УДК 621.391

М. В. Будаш [1]
А. В. Прикмета[1]
А. О. Олійник[1]
Н. В. Грабчак[1]

ІНФОРМАЦІЙНА БЕЗПЕКА ІНТЕЛЕКТУАЛЬНИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

[1] Вінницький національний технічний університет

Анотація

Досліджено використання периферійного ШІ для розгортання додатків на межі мережі, що створює потужну інфраструктуру для високопродуктивних та безпечних додатків. Розглянуто застосування блокчейну у федеративних системах охорони здоров'я, що допомагає забезпечити інформаційну безпеку, прозорість і незмінність даних, а також децентралізований характер спільного навчання, що робить цю технологію дуже привабливою для областей, де є важливими конфіденційність та точність.

Ключові слова: штучний інтелект, інфокомунікаційна система з використанням блокчейну, інтегрована радіолокаційно-комунікаційна система, голографічна телеприсутність, розширена реальність

Abstract

The use of edge AI for deploying applications at the edge of the network, which creates a powerful infrastructure for high-performance and secure applications, is investigated. The application of blockchain in federated healthcare systems is considered, which helps to ensure information security, transparency and immutability of data, as well as the decentralized nature of collaborative learning, which makes this technology very attractive for areas where confidentiality and accuracy are important.

Keywords: artificial intelligence, blockchain-based information and communication system, integrated radar and communication system, holographic telepresence, augmented reality

Вступ

Периферійний ШІ забезпечить роботу багатьох вертикальних додатків, які потребують розширеної периферійної аналітики і прийняття рішень в режимі реального часу. Як наслідок, використання алгоритмів ШІ для обробки та аналізу даних на межі мережі є необхідним. Граничні обчислення - це засіб для надання спеціалізованого обладнання та засобів навчання для розгортання послуг ШІ на периферії мережі. Крім того, безпека мережі та конфіденційність даних є основними питаннями в периферійному ШІ. Деякі додатки, такі як підключені транспортні засоби, додатки соціальних мереж і додатки для охорони здоров’я, використовують периферійні обчислення для зменшення затримок і підвищення точності результатів розрахунків за допомогою алгоритмів ШІ, особливо глибокого навчання з можливістю вивчення репрезентативних ознак на основі необроблених даних Інтернету речей і мобільних пристроїв. Додатки, що генерують чутливі дані користувачів, такі як персональні дані, дані про стан здоров'я, місцезнаходження та комунальні послуги, можуть мати підвищений ризик порушення безпеки. Разом з тим, відмінні властивості блокчейну включають розподілену природу, відстежуваність і незмінність, що робить його ідеальним рішенням для подолання проблем безпеки периферійних додатків штучного інтелекту [1].

Метою роботи є дослідження інформаційної безпеки інтелектуальних телекомунікаційних систем для забезпечення захисту конфіденційності, цілісності та доступності інформації а також забезпеченні безпеки користувачів та систем у цілому.

Основна частина

Наведемо кілька сфер, в яких зумовлено подальше використання периферійного штучного

інтелекту. Граничний ШІ забезпечить інтелектуальний процес виявлення камер безпеки. Традиційні камери спостереження записують зображення годинами, а потім зберігають і використовують їх у разі потреби. Однак, завдяки периферійному ШІ, алгоритмічні процеси будуть виконуватися в режимі реального часу в самій системі, тому камери зможуть виявляти і обробляти підозрілі дії в режимі реального часу для більш ефективного і менш витратного обслуговування. Автономні транспортні засоби збільшать свою здатність обробляти дані та зображення в режимі реального часу для виявлення дорожніх знаків, пішоходів, інших транспортних засобів та доріг, підвищуючи рівень безпеки на транспорті. Граничний ШІ можна використовувати в обробці зображень і аналізі відео для формування реакцій на аудіовізуальні стимули або для розпізнавання сцен і просторів у реальному часі, наприклад, у смартфонах. Граничний ШІ знижує витрати і підвищує безпеку в умовах промислового інтернету речей (IIoT). ШІ може контролювати обладнання на предмет можливих дефектів або помилок у виробничому ланцюжку, в той час як МН дозволяє перекомпілювати дані в реальному часі всього процесу. Граничний ШІ використовується для аналізу медичних зображень в екстреній медичній допомозі. Розгортання мереж технології 6G означає більшу швидкість і дуже низьку затримку для мобільної передачі даних, що робить периферійний ШІ більш корисним. Для технології периферійного штучного інтелекту немає обмежень у застосуванні. У сфері охорони здоров'я ШІ допомагає в моніторингу, тестуванні та лікуванні пацієнтів [2].

Використання блокчейну в периферійних обчисленнях і IoT (тобто інтернеті речей) може стати наступною революцією в ІКТ і периферійному ШІ, коли постачальники додатків зможуть надавати користувачам безпечні, прозорі, незмінні, децентралізовані додатки зі зменшеною затримкою, аналітикою в реальному часі і точними рекомендаціями. На рис. 1 показано раунд комунікації у федеративній системі охорони здоров'я з використанням блокчейну, де окремі моделі ШІ навчаються повністю на локальних пристроях, а блокчейн допомагає координувати розрахунок глобальної моделі за допомогою блокового консенсусу між учасниками на основі принципу "рівний-рівному" [3]. Процедура в глобальному раунді комунікації такої федеративної системи навчання на основі блокчейну складається з п'яти основних етапів.

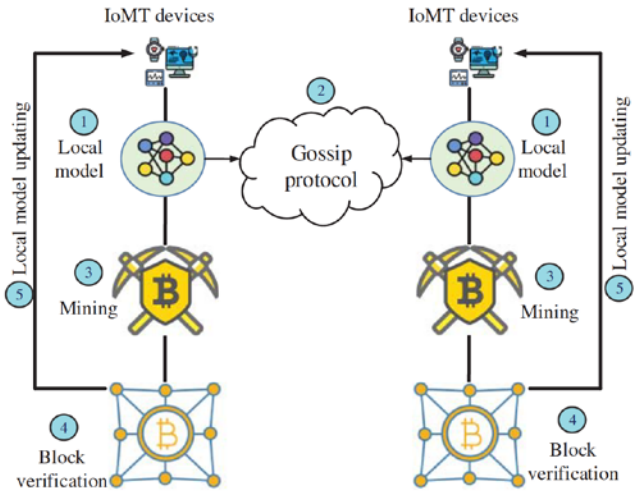

Рисунок 1 - Алгоритм взаємодії інфокомунікаційних систем з використанням блокчейну

На першому етапі локального навчання кожен пристрій Інтернету медичних речей (IoMT) тренує локальну навчальну модель, використовуючи свої локальні дані. Наступним кроком є трансляція та верифікація моделі, коли кожен пристрій додає свій цифровий підпис до моделі та транслює модель іншим пристроям IoMT за допомогою певних протоколів обміну даними. Транзакція пристрою потім перевіряється всіма іншими IoMT-пристроями в мережі. Потім, отримавши локальні моделі від інших пристроїв, кожен IoMT-пристрій намагається врахувати поточний блок. Після цього, на етапі валідації блоку, поточний блок, якщо він підтверджений, додається до локальних журналів IoMT-пристроїв. Нарешті, отримавши підтвердження, кожен пристрій оновлює свою локальну модель і починає новий раунд комунікації [4].

З точки зору кінцевих пристроїв (наприклад, датчиків, носимих пристроїв, телефонів і пристроїв Інтернету речей), межа мережі може забезпечити потужну платформу для збору і обробки великої кількості даних. Більше того, проблеми якості та неоднорідності даних можуть бути вирішені шляхом розгортання передових методів глибокого навчання (DL) на границі мережі. Наприклад, згорткова нейронна мережа є однією з найуспішніших глибинних архітектур з великими можливостями для обробки високорозмірних неструктурованих даних (наприклад, зображень), а також тексту, сигналів та інших безперервних відгуків. В результаті, згорткові нейронні мережі були використані для розробки алгоритмів на основі даних для покращення та оптимізації бездротових мереж, таких як класифікація модуляції радіосигналів [1] та розпізнавання форми сигналу в інтегрованих радіолокаційно-комунікаційних системах [2]. Отже, периферійний ШІ розглядається як ключовий фактор створення інтелектуальних і автономних мереж 6G, в яких багато структурних елементів і мережевих операцій можуть бути оптимізовані за рахунок розгортання алгоритмів на основі ШІ і даних на межі мережі.

Перевірені та потенційні можливості периферійного оброблення і навчання на межі мережі відкриють можливості для впровадження та вдосконалення нових послуг і додатків 6G, таких як голографічна телеприсутність, розширена реальність, "розумні" мережі 2.0 і "Індустрія 5.0" [1-3]. Разом з тим, ефективне розгортання периферійного ШІ залежить від багатьох важливих факторів, таких як обмеженість ресурсів мобільних пристроїв, високе комунікаційне навантаження периферійної хмари і тривалі затримки в централізованій хмарі. Наприклад, в роботі [3] пропонується триступенева структура для зниження вартості обчислень і витрат на зв'язок при спільному навчанні і обробленні на периферійних пристроях, що є рівнем 4 в п'ятирівневій архітектурі периферійного ШІ [4].

Висновки

Отримані результати цієї роботи підкреслюють важливість проектування глибоких нейронних мереж для зниження обчислювальних витрат і витрат на зв'язок для периферійного ШІ. Для подальшого сприяння розгортанню і застосуванню периферійного ШІ в мережах 6G потрібно все більше і більше дослідницьких зусиль в області периферійного виведення і периферійного навчання для подолання його проблем: апаратний дизайн, програмна платформа і архітектура периферійного ШІ, і це лише деякі з них, які можна перерахувати. Поєднання локального навчання на пристроях IoT, блокчейн-технологій та глибокого навчання в периферійних обчисленнях відкриває широкі перспективи для розробки інтелектуальних та автономних систем, які можуть обробляти великі обсяги даних в режимі реального часу та забезпечувати якісні послуги в багатьох галузях.

Зазначена перспективність і безмежні можливості застосування периферійного ШІ свід-чать про значущість цієї технології в різних галузях та її потенціал для поліпшення проду-ктивності, безпеки та якості обслуговування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Q.-V. Pham, R. Ruby, F. Fang, D. C. Nguyen, Z. Yang, M. Le, Z. Ding, and W.-J. Hwang, “Aerial computing: A new computing paradigm, applications, and challenges,” IEEE Internet of Things Journal, vol. 9, 2022., pp. 8339–8363.

2. Q. Duan, “Intelligent and autonomous management in cloud-native future networks–a survey on related standards from an architectural perspective,” Future Internet, vol. 13, no. 2, 2021., p. 42

3. М. Васильківський, О. Болдирева, Г. Варгатюк, і М. Будаш, «Керування телекомунікаційними мережами з використанням технологій AI/ML», ВОТТП, вип. 1, с. 89–100, Бер 2023. doi: 10.31891/2219-9365-2023-73-1-13

4. М. Васильківський, Д. Нікітович, Н. Грабчак, і Н. Якубівська, «Оптимізація адаптивних радіосистем із використанням алгоритмів ШІ та МН», ВОТТП, вип. 2, с. 112–124, Чер 2023. doi.org/10.31891/2219-9365-2023-74-15

Будаш Михайло Володимирович — аспірант групи 172-22а, факультет інформаційних електронних систем, Вінницький національний технічний університет, Вінниця, e-mail: mika@budash.dp.ua

Прикмета Андрій Володимирович — аспірант групи 172-22а, факультет інформаційних електронних систем, Вінницький національний технічний університет, Вінниця, e-mail: botan.mua@gmail.com

Олійник Андрій Олегович — аспірант групи 172-22а, факультет інформаційних електронних систем, Вінницький національний технічний університет, Вінниця, e-mail: w0lfend00@gmail.com

Грабчак Назарій Віталійович — аспірант групи 172-23а, факультет інформаційних електронних систем, Вінницький національний технічний університет, Вінниця, e-mail: nazarii.hrabchak@gmail.com

Науковий керівник: ***Васильківський Микола Володимирович*** — кандидат технічних наук, доцент, доцент кафедри інфокомунікаційних систем і технологій, Вінницький національний технічний університет, м. Вінниця

Budash Mykhailo V. — graduate student of group 172-22a, Faculty of Information Electronic Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: mika@budash.dp.ua

Prykmeta Andrii V. — graduate student of group 172-22a, Faculty of Information Electronic Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: botan.mua@gmail.com

Oliinyk Andrii O. — graduate student of group 172-22a, Faculty of Information Electronic Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: w0lfend00@gmail.com

Hrabchak Nazarii V. - graduate student of group 172-23a, Faculty of Information Electronic Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: nazarii.hrabchak@gmail.com

Supervisor: ***Vasylkivskyi Mykola V.*** — candidate of technical sciences, associate professor, associate professor of the Department of Information Communication Systems and Technologies, Vinnytsia National Technical University, Vinnytsia