准确性

由于其分散的安全计算模型，我们已经见证了区块链最近的成功。在类似的意义上，由于其保护隐私的分散学习模型，FL 研究正在迅速发展。然而，FL 的真正成功取决于它的核心挑战，这些需要解决它的适用性。FL 框架不仅要安全，而且要足够高效和准确。阻碍 FL 性能的核心挑战是昂贵的通信、系统异构和统计异构。在本节中，我们将讨论一些解决这些挑战的研究。在 FL 设置中，更新的模型参数在终端设备和中央服务器之间定期交换，这会导致联邦网络性能的主要瓶颈。为了减轻这种通信开销和减少延迟，文献中已经研究了诸如压缩(例如[39])、聚类(例如[40])、优化全局联邦学习(例如[26])、时间等方法。减少延迟的方法可能会影响学习模型的准确性。一些工作也涉及到保持或提高准确性，在大多数情况下，所提出的解决方案的准确性已经通过比较来验证他们使用集中式模型。

为了减少 FL 中的通信开销，Sattler 等。 [39]设想了一种压缩方法，并提出了一种新的稀疏三元压缩(STC)框架。该框架是通过扩展现有的 top-k 梯度稀疏化压缩技术而*创*建的。作者采用了一种机制，使下行压缩作为三化和最优 Golomb 编码。的

作者通过四种不同的学习任务对所提出的框架进行了实验观察到 STC 在高频和低带宽通信的常见 FL 学习场景中表现良好。通过压缩提高通信效率，从而减少通信消息的大小，Lu 等。[72]设计并改进了梯度压缩算法，在精度仅降低 0.03%的情况下，实现了原通信时间的 8.77%。这种保护隐私的边缘异步 FL 机制采用边缘网络中离散节点的协作学习，同时保证了局部信息的隐私。本文还研究了异步 FL，以更好地处理边缘节点的不同特性。在 FL 中应用高比率稀疏化的同时保持精度，Li 等。[70]提出了一种用于自适应优化器的通用梯度稀疏化(GGS)框架。该框架由梯度校正和批归一化(BN-LG)组成，分别在很大程度上保持收敛性和最小化延迟梯度对训练的影响。一些研究人员通过调整全局模型的聚合来解决通信开销问题。然而，Hsieh 等人。[26]仅在全局模型的权重相差一些经验选择的阈值时才使用全局模型聚合的方法。与[26]中定义的目标和方法相似，[27]中提出了一种寻找全局聚合频率的控制算法。在理论分析的基础上设计的控制算法实时动态学习系统和数据特征，根据可用资源找到合适的聚合频率，从而提高学习精度。

非 iid 数据在 FL 网络中的分布可能会影响全局模型的质量。 为了解决这一问题，Yao 等人。[28]采用局部和全局模型聚合的特征融合方法。该模型优于基线 FL 模型，具有更好的精度，对新传入客户端进行初始化，加快了收敛过程。Wang 等。[44]提出了一种控制算法，可以在 FL 中局部更新和全局参数聚合之间进行最佳权衡，以在给定资源预算下最小化损失函数。考虑到统计异质性的影响，work[29]提出了一种新的 FMTL 框架，该框架基于具有联合可训练数据分布的 FL 表面的几何属性形成客户端集群。这种聚类方法在客户端的本地数据是分布式且非 iid 的 FL 场景中提供了更好的结果。与现有方法相比，该方法的优点是它可以与现有的 FL 通信协议一起工作，并且也适用于一般的非凸目标。此外，关于许多集群的信息不需要事先知道。

聚类方法也被寻求作为解决一些 FL 问题的解决方案。[40]中的一项工作提出了一种聚类方法，在密集的设备之间形成集群。然后选择一个簇头，它负责启用自组织 FL。在选择簇头时，考虑了电池寿命、计算资源和更好的连接(与其他设备)参数。然后，集群头充当中央服务器并执行以下操作 FL 的聚合任务。作者还提出了一种启发式算法来优化全局 FL 时间。为了快速收敛模型，work[46]使用基于区块链的方法选择节点子集来更新全局模型中的两种类型的权重。一个子集根据其局部学习精度更新权重，另一个子集根据其参与频率更新权重。在[36]中，提出了一种联邦克隆模型，用于车联网网络的边缘工作。使用参数化的 EdgeServer 来协调分布的参与车辆。每辆车都用自己的私人训练数据本地训练自己的学习模型。经过一个 epoch，每辆车将参数的当前值推送给参数 EdgeServer, EdgeServer 通过计算加权平均值将分布在不同车辆上的所有这些参数聚合起来。对于下一个 epoch，每辆车从 EdgeServer 中提取更新后的参数作为当前参数，并重复该过程。如果一辆新车加入网络，它将从参数 EdgeServer 中提取当前聚合的参数，作为其初始参数用于训练。遵循异步通信而无需停止和等待其他车辆完成一个 epoch 减少了延迟。系统异质性是美联储面临的大问题之一有价值的网络，不容忽视。Ren 等人。[20]结合了 FL 和数据卸载的思想来缓解物联网设备的限制和挑战。对于密集的计算任务，物联网设备将数据卸载到边缘节点，从而节省能源并提供所需的服务质量。在物联网设备上部署了多个深度强化学习(DRL)代理，以根据物联网系统的动态工作负载和无线电环境协助卸载决策。使用 FL 在分布式设置中训练 DRL 代理，并进行实验以验证使用数据卸载和 FL 的边缘计算支持的物联网系统的有效性。

一些作品采用了由边缘节点组成的基于区块链的联邦模型架构。“FLchain”[65]将用于每个全局聚合的本地参数存储在通道特定分类账的块中，以增强安全性和审计跟踪在 FLchain 中，对于每一个新的全局学习模型，都会创建一个新的通道。然而，该模型的局限性在于区块链模型不使用参与节点的奖励机制，终端设备不直接参与 BC，实际上，边缘设备代表这些设备完成所有交易。此外，该模型没有考虑通信延迟、终端设备的计算和存储能力。Doku 和 Rawat[73]提出了 iFLBC:FL 和基于区块链的 ML，将边缘人工智能带到终端设备。为了缓解数据的稀缺性，一个经过训练的联邦共享模型存储在区块链中，该模型使用称为共同利益证明(PoCI)的机制来分离相关和不相关的数据。

V. 机器学习模型、算法和技术

在本节中，我们将重点介绍表 III 中调查研究中使用的所有 ML 模型、算法和技术。除了这些信息，我们还提供了有关进行仿真的工具和环境的信息

表 3
机器学习模型，算法和技术在最先进的研究工作中使用

Model	FL	ML Models, Algorithms, Technology	Tools and Environment
[45]	✓	SVM	CORE/EMANE Network emulator, TensorFlow
FoolsGold [30]	✓	Softmax classifier, SqueezeNet1.1,	FL prototype using python, VGGNet11
[44]	✓	Squared-SVM, linear regression, K-means, DCNN	Raspberry Pi, Laptops
[49]	✓	SVM, LSTM	virustotal api
PAFLM [72]	✓		GPU server,PCs
[31]	✓	three-layer MLP, threshold gradient compression IDS	Simulated using Raspberry Pi devices
DeepFed [32]	✓		CPU,GPU,Keras API, Flask
FNTAE [50]	✓	CNN-GRU,IDS, Paillier cryptosystem RNN	Simulated on workstations
DIoT [59]	✓		Simulated using IoTs and Gateways
VerifyNet [62]	✓	CNN, DNN,GRU,IDS	PCs
VFL [74]	✓	Lagrange interpolation, MLP, CNN Elliptic Curve	Simulated using PCs and Alibaba cloud
[75]	✓	MLPs	Tensorflow, Keras
FDC [76]	✓	DNN, blockchain	Libra, Tensorflow
PriModChain [77]	✓	DNN, Blockchain,Smart contract, Differential privacy	Python, Ethereum, Ganache, Kovan, Scyther
FED-IIoT [79]	✓	GAN	Tensorflow, Keras
[3]	✓	CNN	Simulated at LAN-security Monitoring Project
Gaia [26]	✓	GoogLeNet-CNN,	Amazon-EC2, Emulation-EC2
[27]	✓	SVM, CNN, linear regression, K-means	Simulated using Raspberry Pi and laptops
[52] [109]	✓	CNN	✗
[69]	✓	Q-learning	Ns-3 for mobility
[71]	✓	SAE	LEAF
[28]	✓	CNN	✓ [114]
ASTW_FedAVG [41]	✓		Simulated with designed framework
FLchain [65]	✓	Linear regression CNN LSTM	✗
[78]	✓	DNN	Simulated with designed framework
STC [39]	✓	sparse ternary compression, LSTM, LR, VGG11	Simulated with designed framework
CLONE [36]	✓	LSTM	
[20]	✓	DRL	Intel FogNodes and Jetson TX2 IoTs
iFLBC [73]	✓	ML, Blockchain	Simulated with designed framework
[46]	✓	MLP	Simulated with designed framework
DRAFT [48]	✗	-	Fed4FIRE+federated testbeds
[68]	✓	✗	Theoretical concept only
[40]	✓	clustering algorithm	✓
CFL [29]	✓	DCNN, DRNN, clustering	Simulated with designed framework
[70]	✓	CNNs-LeNet-5, DenseNet-121, CharNet, AlexNet	Simulated with designed framework

出去了。我们的调查主要集中在物联网环境的网络安全，重要的是使用 FL。基于所提出作品的性质和复杂性，作者采用了各种 ML 模型。本节的唯一目的是向读者提供有关被调查作品所使用的各种 ML 模型、算法和技术的趋势的信息，以及评估所提议作品的工具和环境。

对于所有提出的工作，作者采用了各种 ML 模型，如神经网络，支持向量机，线性回归，q -学习等。FL 本身就支持隐私和安全性(与集中式学习相比)，但为了加强这些，一些作品还使用了椭圆曲线加密、差分隐私、区块链等。大多数的研究都将 cnn 作为他们的机器学习模型。cnn 的不同变体，如 LeNet、AlexNet、GoogLeNet、VGGNet 等，已经被使用。LSTM(一种循环神经网络)和 mlp(一种前馈神经网络)也被一些研究使用。一些工作采用了多个 ML 模型，并比较了结果来验证他们提出的模型。

VI. 用于评估学习模型的流行数据集

由于与物联网和网络物理系统相关的几个挑战，如第 1 节所述，这些系统近年来一直是各种网络攻击的主要目标。由于通过物联网网络的大量数据流，数据驱动的复杂异常检测系统对于检测此类攻击是必要的。 一个更好的系统需要足够的高质量网络数据来学习被入侵网络的模式目前已经有几项工作产生了真实的数据集，可以用来训练和测试 IDS。此外，还致力于创建数据集来评估 FL 模型的性能。因此，在本节中，我们根据表 IV 中提出的工作使用的数据集对研究工作进行分类。这种分类提供了关于本文中考虑的几项工作所使用的最常见数据集的概念。我们还讨论了这些数据集是什么以及它们包含什么内容，以便研究人员根据自己的需要选择数据集。

表 4
网络安全领域的各种研究工作使用的数据集列表

Dataset	Dataset used in References	Federated Learning
NSL-KDD	[31], [75]	√
AWID [115]	[71]	√
MNIST [116]	[27], [43], [46], [62], [74], [109]	√
MNIST, CIFAR-10 [117]	[72][29][28]	√
MNIST,HAR [118]	[41]	√
MNIST,HAR [119]	[26]	√
ImageNet	[39]	√
CIFAR,KWS [120],MNIST	[30]	√
MNIST, VGGFace2 [121], KDDCup , Amazon reviews [122]	[44]	√
MNIST, MNIST-F, CIFAR-10	[70]	√
MNIST, CIFAR-10,ImageNet [123]	[50]	√
KDD99 [122]	[56]	
KDD99 , NSL-KDD	[59]	√ ✗
Mirai [124]	[57]	
KDDCup 99 ,NSL-KDD, UNSW-NB15 [80], Kyoto, WSN-DS, CICIDS 2017	[79]	√ ✗
Drebin, Genome, Contagio	[76]	√
Wearable sensor data collected at kindergarten	[48]	
Fed4FIRE+federated testbeds [125]	[78]	√ ✗
KDD, NSLKDD, UNSW-NB15, N-BaIoT	[49]	√
virustotal api		

KDDCup99[126]和 NSL-KDD[115]是比较流行的入侵检测数据集，它们都包含如下 5 个主要的入侵类别。

1) *正常:* 没有网络入侵。
2) *拒绝服务:* 由于信息和请求过多而使网络资源不可用。
3) *远程用户(R2L):* 一种涉及从远程计算机对用户计算机进行未经授权访问的攻击。
4) *用户到根攻击(U2R):* 入侵者以合法用户的身份访问网络。
5) *调查:* 扫描网络，找出弱点。

kddcup99 是 1999 年创建的入侵数据集，目的是提高入侵防御系统的能力。 KDDCup99 的训练集包含 3 925 650 条攻击记录，其中只有 262 178 条是不同的，而测试集包含 250 436 条攻击记录，其中只有 29 378 条是不同的。在正常交通数据的情况下，训练集共包含 972 781 条记录，其中有 812 814 条不同的记录，同样，在测试集中，60 591 条记录中有 47 911 条记录是不同的。 NSL-KDD 是 2009 年创建的 KDDCup99 的子集，用于纠正与 KDDCup99 相关的低效率。KDDCup99 的主要问题是它包含大量冗余记录，这使得学习模型倾向于更频繁的记录[115]。

京都 2006[+7]是另一个 NIDS 评估数据集，该数据集是通过处理部署在京都大学五个不同网络(内部和外部)的 348 台摄像机收集的数据而产生的。实机和虚拟机，包括两个黑洞传感器和 318 个未使用的 IP 地址，被实现为蜜罐，以捕获三年(2006-2009)的真实网络流量数据。在此时间范围内，共收集了 50 033 015 个正常会话，42 617 536 个已知攻击会话和 425 719 个未知攻击会话，并对其进行进一步处理，提取了 24 个特征，其中 14 个特征来自 KDDCup99 数据集。

VirusTotal API[128]是一种网络威胁扫描服务，允许用户在线分析文件或 URL 地址。它包含大量的分析程序，包括反病毒应用程序引擎和网站扫描程序，来自 60 多个安全供应商。 通过 VirtusTotal 服务，用户可以对提交的文件或 url 获得完整的分析报告，如果需要，还可以获取以前的分析报告。VirusTotal API 以 JSON 对象的形式提供扫描结果，使用该对象，可以根据需要开发评估数据集。AWID[116]是另一个入侵数据集包含发生在 802.11 Wi-Fi 网络中的正常和异常活动的真实事件。数据集中的每条记录包含 155 个属性，其中包含一个类属性，用于指定该记录是正常流量还是攻击流量。根据类分布，AWID 分为两种主要类型，即高级标记数据集(AWID- cls)和细粒度标记数据集(AWID- atk)。AWID-CLS 是从一个大的数据包集创建的，而另一个是从较小的子集创建的。 这两组数据集是在不同的时间、不同的环境、使用不同类型的设备捕获数据包形成的，并包含各自的一组训练集和测试集。AWID 中的每条记录被分类为正常或特定的入侵类型。在 AWID-CLS 中，入侵类型被分为四个主要的类，分别是泛水、模拟、注入和正常，而 AWID-ATK 则指定了更详细的类标记。AWID-ATK 的训练集包含 10 个类，而测试集包含另外 7 个类。大数据集包含 162 375 247 条训练记录和 48 524 866 条测试记录，而简化数据集包含 1 795 575 和 575 643 条训练和测试记录分别[116]。

UNSW-NB15[80]是另一个评估 nids 的入侵数据集。创建此数据集的动机是为了减轻过去入侵数据集的不足，并帮助识别新的和正在出现的网络攻击，包括低足迹攻击。UNSW-NB15 数据集由澳大利亚网络安全中心(ACCS)创建，包括真实的现代和合成的网络流量。在实验室中创建了包含正常流量和异常流量的综合数据集

使用 IXIA PerfectStorm 工具设置[129]。此工具包含所有最新的公开攻击信息，并用于模拟九种攻击，分别为 normal, fuzzers, analysis， 后门， DoS, exploit, generic, reconnaissance, shellcode 和蠕虫。此外，还利用其他工具和算法集生成了 49 个特征，以涵盖网络数据包的特征。

WSN- ds[130]是为无线传感器网络(WSN)创建的入侵数据集，用于训练和评估 ids，有效识别四类 DoS 攻击，即黑洞攻击、灰洞攻击、洪水攻击和调度攻击。为了收集创建 WSN- ds 所需的数据，我们使用网络模拟器 2 (NS-2)模拟了一个 WSN 环境，其中采用 LEACH[131]协议作为路由协议。然后对收集到的数据集进行处理，得到 23 个特征。通过训练和测试人工神经网络(ANN)来评估数据集的有用性。

在另一项开发具有最新威胁信息和特征的入侵数据集的尝试中，加拿大网络安全研究所通过收集加拿大网络安全研究所网络环境中包含正常流量和攻击流量的五天网络数据，创建了 CICIDS 2017[54]。对所有文件进行处理和合并，最终得到一个满足真实入侵数据集所有标准的单一数据集。结果数据集有 2830540 条记录，每条记录有 83 个特征，包括一个类标签，代表正常流量或 14 个攻击类之一。

Mirai 实际上不是一个数据集，而是一个类似蠕虫的恶意软件，于 2016 年推出[124]。恶意软件感染了分布式物联网设备，并将其转化为僵尸网络，最终导致了历史上最流行的 DDoS 攻击之一。Mirai 攻击的来源是公开的，在研究界很受欢迎。在物联网网络环境中启动源代码，收集和分析网络流量以创建入侵数据集，并且还用于评估所开发的 IDS 模型的性能。

Fed4FIRE+ 25]是 Fed4FIRE 的后续项目，是欧盟地平线 2020 计划下的一个项目，于 2017 年启动，旨在为支持实验驱动的研究提供开放、可访问和可靠的设施。它提供了全球最大的下一代互联网(NGI)测试平台联盟。它旨在支持欧洲的研究和创新社区和倡议，包括 5G PPP 项目和倡议。 Fed4FIRE 通过基础设施的联合实现各种创新实验。此外，它还提供了联合的硬件和软件测试平台资源，可以方便地创建网络环境仿真，并可以高效地进行网络攻击实验。

FL 研究基本上利用了几个 ML 和 DL 模型，并且可访问的基准数据集的可用性允许更好地训练和测试这些模型。已经有大量的工作来创建这样的标准现实数据集，这些已经在文献中大量使用。MNIST 数据集[117]是此类数据集中最流行和最常用的数据集之一。这是一个简单和最初学者友好的标签数据集，包含 70000 张从 0 到 9 的手写数字图像。MNIST 有不同的变体，称为 MNIST- f 和 MNIST- o。MNIST- f，即时尚 MNIST，包含一个更复杂的替代图像数据集，与十类时尚物品相关。mist - f 因其简单易用而被 CNN 广泛采用。

加拿大高级研究所(CIFAR)
10) [132]是另一个图像数据集，由 5 万张训练图像和 1 万张测试图像组成，分为 10 个类别。mist - f 包含灰度图像，而 CIFAR-10 是包含彩色图像的数据集，是物体识别中广泛使用的计算机视觉数据集之一。

多媒体数据可用性的迅速增加和计算能力的增强有助于构建复杂而健壮的机器学习模型。那些复杂的机器学习技术上的简单数据集已经不再有用，无法识别这些算法的真正潜力。为了获得更好的结果，对复杂数据集的需求是内在的，这种需求导致了创建 ImageNet[123]数据集。与大多数现有的基准图像数据集相比，它是一个具有高多样性和准确性的大规模数据集，主要用于图像分类，目标定位和目标检测。该数据集是一个包含 80,000 个 WordNet 同义词集的存储库，平均有 500-1000 个干净的全分辨率图像。该数据集有 12 个子树 320 万张清晰标注的图像，分布在 5247 个类别中。

VGGFace2[121]是一个大规模的人脸数据集，由 9131 名受试者的 331 万张图像组成，涵盖了广泛的种族、职业、姿势、年龄和光照。使用谷歌图片搜索下载所有受试者的图片，保持大致的性别平衡。该数据集包含人脸周围经过人类验证的边界框和由级联 CNN 预测的五个基准关键点的图像。数据集被划分为包含 8631 个类的训练集和包含 500 个类的测试集。

人体活动识别(HAR)[119]数据集收集了 30 名受试者的日常生活活动(ADL)记录，受试者配备了内置惯性传感器的腰装智能手机。该数据集也是公开可用的，并已被研究人员广泛用于活动识别任务。

关键词识别(KWS)是一种从文本图像、语音命令和其他内容中识别关键字的活动，然而，在本文中，我们讨论了[39]研究中使用的音频数据集[120]。该数据集包含 2168 个说话人的 35 个单词的 105829 个发音的集合。每个话语存储在 WAVE 格式文件中，最长长度为 1 秒。该数据集广泛用于语音识别模型的训练和评估。

亚马逊评论[122]数据集是从亚马逊商务网站上客户对产品评论的文本语料库中生成的，用于识别作者身份。记录集包含 1500 个实例，10000 个属性和 50 个类。每条记录都包含与作者的语言风格相关的属性，比如数字的使用标点符号、单词和句子的长度、单词的使用频率等等。

VII. 开放的挑战与未来研究方向

数据对于个人和公司来说都是至关重要的资产，应该加以保护，以确保机密性、完整性和可用性(CIA)。诸如美国的《消费者数据保护法》和《数据护理法》以及欧洲的《通用数据保护条例》等立法已经出台，以加强数据保护然而，由于数据的快速增长，ML 不可避免地要对数据进行分析和学习。然而，由于不安全的数字高速公路、有限的带宽和服务提供商的单独控制，传统的学习模式(集中式)带来了很多问题。在这方面，FL 提供了一个创新的框架，通过数据本地化和培训本地化来促进学习。然而，它仍然处于早期阶段，特别是在物联网环境中完全适用。近年来，FL 在研究界获得了显著的关注。许多作品已经利用不同的机器学习算法、框架和技术提出了他们的模型。然而，在我们的调查中，我们发现大多数提出的模型使用神经网络。神经网络在 FL 设置中最受欢迎，然而，它增加了复杂性，可能会增加实际异构物联网环境中的开销。此外，大多数提出的模型都是在由少数设备组成的环境中模拟的，并且仅针对少数数据集进行了测试。为了开发一个高效且稳健的 FL 模型，研究工作需要考虑 ML 算法、数据集和工作动态的不同排列和组合，并衡量所开发系统的真正功效。

考虑到物联网网络中有限的资源和通信带宽，大量的研究工作已经提出了一种边缘服务器聚合来自终端设备的更新并将其传递到中央服务器的 FL 场景。这种方法通常可能不起作用，因为所有物联网网络可能都没有这样的理想配置。此外，基线算法 fedag 主要用于对更新后的模型进行聚合和加权。 由于物联网环境的系统和统计异构特性，实际联邦网络中的融合可能不会像预期的那样发生。因此寻求其他解决此类问题并导致快速收敛的方法将是有价值的。

差分隐私(如[23])、同态加密(如[25])和安全函数评估或多方计算(如[24])已在 FL 中用于隐私保护学习。使用这些方法的 FL 仅在小规模分布式网络中实现和实验。因此，在大规模网络场景下，由于额外的通信和计算负担，可能会带来新的挑战。

在文献中，梯度压缩方案(例如[39]和[70])已被广泛应用于压缩通信消息，从而减少延迟。虽然这减少了要传输的数据量，但也可能导致数据丢失，影响学习模型的准确性。

在调查工作中，机器学习参数已经聚集在一个集中的服务器上。 这种方法会导致单点故障的风险网络攻击或者其他原因。此外，在这种情况下，通信效率也可能受到集中式服务器地理位置的影响。一种设计多层分布式聚合服务器的新方法可以提高 FL 通信的效率和鲁棒性。

已经提出了几种方法来解决 FL 中昂贵的通信问题，然而，这些方法仅在小规模的联邦网络中进行了测试。这种方法在由数以百万计的系统异构和统计异构设备组成的大规模联合网络中可能执行效率不高。在大规模的网络环境中，由于网络连接和有限的资源，设备采样和辍学加剧了这种情况，目前的方法仅限于测量系统异质性和统计异质性的水平。这一缺陷可能会直接影响学习模型的准确性。大规模 FL 已经在许多文章中得到了强调。这些问题的解决大多是在 i.d、未修改和数据分布均等的假设下进行的。在不降低性能和准确性的情况下识别和减轻对真实 FL 设置的攻击仍然是一个开放的研究领域。

VIII. 结论

在本调查中，我们首先强调了与物联网系统相关的风险和威胁。 在机器学习从海量数据中学习并保持物联网网络安全的作用的激励下，我们讨论了不同的学习模型，并指出了每种模型的优点和缺点。然后，我们将研究扩展到 FL 的应用，这是一种新的创新学习模式;确保物联网网络的安全。讨论了最近关于物联网环境安全方面的几项工作我们还讨论了为减轻 FL 范例中的攻击而进行的几项研究工作。尽管 FL 具有固有的数据保护框架，但要成功采用它还需要解决几个挑战。因此，我们讨论了解决此类性能问题的几个现有研究。为了帮助读者获得总体信息的研究方向，我们介绍了大多数调查作品以及所解决的问题和所有 ML 算法-算法，框架，技术和所建议作品使用的数据集。最后，提出了 FL 研究中存在的一些问题，并展望了未来的研究方向。

鸣谢

本文件中表达的任何意见、发现、结论或建议均为作者的观点，不应被解释为一定代表资助机构的官方政策，无论是明示的还是暗示的。

参考文献

[1] S. A. Rahman, H. Tout, H. old - slimane, A. Mourad, C. Talhi, and M. Guizani，“关于联合学习的调查: 从集中式到分布式的现场学习之旅，”IEEE 互联网物联网杂志，第 8 卷，第 1 期。7，*第 5476-5497 页，四月 2021*。

[2] P. Dube, T. Suk, C. Wang，《人工智能测量: 在云中深度学习的运行时估计”。*31 日 Int。计算机协会。 第一版。 Archit。高执行。第一版。(中国生物医学工程学报)*，2019,pp. 160-167。

[3] 孙宇军，王志军，“基于多区域网络的入侵检测方法”，计算机工程学报。*Int*。*联合会议*。*神经*。*(国际有线电视新*闻网)，2020,pp. 1-8。
[4] 张建军，张建军，张建军，“基于粒子群算法的工业物联网和智能城市服务”，2018,vol . 39(4): 559 - 559。
[5] 邢健，蒋志贤，尹宏，“木星: 区域医疗保健的现代联合学习平台。*IEEE Int*。*相依*。*联合云计算*。，*2020*，*第21*页。
[6] A. Jalalirad, M. Scavuzzo, C. Capota 和 M. Sprague，“一个简单而有效的联合推荐系统”，在 Proc。*第6届IEEE/ACM 学术年会*。*相依*。*大数据计算*。*达成*。*抛光工艺*。，*2019*，第53-58页。
[7] S. Niknam, H. S. Dhillon 和 J. H. Reed，“无线通信的联邦学习: 动机、机会和挑战”，IEEE common。*杂志*，第58卷，第2号。6，第46-51页，2020年6月。
[8] L. U. *Khan* 等人，“边缘网络的联邦学习: 资源优化与激励机制”，IEEE common。*杂志*，*第*58卷，第2号。10，第88-93页，2020年10月。
[9] Y. M. Saputra, D. T. Hoang, D. N. Nguyen, E. Dutkiewicz M. D. Mueck 和 S. Srikanteswara，“基于联合学习的电动汽车网络能源需求预测”，《科学进展》。*IEEE 全球通用*。*相依*。*(地球科学)*，*2019,pp. 1-6*。
[10] 余志强，胡建军，闵国光，赵志强，苗伟，M. S. Hossain，“基于联合学习的互联汽车移动感知主动边缘缓存”，IEEE，*智能*。*透明*。*系统*。，*第22卷*，第2期。8, pp. 5341-5351, august 2021。
[11] 李 t .， A. K. Sahu, A. Talwalkar，和 V. Smith，“联合学习: 挑战、方法和未来方向”，IEEE 信号处*理*。*杂志*，第37卷，no。3, pp. 50-60, 2020年5月。
[12] L. U. Khan, W. Saad, Z. Han, E. Hossain, C. S. Hong，“物联网的联邦学习: 最新进展、分类和开放挑战”，2020,arXiv:2009.13012。
[13] 黄玉娟，黄玉娟，“联合学习的安全性与隐私性研究”，《未来》杂志。*第一版*。*系统*。*第*115卷，第619-640页，2021年2月。
[14] 吕磊，余洪，杨琪，“联邦学习的威胁: [j] .地理学报，2016,35(2):555 - *557*。
[15] Q. Li 等人，“联邦学习系统调查: 数据隐私与保护的愿景、炒作与现实[j]， 2019, arXiv:1907.09693。
[16] H. George 和 A. Arnett，“炼油厂电力基础设施实施网络安全最佳实践的案例研究”，《工程学报》。*IEEE 石油化学*。*第三委员会会议(PCIC)*， *2019, pp.* 103-108。
[17] T. Choudhury, A. Gupta, S. Pradhan, P. Kumar 和 Y. S. Rathore，“基于云的物联网(IoT)的隐私和安全”，程序。*第三Int*。*相依*。*第一版*。*智能*。*Netw*。*(电影)*，*2017,pp.* 40-45。
[18] L. Ashiku 和 C. Dagli，“使用 SoS explorer 作为工具的集中定向系统的网络安全”，《程序》。 *14日为基础*。 *相依*。*系统*。*系统*。*Eng*。*(SoSE)*， *2019, pp. 140-145*。
[19] A. Sinaeepourfard, S. Sengupta, J. Krogstie, R. R. Delgado，“大规模智慧城市的网络安全:“从边缘到云的异常检测的新建议”，在程序。*Int*。*相依*。*物联网嵌入式系统*。*Commun*。*(国际生物工程学报)*，2019,pp. 130-135。
[20] 任建军，王辉，侯涛，郑思，唐志明，“基于边缘计算支持的物联网中基于联邦学习的计算卸载优化”，IEEE Access, vol. 7, pp. 69194-69201, 2019。
[21] B. McMahan, E. Moore, D. Ramage, S. Hampson 和 B. A. Y. Arcas，“基于分散数据的深度网络的高效通信学习”，Proc。*Artif*。*智能*。*统计*，*2017*，*第*1273-1282页。
[22] *通用数据保护条例(GDPR)*，*卷1,Intersoft Consult*。*2018年10月*，*美国加州弗里蒙*特。
[23] O. Choudhury 等人，*“敏*感健康数据的差分隐私联邦学习”，2019,arXiv:1910.02578。
[24] j . Bonawitz *等*，“基于用户持有数据的联合学习的实用安全聚合”，2016,vol . 39(4): 1033 - 1042。
[25] 程凯，范涛，金毅，刘毅，陈涛，杨琪，“Secureboost: 一种无损联邦学习框架[j]， 2019, arXiv:1901.08755。
[26] K. Hsieh 等人，*“盖亚*: 地理分布式机器学习方法-局域网速度”，在程序*中*。*第14届USENIX 会议 Netw*。*系统*。*设计实现*。，*2017*，*第629-647页*。
[27] S. Wang *等*，“当边缘遇到学习时: 资源受限的分布式机器学习的自适应控制”，在 Proc。*IEEE 会议*。*第一版*。*Commun*。，*2018*，*第63-71页*。
[28] 姚晓霞，黄涛，吴翀，张仁，孙丽，“迈向更快更好的联邦学习: 一种特征融合方法。” *IEEE Int*。*相依*。*图像的过程*。*(国际知识产权*杂志)，2019,pp. 175-179。

[29] F.萨特勒，k.r。Müller 和 W. Samek，“集群联合学习: 隐私约束下的模型不可知分布式多任务优化"，IEEE Trans。 *神经。学习。 系统。，第 32* 卷，第 2 期。8, pp. 3710-3722, august 2021。

[30] 冯志刚，尹志杰，刘志刚，“联邦学习中毒的缓解机制”2018，第 14 期:1808 - 1808。

[31] S. A. Rahman, H. Tout, C. Talhi, A. Mourad，“物联网入侵检测: 集中式、设备式还是联合式学习?”*IEEE Netw。，第 34 卷，no。6，第*310-317 页，11 / 12 月。2020.

[32] 李斌，吴勇，宋建军，吕仁，李涛，赵磊，“深度人工智能: 工业网络物理系统中入侵检测的联合深度学习，“IEEE Trans”。*印第安纳州, 备用。，第 17 卷*，no。8, pp. 5615-5624, august 2021。

[33] I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy, and Ming，“AD-IoT: 利用机器学习对智慧城市中的物联网网络攻击进行异常检*测。IEEE 第 9 届年会。第一版。Commun。车间设计。(CCWC)， 2019, pp.* 305-310。

[34] M. Malomo, D. B. Rawat 和 M. Garuba，“自适应网络防御和分布式计算的联合云计算框架”，《科学进展》。*IEEE 会议。第一版。Commun。研讨会(INFOCOM WKSHPS)， 2017，第 1-6 页。*

[35] O. Malomo, D. Rawat 和 M. Garuba，“通过区块链支持的联合云框架中的块保险库进行安全性”，苹果公司。*Netw。科学。*，第 5 卷，第 5 期。1, pp. 1 - 18, 2020。

[36] 卢思、姚旸、石伟，“基于边缘的协作学习:研究”互联汽车的案例研究”，《科学进展》。*第二届 USENIX 研讨会热点话题边缘计算。(酒店管理)，2019，第 1-8* 页。

[37] O. Abdulkader, A. M. Bamhdi, V. Thayananthan, F. Elbouraey, and B. Al-Ghamdi，“物联网环境中基于轻量级区块链的网络安全”，Proc。*IEEE 第 6 期。相依。网络安全云计算。(CSCloud)/第 5 届 IEEE Int。相依。边缘第一版。可扩展云(EdgeCom)， 2019, pp. 139-144。*

[38] 卢仁杰，郑勇，邵杰，A. Ghorbani，“基于雾的物联网 O(log3n) 通信高效隐私保护范围查询”，电子学报，vol. 7, no. 5。6, pp. 5220-5232, 2020 年 6 月。

[39] F. Sattler, S. Wiedemann, k - r。Müller 和 W. Samek，“来自非 iid 数据的健壮且通信高效的联邦学习”，IEEE 翻译。*神经。 学习 系统。，第*31 卷，第 31 期。9, pp. 3400-3413, 2020 年 9 月。

[40] L. U. Khan, M. Alsenwi, Z. Han, C. S. Hong，“无线网络上的自组织联邦学习: 一种具有社会意识的聚类*方法。Int。相依。正无穷。Netw。(ICOIN)， 2020, pp. 453-458。*

[41] 陈毅，孙晓燕，金毅，“基于分层异步模型更新和时间加权聚合的高效通信联合深度学习”，IEEE Trans。*神经。学习。系统。，第 31 卷*，第 31 期。10, pp. 4229-4238, october 2020。

[42] J. Kuusijärvi, R. Savola, P. Savolainen, a . Evesti，“基于可信任网络元素的物联网安全威胁缓解”，Proc。*11 日 Int。相依。互联网抛光工艺。反式。(ICITST)， 2016, pp. 260-265。*

[43] 王 s .，梁国强，“资源约束下网络环境下的联合学习”，《科学》杂志。*IEEE Int。相依。聪明的第一版。(《智能家居》，2019，第 484-486 页*)

[44] Wang *S.* et al.，“资源约束边缘计算系统中的自适应联邦学习”，IEEE J. Sel。*Commun 领域。，第 37 卷，no。6，第 1205-1221 页*，2019 年 6 月。

[45] E. Gyamfi, J. A. Ansere, L. Xu，“基于 ECC 的基于多址移动边缘计算的物联网网络轻量级网络安全解决方案”，第 2 期。*4 日 Int。相依。雾移动边缘计算。(中国林业大学*学报，2019,pp. 149-154)

[46] Y. J. Kim 和 C. S. Hong，“基于区块链的节点感知动态加权方法，用于提高联邦学习性能，”Proc。*亚太新闻网第 20 期。③。管理。计算机协会。(APNOMS)， 2019, pp. 1-4。*

[47] James，“基于物联网网络安全的智能家居入侵防御系统”，中国科学院学报。 *第三网络安全网络 相依。(CSNet)， 2019, pp. 107-113。*

[48] S. K. Datta，“物联网平台的网络安全框架草案- a”，程序。*缩放创新。Consum。抛光工艺。相依。(锌)，2020,pp. 77-81。*

[49] K.-Y。林和 w - r。黄，“在恶意软件分类中使用联合学习”，《科学进展》。*22 日 Int。相依。睡觉。Commun。抛光工艺。(ICACT)， 2020, pp. 585-589。*

[50] 彭志强，彭勇，潘涛，A. Sarrafzadeh，“一种基于网络安全的网络流量分析引擎”，计算机工程学报。*Int。联合会议。神经。(IJCNN)， 2015, pp. 1-8。*

[51] L. Incipini, A. Belli, L. Palma, R. Concetti 和 P. Pierleoni， < MIMIC: 网络安全威胁变成了物联网系统的雾计算代*理。第 42 Int 。修道院。正无穷。Commun 。抛光工艺。电子。Microelectron。(MIPRO)， 2019, pp. 469-474*。

[52] A. M. Zarca, J. B. Bernabe, A. Skarmeta, J. M. A. Calero，“虚拟物联网蜜网在支持 SDN/ nfv 的物联网网络中减轻网络攻击”，IEEE J. Sel。*Commun 领域。，第 38 卷，no。6，第 1262-1277 页*，2020 年 6 月。

[53] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood 和 A. Anwar，“TON_IoT 遥测数据集: 数据驱动入侵检测系统的新一代物联网和工业物联网数据集，”IEEE Access, vol. 8, pp. 165130-165150, 2020。

[54] 王晓明，“基于网络的入侵检测方法研究”，计算机工程学报。*ICISSP, 2018, pp.* 108-116。

[55] R. Neisse, J. L. Hernández-Ramos, S. N. Matheu, G. Baldini, and a . Skarmeta，“基于区块链的平台来管理物联网设备的网络安全认证”，Proc。*IEEE 会议。的立场。Commun。Netw。生物医学工程学*报，2019，第 1-6 页。

[56] 舒建军，周丽丽，张伟，杜晓霞，Guizani M.，“协同入侵检测技术在 vanet 中的应用”。 一种基于深度学习的分布式 SDN 方法，《IEEE Trans》。 *智能。透明。系统。，第* 22 卷，第 2 期。7, pp. 4519-4530, 2020 年 7 月。

[57] R. Vinayakumar, M. Alazab, K. Soman, P. Poornachandran，A. Al-Nemrat 和 S. Venkatraman，“智能入侵检测系统的深度学习方法”，IEEE Access, vol. 7, pp. 41525-41550, 2019。

[58] A. *Rege* 等人，“使用自回归神经网络预测对抗性网络入侵阶段”，IEEE intel。*系统。，第* 33 卷，第 33 期。2，第 29-39 页，3 / 4 月。2018.

[59] t.d. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan, a . r。Sadeghi,”d # 207;不: 一种用于物联网的联邦自学习异常检测系*统。IEEE 第 39 期。相依。Distrib。第一版。系统。(ICDCS)， 2019, pp. 756-767*。

[60] S. Sen 和 C. Jayawardena，“大数据物联网和网络物理系统中的网络攻击分析——一种网络安全建模的技术方法”，中国科学院学报。*IEEE 第 5 版。相依。Converg。抛光工艺。[中文信息学报*]，2019，第 1-7 页。

[61] H. Abie，“基于 CPS-IoT 的医疗保健生态系统的认知网络安全”，Proc。*13 日 Int。计算机协会。地中海。正无穷。Commun。抛光工艺。(中国生物医学工程学*报)，2019,pp. 1-6。

[62] 徐国光，李红华，刘思，杨凯，林晓霞，“验证网”: 安全且可验证的联合学习”，IEEE 译。*正无穷。法医安全，卷 15,pp. 911-926,* 2019。

[63] O. Hachinyan, A. Khorina 和 S. Zapechnikov，“保护物联网设备免受 Mirai 僵尸网络攻击的博弈论技术”，Proc。*IEEE 会议。俄罗斯青年研究人员电气。电子。Eng。(EIConRus)， 2018, pp. 1500-1503*。

[64] S. Sen 和 C. Jayawardena，“基于物联网的智能基础设施无线传感器网络的可靠性和网络安全改进策略”，第 2 期。*全球会议。睡觉。抛光工艺。(地球物理学报*)，2019，第 1-8 页。

[65] U. Majeed 和 C. S. Hong，《FLchain: 通过 MEC 支持的区块链网络进行联合学习。 *亚太新闻网第 20 期。③。管理。计算机协会。(APNOMS)， 2019, pp. 1-4*。

[66] 李昕，王琪，兰昕，陈昕，张宁，陈迪，“通过可信赖的云服务增强基于云的物联网安全: 一种集成安全性和声誉的方法，”IEEE Access, vol. 7, pp. 9368-9383, 2019。

[67] 陈建军，陈建军，陈建军，“基于硬件辅助的物联网设备网络安全”，计算机工程学报。*18 Int。车间微处理器 SoC 测试验证 (MTV)， 2017, pp. 51-56*。

[68] 赵丽，唐晓霞，游忠，庞勇，薛海，朱丽，“基于计算优先网络的联邦学习平台的运行和安全考虑”，中国科学院学报。*IEEE / 中投 Int。相依。Commun。中国(ICCC workshop)， 2020, pp. 117-121*。

[69] N. I. Mowla, N. H. Tran, I. Doh 和 K. Chae，《AFRL: 基于自适应联邦强化学习的智能干扰防御 [j]。*Netw。，第 22 卷，*第 2 期。3，第 244-258 页，2020 年 6 月。

[70] 李世生，齐琪，王健，孙慧，李勇，余福荣，“GGS: 边缘计算中联邦学习的一般梯度稀疏化”，在 Proc。*IEEE Int。相依。Commun。(ICC)， 2020, pp.* 1-7。

[71] 吴国强，吴国强，吴国强，“联邦无线网络入侵检测”，计算机工程学报。 *IEEE Int。相依。 《大数据》，2019，第 6004-6006 页*。

[72] 吕晓霞，廖勇，廖鹏，许鹏，“边缘网络计算中保护隐私的异步联合学习机制”，IEEE Access, vol. 8, pp. 48970-48981, 2020。

[73] R. Doku 和 D. B. Rawat, IFLBC: 关于使用联合学习区块链网络的边缘智能，”在 Proc。*IEEE 第 6 版。相依。大数据安全云 (BigDataSecurity) IEEE Int。相依。高执行。聪明的第一版。IEEE 国际标准相依。智能。数据安全(IDS)， 2020, pp. 221-226*。

[74] 傅爱华，张晓明，熊宁，高勇，王辉，张军，“VFL: 工业物联网中具有隐私保护的可验证联合学习”，IEEE Trans。 *印第安纳州,备用。，第 18 卷*，no。5, pp. 3316-3326, 2022 年 5 月。

[75] 不，不，不。Al-Marri, b.s. Ciftler 和 M. M. Abdallah，“保护隐私的入侵检测的联邦模拟学习”，程序。*IEEE Int。黑海会议 Commun。 Netw。 (BlackSeaCom)， 2020, pp. 1-6*。

[76] 尹斌，尹辉，吴艳，蒋忠，“FDC: 物联网数据协作的安全联合深度学习机制，”IEEE Internet Things J. vol. 7, no. 5。7, pp. 6348-6359, 2020 年 7 月。

[77] P. C. M. Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepe, M. Atiquzzaman，“工业物联网系统中机器学习的可信赖隐私保护框架”，IEEE Trans。*印第安纳州,备用。，第* 16 卷，第 2 期。9, pp. 6092-6102, 2020 年 9 月。

[78] t.v. Khoa 等人，“物联网工业 4.0 中网络攻击检测系统的协作学习模型”，Proc。*IEEE 无线通信。Netw。相依。(中国生物医学工*程学报)，2020,pp. 1-6。

[79] R. Taheri, M. Shojafar, M. Alazab, R. Tafazolli，《Fed-IIoT: 工业物联网中强大的联合恶意软件检测架构，”IEEE Trans。*印第安纳州,备用。，第 17 卷*，no。12, pp. 8442-8452, december 2021。

[80] N.穆斯塔法和 J.斯雷，UNSW-NB15; 网络入侵检测系统的综合数据集(UNSW-NB15 网络数据集)。*军事 Commun。正无穷。系统。相依。(MilCIS)， 2015, pp. 1-6*。

[81] “安全项目(网络边缘的安全)。”网站管理员。2014 年 1 月。(在线)。可用: https://www.secured-fp7.eu/

[82] A. N. Bhagoji, S. Chakraborty, P. Mittal 和 S. Calo，“通过对抗镜头分析馈馈式学习”，《科学进展》。*Int。相依。马赫。学习。， 2019*，第 634-643 页。

[83] M. Nasr, R. Shokri 和 A. Houmansadr，“深度学习的综合隐私分析: 被动和主动白盒推理攻击针对集中式和联邦式学习。*IEEE 计算机协会。安全隐私(SP)， 2019, pp. 739-753*。

[84] B. Wang 和 n.z. Gong，“窃取机器学习中的超参数”，Proc。*IEEE 计算机协会。安全隐私(SP)， 2018, pp. 36-52*。

[85] B. Hitaj, G. Ateniese 和 F. Perez-Cruz，“GAN 下的深度模型: 协同深度学习带来的信息泄漏”。*ACM SIGSAC 会议第一版。Commun。安全，2017,pp. 603-618*。

[86] L. Melis, C. Song, E. De Cristofaro 和 V. Shmatikov，“利用协作学习中的意外特征泄漏”，《科学进展》。*IEEE 计算机协会。安全隐私(SP)， 2019, pp. 691-706*。

[87] 朱磊，韩思，“梯度的深度泄漏”，《联*邦学习》*。瑞士 Cham: 施普林格出版社，2020，第 17-31 页。

[88] L. Lamport, R. Shostak 和 M. Pease，“拜占庭将军问题”，并发: *莱斯利·兰波特的作品*。美国加州圣拉斐尔市: 中国计算机学报，2019,pp. 203-226。

[89] j·r·杜克尔，《西比尔袭击案》，诉讼程序。*Int。工作坊点对点系统， 2002，第 251-260 页*。

[90] E. Bagdasaryan, A. Veit, Y. Hua, D. Estrin，和 V. Shmatikov，“如何后门联合学习”，Proc。*Int。相依。Artif。智能。Stat.， 2020, pp.* 2938-2948。

[91] H. Wang 等，“尾巴的攻击: 是的，你真的可以后门联邦学习，”2020,arXiv:2007.05084。

[92] P. Blanchard, E. M. El Mhamdi, R. Guerraoui 和 J. Stainer，“与对手的机器学习: 拜占庭容忍梯度下降，”在程序。*31 日 Int。相依。神经正无穷。的过程。系统。，* 2017，第 118-128 页。

[93] M. Baruch, G. Baruch 和 Y. Goldberg，“一点点就足够了; 规避分布式学习的防御”，2019,arXiv:1902.06156。

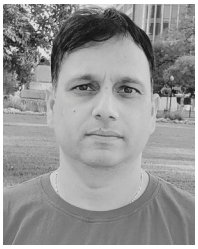
[94] 尹 D.，陈 y .， R. Kannan, P. Bartlett，“拜占庭鲁棒分布式学习: 向最佳统计率迈进。”*Int。相依。马赫。学习。， 2018*，第 5650-5659 页。

[95] 陈晓明，陈晓明，陈晓明，“基于分布式学习的隐式漏洞研究”，《计算机工程学报》，2018，第 4 期:559 - 559。

[96] 李磊，徐伟，陈涛，G. B. Giannakis, Ling Q.，“RSA: 拜占庭-鲁棒随机聚合方法，用于从异构数据集进行分布式学习。*AAAI 相依。Artif。智能。， vol.* 33, 2019, pp. 1544-1551。

[97] M. Nasr, R. Shokri 和 A. Houmansadr，“深度学习的综合隐私分析: 被动和主动白盒推理攻击下的独立和联合学习”，2018,arXiv:1812.00910。
[98] C. Xie, O. Koyejo, I. Gupta， <芝诺: 随机梯度下降算法研究[j] .计算机工程学报，2018,34(1):551 - 551。
[99] 孙国光，丛勇，董军，王强，刘杰，“数据中毒攻击在联邦机器学习中的应用”，2020，第 14 期:2004.10020。
[100] Z. Sun, P. Kairouz, A. T. Suresh 和 H. B. McMahan，“你真的能后门联邦学习吗?”2019 年,arXiv: *1911.07963*。
[101] 张超，李世生，夏军，王伟，闫峰，刘勇，“批加密”; 跨竖井联邦学习的高效同态加密。*USENIX 物质。技术。科学通报，2020,pp.* 493-506。
[102] 陈志*强，*“基于实体解析和加性同态加密的垂直分区数据的私有联邦学习”，2017,vol . 11:1711.10677。
[103] S. Truex, N. Baracaldo, A. Anwar, T. Steinke, H. Ludwig, and 张 r . ，“一种混合方法的隐私保护联邦学习”，2018,arXiv:1812.03224。
[104] R. C. Geyer, T. Klein 和 M. Nabi，“差异私人联合学习:客户层面的视角[j] .， 2017, vol . 11:1712.07557。
[105] L. Zhang, B. Shen, A. Barnawi, S. Xi, N. Kumar, and Y. Wu, “FedDPGAN: 用于检测 COVID-19 肺炎的联邦差异私有生成对抗网络框架，" 6。*系统。前面。，第 23* 卷，第 1403-1415 页，2021 年 6 月。
[106] A. Shafee, M. Baza, D. A. Talbert, M. M. Fouda, M. Nabil, and “模拟学习生成可共享的网络入侵检测模型”，《计算机工程》。*IEEE 第 17 届年会。Consum。Commun。Netw。相依。(中国农业科学*)，2020,pp. 1-6。
[107] X. Yi, R. Paulet, E. Bertino，“同态加密”，《同态加密与应*用》*。瑞士 Cham: 斯普林格出版社，2014 年，第 27-46 页。
[108] B. Ghimire 和 D. B. Rawat，“安全、隐私保护和可验证的车联网区块链联合学习”，IEEE 消费。*电子。杂志，*抢先访问，2021 年 7 月 29 日，doi:10.1109 / MCE.2021.3097705。
[109] C. *Ma* 等人，“在联邦学习框架中保护隐私和安全”，IEEE 网。，第 34 卷，no。4，第 242-248 页，7 / 8 *月*。2020.
[110] R. Cramer 和 I. B. Damgå d，*安全多方计算*。英国剑桥。剑桥大学。出版社,2015 年。
[111] H. Fereidooni 等人，“safelearning:私有馈入式学习的安全聚合。*IEEE 安全隐私研讨会(SPW)， 2021, pp. 56-62*。
[112] S. R. Pokhrel 和 J. Choi，“自动驾驶汽车的区块链联合学习:《分析与设计挑战》，IEEE 译。*Commun。，第 68 卷，第 68* 期。8，第 4734-4746 页，2020 年 8 月。
[113] P. Ramanan 和 K. Nakayama，《困惑: 基于区块链的聚合器自由联邦学习”，在程序中。*IEEE Int。相依。区块链(Blockchain)，2020, pp. 72-81*。
[114] S. Caldas 等人，" *LEAF:* 联邦设置的基准，”2018 年，*arXiv: 1812.01097*。
[115] M. Tavallaee, E. Bagheri, W. Lu 和 A. A. Ghorbani，“对 KDD CUP 数据集的详细分析”，《科学进展》。*IEEE 计算机协会。 第一版。智能。安全防御应用。， 2009，第 1-6 页*。
[116] J. Samarabandu, S. K. P. Thanthrige，“基于公共数据集的入侵检测的机器学习技术”，科学进展。*IEEE 即可。相依。电工实习。第一版。Eng。(CCECE)， 2016, pp. 1-4*。
[117] 李志强，李志强，“基于梯度的学习方法在文档识别中的应用”，中文论文。 *IEEE，第 86 卷*，第 86 期。11，第 2278-2324 页，1998 年 11 月。
[118] 赵毅，李明，赖莱，N. Suda, D. Civin, V. Chandra，“基于非 iid 数据的联邦学习”，2018，第 14 期:186.00582。
[119] D. Anguita, A. Ghio, L. Oneto, X. Parra 和 J. L. Reyes-Ortiz，“使用智能手机进行人类活动识别的公共领域数据集”，《科学进展》。*网络学报，2013,vol.* 3, pp. 437-442。
[120] P. Warden， “语音命令: 有限词汇量语音识别的数据集”，2018,arXiv:1804.03209。
[121] 曹强，沈丽丽，谢伟，O. M. Parkhi, A. Zisserman， " VGGFace2: 一个用于识别不同姿势和年龄的人脸的数*据集。 第 13 届 IEEE 国际会议。相依。奥特曼。面部手势识别。(FG)， 2018,* pp. 67-74。
[122] 巴赫和利奇曼。UCI 机器学习存储库。2013.(在线)。可用: http://archive.ics.uci.edu/ml
[123] 邓建军，董伟，R. Socher, l - j。李凯，李飞飞，“ImageNet: 一个大规模的分层图像数据库，”在程*序。IEEE 会议。第一版。视觉模式识别。， 2009，第 248-255 页*。
[124] M. Antonakakis 等人，“理解 *mirai 僵尸*网络”，在 Proc。*第 26 届 USENIX 安全研讨会。， 2017，第 1093-1110 页*。

[125] m . Facca。“Fed4Fire 回家。”2020 年 12 月。(在线)。可用: https://www.fed4fire.eu/
[126] “1999 年 KDD 杯数据”。 2007. (在线)。 可用: http://kdd.ics.uci。edu/databases/kddcup99/kddcup99.html
[127] J. Song, H. Takakura, Y. Okabe, M. Eto, D. Inoue 和 K. Nakao，“用于 NIDS 评估的蜜罐数据的统计分析和京都 2006+数据集的构建”，Proc。 *第一车间大楼肛门。数据集收集 Exp。退货安全，2011,pp. 29-36*。
[128] 朱磊，刘志强，韩生，“梯度深泄漏”，第 2 期。*神经正无穷。Process.Syst*。2019 年第 32 卷。
[129] S. Axelsson，“入侵检测系统: 调查和分类，“部门计算。Eng。查尔姆斯大学 抛光工艺。，瑞典哥德堡，众议员。2000 年,2000 年。
[130] I. Almomani, B. Al-Kasasbeh 和 M. Al-Akhras，《WSN-DS》; 无线传感器网络中入侵检测系统的数据集，“J.传感器，vol. 2016, Sep. 2016, Art。不。4731953.
[131] 陈志强，“无线微传感器网络的节能通信协议”，中国科学院学报。*第 33 为基础。夏威夷 Int。相依。系统。科学。*，2000，第 10 页。
[132] A. Krizhevsky, V. Nair 和 G. Hinton, 2009，“Cifar-10 和 Cifar-100 数据集”[在线]。可用: https://www.cs.toronto.edu/kriz/cifar。超文本标记语言



Bimal Ghimire (IEEE 研究生会员)于 2003 年在尼泊尔 Kirtipur Tribhuvan 大学 Pulchowk 校区工程学院获得计算机工程学士学位，并获得理工硕士学位。2012 年在印度 Kharagpur 的印度理工学院获得信息技术学位。他目前在美国华盛顿特区霍华德大学电气工程与计算机科学系攻读计算机科学博士学位，导师是 d.b. Rawat 教授。

他的研究兴趣包括网络安全、机器学习/联邦学习、数据分析、区块链、车联网和物联网。

Danda B. Rawat (IEEE 高级会员)，2010 年毕业于美国弗吉尼亚州诺福克 Old Dominion University，获博士学位。

他是负责研究的副院长;研究生教育，工程学院，电气工程和计算机科学系的正教授，数据科学和网络安全中心的创始人和主任，国防部人工智能和机器学习卓越中心的主任，以及霍华德 CS 研究生的研究生项目主任美国华盛顿特区霍华德大学项目。他从美国国家科学基金会(NSF)、美国国土安全部(DHS)、美国国家安全局、美国能源部、国家核安全管理局、国防部和国防部研究实验室、工业界(微软、英特尔和 Facebook/Meta)和私人基金会获得了超过 1600 万美元的研究经费。他从事网络安全、机器学习、大数据分析和新兴网络系统的无线网络领域的研究和教学，包括网络物理系统、物联网、多域运营、智能城市软件定义系统和车载网络。

拉瓦特博士是 2016 年美国国家科学基金会职业奖、2017 年国土安全部科学领导奖、2021 年教务长杰出服务奖、2017 年美国空军研究实验室(AFRL)暑期教师访问奖学金以及 IEEE CCNC、IEEE ICII 和 BWCA 等最佳论文奖的获得者。他曾担任 70 多份国际期刊的编辑/客座编辑，其中包括《IEEE 服务计算学报》和《IEEE 网络科学与工程学报》的副主编，《IEEE 物联网学报》和《IEEE 网络科学与工程学报》的编辑IEEE 网络技术编辑。他曾在 IEEE INFOCOM、IEEE CNS 和 IEEE GLOBECOM 等多个 IEEE 旗舰会议的组织委员会任职。他是 ACM 的高级会员，ASEE 和 AAAS 的成员，以及工程与技术学会的研究员。他是 2021-2023 年度 ACM 杰出演讲者。