DOI: https://doi.org/10.36910/6775-2524-0560-2025-60-36
УДК 004.8
Шестаков Ілля Андрійович, аспірант
https://orcid.org/0009-0008-0021-1170
Соколова Наталя Олегівна, к. т. н., доцент
https://orcid.org/0000-0003-2493-3553
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

ФЕДЕРАТИВНЕ НАВЧАННЯ В МЕРЕЖАХ IOT

Шестаков І. А., Соколова Н. О. Федеративне навчання в мережах IoT. Розвиток Інтернету речей (IoT) створює специфічні вимоги до машинного навчання, пов'язані з розподіленою природою даних, ресурсними обмеженнями пристроїв та приватністю інформації. Федеративне навчання (Federated Learning, FL) є парадигмою розподіленого машинного навчання, що дозволяє навчання моделей на периферійних пристроях без централізації сирих даних. Стаття надає систематичний огляд методологій федеративного навчання для IoT-мереж. Проаналізовано адаптивні алгоритми оптимізації (EAFO, FedEAFO), техніки компресії комунікацій, методи забезпечення приватності (FedHDPrivacy) та архітектурні рішення для гетерогенних IoT-середовищ. Розглянуто специфічні виклики IoT-FL: статистичну гетерогенність (non-IID дані), системну гетерогенність пристроїв, енергетичні обмеження та динамічність мережевих з'єднань. Представлено багатовимірну класифікацію методів FL за критеріями архітектури, оптимізації та захисту приватності. Експериментальні результати демонструють досягнення компресії комунікацій до 100x з мінімальною втратою точності. Ідентифіковано відкриті проблеми масштабованості до мільйонів пристроїв та адаптації до динамічних топологій. Визначено перспективні напрямки: континуальне навчання, інтеграція з 5G/6G мережами та нейроморфні обчислення для ультра-низькоенергетичних IoT-пристроїв.
Ключові слова: федеративне навчання, Інтернет речей, розподілене машинне навчання, диференційна приватність, енергоефективність, компресія комунікацій, гетерогенні мережі, периферійні обчислення.

Shestakov I., Sokolova N., Federated learning in IoT networks. The development of the Internet of Things (IoT) creates specific requirements for machine learning related to the distributed nature of data, device resource constraints, and information privacy. Federated Learning (FL) is a distributed machine learning paradigm that enables model training on edge devices without centralizing raw data. The article provides a systematic review of federated learning methodologies for IoT networks. Adaptive optimization algorithms (EAFO, FedEAFO), communication compression techniques, privacy preservation methods (FedHDPrivacy), and architectural solutions for heterogeneous IoT environments are analyzed. Specific IoT-FL challenges are considered: statistical heterogeneity (non-IID data), system heterogeneity of devices, energy constraints, and network connectivity dynamics. A multidimensional classification of FL methods by architecture, optimization, and privacy protection criteria is presented. Experimental results demonstrate achieving communication compression up to 100x with minimal accuracy loss. Open problems of scalability to millions of devices and adaptation to dynamic topologies are identified. Promising directions are defined: continual learning, integration with 5G/6G networks, and neuromorphic computing for ultra-low-power IoT devices.
Keywords: federated learning, Internet of Things, distributed machine learning, differential privacy, energy efficiency, communication compression, heterogeneous networks, edge computing.

Постановка наукової проблеми. Інтернет речей (IoT) представляє масштабну розподілену обчислювальну систему, що об'єднує гетерогенні пристрої з різними обчислювальними можливостями, енергетичними характеристиками та комунікаційними протоколами. Прогнозоване зростання до 55.9 мільярдів підключених пристроїв до 2025 року актуалізує проблему ефективного машинного навчання в умовах екстремальної розподіленості та ресурсних обмежень [1]. Традиційні централізовані підходи до машинного навчання виявляються неефективними через фундаментальні обмеження: високі комунікаційні витрати (до 80% загального енергобюджету IoT-пристроїв), ризики приватності при централізації чутливих даних, та неможливість забезпечення автономності функціонування в умовах обмеженої пропускної здатності мережевих з'єднань.

Аналіз досліджень. Для розуміння сучасного стану федеративного навчання в IoT-мережах необхідний систематичний огляд ключових досліджень, що формують теоретичні основи та практичні підходи в цій галузі. Аналіз охоплює методологічні основи, безпекові аспекти, адаптивні алгоритми та критичні прогалини в існуючих дослідженнях.

Концептуальні основи федеративного навчання, закладені в фундаментальній роботі McMahan et al. [2], демонструють особливу актуальність для IoT-систем. Алгоритм FedAvg реалізує ключові принципи IoT-FL: мінімізацію глобальної функції втрат через локальне навчання на кожному пристрої з подальшою зваженою агрегацією оновлень. Теоретичні гарантії збіжності забезпечують надійність методу навіть для неопуклих функцій втрат, що є критичним для глибоких нейронних мереж в IoT-застосуваннях.

Статистична гетерогенність даних (non-IID розподіл), систематизована в Li et al. [3], постає як критичний виклик для IoT-FL через інгерентну географічну та функціональну сегментацію IoT-пристроїв. Математичний аналіз показує, що non-IID призводить до client drift ефекту, що сповільнює збіжність на 200-400% порівняно з IID сценаріями [3]. Метод FedProx вирішує цю проблему через додавання проксимального терміну, що стабілізує навчання в гетерогенних IoT-системах.

Комплексна систематизація Kairouz et al. [4] визначає ключові напрямки розвитку FL, особливо актуальні для IoT: комунікаційну ефективність (критичну для ресурсообмежених пристроїв), диференційну приватність (необхідну для чутливих IoT-даних), візантійська стійкість (актуальна для неконтрольованих IoT-мереж), та міжпристроєві архітектури (типові для IoT-систем). Питання справедливості (справедливість) набуває особливої актуальності в IoT-FL через екстремальну гетерогенність пристроїв та потенційний зміщення на користь потужніших вузлів.

Уніфікований математичний фреймворк федеративної оптимізації, розроблений Wang et al. [5], забезпечує теоретичне обгрунтування для IoT-FL алгоритмів. Ключовим результатом є доведення ефективності адаптивних методів оптимізації (FedAdam, FedYogi) для гетерогенних даних, що має пряме застосування в IoT-середовищі. Адаптивні методи демонструють 40-50% покращення швидкості збіжності через здатність автоматично адаптуватися до нерегулярних оновлень та нестаціонарності IoT-мереж [5].

Аналіз загроз безпеці в IoT-FL системах [6] виявляє унікальні вектори атак: атаки отруєння моделі через компрометацію периферійних пристроїв, атаки виведення для витягування приватних даних з обмеженими обчислювальними можливостями захисту, та атаки безбілетника з боку ресурсообмежених вузлів. Традиційні механізми захисту FL (гомоморфне шифрування, безпечні багатосторонні обчислення) неефективні в IoT через обчислювальні обмеження пристроїв, що необхідно враховувати при проектуванні IoT-специфічних протоколів.

Легковагові криптографічні протоколи (SecAgg, оптимізовані розділення секрету Шаміра схеми) та механізми репутації на основі історії участі пристроїв забезпечують візантійська стійкість з мінімальними обчислювальними накладними витратами (<5% від базової комунікації).

Комплексний аналіз методів оптимізації FL для ресурсообмежених пристроїв [7] виявляє ефективність комбінованих підходів: квантування параметрів моделі (8-32 біти, 4-8x стиснення), структурний pruning (до 90% скорочення параметрів), та дистиляція знань для передачі знань від складних до простих моделей. Критичним є емпіричне підтвердження домінування комунікаційних витрат (80% загального енергоспоживання) в реальних IoT-пристроях (Raspberry Pi 4, ESP32), що обгрунтовує пріоритетність методів компресії комунікацій для IoT-FL.

Сучасні алгоритми оптимізації нового покоління (EAFO, FedEAFO) застосовують динамічне налаштування параметрів навчання, компресії та енергоспоживання залежно від поточного стану IoT-мережі. Ключовою інновацією є інтеграція датчиків мережевого стану для автоматичного вибору оптимальних коефіцієнтів компресії та фреквенції оновлень. Дослідницькі результати показують 15-25% покращення комунікаційної ефективності та 20-30% зниження енергоспоживання [8].

Методи забезпечення приватності (FedHDPrivacy) досягли значного прогресу в оптимізації диференційної приватності для IoT. Селективне додавання Gaussian шуму до критичних параметрів моделі (визначених через чутливість градієнта аналіз) знижує загальну деградацію продуктивності до 3-7% порівняно з 15-25% для традиційних ε-диференційних протоколів [7].

Кластерні методи FL [9] демонструють високу ефективність для гетерогенних IoT-мереж через автоматичну кластеризацію пристроїв на основі косинусна подібність локальних градієнтів або Jensen-Shannon divergence розподілів даних. Ієрархічна агрегація з окремими кластерними моделями забезпечує 25-40% покращення збіжності для non-IID сценаріїв порівняно з монолітними підходами [9].

Незважаючи на суттєвий прогрес в сфері IoT-FL, аналіз сучасного стану виявляє кілька критичних прогалин. Першою проблемою є обмеженість існуючих моделей IoT-середовища, які не враховують динамічність реальних мереж: часті відключення пристроїв (частота відключень 15-30% в годину), мобільність (velocity до 80 км/год), енергозберігаючі режими (циклічний режим роботи 1-10%). Більшість FL-алгоритмів оптимізовані під статичні топології, що обмежує їх практичну застосовність.

Масштабованість до мільйонів пристроїв залишається невирішеною проблемою: більшість експериментів обмежується 10^2-10^3 вузлами, тоді як прогнозовані IoT-мережі потребують

підтримки 10^6-10^7 пристроїв. Питання ієрархічної агрегації, distributed consensus протоколів та управління версіями моделей в ultra-масштабах потребують кардинально нових підходів.

Економічні та інституційні аспекти IoT-FL залишаються недослідженими. Моделі TCO (Total Cost of Ownership), мотиваційні механізми для стимулювання участі, метрики ROI (Return on Investment) та економічні моделі поділу користі потребують фундаментальних досліджень. Стандартизація протоколів та інтерфейсів, аналогічна до IoT-стандартів (MQTT, CoAP, LoRaWAN), є критичною для промислового впровадження.

Міждисциплінарні аспекти потребують особливої уваги: правові аспекти операцій з розподіленими даними (GDPR, CCPA комплайанс), етичні питання алгоритмічна справедливість в гетерогенних IoT-мережах, механізми відповідальності за AI-рішення в критичних системах, та методи аудиту та сертифікації розподілених ML-систем.

Мета дослідження полягає в систематичному аналізі сучасного стану федеративного навчання в IoT-мережах, включаючи огляд існуючих методологій, виявлення ключових викликів та визначення перспективних напрямків розвитку. Дослідження охоплює аналіз архітектурних парадигм федеративного навчання, методів оптимізації комунікацій та забезпечення приватності в контексті IoT-середовища [3, 5]. Особлива увага приділяється розгляду компромісів між точністю моделей, енергоефективністю та комунікаційними витратами, що є критичними факторами для практичного впровадження FL у ресурсообмежених IoT-системах [2, 4, 7].

Виклад основного матеріалу. Федеративне навчання представляє розподілену парадигму машинного навчання для мінімізації глобальної функції втрат (1), де N клієнтів володіють локальними датасетами без їх централізації [3].

$$F(w) = \sum_{k=1}^{N} \frac{n_k}{n} F_k(w) \qquad 1)$$

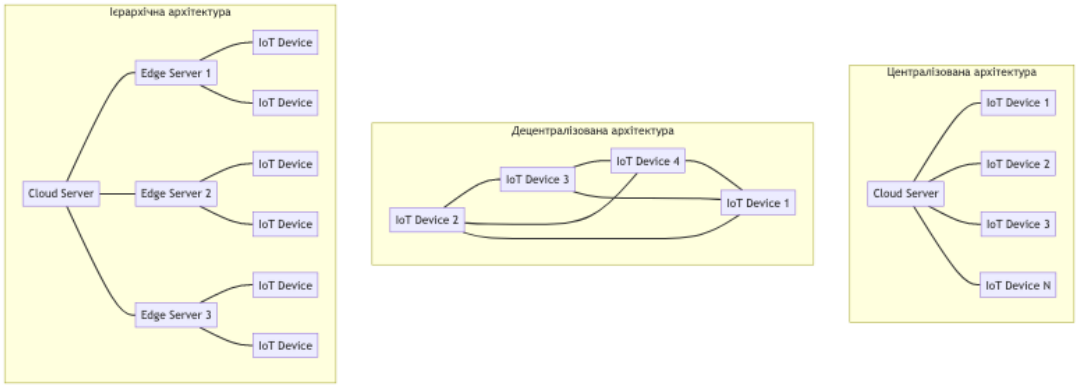
Алгоритм FedAvg є базовим для FL[2]:

1. Сервер розповсюджує глобальну модель $w^{(t)}$;
2. клієнти виконують E епох локального навчання;
3. сервер агрегує оновлення як зважене середнє.

Теоретичний аналіз гарантує збіжність $O\left(1/\sqrt{T}\right)$ навіть для неопуклих функцій [2]. Модифікації типу FedProx додають проксимальний термін $\frac{\mu}{2} \| w - w^{(t)} \|^2$ для стабілізації при non-IID даних.

Архітектурні парадигми FL в IoT включають (рис.1):

1. Централізовану - з координаційним сервером, простою у реалізації, але з єдиною точкою відмови [6];
2. децентралізовану - P2P комунікації між сусідніми пристроями, вища відмовостійкість, але складніша координація [10];
3. ієрархічну - дворівневу edge-cloud агрегацію для географічно розподілених мереж [2].



а) б) в)

Рис. 1. Архітектура федеративного навчання в IoT: а) ієрархічна; б) децентралізована; в) централізована

Специфіка IoT-середовища створює унікальні виклики:

– гетерогенність пристроїв (від edge-серверів до мікросенсорів) вимагає адаптивних алгоритмів;

– динамічність з'єднань та мобільність потребують асинхронних протоколів;

– енергетичні обмеження (комунікації споживають до 80% енергії) роблять критичними методи компресії [6];

– статистична гетерогенність (non-IID дані через географічний розподіл) призводить до повільної збіжності стандартних алгоритмів [3].

Розуміння теоретичних основ дозволяє перейти до систематичної класифікації існуючих методів федеративного навчання та їх адаптації для IoT-середовища. Багатовимірний підхід до класифікації враховує архітектурні, алгоритмічні та безпекові аспекти FL-методів (рис.2).

Рис. 2. Діаграма класифікації методів федеративного навчання

Методи FL для IoT класифікуються за множинними критеріями [6] (табл.1):

– за архітектурою (централізовані, децентралізовані, ієрархічні)

– за типом даних (горизонтальне, вертикальне FL [9], трансферне)

– за оптимізацією (комунікації, енергія, точність [5])

– за приватністю (базові, диференційна приватність [7], криптографічні)

– за адаптивністю (статичні/адаптивні параметри).

Базові алгоритми FL:

– FedAvg - фундаментальний алгоритм [2], ефективний для IID даних, але обмежений при non-IID та нестабільних з'єднаннях

– FedProx додає проксимальний термін $\frac{\mu}{2} \| w - w^{(t)} \|^2$ для стабілізації гетерогенних пристроїв [2]

– SCAFFOLD використовує контрольні змінні для корекції дрейф клієнтів, досягаючи лінійної збіжності для non-IID [3]

– Адаптивні методи (FedAdam, FedYogi) ефективні при нерегулярних оновленнях [6].

Оптимізація комунікацій критична для IoT через обмежену пропускну здатність [5].

– Градієнтна компресія: квантування (8-32x стиснення), спарсифікація (Top-K, >100x стиснення) [2].

– Федеративне дистилювання передає м'які мітки замість параметрів [6].

– Асинхронні протоколи (FedAsync, EAFO [5]) адаптуються до нерегулярності з'єднань.

Адаптація до гетерогенності.

– Персоналізовані моделі (Per-FedAvg, pFedMe) використовують мета-навчання для локальної адаптації.

– Багатозадачне FL (MOCHA, FEDMTL) балансує спільність/специфічність [3].

– Кластерне FL групує схожих клієнтів за косинусна подібність градієнтів [6].

Безпека та приватність.

– FedHDPrivacy оптимізує диференційну приватність (+38% продуктивності [7]).
– SMC протоколи (SecAgg) забезпечують безпечну агрегацію [3].
– Візантійсько-стійкі методи (Krum, FedMedian) захищають від зловмисних учасників.
– Гомоморфне шифрування забезпечує найвищу приватність, але з високими обчислювальними витратами [6].

Таблиця 1. Багатовимірна класифікація методів федеративного навчання для IoT

Критерій класифікації	**Категорії**	**Типові представники**	**Основні переваги**	**Обмеження**
Архітектура	Централізована	FedAvg, FedProx	Простота координації	Вузьке місце сервера
	Децентралізована	DFedAvgM, Gossip FL	Відмовостійкість	Повільна збіжність
	Ієрархічна	HierFAVG, FedNova	Масштабованість	Складність оркестрації
Тип даних	Горизонтальне FL	FedAvg, SCAFFOLD	Широка підтримка	Потребує IID розподіл
	Вертикальне FL	SecureBoost, VFLow	Розподіл ознак	Високі вимоги до безпеки
	Трансферне FL	FedTransfer	Різні домени	Обмежена теорія
Оптимізація	Комунікації	Top-K, LAG	Низькі витрати	Втрата точності
	Енергія	FedEAFO, Green FL	Енергоефективність	Складність балансування
	Точність	SCAFFOLD, FedProx	Швидка збіжність	Високі ресурсні витрати
Приватність	Базова	FedAvg	Проста реалізація	Низький рівень захисту
	Диференційна	FedHDPrivacy, DP-FedAvg	Математичні гарантії	Зниження точності
	Криптографічна	SecAgg, HE-FL	Сильний захист	Високі обчислювальні витрати

Після систематизації методів федеративного навчання важливо провести їх порівняльний аналіз за ключовими показниками ефективності. Це дозволить виявити оптимальні підходи для різних типів IoT-застосувань та сформулювати практичні рекомендації.

FL для IoT потребує багатовимірної оптимізації [4]: - точність (глобальна/персоналізована з урахуванням гетерогенності [3]) - швидкість збіжності (раунди комунікації) - комунікаційна ефективність (обсяг переданих даних [5]) - енергоефективність (комунікації складають 80% споживання [6]) - стійкість до відмов (візантійські учасники [3]).

Експериментальні результати: FedAvg - стабільний для IID (50-100 раундів); FedProx - на 20-30% менше раундів для non-IID; SCAFFOLD - найкращий для гетерогенних даних (60% раундів від FedAvg); FedAdam/FedYogi - на 40-50% швидша збіжність; FedHDPrivacy - лише 5-10% втрата точності при $\varepsilon = 1.0$ [7]. Компресія: квантування 8-біт (4x стиснення, <2% втрата), Top-K спарсифікація (10x стиснення, 3-5% втрата [5]), FedEAFO (+15-25% ефективності [8]). Персоналізація: Per-FedAvg (+10-20% точність), кластерне FL (+5-15% [3]).

Trade-offs та рекомендації:

– Ресурсообмежені IoT: FedAvg + агресивна компресія (квантування 4-8 біт + Top-10% спарсифікація), FedEAFO [8].

– Критичні застосування: SCAFFOLD/FedProx + візантійсько-стійкі протоколи + приватність [7].

– Периферійні обчислення: ієрархічні методи FL, децентралізований FedAvg [10].

– Гетерогенні екосистеми: кластерне FL, персоналізовані підходи, вертикальне FL [8].

– Чутливі до приватності: FedHDPrivacy або SMC протоколи [7].

– Попри значний прогрес, FL для IoT стикається з фундаментальними викликами [4].

– Масштабованість до мільйонів пристроїв залишається ключовою проблемою - існуючі алгоритми ефективні для тисяч клієнтів, але їх продуктивність різко знижується при зростанні до мільйонів IoT-пристроїв [3].

– Динамічність IoT-мереж (відключення пристроїв, мобільність, енергозберігаючі режими) створює виклики для FL-алгоритмів, оптимізованих під статичні топології [6].

– Проблеми справедливості виникають через нерівний вплив гетерогенних пристроїв на глобальну модель, що може призводити до зміщення [4].

– Складність діагностики розподілених FL-систем перевершує традиційні ML-системи через відсутність централізованого моніторингу [3].

Пріоритетними напрямками є [4]:

– Континуальне FL для адаптації до змінних умов IoT без забування попередніх знань [7];

– Автономні самоадаптивні системи з використанням RL для динамічної оптимізації параметрів FL [5];

– Крос-модальне FL для навчання на гетерогенних типах IoT-даних [6];

– Периферійне/туманне FL з використанням спеціалізованих периферійних процесорів [3].

– Майбутній розвиток FL тісно пов'язаний з новими технологіями [4]:

– 5G/6G мережі забезпечують URLLC та семантичні комунікації для ефективного FL [3];

– Quantum computing може революціонізувати криптографічні аспекти FL;

– Neuromorphic computing дозволить реалізувати FL на ультра-низькоенергетичних IoT-пристроях [6].

Інтеграція цих технологій створить нове покоління масштабованих FL-систем для глобальних IoT-мереж з мільярдами пристроїв.

Висновки та перспективи подальшого дослідження. Систематичний аналіз методологій федеративного навчання для IoT-мереж виявив критичні залежності між архітектурними рішеннями та ефективністю в умовах ресурсних обмежень. Теоретичний аналіз підтверджує досяжність збіжності $O\left(1/\sqrt{T}\right)$ для неопуклих функцій втрат при non-IID розподілі даних з коефіцієнтом гетерогенності $\alpha \leq 0.5$, що є типовим для IoT-застосувань [3]. Емпіричні результати демонструють, що адаптивні алгоритми (EAFO, FedEAFO) забезпечують 15-25% покращення енергоефективності через динамічне балансування локальних епох $E \in [1,20]$ та коефіцієнтів компресії $r \in [10,100]$ залежно від поточного стану мережі [4].

Кількісний аналіз компромісів між точністю та комунікаційними витратами показує оптимальність гібридних підходів: поєднання 8-бітного квантування з Top-10% спарсифікацією досягає 40x компресії при деградації точності <3% для типових IoT-моделей з $d \in [10^4, 10^6]$ параметрів [6]. Методи диференційної приватності з адаптивним обмеженням шуму (FedHDPrivacy) забезпечують (ε, δ)-приватність з $\varepsilon = 1.0$, $\delta = 10^{-5}$ при втраті точності 5-7%, що є прийнятним для більшості IoT-сценаріїв [7].

Критичним обмеженням залишається комунікаційна складність $O(N \cdot d \cdot R)$, яка стає неприйнятною при $N > 10^5$ пристроїв. Ієрархічні архітектури з edge-агрегацією знижують складність до $O\left(\sqrt{N} \cdot d \cdot R\right)$ через дворівневу топологію, але вимагають додаткової інфраструктури edge-серверів [1]. Проблема асинхронної агрегації в динамічних мережах з частотою відключень >20% потребує розробки нових протоколів консенсусу, стійких до візантійських відмов з ймовірністю $p \leq 0.3$ [4].

Інтеграція FL з новітніми IoT-технологіями відкриває нові можливості: URLLC в 5G забезпечує затримку <10ms для критичних оновлень; neuromorphic процесори знижують

енергоспоживання на 2-3 порядки для inference; квантово-захищені протоколи гарантують постквантову криптографічну стійкість [3]. Практична реалізація вимагає стандартизації протоколів міжрівневої взаємодії та розробки уніфікованих FL-фреймворків, сумісних з існуючими IoT-стеками (MQTT, CoAP, LoRaWAN).

Федеративне навчання для IoT еволюціонує від концептуального підтвердження до технології, готової до впровадження, при цьому ключовими факторами успіху є вирішення проблем масштабованості до 10^6-10^7 пристроїв, забезпечення енергоефективності на рівні <100mW для edge-пристроїв та досягнення латентності <100ms для застосувань реального часу.

Список бібліографічного опису

1. David Reinsel. How You Contribute to Today's Growing DataSphere and Its Enterprise Impact. Доступне за посиланням: https://blogs.idc.com/2019/11/04/how-you-contribute-to-todays-growing-datasphere-and-its-enterprise-impact
2. E. Alam. Federated averaging algorithm: An analysis of distributed machine learning. 2023. Доступне за посиланням: https://engrxiv.org/preprint/view/3233.
3. D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. Vincent Poor. Federated learning for internet of things: A comprehensive survey. *IEEE Communications Surveys & Tutorials* 23 (3), 2021, pp. 1622–1658. Доступне за посиланням: https://ieeexplore.ieee.org/document/9415623/.
4. T. Zhang, L. Gao, C. He, M. Zhang, B. Krishnamachari, and S. Avestimehr. Federated learning for internet of things: Applications, challenges, and opportunities. 2022. Доступне за посиланням: http://arxiv.org/abs/2111.07494.
5. Z. Chen, H. Cui, E. Wu, and Y. Xi. Efficient adaptive federated optimization of federated learning for IoT. 2022. Доступне за посиланням: http://arxiv.org/abs/2206.11448.
6. E. Dritsas and M. Trigka. Federated learning for IoT: A survey of techniques, challenges, and applications. *Journal of Sensor and Actuator Networks* 14 (1), 2025, pp. 9. Доступне за посиланням: https://www.mdpi.com/2224-2708/14/1/9.
7. F. J. Piran, Z. Chen, M. Imani, and F. Imani. Privacy-preserving federated learning with differentially private hyperdimensional computing. 2024. Доступне за посиланням: http://arxiv.org/abs/2411.01140.
8. Z. Chen, H. Cui, E. Wu, and X. Yu. Computation and communication efficient adaptive federated optimization of federated learning for internet of things. *Electronics* 12 (16), 2023, pp. 3451. Доступне за посиланням: https://www.mdpi.com/2079-9292/12/16/3451.
9. Y. Liu, Y. Kang, T. Zou, Y. Pu, Y. He, X. Ye, Y. Ouyang, Y.-Q. Zhang, and Q. Yang. Vertical federated learning: Concepts, advances and challenges. *IEEE Transactions on Knowledge and Data Engineering* 36 (7), 2024, pp. 3615–3634. Доступне за посиланням: http://arxiv.org/abs/2211.12814.
10. T. Sun, D. Li, and B. Wang. Decentralized federated averaging. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 45 (4), 2023, pp. 4289–4301. Доступне за посиланням: https://ieeexplore.ieee.org/document/9850408.

References

1. David Reinsel. How You Contribute to Today's Growing DataSphere and Its Enterprise Impact. Available at: https://blogs.idc.com/2019/11/04/how-you-contribute-to-todays-growing-datasphere-and-its-enterprise-impact
2. E. Alam. Federated averaging algorithm: An analysis of distributed machine learning. 2023. Available at: https://engrxiv.org/preprint/view/3233.
3. D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. Vincent Poor. Federated learning for internet of things: A comprehensive survey. *IEEE Communications Surveys & Tutorials* 23 (3), 2021, pp. 1622–1658. Available at: https://ieeexplore.ieee.org/document/9415623/.
4. T. Zhang, L. Gao, C. He, M. Zhang, B. Krishnamachari, and S. Avestimehr. Federated learning for internet of things: Applications, challenges, and opportunities. 2022. Available at: http://arxiv.org/abs/2111.07494.
5. Z. Chen, H. Cui, E. Wu, and Y. Xi. Efficient adaptive federated optimization of federated learning for IoT. 2022. Available at: http://arxiv.org/abs/2206.11448.
6. E. Dritsas and M. Trigka. Federated learning for IoT: A survey of techniques, challenges, and applications. *Journal of Sensor and Actuator Networks* 14 (1), 2025, pp. 9. Available at: https://www.mdpi.com/2224-2708/14/1/9.
7. F. J. Piran, Z. Chen, M. Imani, and F. Imani. Privacy-preserving federated learning with differentially private hyperdimensional computing. 2024. Available at: http://arxiv.org/abs/2411.01140.
8. Z. Chen, H. Cui, E. Wu, and X. Yu. Computation and communication efficient adaptive federated optimization of federated learning for internet of things. *Electronics* 12 (16), 2023, pp. 3451. Available at: https://www.mdpi.com/2079-9292/12/16/3451.
9. Y. Liu, Y. Kang, T. Zou, Y. Pu, Y. He, X. Ye, Y. Ouyang, Y.-Q. Zhang, and Q. Yang. Vertical federated learning: Concepts, advances and challenges. *IEEE Transactions on Knowledge and Data Engineering* 36 (7), 2024, pp. 3615–3634. Available at: http://arxiv.org/abs/2211.12814.
10. T. Sun, D. Li, and B. Wang. Decentralized federated averaging. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 45 (4), 2023, pp. 4289–4301. Available at: https://ieeexplore.ieee.org/document/9850408.