基于区块链联邦学习的物联网安全数据激励共享系统设计与实现

HOSSAIN MD ASIBUL（阿布） 郑广海

大连交通大学，辽宁大连，116028；

摘要：随着物联网技术的快速发展，海量终端设备在实际应用中持续产生大量具有高价值的数据资源。然而，受限于数据隐私泄露风险、节点间信任缺失以及缺乏有效激励机制等因素，物联网环境下的数据共享效率与参与积极性普遍较低。针对上述问题，本文提出了一种融合区块链与联邦学习的物联网安全数据激励共享方法。该方法通过联邦学习实现数据在本地训练与模型参数共享，在保障数据隐私与安全性的同时避免原始数据的集中上传；引入区块链技术构建去中心化的可信协作环境，利用其不可篡改和可追溯特性确保模型更新与激励分配过程的透明性与可信性；同时，设计了一种基于贡献度评估的数据激励机制，对参与节点的模型贡献进行量化评估并实现公平合理的收益分配，从而有效提升节点参与数据共享与模型训练的积极性。实验结果表明，所提出的方法在保证数据安全与隐私保护的前提下，能够显著提高系统整体训练性能与节点参与度，验证了该方法在物联网安全数据共享场景中的可行性与应用价值。

关键词：区块链；联邦学习；物联网；数据安全；激励机制；数据共享

DOI：10.69979/3041-0673.26.05.012

1 物联网数据共享需求与区块链联邦学习技术适配分析

1.1 物联网数据共享的安全与隐私挑战

随着物联网技术在智慧城市、工业互联网、智能制造及医疗健康等领域的广泛应用，大量异构终端设备在运行过程中持续产生具有重要价值的数据资源。这些数据为智能分析、协同决策与模型训练提供了基础支撑，但在实际应用中，物联网数据共享仍面临诸多安全与隐私挑战。一方面，物联网终端数量庞大、分布广泛，设备计算能力与安全防护水平参差不齐，数据在采集、传输与存储过程中易受到窃取、篡改及非法利用等威胁；另一方面，数据通常由不同组织或主体持有，受隐私保护、商业利益及合规要求等因素影响，各参与方普遍缺乏共享原始数据的意愿，导致数据孤岛现象严重。

此外，传统的集中式数据共享模式依赖中心服务器进行数据汇聚与管理，一旦中心节点遭受攻击或发生故障，将对系统整体安全性与可靠性造成严重影响。同时，该模式难以满足对数据访问过程的可审计性与责任可追溯性的要求，进一步削弱了多方协同场景下的数据可信度。因此，如何在保障数据隐私与安全的前提下，实现多主体之间的高效、可信数据共享，已成为物联网应用发展过程中亟待解决的关键问题。

1.2 联邦学习在隐私保护数据共享中的优势

联邦学习作为一种分布式机器学习范式，为解决数据隐私与共享矛盾提供了新的技术思路。该机制通过在数据本地完成模型训练，仅在各参与节点之间共享模型参数或梯度信息，从根本上避免了原始数据的集中上传与存储，有效降低了隐私泄露风险。在物联网场景中，联邦学习能够充分利用边缘设备或本地节点的计算能力，在不暴露敏感数据内容的情况下实现协同建模，具有良好的隐私保护特性和扩展性。

然而，联邦学习在实际应用中仍面临一定局限。一方面，由于缺乏统一的信任机制，模型参数上传与聚合过程的真实性与完整性难以得到有效保障，存在恶意节点上传虚假参数或篡改结果的风险；另一方面，联邦学习通常假设参与节点具有较高的协作意愿，而在真实物联网环境中，节点往往更加关注自身资源消耗与收益回报，缺乏有效的激励机制将导致节点消极参与甚至中途退出，从而影响模型训练效果与系统稳定性。因此，有必要引入可信机制与激励手段，对联邦学习过程进行进一步完善。

1.3 区块链与激励机制在可信数据协同中的作用

区块链技术以其去中心化、不可篡改和可追溯等特性，为构建多方参与的可信协作环境提供了有力支撑。通过将模型更新记录、参数提交行为以及收益分配结果

等关键信息上链存证，可有效提升联邦学习过程中各参与节点行为的透明性与可审计性，降低对中心化机构的依赖，增强系统整体的安全性与可信度。同时，基于智能合约的自动执行机制能够确保联邦学习流程与激励规则的公开一致，避免人为干预带来的不公平问题。

在此基础上，引入合理的数据激励机制，对参与节点在模型训练过程中的贡献度进行量化评估，并据此实现收益分配，是提升节点参与积极性的重要手段。通过将激励机制与区块链技术相结合，不仅可以保证激励分配过程的公平性与可信性，还能够有效防止激励结果被篡改或伪造，从而在保障数据隐私与系统安全的前提下，促进物联网环境中数据与模型的持续共享与协同优化。基于上述分析，融合区块链、联邦学习与激励机制，构建一种安全、可信且具备激励能力的物联网数据共享方法，具有重要的研究意义与应用价值。

2 基于区块链联邦学习的物联网数据激励共享系统架构设计

为有效解决物联网环境中数据共享过程中存在的隐私泄露风险、协作信任不足以及节点参与积极性不高等问题，本文结合联邦学习与区块链技术的优势，构建了一种面向物联网场景的安全数据激励共享系统。该系统在不暴露原始数据的前提下，实现多节点协同模型训练，并通过区块链与激励机制保障协作过程的可信性与公平性。系统整体架构及关键模块设计如下。

2.1 系统整体架构与网络模型

所提出的物联网安全数据激励共享系统采用分层式架构设计，整体由物联网设备层、联邦学习协同层以及区块链激励与管理层三部分构成，旨在在保障数据隐私与系统安全的前提下，实现多节点协同建模与激励约束机制的有效融合。

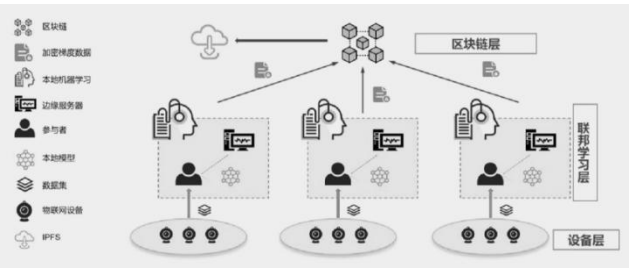

图 1 基于区块链联邦学习的物联网安全数据激励共享系统总体架构示意图

如图 1 所示，物联网设备层由大量异构终端设备组成，主要负责原始数据的本地采集、存储及模型训练，各节点仅在本地环境中处理数据，不直接上传原始数据，从而降低隐私泄露风险；联邦学习协同层负责接收各参与节点上传的本地模型参数，对其进行聚合与更新，并生成全局模型，实现跨节点的协同训练与模型迭代优化；区块链激励与管理层基于联盟链架构，对模型更新记录、节点贡献信息及激励分配结果进行链上存证，构建去中心化、可追溯的可信协作环境。

在网络模型设计方面，各物联网节点既作为联邦学习的参与方，同时作为区块链网络中的轻节点，能够完成本地模型训练、参数上传及激励信息查询等操作；联邦学习服务器主要承担全局模型聚合与分发功能，不直接接触任何原始数据，从系统架构层面降低数据集中存储带来的安全风险。区块链网络采用联盟链模式，由联邦学习服务器、部分可信物联网节点及监管节点共同维护，通过共识机制保证链上数据的一致性与不可篡改性，在兼顾系统运行效率的同时，有效降低多方协作场景下的信任成本，为后续激励机制的实现提供可靠支撑。

2.2 联邦学习训练流程与安全机制设计

在系统运行过程中，各物联网节点基于联邦学习机制参与模型训练。具体流程如下：首先，联邦学习服务器初始化全局模型参数并下发至各参与节点；随后，各节点利用本地采集的数据进行模型训练，仅生成模型参数或梯度信息，而不上传原始数据；完成本地训练后，节点将加密后的模型更新结果提交至联邦学习服务器；服务器对接收到的模型参数进行聚合，形成新的全局模型，并再次分发给各节点，进入下一轮训练迭代。

为保障训练过程中的数据安全与隐私，系统在联邦学习流程中引入多重安全机制。一方面，通过本地训练与参数共享的方式，从根本上避免了原始数据集中上传所带来的隐私泄露风险；另一方面，在模型参数传输过程中结合加密技术与身份认证机制，防止参数被窃取或篡改。此外，区块链技术被用于记录模型更新的关键信息，包括参数提交时间、参与节点身份以及训练轮次等，实现模型训练过程的可追溯与可审计，有效提升系统整体的安全可信水平。

2.3 基于区块链的激励共享与收益分配机制设计

在物联网联邦学习环境中，节点计算资源与数据质量存在显著差异，若缺乏合理的激励机制，容易导致部分节点消极参与甚至退出协作过程。针对这一问题，本文设计了一种基于区块链的数据激励共享与收益分配机制，通过对节点贡献度进行量化评估，实现激励分配的公平性与透明性。

具体而言，系统在每一轮联邦学习训练完成后，对各参与节点在模型训练过程中的贡献进行评估，并将评估结果作为激励分配的重要依据。为实现节点贡献的客观量化，本文引入基于模型性能改进的贡献度评估方法。

设系统中参与联邦学习的节点集合为

$$N = \{1,2,...,n\},$$

第 t 轮训练中，全局模型参数为 $w^{(t-1)}$，节点 i 基于本地数据训练得到的模型参数为 $w_i^{(t)}$，模型的损失函数记为 $\mathcal{L}(\cdot)$。则节点 i 在第 t 轮训练中的模型贡献定义为其带来的损失下降量：

$$\Delta\mathcal{L}_i^{(t)} = \mathcal{L}(w^{(t-1)}) - \mathcal{L}(w_i^{(t)}).$$

为保证不同节点贡献度的可比性，并避免负向贡献对激励分配造成干扰，对贡献值进行归一化处理，得到节点 i 的贡献度评分：

$$C_i^{(t)} = \frac{\max\left(0,\Delta\mathcal{L}_i^{(t)}\right)}{\sum_{j\in N}\max\left(0,\Delta\mathcal{L}_j^{(t)}\right)},$$

其中 $C_i^{(t)} \in [0,1]$，且满足

$$\sum_{i\in N} C_i^{(t)} = 1。$$

该贡献函数能够有效反映各节点对全局模型性能提升的实际贡献，确保激励机制的公平性与合理性。

在此基础上，设第 t 轮联邦学习的总激励预算为 $B^{(t)}$，则节点 i 在该轮训练中获得的激励收益定义为：

$$R_i^{(t)} = B^{(t)} \cdot C_i^{(t)},$$

其中 $R_i^{(t)}$表示分配给节点 i 的激励奖励。该奖励分配方式能够根据节点实际贡献动态调整收益水平，有效激励节点持续参与模型训练过程。

节点贡献信息及对应的激励结果通过智能合约自动写入区块链，实现激励过程的去中心化执行与不可篡改存证。借助区块链的公开透明特性，各节点可随时查询自身贡献与收益情况，有效避免激励分配过程中的信任争议。同时，激励机制的引入能够显著提升节点参与模型训练的积极性，促进系统长期稳定运行。

通过将联邦学习、区块链与基于贡献度评估的激励机制进行有机融合，所提出的系统不仅实现了物联网数据共享过程中的隐私保护与安全保障，还在可信协作与激励约束层面形成闭环，为后续系统实验验证与应用分析奠定了技术基础。

3 系统实现与实验结果分析

3.1 实验环境与参数设置

为验证所提出的基于区块链联邦学习的物联网安全数据激励共享方法的有效性与可行性，本文在仿真环境下构建了实验平台，对系统的训练性能、安全性以及激励效果进行综合评估。实验环境基于 Python 语言进行实现，联邦学习训练过程在多节点模拟场景下完成，各节点通过逻辑网络方式模拟物联网终端设备。区块链模块采用联盟链架构进行设计，用于记录模型更新信息及节点激励分配结果，以确保数据交互过程的可信性与可追溯性。

在实验设置中，假设系统包含多个参与节点，每个节点持有本地私有数据集并独立完成模型训练，节点之间不直接共享原始数据，仅上传本地模型参数或梯度信息至聚合节点。为模拟真实物联网环境中数据分布不均衡的特征，实验采用非独立同分布（Non-IID）数据划分方式对各节点数据进行分配。联邦学习训练采用固定轮数的迭代方式，在每一轮训练结束后，系统对各节点的模型贡献进行评估，并通过区块链智能合约自动完成激励计算与记录。

为保证实验结果的对比性与公平性，本文将所提出的方法与不引入激励机制的传统联邦学习方案进行对比分析，重点考察在相同训练条件下系统性能与节点参与行为的变化情况。

3.2 系统安全性与性能分析

在系统安全性方面，所提出的方法通过联邦学习机制实现模型在本地训练与参数共享，有效避免了原始数据在网络中的直接传输，从源头上降低了数据泄露风险。同时，引入区块链技术对模型更新记录与激励分配结果进行链上存证，利用其不可篡改和时间戳特性，确保训练过程的透明性与可审计性，防止恶意节点对模型参数或收益分配结果进行篡改。

在性能分析方面，实验结果表明，所提出的方法在整体模型收敛速度与最终训练精度方面与传统联邦学习方案保持一致，未因引入区块链与激励机制而对模型训练效果产生明显负面影响。虽然区块链的引入在通信与计算层面带来了一定的额外开销，但该开销主要集中于模型更新记录与激励结果上链过程，对联邦学习核心训练流程影响较小，整体系统仍能够满足物联网应用场景下对效率与稳定性的要求。

此外，通过对训练过程的多轮实验观察发现，系统在面对部分节点不稳定参与或短暂离线的情况下，仍能够保持较好的鲁棒性，验证了所提出方法在复杂物联网

环境中的适应能力。

3.3 激励机制效果验证与对比分析

为进一步验证所提出激励机制在提升节点参与积极性方面的作用，本文对引入激励机制前后的节点参与行为进行了对比分析。实验结果显示，在未引入激励机制的联邦学习场景中，部分节点在训练过程中存在参与意愿不足或中途退出的现象，导致系统有效参与节点数量波动较大，从而影响整体训练效率。

相比之下，在引入基于贡献度评估的激励机制后，各节点的参与稳定性与持续性均得到明显提升。通过对节点模型贡献进行量化评估，并结合区块链实现公平透明的收益分配，系统能够有效激励节点持续参与模型训练过程。实验结果表明，激励机制的引入显著提高了系统的有效参与节点比例，同时在保证公平性的前提下实现了收益分配的合理性。

综合对比分析结果可以看出，所提出的基于区块链联邦学习的激励共享方法在不牺牲系统安全性与训练性能的基础上，有效改善了物联网环境下联邦学习中节点参与积极性不足的问题，进一步验证了该方法在实际应用场景中的可行性与推广价值。

4 结语

本文针对物联网环境下数据共享存在的隐私泄露、节点信任缺失以及参与积极性不足等问题，提出了一种基于区块链与联邦学习的安全数据激励共享方法。通过联邦学习实现数据在本地训练与模型参数共享，在保证数据隐私和安全的前提下，避免了原始数据的集中上传；利用区块链构建去中心化、不可篡改的协作环境，实现了模型更新及激励分配的透明记录；同时，设计基于贡献度评估的激励机制，实现了公平合理的收益分配，从而显著提升了节点参与数据共享与模型训练的积极性。

实验结果表明，所提出的方法在不影响系统训练性能的前提下，有效提高了节点参与度，验证了方法的可行性与应用价值。总体来看，该方法为物联网安全数据共享提供了一种可落地、可信且高效的解决方案。

未来工作可进一步从以下几个方面展开：一是扩展系统在大规模异构物联网环境下的适应性，优化激励机制在不同节点类型和数据分布下的公平性；二是探索更高效的区块链共识算法，以降低通信和计算开销，提高系统整体效率；三是结合智能合约与自动化策略，进一步增强系统的智能化管理与动态激励能力，以满足实际物联网应用中多样化、安全可靠的数据共享需求。

参考文献

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[EB/OL]. 2008.

[2] Buterin V. Ethereum: A next-generation smart contract and decentralized application platform[EB/OL]. 2013.

[3] McMahan B, Moore E, Ramage D, et al. Communication-efficient learning of deep networks from decentralized data[C]//Proceedings of the 20th International Conference on Artificial Intelligence and Statistics. 2017: 1273-1282.

[4] Kairouz P, McMahan H B, Avent B, et al. Advances and open problems in federated learning[J]. Foundations and Trends in Machine Learning, 2021, 14(1-2): 1-210.

[5] Bonawitz K, Ivanov V, Kreuter B, et al. Practical secure aggregation for privacy-preserving machine learning[C]//Proceedings of the ACM Conference on Computer and Communications Security. 2017: 1175-1191.

[6] Zheng Z, Xie S, Dai H, et al. Blockchain challenges and opportunities: A survey[J]. International Journal of Web and Grid Services, 2018, 14(4): 352-375.

[7] 王伟，李强，张磊. 区块链技术在物联网数据安全中的应用研究[J]. 计算机工程与应用，2020，56(18)：15-22.

[8] 刘洋，陈杰. 联邦学习隐私保护机制及其应用研究[J]. 计算机科学，2021，48(6)：45-52.

[9] 张强，赵磊，王磊. 面向物联网的数据安全共享机制研究[J]. 通信学报，2019，40(10)：45-53.

[10] 李明，周涛. 区块链在去中心化数据管理中的应用与挑战[J]. 软件学报，2020，31(6)：1832-1845.

[11] 陈志强，黄伟. 联邦学习在隐私保护计算中的研究进展[J]. 电子学报，2021，49(8)：1581-1592.

[12] 周凯，刘峰. 基于激励机制的数据共享模型研究[J]. 系统工程理论与实践，2018，38(9)：2314-2322.