УДК 004.8:004.056
DOI: https://doi.org/10.30837/IYF.IRTTPI.2024.489

ЗАГРОЗИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ НА МАЛОПОТУЖНИХ ПРОЦЕСОРАХ ДЛЯ ОРГАНІЗАЦІЇ АКУСТИЧНОГО КАНАЛУ ВИТОКУ

Передерій І.А
Науковий керівник – доц. Ликов Ю.В.
Харківський національний університет радіоелектроніки, каф. КРіСТЗІ
e-mail: illia.perederii@nure.ua

Artificial intelligence (AI) has emerged as a powerful ally in the ongoing battle against cybersecurity threats. With the proliferation of connected devices and the Internet of Things (IoT), the need for robust and adaptive security solutions has never been more pressing. This article explores the convergence of AI and low-power processors in fortifying cybersecurity defenses, presenting both opportunities and challenges in this rapidly evolving landscape.

На сьогоднішній день штучний інтелект і машинне навчання стрімко зростає і набирає популярності та застосування у наукових колах. Однак у сучасному світі моделі машинного навчання та штучного інтелекту мають певні обмеження: вони повинні мати багату кількість обчислювальних і процесорних потужностей для точного та бажаного результату. Використання нових технологій також призвело до швидкої еволюції кіберзагроз і атак.

Кібербезпека захищає інформаційні та комунікаційні системи, що виходять в Інтернет, від зловмисних атак та загроз. Концепція штучного інтелекту у кібербезпеці починається з 1990-х років коли було розроблено система виявлення аномалій (ADS) та систем виявлення вторгнень (IDS). Сьогодні штучний інтелект є невід'ємною частиною кібербезпеки.

Машине навчання як людина вчиться поступово та адаптується через досвід. Він вважається підмножиною штучного інтелекту, і він зосереджений на реалізації певних типів систем, які можуть навчатися на історичних даних, щоб ідентифікувати закономірності та самостійно приймати рішення.

Величезні обсяги даних, які генерують організації, надають можливості для широкого спектру додатків ML(Meta Language) у кіберпросторі, включаючи розвідку про загрози, виявлення аномалій та автоматизацію завдань, пов'язаних із кібербезпекою

Високий попит на додатки штучного інтелекту на периферії призвів до значного збільшення апаратного забезпечення, оптимізованого для рівнів низького енергоспоживання. Наприклад, Google представив полегшену версію блоку обробки тензорів (TPU) під назвою Edge TPU, яка здатна забезпечити енергоефективні висновки з 2 трильйонами операцій MAC на

секунду на ват (2TMAC/c/Вт). Цей ультрасучасний пристрій здатний запускати моделі мобільних версій, такі як MobileNet V2, зі швидкістю майже 400 FPS.

Cloud TPU зосереджується на навчанні складних моделей, тоді як Edge TPU розроблено для виконання логічних висновків у системах із низьким енергоспоживанням.

Орієнтуючись на значно меншу потужність, ніж Edge TPU, Ambiq випустив сімейство майже порогових процесорів Apollo на основі 32-розрядного процесора ARM Cortex-M4F. Ці пристрої можуть досягати значно нижчого споживання енергії, виміряного лише на рівні 6 мкА/МГц при 3,3 В у робочому режимі та 1 мкА/МГц при 3,3 В у режимі сну. Пристрій Apollo3, присутній на платі SparkFun, має 1 МБ флеш-пам'яті та 384 КБ оперативної пам'яті з низьким витоком.

Подібним чином Eta Compute націлилася на енергоефективні кінцеві рішення ШІ з процесором ECM3532. Цей пристрій базується на 32-розрядному ЦП ARM Cortex-M3 і окремому процесорі CoolFlux DSP для прискорення операцій машинного навчання енергоефективним способом. ECM3532, доступний у платі AI Vision, споживає менше 5 мкА/МГц у нормальному робочому режимі та 1 мкА/МГц у сплячому режимі. Відповідно до Eta Compute, його реалізація технології безперервного масштабування напруги та частоти (CVFS) забезпечує профіль потужності лише 1 мВт. Характерною рисою цих пристроїв із майже пороговими значеннями є те, що масштабування напруги застосовується до ядра, але воно не застосовується до SRAM/флеш-пам'яті пристрою через обмежений запас, можливий у комірках пам'яті.

І Apollo3, і ECM3532 базуються на популярній архітектурі ARM, але останнім часом архітектура набору інструкцій з відкритим вихідним кодом RISC-V також отримала значну увагу в цій галузі.

Наприклад, GAP8, розроблений GreenWaves Technologies, має 8-ядерний обчислювальний кластер процесорів RISC-V і додатковий прискорювач CNN. Обчислювальний кластер поєднується з додатковим наднизьким мікроконтролером із потужністю 30 мкВт, що зберігає стан, для функцій керування та зв'язку. Для висновку CNN (90 МГц, 1,0 В), GAP8 забезпечує енергоефективність 600 GMAC/c/Вт і найгіршу огинаючу потужності 75 мВт.

Інші приклади компаній, які вивчають майже пороговий режим, включають Minima, який брав участь у розробках, що демонструють досяжне енергозбереження. Minima пропонує ультраширокe динамічне масштабування напруги та частоти (DVFS), яке здатне масштабувати частоту та/або робочу напругу залежно від робочого навантаження.

Цей підхід у поєднанні з підходом динамічної маржі від Minima та ARM дозволяє заощаджувати енергію від 15 до 20 раз. Інтерес до апаратного забезпечення адаптивного масштабування напруги призвів до євро-

пейського проекту вартістю 100 мільйонів євро під керівництвом STMicroelectronics з розробки наступного покоління периферійних мікроконтролерів штучного інтелекту та програмного забезпечення з використанням малопотужної технології FD-SOI та зміни фази. Цей проект спрямований на надання чіпсетів і рішень для автомобільного та промислового ринків з дуже високою обчислювальною потужністю 10 TOPS на ват, що є значно потужнішим, ніж існуючі мікроконтролери.

TinyML - це методи машинного навчання мікроконтролерів. Програма TinyML пропонує «full-stack» рішення (обладнання, системи, програмного забезпечення та додатків), включаючи архітектури машинного навчання, методи, інструменти та підходи здатні виконувати аналітику на пристрої на межі з хмарою.

TinyML може бути реалізований в системах з низьким енергоспоживанням, таких як датчики або мікроконтролери з метою виконання автоматизованих завдань. Основною перевагою якої буде створення інтелектуальних IoT-пристроїв і, що не менш важливо, популяризація їх за рахунок ймовірного зниження вартості.

Можна з упевненістю сказати, що TinyML – це об’єднання програмного забезпечення, апаратного забезпечення та алгоритмів, які працюють синхронно один з одним, щоб забезпечити бажану продуктивність. Аналогові обчислення або обчислення пам’яті можуть знадобитися, щоб забезпечити кращий і ефективний досвід навчання для обладнання та пристроїв Інтернету речей, які не підтримують апаратні прискорювачі. Що стосується програмного забезпечення, програми, створені за допомогою TinyML, можна розгортати та впроваджувати на таких платформах, як Linux або вбудований Linux, а також на хмарному програмному забезпеченні. Нарешті, програми та системи, створені на основі алгоритму TinyML, повинні мати підтримку нових алгоритмів, які потребують моделей з малим розміром пам’яті, щоб уникнути її великого споживання.

З іншого боку, останнім часом розвиваються технології LPWAN (Low-power Wide-area Network), які мають такі переваги як висока енергоефективність, велика дальність передачі інформації, шифрування інформації, підвищена скритність сигналу в ефірі, тому можуть бути перспективними з точки зору застосування їх для організації технічних каналів витоку інформації. Єдиним стримуючим фактором застосування цих технологій зловмисниками була мала пропускна здатність більшості протоколів LPWAN, що унеможливлює передачу аудіо а тим більш відео трафіку (підслуховування, підглядання).

Застосування штучного інтелекту може дозволити перетворювати аудіо трафік у текст, що значно зменшує вимоги до пропускної здатності каналу зв’язку. Тому комбінація технології штучного інтелекту на малопотужних мікроконтролерах з технологіями LPWAN можуть становити принципіальну нову загрозу безпеці об’єктів інформаційної діяльності.

Список використаних джерел:

1. TinyML програми, обмеження та його використання в пристроях IoT і Edge. URL: (https://www.unite.ai/uk/обмеження-додатків-tinyml-та-їх-використання-в-пристроях-iot-edge/)

(дата звернення: 26.02.2024)

2. The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review.

URL:
(https://www.sciencedirect.com/science/article/pii/S2543925123000372)

(дата звернення: 26.02.2024)

3. Lykov, Y.; Paniotova, A.; Shatalova, V.; Lykova, A. Energy Efficiency Comparison LPWANs: LoRaWAN vs Sigfox. In Proceedings of the 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S T), Kharkiv, Ukraine, 6–9 October 2020; pp. 485–490.

4. Y. Lykov, M. Bolinova, V. Slobodiuk, A. Lykova, and S. Makovetskyi, “Investigation of Potential Opportunities for LoRaWAN Technology in Conditions of Urban Construction onthe Example of Pycom Modules,” in 2018 International Scientific-Practical Conference onProblems of Infocommunications Science and Technology, PIC S and T 2018 - Proceedings,pp. 543–547 (2019)