

<https://doi.org/10.31891/2219-9365-2024-80-11>

УДК 004.[6+8]

ПАВЛЮК Олена

Національний університет "Львівська політехніка"

<https://orcid.org/0000-0003-4561-3874>

e-mail: olena.m.payliuk@lpnu.ua

МЕДИКОВСЬКИЙ Микола

Національний університет "Львівська політехніка"

<https://orcid.org/0000-0003-2492-8578>

e-mail: mykola.o.medykovskiy@lpnu.ua

МІЩУК Мирослав

Національний університет "Львівська політехніка"

<https://orcid.org/0000-0001-8723-2514>

e-mail: myroslav.mishchuk.mknus.2023@lpnu.ua

ЛИТОВСЬКА Олена

Національний університет "Львівська політехніка"

<https://orcid.org/0009-0000-5246-4008>

e-mail: olena.litovska.kn.2021@lpnu.ua

КОСТИНСЬКИЙ Дмитро

Національний університет "Львівська політехніка"

<https://orcid.org/0009-0001-8970-1473>

e-mail: dmytro.kostynskiy.kn.2021@lpnu.ua

ЗАБОЛОТНА Анастасія

Національний університет "Львівська політехніка"

<https://orcid.org/0009-0003-0389-3801>

e-mail: anastasiia.zabolotna.oi.2024@lpnu.ua

АСПЕКТИ РОЗРОБКИ СИСТЕМ ФЕДЕРАТИВНОГО НАВЧАННЯ В ЛЮДИНООРІЄНТОВАНОМУ ПРОМИСЛОВОМУ ПІДПРИЄМСТВІ

При переході від Індустрії 4.0 до Індустрії 5.0 фокус сучасної промисловості зміщується від людиноорієнтованості до людиноцентричності. Федеративне навчання (ФН) є найбільш ефективною інноваційною концепцією машинного навчання смарт індустрії. У цій публікації проаналізовано підходи до розробки людиноцентричних систем ФН, що впроваджуються на промислових підприємствах з використанням керованих робототехнічних платформ, інтернету речей персоналу та промислового інтернету речей. Проаналізовано схеми локально-централізованих і глобально-централізованих ФН. Для промислового підприємства розроблено покрокову реалізацію локально-централізованої та глобально-централізованої ФН.

Виявлено, що локально-централізоване ФН забезпечує високий рівень захисту конфіденційності, оскільки дані обробляються і зберігаються безпосередньо на пристрої. Використання централізованого сервера зменшує затримки обробки даних. Однак загальність моделі обмежена, оскільки агреговані дані можуть не враховувати умови роботи всього підприємства.

Широкий спектр умов може бути врахований і модель може бути збагачена за допомогою глобально-локально-централізованої ФН. Модель виявилася корисною при розробці систем для промислових компаній, що використовують інтернет речей персоналу та промисловий інтернет речей. Така архітектура підвищує ризик втрати конфіденційності через централізований обмін даними. Передача великих обсягів оновлених моделей є критичною у випадку ресурсомістких процесів.

Ключові слова: Індустрія 4.0, Індустрія 5.0, людиноорієнтованість, захист, моделі.

PAVLIUK Olena, MEDYKOVSKYY Mykola, MISHCHUK Myroslav, LITOVSKA Olena,
KOSTINSKYI Dmytro, ZABOLOTNA Anastasiia
Lviv Polytechnic National University

ASPECTS OF THE DEVELOPMENT OF FEDERATION LEARNING SYSTEMS IN A HUMAN-ORIENTED INDUSTRIAL ENTERPRISE

In the transition from Industry 4.0 to Industry 5.0, the focus of modern industry shifts from people-oriented to people-centric. Federated learning (FL) is the most effective innovative concept of machine learning in the smart industry. This publication analyzes approaches to the development of human-centric FL systems implemented in industrial enterprises using controlled robotic platforms, the Internet of personel Internet of Things, and the Industrial Internet of Things. The schemes of locally-centralized and globally-centralized FL are analyzed. A step-by-step implementation of locally-centralized and globally-centralized FL has been developed for an industrial enterprise.

It was found that locally-centralized FL provides a high level of privacy protection, since data is processed and stored directly on the device. Using a centralized server reduces data processing delays. However, the generality of the model is limited, since the aggregated data may not take into account the operating conditions of the entire enterprise.

A wide range of conditions can be taken into account and the model can be enriched with the help of global-local-

centralized FL. The model proved to be useful in the development of systems for industrial companies using the Internet of personel Internet of Things and the Industrial Internet of Things. Such an architecture increases the risk of loss of privacy due to centralized data exchange. The transfer of large volumes of updated models is critical in the case of resource-intensive processes.

Key words: Industry 4.0, Industry 5.0, human orientation, protection, models.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Сучасна промисловість при переході від Індустрії 4.0 до Індустрії 5.0 все більше уваги приділяє використанню нових технологій, які автоматизують процеси та підвищують ефективність компаній. Однак існує багато викликів щодо інтеграції технологій в існуючі промислові системи. Серед них - забезпечення гнучкості системи з точки зору людського фактору, адаптація до нових умов праці працівників та захист конфіденційних даних. Створення комфортного та безпечного середовища для працівників - ще один аспект успішного впровадження технологій.

На промислових підприємствах особливо важливо впроваджувати як людиноцентричний, так і людиноорієнтований підходи, оскільки безпека і конфіденційність мають першорядне значення. В інтелектуальних галузях, орієнтованих на людину, федеративне навчання (ФН) є найбільш ефективною інноваційною концепцією машинного навчання (МН). Дані не централізовані, а обробляються на різних пристроях. Це забезпечує захист конфіденційної інформації. Навчання рою (НР) слід використовувати в поєднанні з ФН для підвищення безпеки, конфіденційності, децентралізації та ефективності обробки даних. Високий рівень безпеки, який забезпечує технологія блокчейн, гарантує підвищення ефективності. Це важливо для промислових компаній, які працюють з конфіденційними даними. Розробка архітектури системи вимагає ретельного проектування для впровадження ФН, оскільки враховуються як технічні аспекти, так і специфіка взаємодії між персоналом.

У «розумних» галузях промисловості дані надходять з багатьох пристроїв. Інтернет речей (ІР) можна використовувати для моніторингу стану навколишнього середовища, здоров'я персоналу та логістичних операцій. Виробничі обладнання, роботизовані системи і камери збирають інформацію про ефективність і якість процесів. Єдина мережа збору та обробки даних дозволяє компаніям швидко приймати рішення, покращувати прогнозування та виробничі витрати, а також виявляти потенційні помилки.

У пропонованій роботі розглядаються дані, отримані з сенсорів ІР персоналу, таких як смарт-годинники і мобільні телефони, а також з керованих роботизованих платформ (КРП). Зібрана інформація включає показники активності, рухів та фізіологічного стану персоналу, отримані за допомогою сенсорів портативних пристроїв; дані з КРП фіксують ключові параметри поведінки робота, такі як рухи робота, виконані завдання та стан технічної системи.

АНАЛІЗ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

У дослідженнях показано високий потенціал ФН для використання на промислових підприємствах. Це особливо актуально, коли йдеться про захист конфіденційної інформації або коли централізація даних небажана з технічних чи економічних причин. Використання федеративного підходу дозволяє підвищити рівень довіри співробітників і клієнтів до систем штучного інтелекту (ШІ) на підприємстві, що є важливим фактором у процесі впровадження інновацій.

У статті [1] представлено ФН та систему обміну даними зі збереженням конфіденційності на основі блокчейну. Проблеми конфіденційності та масштабованості були вирішені технічною синергією. Запропонована міжрівнева архітектура, яка включає диференційований обмін даними та цільовий механізм стимулювання. Це показало значні покращення продуктивності порівняно з існуючими схемами з точки зору швидкості та корисності постачальника. У публікації [2] представлено інтегровану структуру ФН, яка поєднує гібридну диференціальну конфіденційність і адаптивне стиснення для підвищення конфіденційності промислових даних під час навчання моделі на межі. Підхід, запропонований авторами, максимізує захист конфіденційності від атак логічного висновку шляхом адаптивного стиснення градієнта та застосування диференційованої конфіденційності, демонструючи значну ефективність у захисті даних терміналів у периферійних обчислювальних середовищах.

У публікаціях [3, 4] розглядаються поточні рішення безпеки та конфіденційності для КРП і аналізуються проблеми їх інтеграції та ефективність із розподіленими технологіями. Існує потреба в надійних механізмах конфіденційності та безпеки для забезпечення безпеки і прозорості даних. Виділено різні сценарії кібератак, а також стратегії стійкості для захисту безпеки і прозорості даних. Для підвищення безпеки в кіберфізичних системах, заснованих на Інтернеті медичних речей, пропонується легка гібридна модель, яка поєднує контрольоване машинне навчання (МН) та криптоаналіз. У [5] запропонована система має на меті покращити швидкість автентифікації та зменшити накладні витрати на зв'язок, одночасно здійснюючи безпечну передачу даних, демонструючи значні переваги в безпеці та продуктивності порівняно з попередніми підходами. У [6] автори представили багаторівневу структуру ФН, яка поєднує ІР і краудсорсингове навчання для створення динамічного середовища для багатоцільового навчання. Цей підхід

підтримує такі інтелектуальні програми, як прогнозоване технічне обслуговування в інтелектуальному виробництві, а також сприяє досягненню цілей сталого розвитку шляхом зменшення викидів вуглецю.

Публікації [7, 8, 9] демонструють, як ФН може покращити прогноз споживання енергії КРП, використовуючи розподілені знання між ними. Багаторандомний підхід і нещодавні експерименти на реальних даних КРП показують, що ФН краще виявляє аномалії, ніж централізовані методи. Таким чином сприяють більш ефективному управлінню автопарком у інтелектуальному виробництві.

Наукові дослідження у цій сфері показують, що питання захисту даних стає особливо важливим на підприємствах з високими вимогами до безпеки, таких як оборонна промисловість, фармацевтика чи фінансовий сектор. Огляд літератури свідчить, що впровадження ФН разом з НР з підходами до захисту даних може знизити ризики компрометації інформації та підвищити довіру до нових технологій серед працівників та керівництва.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Однією з основних цілей статті є глибокий аналіз підходів до розробки систем ФН, орієнтованих на потреби людини, які впроваджують на промислових підприємствах із використанням КРП та ІР персоналу.

Метою даної наукової публікації є аналіз та розробка ефективних підходів до реалізації систем ФН у промислових підприємствах орієнтованих на людину. Для цього необхідно оцінити можливості та обмеження ФН для інтеграції з системами КРП та ІР персоналу. А також розробити рекомендації для впровадження таких систем з врахуванням специфіки промислових середовищ і людських факторів. Тим самим забезпечити практичні аспекти впровадження технологій ФН для покращення ефективності, безпеки та продуктивності в промислових підприємствах.

Основні завдання дослідження є:

1. Аналіз сучасних підходів до ФН (детальний огляд існуючих методів та оцінка їх застосування в контексті промислових підприємств які використовують КРП і ІР персоналу).
2. Оцінка специфіки людиноорієнтованих підходів у промисловості та аналіз можливості інтеграції технологій ФН з урахуванням людського фактору дослідивши як ці підходи впливають на ефективність і безпеку в промислових умовах.
3. Розробка архітектури ФН для КРП та ІР персоналу (розробити та описати архітектуру системи та визначити її основні компоненти, моделі взаємодії між ними та ролі персоналу).
4. Оцінка викликів та рішень при впровадженні: виявити основні виклики при зборі, зберіганні та обробці даних у децентралізованих системах; розробити рішення для забезпечення безпеки та конфіденційності даних та проаналізувати технічні обмеження, такі для подальших досліджень і вдосконалення технологій в контексті людиноорієнтованих промислових підприємств.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Забезпечення конфіденційності є одним із найважливіших аспектів у контексті ФН. Під час передачі оновлень моделі між локальними пристроями та центральним сервером виникають ці проблеми. Одним із найпопулярніших підходів до забезпечення конфіденційності є диференціальна конфіденційність, яка дозволяє приховувати дані окремих користувачів у великих наборах даних. Інші методи, такі як захищене багатоагентне обчислення та гомоморфне шифрування, дозволяють виконувати операції над зашифрованими даними без необхідності їх розшифрувати. Таким чином можна забезпечити високий рівень захисту в процесі обміну даними між різними пристроями або підрозділами підприємства. Управління доступом та контроль прав – це теж ефективні механізми, які обмежують доступ до даних, надаючи лише уповноваженим користувачам можливість працювати з інформацією. Проте найефективнішим методом є ФН, яке дозволяє навчати моделі без передачі даних на централізований сервер, обробляючи їх локально на пристроях, що підвищує захист конфіденційності.

ФН — це нова концепція у сфері МН, яка дозволяє навчати моделі на розподілених даних без необхідності зберігати їх у централізованому місці. Основна ідея ФН полягає в тому, що дані залишаються на локальному пристрої або серверах, а модель, яка підлягає навчанню, надсилається на ці пристрої для оновлення. Єдина глобальна модель оновлюється центральним сервером на основі поєднання локальних.

Основні переваги ФН для промислових підприємств:

- дані не залишають локальні пристрої, зменшує ризик витоку інформації або компрометації.
- оскільки більша частина обробки відбувається на локальних пристроях, зменшення навантаження на центральний сервер є найкращим способом зменшення обчислювальних ресурсів.
- ця технологія добре підходить для великих промислових підприємств з централізованою структурою, де дані збираються з різних джерел.

В людино орієнтованому промисловому підприємстві яке використовує КРП і ІР персоналу, доцільно використовувати ФН у поєднанні з іншими методами, такими як розподілене, передане або онлайн-навчання, навчання роїв (НР) тощо. Модель навчається на даних, розподілених між різними

клієнтськими пристроями без передачі самих даних на центральний сервер. Головною перевагою є збереження конфіденційності даних і зниження ризиків порушення безпеки.

На рис.1 представлено типову схему збору інформації в ФН на промисловому підприємстві яке використовує КРП, IP персоналу та інших типів промислового IP.

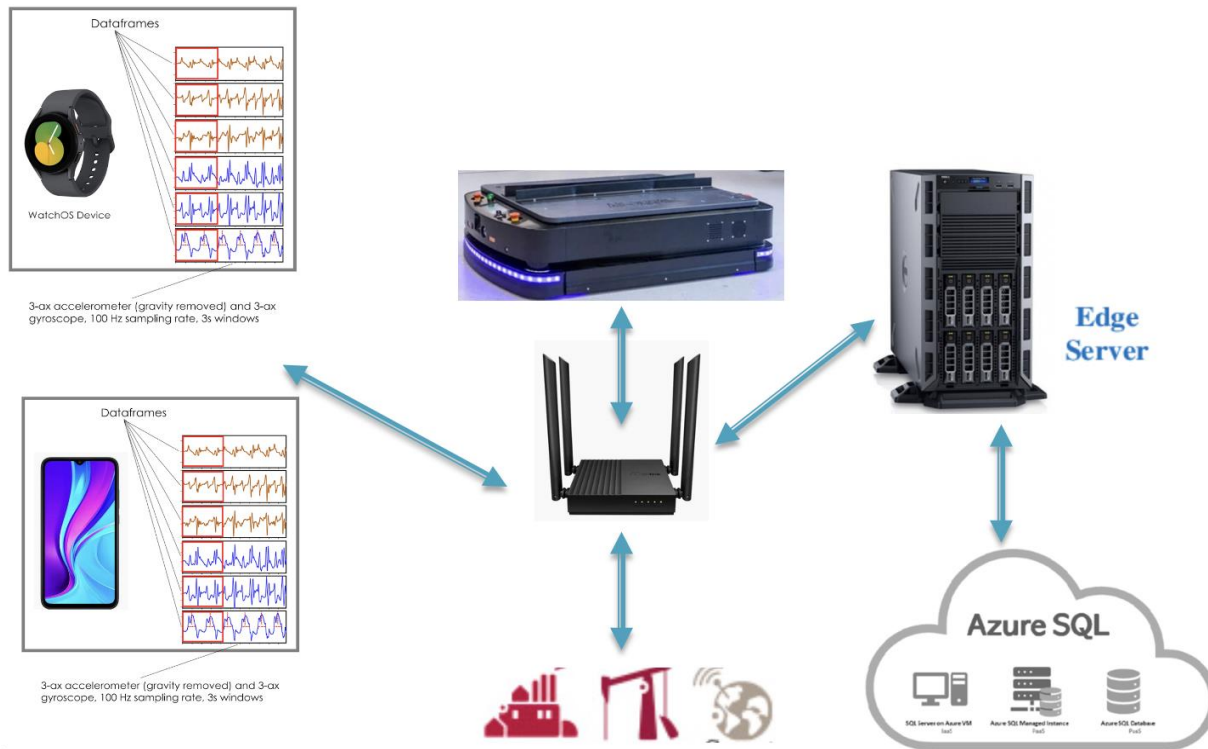


Рис 1 Схема збору даних з IP в межах однієї робочої зони промислового підприємства яке використовує КРП

Дані зібрані з сенсорів по Wi-fi передаються на локальний фізичний крайовий сервер (Edge Server) розміщений переважно на конкретній дільниці промислового підприємства. Він бере на себе деякі функції центрального сервера для оптимізації процесу навчання та підвищення безпеки. Проте його основними функціями є: локальне агрегування даних; покращення швидкості та ефективності навчання; розвантаження центрального сервера; забезпечення конфіденційності та безпеки; підтримка навчання в умовах обмеженої пропускної здатності мережі. Глобальний сервер виконує роль центрального координатора, який збирає локальні оновлення моделей від усіх кінцевих пристроїв або від проміжних крайових серверів, об'єднує їх і створює оновлену глобальну модель. Основні функції та роль глобального сервера у ФН: збір локальних оновлень; агрегування моделей; оновлення глобальної моделі; безпека і контроль доступу; адаптація до змін у середовищі; моніторинг якості моделі.

Кожен КРП та портативний пристрій промислового персоналу має можливість локально навчати моделі на основі зібраних даних. Це дозволяє пристроям адаптуватися до конкретних умов та потреб виробничого процесу без передачі даних на централізований сервер. Дані, зібрані від різних пристроїв IP агрегуються для створення загальної моделі, яка враховує різноманітність умов і використання в реальному часі. ФН дозволяє зберігати конфіденційність даних, оскільки вони залишаються на пристроях і не передаються централізовано. Це особливо важливо у людиноорієнтованих виробничих середовищах, де дані можуть містити комерційно чутливу інформацію. Завдяки ФН система здатна оптимізувати маршрути КРП, покращувати координацію між ними та працівниками, а також зменшувати час налагодження та енергоспоживання.

ФН може мати чотири варіанти реалізації, які враховують специфіку і потреби конкретного виробничого процесу:

1. ФН з локальним агрегуванням моделей - кожен КРП та портативні пристрої промислового персоналу навчають моделі на основі локально зібраних даних. Локальні моделі агрегуються на централізованому сервері, щоб створити загальну модель, яка враховує різноманітність умов і задач.

2. ФН з глобальною координацією - КРП та портативні пристрої збирають дані, які передаються на централізований сервер для глобального навчання моделі. Централізований сервер навчає глобальну модель, використовуючи дані з усіх пристроїв, що дозволяє врахувати загальні тенденції і забезпечує однорідність прийняття рішень.

3. ФН з диференційованою передачею моделі - КРП та портативні пристрої навчають моделі на основі локальних даних. Для агрегації передаються на централізований сервер тільки параметри моделі. Централізований сервер координує процес агрегації моделей, не отримуючи прямий доступ до вихідних даних.

4. ФН з розподіленими обчисленнями - КРП та портативні пристрої обчислюють параметри моделі локально, а результати передаються на централізований сервер для фінальної агрегації. Централізований сервер координує і аналізує результати, оптимізуючи модель з урахуванням всіх локальних обчислень.

Моделі федеративного навчання на людиноорієнтованому підприємстві

ФН дозволяє декільком вузлам (пристроєм) навчати спільну модель МН, залишаючи при цьому всі дані на пристроях. Типовий навчальний раунд у ФН можна розбити на такі кроки:

1. Ініціалізація глобальної моделі

$$\omega^0 \tag{1}$$

2. Вибір клієнтів

На кожному раунді t , сервер вибирає набір клієнтів $K_t \subseteq 1, \dots, N$, де N - загальна кількість клієнтів.

3. Локальне навчання

Кожен вибраний клієнт $k \in K_t$ завантажує глобальну модель ω^t і виконує локальне навчання на своїх даних. Локальне оновлення моделі ω_k^{t+1} отримується за допомогою градієнтного спуску:

$$\omega_k^{t+1} = \omega^t - \eta \Delta L_k(\omega^t) \tag{2}$$

де η - швидкість навчання, $\Delta L_k(\omega^t)$ - градієнт локальної функції втрат клієнта k .

4. Агрегування моделей

Сервер агрегує оновлені моделі від усіх вибраних клієнтів, використовуючи вагове середнє:

$$\omega^{t+1} = \sum_{k \in K_t} \frac{n_k}{n} \omega_k^{t+1} \tag{3}$$

де n_k - кількість даних у клієнта k , $n = \sum_{k \in K_t} n_k$ - загальна кількість даних у всіх вибраних клієнтів.

5. Оновлення глобальної моделі

Оновлена глобальна модель ω^{t+1} розсилається клієнтам для наступного раунду навчання.

На рис. 2 зображена схема типового навчального раунду ФН в людиноорієнтованому підприємстві з локальним агрегуванням моделей. У ньому процес розпочинається з того, що кожен пристрій (наприклад, смарт-годинник або КРП) отримує глобальну модель та оновлює її на основі локальних даних. Після локального навчання оновлені параметри не передаються на централізований сервер, а локально агрегуються між пристроями в межах певної групи або зони, утворюючи консолідовану модель, яка зменшує обсяг передачі даних і підвищує конфіденційність.

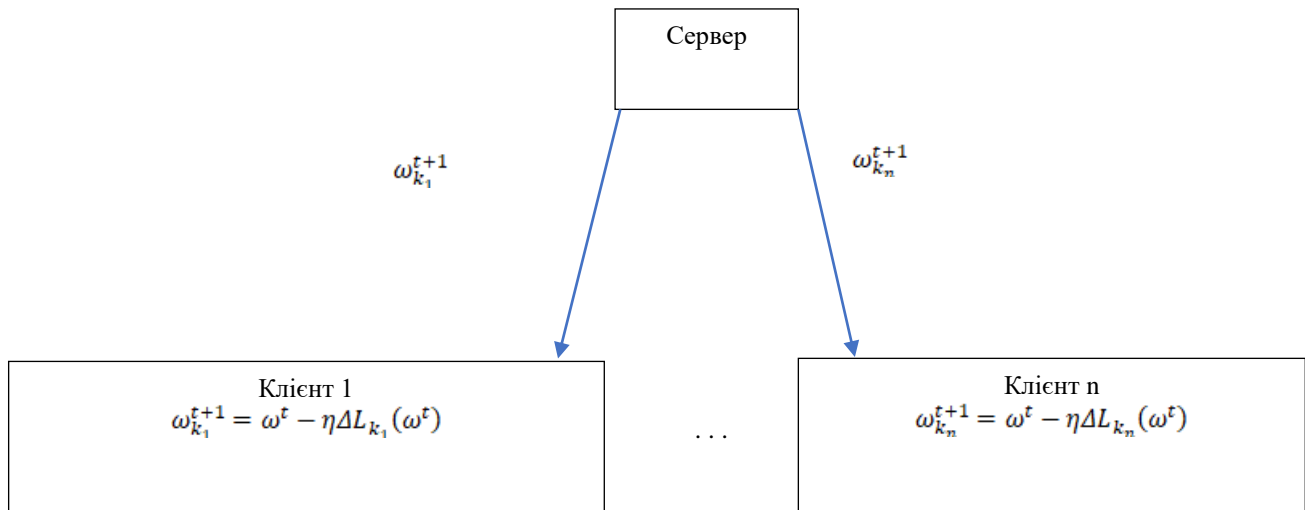


Рис. 2. Схема типового навчального раунду ФН в людиноорієнтованому підприємстві з локальним агрегуванням моделей

Однією з головних переваг цієї схеми є підвищена масштабованість. Розподіл обчислювальних навантажень між локальними координаторами є однією з головних переваг цієї схеми. Завдяки цьому зменшуються затримки на центральному сервері та покращує загальну продуктивність системи. Локальна

агрегація допомагає зберегти конфіденційність даних, оскільки необроблені дані залишаються на рівні локальних пристроїв і не передаються на центральний сервер. Тому знижуються ризики витоку інформації. Ця схема має свої недоліки, зокрема, складна реалізація, яка вимагає додаткових зусиль для налагодження ефективної координації між локальним і глобальним сервером. Вона також може піддаватися певним ризикам у плані безпеки, оскільки кожен локальний координатор стає потенційно вразливим. Забезпечення узгодженості та стабільності моделі під час агрегації може бути проблемою для вирішення якої потрібно ретельного проектування алгоритмів агрегування та синхронізації.

На рис. 3 представлено модель ФН в людиноорієнтованому підприємстві з глобальною координацією. У цій моделі центральний сервер або координатор ініціює процес навчання, надіславши глобальну модель на всі пристрої пристроям (наприклад, КРП, смарт-годинники). Кожен пристрій оновлює цю модель на основі своїх локальних даних, а потім надсилає оновлені параметри глобальному координатору, де вони агрегуються в єдину глобальну модель. Цей підхід вимагає стабільного зв'язку та має вищі вимоги до конфіденційності та безпеки даних. Він забезпечує централізоване керування навчанням, покращує точність і узгодженість моделі при наявності стабільного зв'язку.

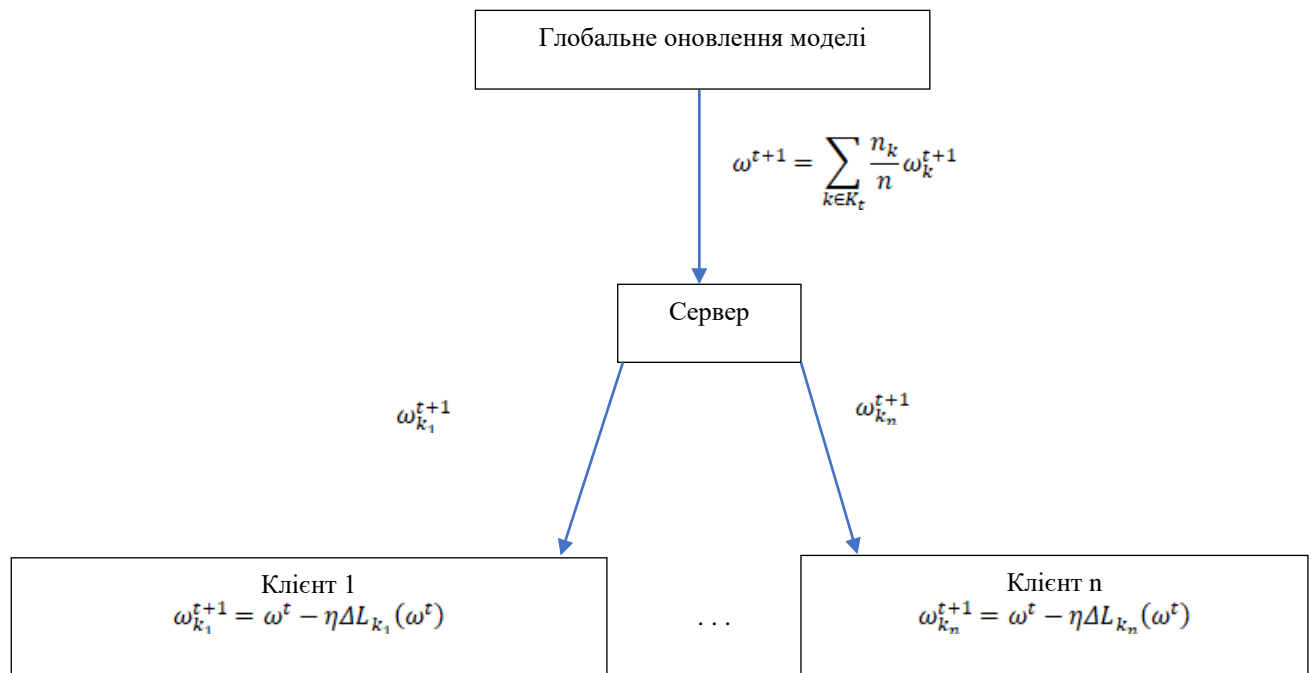


Рис. 3 Модель ФН в людиноорієнтованому підприємстві з глобальною координацією

Основною перевагою цієї схеми є простота впровадження та управління, оскільки централізований сервер координує всіх клієнтів. Він забезпечує єдину точку контролю для збирання, агрегації та оновлення моделей. Це спрощує процес забезпечення узгодженості моделі, що є критично важливим для досягнення високої точності навчання. У випадку великомасштабних систем з великою кількістю клієнтів централізований підхід може викликати велике навантаження на глобальний сервер. Промислові підприємства, орієнтовані на людину, є саме такими. Це може призвести до низької продуктивності системи. Крім того, централізована координація підвищує ризик відмови однієї точки та є вразливою до атак, що може негативно вплинути на надійність і безпеку системи. Хоча схема ФН із глобальною координацією пропонує спрощене керування та узгодженість моделі, вона також має обмеження, пов'язані з продуктивністю та безпекою в контексті великих розподілених систем.

В таблиці 1 здійснено порівняльний аналіз основних видів ФН в людиноорієнтованому підприємстві.

ФН з глобальною координацією включає один глобальний сервер, який збирає моделі для агрегації та надсилає їх усім клієнтам. Локально-централізоване ФН включає локальних координаторів, які збирають моделі від своїх клієнтів і передають оновлені моделі до глобального сервера. Воно має кращу масштабованість і зменшення навантаження на глобальний сервер проте складнішу реалізацію і наявність централізованого компоненту. Завдяки простоті впровадження та централізованому управлінню його доцільно використовувати, але є висока затримка та навантаження на глобальний сервер. Локальні координатори збирають моделі від своїх клієнтів і передають їх на глобальний сервер. Має менше навантаження на глобальний сервер, але більш складну реалізацію та наявність централізованого компонента. Децентралізоване ФН виключає глобальний сервер; клієнти обмінюються моделями

безпосередньо один з одним. Воно має високу масштабованість, низьку затримку, рівномірний розподіл обчислювальних ресурсів. Але має складну реалізацію і складно забезпечити безпеку.

Таблиця 1

Порівняльний аналіз основних видів ФН в людиноорієнтованому підприємстві

| Критерій | ФН з глобальною координацією | Локально-централізоване ФН | Децентралізоване ФН |
|-----------------------------|---|--|--|
| Складність реалізації | Середня | Середня | Висока |
| Масштабованість | Обмежена через вузьке місце в глобальному сервері | Висока | Дуже висока |
| Затримка | Висока через централізовану координацію | Середня | Низька |
| Обчислювальні ресурси | Високі вимоги до глобального сервера | Зменшені вимоги до локальних координаторів | Рівномірний розподіл ресурсів |
| Витрати на зв'язок | Високі | Середні | Низькі |
| Безпека та конфіденційність | Висока (централізований контроль) | Висока (частково централізований контроль) | Середня (декілька точок вразливості) |
| Надійність | Низька через єдину точку відмови | Вища через розподіл координації | Дуже висока (відсутність єдиної точки відмови) |

Модель локально-централізованого федеративного навчання на людиноорієнтованому підприємстві

Як показав аналіз, локально-централізована ФН з декількома локальними координаторами, яка здійснює обмін та агрегацію моделей та досить проста у реалізації. ФН з декількома локальними координаторами замість одного глобального, які здійснюють обмін та агрегування моделей. У цій моделі клієнти об'єднуються в локальні групи, де кожна група має свого координатора. Локальні координатори здійснюють агрегацію моделей для своєї групи, а потім передають оновлені моделі до глобального сервера. Це дозволяє зменшити навантаження на глобальний сервер та покращити масштабованість системи.

Наведемо приклад моделі локально-централізованого ФН на підприємстві, яке використовує КРП, смартгодинники та смартфони персоналу з ціллю прогнозування навантаження на працівників та стану обладнання.

Основні кроки локально-централізованого ФН

1. Збір даних. Смартгодинники та смартфони персоналу збирають інформацію про їхні фізіологічні показники (наприклад, частота серцевих скорочень, рівень стресу) та активність протягом робочого дня. КРП, у свою чергу, фіксують інформацію про свої робочі параметри, такі як рівень заряду батареї, швидкість переміщення та час виконання завдань.

2. Локальне навчання. На кожному смартгодиннику, смартфоні та КРП виконується початкове локальне навчання на основі зібраних даних. Потім локальні моделі надсилають оновлені ваги до серверів, розташованих у межах підприємства, для початкової агрегації.

3. Агрегація на локальному сервері. Локальний сервер підприємства приймає оновлені параметри моделей від всіх пристроїв (смартгодинники, смартфони, КРП) та об'єднує їх у єдину загальну модель, враховуючи умови підприємства. Це дозволяє створити цілісну модель, яка оптимізує робочі процеси та знижує ризик перевантаження персоналу та відмов обладнання.

4. Передача до глобального сервера. Локальна агрегована модель відправляється на центральний сервер, де відбудеться обробка та аналіз загальних моделей від кількох підприємств для глобальної оптимізації та обміну досвідом.

На рис. 4 зображене локально-централізоване ФН для людино орієнтованого промислового підприємства.

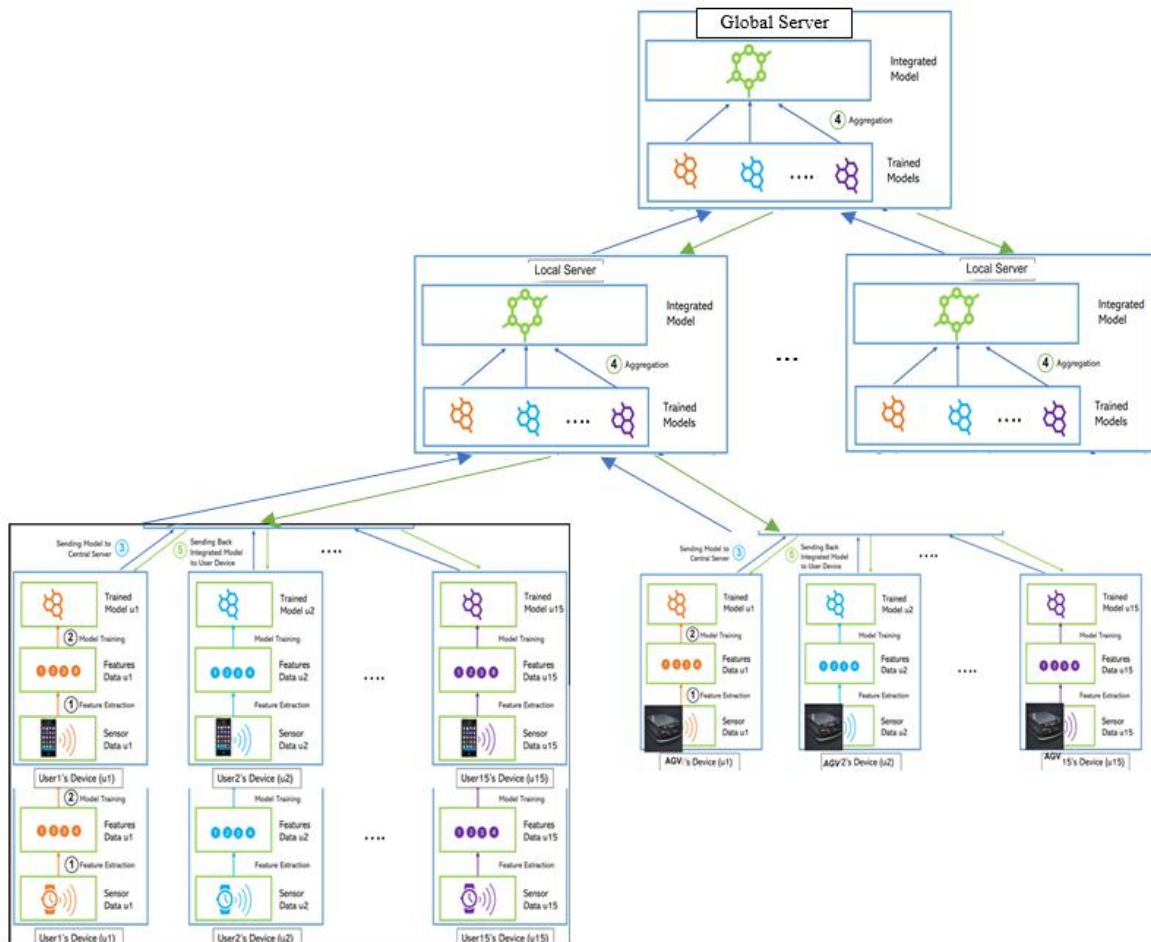


Рис. 4 Локально-централізоване ФН для людино орієнтованого промислового підприємства

В цій структурі глобальний сервер відповідає за збір та агрегацію моделей від локальних координаторів та розсилає оновлену глобальну модель локальним координаторам (наприклад цехам підприємства). Локальні координатори збирають локальні моделі від КРП та портативних пристроїв у своїй зоні відповідальності, агрегують локальні моделі та передають їх глобальному серверу, а також розсилають глобальну модель локальним КРП після отримання від глобального сервера. Локальні клієнти збирають дані про переміщення, завантаження, продуктивність та інші параметри. Далі навчаються на своїх локальних даних і оновлюють локальні моделі та передають оновлені моделі локальному координатору. Портативні пристрої промислового персоналу (смарт годинники та смартфони) збирають дані про активність персоналу, продуктивність, навколишнє середовище та інші параметри, навчаються на локальних даних і оновлюють локальні моделі та передають оновлені моделі локальному координатору.

Локально-централізоване федеративне навчання в людиноорієнтованому підприємстві

Покроково реалізацію локально-централізованого ФН для людино орієнтованого промислового підприємства можна описати таким чином.

1. Ініціалізація. Глобальний сервер розсилає початкову модель ω^f локальним координаторам (Цех 1, Цех 2, ..., Цех n).

2. Розсилання локальних моделей. Локальний координатор Цеху 1 отримує модель ω^f та передає її КРП 1.1, КРП 1.2, ..., КРП 1.k, а також смарт годинникам SW1.1, SW1.2, ..., SW1.o і смартфонам персоналу SP1.1, SP1.2, ..., SP1.p. Локальний координатор Цеху 2 отримує модель ω^f та передає її КРП 2.1, КРП 2.2, ..., КРП 2.l, а також смарт годинникам SW1.1, SW1.2, ..., SW1.o і смартфонам персоналу SP2.1, SP2.2, ..., SP1.g. і т.д. Локальний координатор цеху n отримує модель ω^f та передає її КРП n.1, КРП n.2, ..., КРП n.m. Також смарт, а також смарт годинникам SWn.1, SWn.2, ..., SWn.s і смартфонам персоналу SPn.1, SPn.2, ..., SPn.t.

3. Локальне навчання:

Нехай:

n — кількість цехів.

в першому цеху є k КРП, o смарт годинників та s смартфонів.

в другому цеху є l КРП, p смарт годинників та t смартфонів.

...

в останньому (n -му) цеху є m КРП, r смарт годинників та u смартфонів.

Загальна структура для всіх цехів x від 1 до n

Для кожного КРП i від 1 до до відповідної кількості КРП у цеху x

$$\omega_{kx,i}^{t+1} = \omega^t \eta \Delta L_{kx,i}(\omega^t) \quad (4)$$

де η - швидкість навчання, $\Delta L_{kx,i}(\omega^t) \Delta$ - градієнт локальної функції втрат клієнта $kx.i$.

Для кожного смарт годинника j від 1 до відповідної кількості смарт годинників у цеху x

$$\omega_{px,i}^{t+1} = \omega^t \eta \Delta L_{px,i}(\omega^t) \quad (5)$$

Для кожного смартфона q від 1 до відповідної кількості смартфонів у цеху x

$$\omega_{sx,i}^{t+1} = \omega^t \eta \Delta L_{sx,i}(\omega^t) \quad (6)$$

4. Локальна агрегація. Кожен цех спочатку агрегує свої локальні моделі, щоб отримати одну агреговану модель для кожного типу пристрою (КРП, смарт годинників, смартфонів) Формули агрегації локальних моделей

Агрегація локальних моделей в цеху x . Для кожного цеху x від 1 до n

КРП:

Нехай в цеху x є k_x КРП. Агрегована модель для КРП в цеху x :

$$\omega_{k_x}^{t+1} = \frac{1}{k_x} \sum_{i=1}^{k_x} \omega_{kx,i}^{t+1} \quad (7)$$

Смарт годинники:

Нехай в цеху x є p_x смарт годинників. Агрегована модель для смарт годинників в цеху x :

$$\omega_{p_x}^{t+1} = \frac{1}{p_x} \sum_{j=1}^{p_x} \omega_{px,j}^{t+1} \quad (8)$$

Смартфони:

Нехай в цеху x є s_x смартфонів. Агрегована модель для смартфонів в цеху x :

$$\omega_{s_x}^{t+1} = \frac{1}{s_x} \sum_{q=1}^{s_x} \omega_{qx,j}^{t+1} \quad (9)$$

5. Глобальна агрегація моделей. Глобальний сервер збирає всі локальні агреговані моделі з кожного цеху і обчислює загальну глобальну модель для кожного типу пристрою. Після агрегації моделей в кожному цеху, глобальний сервер агрегує ці моделі для отримання остаточної глобальної моделі.

Агрегована модель для всіх КРП:

Нехай загалом є K КРП (сума всіх КРП в усіх цехах). Глобальна модель для КРП матиме вигляд:

$$\omega_{global,AGV}^{t+1} = \frac{1}{K} \sum_{x=1}^n \sum_{i=1}^{k_x} \omega_{kx,i}^{t+1} \quad (10)$$

Агрегована модель для всіх смарт годинників:

Нехай в цілому є P смарт годинників (сума всіх смарт годинників в усіх цехах). Глобальна модель для смарт годинників:

$$\omega_{llobal,smartwatches}^{t+1} = \frac{1}{P} \sum_{x=1}^n \sum_{j=1}^{p_x} \omega_{px,j}^{t+1} \quad (11)$$

Агрегована модель для всіх смартфонів:

Нехай в цілому є S смартфонів (сума всіх смартфонів в усіх цехах). Глобальна модель для смартфонів:

$$\omega_{lglobal,smartphones}^{t+1} = \frac{1}{S} \sum_{x=1}^n \sum_{q=1}^{s_x} \omega_{sx,q}^{t+1} \quad (12)$$

Загальна глобальна модель. Всі глобальні моделі для різних типів пристроїв комбінуються з урахуванням вагових коефіцієнтів, щоб отримати остаточну глобальну модель.

Фінальна глобальна модель агрегується з урахуванням вагових коефіцієнтів кожного типу пристроїв (КРП, смарт годинників, смартфонів):

$$\omega^{t+1} = \alpha\omega_{global,AGV}^{t+1} + \beta\omega_{global,smartwatches}^{t+1} + \gamma\omega_{global,smartphones}^{t+1} \quad (13)$$

де α , β та γ — вагові коефіцієнти, що відображають важливість внесків від КРП, смарт годинників та смартфонів відповідно.

6. Розсилка оновленої глобальної моделі. Глобальний сервер розсилає нову глобальну модель ω^{t+1} локальним координаторам, і цикл повторюється.

Глобально-локально-централізоване федеративне навчання

Для покращення масштабованості з можливістю підтримки моделю великої кількості клієнтів завдяки багаторівневій агрегації запропоновано використовувати глобально-локально-централізоване ФН (Hierarchical Federated Learning). Така модель поєднує переваги глобального і локального ФН.

Локальна агрегація з меншою обсяг даних які потрібно передавати на глобальний сервер. За рахунок цього зменшується навантаження на нього та затримки в опрацюванні та передачі інформації. Глобальний сервер забезпечує узгодженість та оптимізацію на глобальному рівні. На рис. 5 схематично зображено глобально-локально-централізоване ФН в людиноорієнтованому підприємстві.



Рис.5 Схематичне зображення глобально-локально-централізованого ФН в людиноорієнтованому підприємстві

Покроково реалізацію глобально-локально-централізованого ФН для людино орієнтованого промислового підприємства можна описати таким чином. Є три рівні обробки: локальний рівень (де пристрої збирають дані й виконують попереднє навчання), рівень дільниць підприємства (локальний центральний сервер, що агрегує оновлення для кожної локації) і глобальний рівень (центральний сервер, який об'єднує результати з усіх локацій).

1. Локальний рівень обробки

На кожному пристрої k у певній дільниці підприємства j (наприклад, на смарт-годиннику або КРП) спершу виконується навчання на основі локальних даних. Оцінку моделі ω_k оновлюємо за допомогою стохастичного градієнтного спуску.

1.1. Локальне оновлення моделі на пристрої:

$$\omega_k^{t+1} = \omega_k^t - \eta \Delta f(\omega_k^t; D_k) \quad (14)$$

де:

ω_k^t — модельний вектор параметрів на кроку t ,

η — швидкість навчання,

$\Delta f(\omega_k^t; D_k)$ — градієнт функції втрат для даних D_k на пристрої k .

1.2 Передача локальних оновлень до локального центрального сервера на дільниці підприємства. Після кількох ітерацій навчання пристрій передає оновлену модель ω_k^{t+1} на локальний сервер на дільниці.

2. Рівень агрегації на локальному центральному сервері дільниці

На кожному локальному центральному сервері агрегуються оновлення, отримані від пристроїв у цій дільниці. Нехай дільниця j містить K пристроїв. Тоді локальний сервер j обчислює середнє значення оновлень моделей:

2.1 Агрегація локальних моделей відбувається згідно цієї формули:

$$\omega_j^{t+1} = \frac{1}{K} \sum_{k=1}^K \omega_k^{t+1} \quad (15)$$

Локальний центральний сервер дільниці також може застосовувати додаткові параметри безпеки для шифрування даних перед передачею на глобальний сервер.

3. Глобальний рівень агрегації

Центральний глобальний сервер об'єднує моделі з різних дільниць (наприклад, різних підрозділів або локацій підприємства). Нехай у нас є J регіонів.

3.1 Глобальна агрегація моделей:

$$\omega^{t+1} = \frac{1}{J} \sum_{j=1}^J \omega_j^{t+1} \quad (16)$$

3.2 Оновлення глобальної моделі:

Глобальний сервер обчислює нову загальну модель ω^{t+1} , яка враховує оновлення з усіх регіонів, і передає її на регіональні сервери.

4. Повернення глобальної моделі на рівні дільниць й локальні рівні

4.1 Локальні центральні сервери дільниць приймають глобальну модель і передають її на локальні пристрої для подальшого навчання на основі нових даних. Таким чином, навчання відбувається в циклі, де пристрої регулярно оновлюють модель на своїх локальних даних і обмінюються цими оновленнями.

Загальна мета навчання — мінімізувати функцію втрат для всіх пристроїв на підприємстві описується формулою:

$$\min_{\omega} \sum_{j=1}^J \sum_{k=1}^K f(\omega; D_k) \quad (17)$$

Цей підхід забезпечує збалансоване навчання між локальними і глобальними моделями, що дозволяє інтегрувати різні пристрої з урахуванням конфіденційності й продуктивності. Конфіденційні дані не покидають пристрої й сервери на дільницях підприємства. Локальні й глобальні моделі адаптуються до специфіки кожного підрозділу. Узагальнення оновлень на глобальному сервері дозволяє оптимізувати загальну модель для всього підприємства.

Основними перевагами глобально-локально-централізованого ФН є:

1. Захист конфіденційності даних. Оскільки локальне навчання на пристроях (наприклад, на ІР персоналу або КРП) забезпечує обробку даних без їх передачі на центральний сервер, це знижує ризики витоку особистої інформації працівників та корпоративних даних підприємства.

2. Моделі, орієнтовані на умови роботи. Глобально-локально-централізований підхід дозволяє моделі враховувати специфіку роботи на різних ділянках підприємства. Наприклад, модель може враховувати унікальні умови праці кожного відділу, де використовуються КРП або смарт-пристрої, що підвищує точність і корисність моделей.

3. Гнучке розподілене навчання. Глобальний сервер дозволяє зібрати оновлення з усіх локальних моделей і забезпечити їхній обмін для підвищення загальної ефективності навчання. Це підвищує якість прогнозів, оскільки навчання адаптується до об'єднаних даних з усього підприємства.

4. Оптимізація продуктивності. Централізований сервер ФН забезпечує координацію між моделями, що дозволяє швидше виявляти аномалії, оптимізувати виробничі процеси, а також підвищувати ефективність взаємодії людей і машин.

5. Адаптивність до змін. Глобальна модель постійно оновлюється, що дозволяє підприємству адаптуватися до нових умов (наприклад, змін у робочих процесах, завантаженості, умов праці) і підтримувати актуальність аналізу.

Для цього типу ФН є обмеження. А саме високі вимоги до обчислювальних ресурсів. Обробка локальних оновлень моделі потребує великої обчислювальної потужності. Глобальний сервер може стати перевантаженим якщо дані надходять від великої кількості пристроїв або кінцевих користувачів. Також існують затримки передачі даних. Залежність від глобального сервера викликає затримки, особливо з низькою пропускну здатністю мережі або нестабільними з'єднаннями. Через це оновлення моделей може бути складнішим. Це може знижувати оперативність оновлення моделей. У випадках втрати зв'язку або зниження пропускну здатності мережі можуть виникати збої в обміні даними та оновленні моделі. Перешкоди і високе навантаження на лінії зв'язку - поширене явище на промислових підприємствах. Для ефективної роботи централізованої системи необхідна підтримка стабільного мережевого з'єднання між локальними пристроями та глобальним сервером. На точність і безперервність навчання можуть вплинути збої в мережі. Централізований збір і обробка зведених оновлень може нести ризики, пов'язані з витоків інформації.

Хоча в локальних моделях дані користувачів не передаються безпосередньо агреговані оновлення можуть бути піддані атакам, що вимагає додаткових методів захисту. Налаштування та підтримка глобально-локально-центрального ФН — це складний процес, який вимагає технічних знань і великих ресурсів для управління мережею, безпекою, обчислювальним середовищем і підтримки стабільного зв'язку між компонентами системи. Витрати на підтримку швидкої мережі та оновлення кінцевих пристроїв можуть збільшити витрати підприємства, тому така система потребує інвестицій у потужний сервер. Таким чином, сучасні підходи до розробки систем ФН в промислових підприємствах зосереджуються на забезпеченні балансу між захистом даних, автоматизацією процесів та врахуванням людського фактору, що є ключем до успішного впровадження інновацій.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ

І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

З переходом від Індустрії 4.0 до Індустрії 5.0 фокус промисловості зміщується від людиноорієнтованого на людиноцентричний підхід. ФН є ключовим елементом цієї трансформації, дозволяючи обробляти дані на локальному рівні із використанням КРП та ІР персоналу. Провівши аналіз підходів до розробки систем ФН було виявлено ряд обмежень.

Локально-центрально-обчислюване ФН забезпечує обробку даних на рівні окремих підприємств, що дозволяє зменшити потребу у зовнішніх ресурсах, але обмежує можливість узагальнення моделей і залежить від продуктивності локальних пристроїв. Такий підхід зменшує взаємодію між відділами, що може обмежити доступ до загальної інформації. Локально-центрально-обчислюване ФН має обмежену узагальнюваність моделей; висока залежність від продуктивності локальних пристроїв; мінімізація взаємодії між відділами.

Глобально-локально-центрально-обчислюване ФН використовує центральний сервер для об'єднання моделей, що підвищує ефективність, але створює залежність від центральної інфраструктури та ускладнює масштабування через високі вимоги до ресурсів. Цей підхід є менш гнучким для програм із високими вимогами до конфіденційності через ризики конфіденційності, пов'язані з централізацією. Тому глобально-локально-центрально-обчислюване ФН: залежність від центрального сервера; зниження конфіденційності; високі вимоги до обчислювальних ресурсів; складність масштабування.

Обидва підходи вимагають ретельного балансу між ефективністю, конфіденційністю, обчислювальними потребами і функціональністю мережі в залежності від вимог підприємства. В результаті ми розробили людино-орієнтовану систему ФН для промислових підприємств на основі глобально-локально-центрально-обчислюваної ФН з використанням КРП і персональних пристроїв IoT, таких як смартфони і смарт-годинники.

Подальші дослідження спрямовані на усунення обмежень цієї системи. Для цього було запропоновано використання НР [10]. Наприклад, рій агентів може досліджувати різні комбінації локальних моделей, щоб знайти оптимальне злиття, яке покращує загальну точність; завдяки алгоритму НР агрегацію можна адаптувати, щоб уникнути втрати інформації, зберігаючи при цьому важливі закономірності, які можуть бути присутніми в окремих наборах даних. Алгоритм НР можна адаптувати, щоб уникнути втрати інформації, зберігаючи при цьому важливі закономірності, які можуть бути присутніми в окремих наборах даних. В процесі навчання рій агентів може адаптувати свою стратегію агрегації на основі результатів глобальної та локальної моделей. Це дозволяє підвищити точність і знизити ризики, пов'язані зі зміною даних і умов роботи.

Література

1. Liu, Yuan, Peng Liu, Weipeng Jing, Houbing Herbert Song. "PD2S: A Privacy-Preserving Differentiated Data Sharing Scheme Based on Blockchain and Federated Learning." IEEE Internet of Things Journal, vol. 10, no. 24, Dec. 2023, pp. 21489–501. DOI.org (Crossref), <https://doi.org/10.1109/IJOT.2023.3295763>
2. Jiang, Bin, Jianqiang Li, Huihui Wang, Houbing Song. "Privacy-Preserving Federated Learning for Industrial Edge Computing via Hybrid Differential Privacy and Adaptive Compression." IEEE Transactions on

- Industrial Informatics, vol. 19, no. 2, Feb. 2023, pp. 1136–44. DOI.org (Crossref), <https://doi.org/10.1109/TH.2021.3131175>
3. Khan, Rabia, Amjad Mehmood, Carsten Maple, Kevin Curran, Houbing Herbert Song. "Performance Analysis of Blockchain-Enabled Security and Privacy Algorithms in Connected and Autonomous Vehicles: A Comprehensive Review." IEEE Transactions on Intelligent Transportation Systems, vol. 25, no. 6, June 2024, pp. 4773–84. DOI.org (Crossref), <https://doi.org/10.1109/TITS.2023.3341358>
 4. Adil, Muhammad, Muhammad Khurram Khan, Muhammad Mohsin Jadoon, et al. "An AI-Enabled Hybrid Lightweight Authentication Scheme for Intelligent IoMT Based Cyber-Physical Systems." IEEE Transactions on Network Science and Engineering, vol. 10, no. 5, Sept. 2023, pp. 2719–30. DOI.org (Crossref), <https://doi.org/10.1109/TNSE.2022.3159526>
 5. Ullah, Ihsan, Umair Ul Hassan, Muhammad Intizar Ali. "Multi-Level Federated Learning for Industry 4.0 - A Crowdsourcing Approach." Procedia Computer Science, vol. 217, 2023, pp. 423–35. DOI.org (Crossref), <https://doi.org/10.1016/j.procs.2022.12.238>
 6. Shubyn, B., D. Kostrzewa, P. Grzesik, P. Benecki, T. Maksymyuk, V. Sunderam, J.H. Syu, and J.C.W. Lin. "Federated Learning for Improved Prediction of Failures in Autonomous Guided Vehicles." Journal of Computational Science, 2023, 101956. <https://doi.org/10.1016/j.jocs.2023.101956>
 7. Pavliuk, Olena, Rafal Cupek, Tomasz Steclik, Mykola Medykovskyy, and Marek Drewniak. "A Novel Methodology Based on a Deep Neural Network and Data Mining for Predicting the Segmental Voltage Drop in Automated Guided Vehicle Battery Cells." Electronics, vol. 12, no. 22, Nov. 2023, p. 4636. <https://doi.org/10.3390/electronics12224636>
 8. Shubyn, B., D. Mrozek, T. Maksymyuk, V.S. Sunderam, D. Kostrzewa, and P. Grzesik. "Federated Learning for Anomaly Detection in Industrial IoT-Enabled Production Environment Supported by Autonomous Guided Vehicles." In: Groen, D., de Mulatier, C., Paszynski, M., Krzhizhanovskaya, V.V., Dongarra, J.J., Sloot, P.M.A. (eds) Computational Science – ICCS 2022. Lecture Notes in Computer Science, vol. 13353, Springer, Cham, 2022, pp. 409–421.
 9. Pavliuk, Olena, Myroslav Mishchuk, and Christine Strauss. "Transfer Learning Approach for Human Activity Recognition Based on Continuous Wavelet Transform." Algorithms, vol. 16, no. 2, Feb. 2023, p. 77. <https://doi.org/10.3390/a16020077>
 10. Jamil, Harun, Yang Jian, Faisal Jamil, Shabir Ahmad "Swarm Learning Empowered Federated Deep Learning for Seamless Smartphone-Based Activity Recognition". IEEE Transactions on Consumer Electronics, 2024, pp. 1–1. DOI.org (Crossref), <https://doi.org/10.1109/TCE.2024.3479078>

References

1. Liu, Yuan, Peng Liu, Weipeng Jing, Houbing Herbert Song. "PD2S: A Privacy-Preserving Differentiated Data Sharing Scheme Based on Blockchain and Federated Learning." IEEE Internet of Things Journal, vol. 10, no. 24, Dec. 2023, pp. 21489–501. DOI.org (Crossref), <https://doi.org/10.1109/JIOT.2023.3295763>
2. Jiang, Bin, Jianqiang Li, Huihui Wang, Houbing Song. "Privacy-Preserving Federated Learning for Industrial Edge Computing via Hybrid Differential Privacy and Adaptive Compression." IEEE Transactions on Industrial Informatics, vol. 19, no. 2, Feb. 2023, pp. 1136–44. DOI.org (Crossref), <https://doi.org/10.1109/TH.2021.3131175>
3. Khan, Rabia, Amjad Mehmood, Carsten Maple, Kevin Curran, Houbing Herbert Song. "Performance Analysis of Blockchain-Enabled Security and Privacy Algorithms in Connected and Autonomous Vehicles: A Comprehensive Review." IEEE Transactions on Intelligent Transportation Systems, vol. 25, no. 6, June 2024, pp. 4773–84. DOI.org (Crossref), <https://doi.org/10.1109/TITS.2023.3341358>
4. Adil, Muhammad, Muhammad Khurram Khan, Muhammad Mohsin Jadoon, et al. "An AI-Enabled Hybrid Lightweight Authentication Scheme for Intelligent IoMT Based Cyber-Physical Systems." IEEE Transactions on Network Science and Engineering, vol. 10, no. 5, Sept. 2023, pp. 2719–30. DOI.org (Crossref), <https://doi.org/10.1109/TNSE.2022.3159526>
5. Ullah, Ihsan, Umair Ul Hassan, Muhammad Intizar Ali. "Multi-Level Federated Learning for Industry 4.0 - A Crowdsourcing Approach." Procedia Computer Science, vol. 217, 2023, pp. 423–35. DOI.org (Crossref), <https://doi.org/10.1016/j.procs.2022.12.238>
6. Shubyn, B., D. Kostrzewa, P. Grzesik, P. Benecki, T. Maksymyuk, V. Sunderam, J.H. Syu, and J.C.W. Lin. "Federated Learning for Improved Prediction of Failures in Autonomous Guided Vehicles." Journal of Computational Science, 2023, 101956. <https://doi.org/10.1016/j.jocs.2023.101956>
7. Pavliuk, Olena, Rafal Cupek, Tomasz Steclik, Mykola Medykovskyy, and Marek Drewniak. "A Novel Methodology Based on a Deep Neural Network and Data Mining for Predicting the Segmental Voltage Drop in Automated Guided Vehicle Battery Cells." Electronics, vol. 12, no. 22, Nov. 2023, p. 4636. <https://doi.org/10.3390/electronics12224636>
8. Shubyn, B., D. Mrozek, T. Maksymyuk, V.S. Sunderam, D. Kostrzewa, and P. Grzesik. "Federated Learning for Anomaly Detection in Industrial IoT-Enabled Production Environment Supported by Autonomous Guided Vehicles." In: Groen, D., de Mulatier, C., Paszynski, M., Krzhizhanovskaya, V.V., Dongarra, J.J., Sloot, P.M.A. (eds) Computational Science – ICCS 2022. Lecture Notes in Computer Science, vol. 13353, Springer, Cham, 2022, pp. 409–421.
9. Pavliuk, Olena, Myroslav Mishchuk, and Christine Strauss. "Transfer Learning Approach for Human Activity Recognition Based on Continuous Wavelet Transform." Algorithms, vol. 16, no. 2, Feb. 2023, p. 77. <https://doi.org/10.3390/a16020077>
10. Jamil, Harun, Yang Jian, Faisal Jamil, Shabir Ahmad "Swarm Learning Empowered Federated Deep Learning for Seamless Smartphone-Based Activity Recognition". IEEE Transactions on Consumer Electronics, 2024, pp. 1–1., <https://doi.org/10.1109/TCE.2024.3479078>