ВІДГУК

офіційного опонента на дисертаційну роботу
Северіна Андрія Івановича
на тему «Алгоритмічне та програмне забезпечення захисту приватних наборів даних у задачах класифікації»,
представлену на здобуття ступеня доктора філософії
в галузі знань 12 Інформаційні технології
за спеціальністю 121 Інженерія програмного забезпечення

Актуальність теми дисертації.

Програмні системи інтелектуального аналізу даних все частіше застосовуються у різних сферах. Наприклад, вони дозволяють рекомендувати товари користувачеві в електронній комерції, виявляти небажані повідомлення (спам) та модерувати коментарі в соціальній сфері. Також існують системи для персонального використання, такі як чатботи ChatGPT та Google Bard. Дані є невід'ємною частиною обчислювального інтелекту, тому вони є необхідними для навчання та тестування систем аналізу даних. Наявність якомога більш різнопланового й повного набору даних дозволяє розробляти ефективні програмні системи. Основним джерелом даних є реальний світ, однак, вони також можуть генеруватись програмним шляхом, відтворюючи необхідні ознаки вхідних даних. Попри наявність великої кількості даних у сучасному світі, значна частина з них містить приватну інформацію, що суттєво обмежує їх використання для розроблення загальнодоступних систем. Прикладами приватних даних є конфіденційні (дані, що дозволяють ідентифікувати людину), секретні (військові, фінансові чи державні) та чутливі (медичні дані). Збереження приватності даних при розробленні програмних систем є важливим завданням.

Таким чином, актуальним науково-технічним завданням є вдосконалення алгоритмічного та програмного забезпечення захисту приватних наборів даних у системах з використанням штучного інтелекту, яка вирішується у дисертаційній роботі.

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни.

Наукова новизна результатів дисертаційного дослідження полягає у такому:

1) уперше запропоновано архітектуру програмної системи для вирішення задачі класифікації на основі приватних даних, характерною особливістю якої є захист приватних наборів даних, шляхом функціонального шифрування, що відбувається на стороні клієнта, і дозволяє збільшити кількість наборів даних для навчання загальнодоступних систем аналізу даних і штучного інтелекту;

2) уперше запропоновано модифікацію програмної моделі шифрування даних, яка відрізняється від існуючої використанням двовимірних згорткових нейронних мереж, замість одновимірних, і дозволяє застосовувати модель шифрування з використанням нейронних мереж до даних, що представлені набором пікселів, з яких складається зображення;

3) уперше розроблено алгоритмічно-програмний метод функціонального шифрування наборів даних, особливістю якого є можливість використання приватних наборів даних в загальнодоступних системах аналізу даних та штучного інтелекту шляхом зменшення їх розмірності й функціонального шифрування отриманих даних з використанням приватного ключа;

4) уперше розроблено алгоритмічно-програмний метод пошуку нормальних поліномів серед незвідних, який відрізняється від існуючого використанням простих чисел у десятковому представленні замість поліномів, що дозволяє зменшити обчислювальні витрати алгоритму пошуку незвідних многочленів з $O(n^3)$ до $O(n\log(\log n))$ і, як наслідок, спростити міжбазисні перетворення у бінарних скінченних полях з метою пришвидшення виконання операцій над елементами поля у методах гомоморфного шифрування даних;

5) уперше розроблено модифікований спосіб побудови матриці переходу між поліноміальним та нормальним базисами скінченного поля, який полягає у використанні рекурентної формули $\alpha_{i+1}=t^{p^{i+1}}=t^{p^i\cdot p}=\left(\alpha_i\right)^p$ замість обчислення остачі від ділення елемента $t^{p^{i+1}}$ на незвідний поліном, що дозволяє зменшити кількість використовуваної пам'яті з n^{p^i} до $n\cdot p$, а також обчислювальну складність з $O\left(m^{p^i}\right)$ до $O\left(m^p\right)$.

Отримані у дисертаційній роботі наукові результати достовірні та обґрунтовані, що забезпечується докладним аналізом проблематики, чіткою постановкою задач дослідження, коректністю застосування математичного апарату при доведенні наукових положень дисертації, а також підтверджується результатами виконаних експериментальних досліджень.

Отже, в дисертаційній роботі поставлене наукове завдання виконано повністю, здобувач повною мірою оволодів методологією наукової діяльності.

Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності.

За своїм змістом дисертаційна робота здобувача Северіна А. І. повністю відповідає Стандарту вищої освіти зі спеціальності 121 Інженерія програмного забезпечення та напрямкам досліджень відповідно до освітньої програми Інженерія програмного забезпечення.

Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям інженерії програмного забезпечення.

Розглянувши звіт подібності за результатами перевірки дисертаційної роботи на текстові співпадіння, можна зробити висновок, що дисертаційна робота Северіна Андрія Івановича є результатом самостійних досліджень здобувача і не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень. Використані ідеї, результати і тексти інших авторів мають належні посилання на відповідне джерело.

Мова та стиль викладення результатів

Дисертаційна робота написана українською мовою.

Тексту дисертації характерна послідовність, логічність та доступність для сприйняття. Стиль мовлення у дисертаційній роботі є науковим. Автор дотримується загальноприйнятої науково-технічної термінології. При цьому у тексті дисертації міститься достатня кількість графіків, діаграм та таблиць, що полегшує розуміння матеріалу.

Дисертація складається з вступу, 4 розділів, висновків, списку використаних літературних джерел та додатків. Загальний обсяг дисертації 254 сторінки.

У вступі розглянуто актуальність теми дисертації, наведено мету і задачі дослідження, а також визначено об'єкт, предмет та методи дослідження. Сформульовано наукову новизну та практичне значення одержаних результатів. Наведено інформацію щодо публікацій здобувача та структури дисертаційної роботи.

У першому розділі наведено основні етичні аспекти використання систем штучного інтелекту, проаналізовано загрози приватності даних у таких системах та методи збереження приватності в машинному навчанні, а також сформульовано вимоги до програмного забезпечення.

У другому розділі проведено аналіз особливостей використання скінченних полів в гомоморфних методах збереження приватності, а також визначено залежності часу виконання операцій над елементами скінченних полів від базису, в якому представлені елементи. Розроблено метод пошуку поліномів, який дозволяє зменшити обчислювальну складність процесу пошуку нормальних многочленів. Запропоновано модифікацію способу переходу між базисами, на основі рекурентної формули.

Третій розділ присвячено розробленню методу захисту приватних наборів даних, на основі функціонального шифрування. Розглянуто й проаналізовано модель шифрування даних з використанням нейронних мереж. Модифіковано модель шифрування даних, що дозволяє її використання для даних, представлених набором пікселів. Розроблено метод функціонального

шифрування наборів даних, який надає можливість використання приватних даних в загальнодоступних системах машинного навчання. Здійснено аналіз метрик оцінки методів захисту наборів даних, в результаті якого обрано метрики оцінки розроблених методів.

У четвертому розділі запропоновано архітектуру програмної системи для вирішення задачі класифікації на основі приватних даних, яка поєднує клієнт-серверну архітектуру та функціональне шифрування. Розроблено програмну систему для виконання обчислення над елементами скінченних полів, а також проведення міжбазисних перетворень. Розроблено програмну систему вирішення задачі класифікації на приватних наборах даних, яка дозволяє зберігати приватність наборів даних шляхом функціонально шифрування. Проведено експериментальні дослідження розроблених методів.

У висновках наведено основні результати одержані в дисертації.

Дисертаційна робота оформлена відповідно до вимог наказу МОН України від 12 січня 2017 р. № 40 «Про затвердження вимог до оформлення дисертації».

Оприлюднення результатів дисертаційної роботи

Наукові результати дисертації висвітлені у 4 наукових публікаціях здобувача, серед яких: 2 статті у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України; 2 статті у періодичних наукових виданнях, проіндексованих у базах даних Web of Science Core Collection та Scopus, з яких 1 статтю у виданні, віднесеному до третього квартилю (Q3) відповідно до класифікації SCImago Journal and Country Rank.

Результати дисертації апробовані на 3 Міжнародних наукових конференціях.

Опубліковані праці здобувача повністю відображають результати дисертаційної роботи. Публікаціям притаманний високий науковий рівень й дотримання принципів академічної доброчесності.

Таким чином, наукові результати описані в дисертаційній роботі повністю висвітлені у наукових публікаціях здобувача.

Недоліки та зауваження до дисертаційної роботи.

1. У підрозділі 3.1 краще було б проілюструвати запропоновану модифікацію програмної моделі схемою архітектури модифікованої нейронної мережі.

2. У підрозділі 2.3 вказано, що певна кількість незвідних поліномів буде пропущена під час пошуку нормальних поліномів запропонованим методом порівняно з традиційним. Причини цього пояснено, однак, бажано було б також деталізувати на що це впливає.

3. Обґрунтування доцільності розроблення двох програмних систем з використанням різних технологій бажано було б сформулювати більш чітко.

Вважаю, що зазначені зауваження не є визначальними, не зменшують загальну наукову новизну та практичну значимість результатів та не впливають на позитивну оцінку дисертаційної роботи.

Висновок про дисертаційну роботу

Вважаю, що дисертаційна робота здобувача ступеня доктора філософії Северіна Андрія Івановича на тему «Алгоритмічне та програмне забезпечення захисту приватних наборів даних у задачах класифікації» виконана на високому науковому рівні, не порушує принципів академічної доброчесності та є закінченим науковим дослідженням, сукупність теоретичних та практичних результатів якого розв'язує наукове завдання, що має істотне значення для галузі знань 12 Інформаційні технології. Дисертаційна робота за актуальністю, практичною цінністю та науковою новизною повністю відповідає вимогам чинного законодавства України, що передбачені в пп. 6–9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою Кабінету Міністрів України від 12 січня 2022 р. № 44.

Здобувач Северін Андрій Іванович заслуговує на присудження ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 121 Інженерія програмного забезпечення.

Офіційний опонент:

доцент кафедри штучного інтелекту
Харківського національного
університету радіоелектроніки,
кандидат технічних наук, доцент Олег ЗОЛОТУХІН

М.П. «23» травня 2024 року

доцента кафедри штучного інтелекту Золотухіне

ПІДПИС ЗАСВІДЧУЮ:
Начальник відділу кадрів Сінєвіне
23 травня 2024 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ ВІДДІЛ КАДРІВ №1 №02071197