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.

Системи машинного навчання активно впроваджуються для вирішення різних задач, зокрема, таких як підбір рекомендацій, виявлення спаму та модерація коментарів. Останнім часом такі інструменти також використовуються й для персональних цілей (вирішення типових задач за допомогою чатботів).

Необхідним елементом для побудови програмних систем інтелектуального аналізу даних є дані, які використовуються для навчання й тестування таких систем. Набори даних, в яких наявна якомога більша кількість різнопланових, що можуть бути використані для аналізу, дозволяють будувати більш точні програмні системи. Основним джерелом даних є реальний світ. Також дані можна згенерувати програмним шляхом, відтворюючи необхідні для певної задачі характеристики даних. Однак, попри на те, що кількість даних стрімко збільшується, вони часто містять приватну інформацію, шо суттєво звужує їх використання в системах інтелектуального аналізу даних. Прикладами приватних даних є конфіденційні (наприклад, реєстраційний податковий номер), секретні (наприклад, фінансові) та чутливі (медичні дані). Важливим завданням під час розроблення програмних систем є збереження приватності даних.

Отже, розглянуті завдання визначають актуальну науково-технічну задачу вдосконалення алгоритмічного та програмного забезпечення захисту приватних наборів даних у системах з використанням штучного інтелекту, яка вирішується у дисертаційному дослідженні для задачі класифікації.

Оцінка обгрунтованості наукових результатів дисертації, їх достовірності та новизни.

Наукова новизна результатів дисертаційного дослідження полягає в наступному:

- уперше запропоновано архітектуру програмної системи для вирішення задачі класифікації на основі приватних даних, характерною

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.

Системи машинного навчання активно впроваджуються для вирішення різних задач, зокрема, таких як підбір рекомендацій, виявлення спаму та модерація коментарів. Останнім часом такі інструменти також використовуються й для персональних цілей (вирішення типових задач за допомогою чатботів).

Необхідним елементом для побудови програмних систем інтелектуального аналізу даних є дані, які використовуються для навчання й тестування таких систем. Набори даних, в яких наявна якомога більша кількість різнопланових, що можуть бути використані для аналізу, дозволяють будувати більш точні програмні системи. Основним джерелом даних є реальний світ. Також дані можна згенерувати програмним шляхом, відтворюючи необхідні для певної задачі характеристики даних. Однак, попри на те, що кількість даних стрімко збільшується, вони часто містять приватну інформацію, шо суттєво звужує їх використання в системах інтелектуального аналізу даних. Прикладами приватних даних є конфіденційні (наприклад, реєстраційний податковий номер), секретні (наприклад, фінансові) та чутливі (медичні дані). Важливим завданням під час розроблення програмних систем є збереження приватності даних.

Отже, розглянуті завдання визначають актуальну науково-технічну задачу вдосконалення алгоритмічного та програмного забезпечення захисту приватних наборів даних у системах з використанням штучного інтелекту, яка вирішується у дисертаційному дослідженні для задачі класифікації.

Оцінка обгрунтованості наукових результатів дисертації, їх достовірності та новизни.

Наукова новизна результатів дисертаційного дослідження полягає в наступному:

- 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;

- 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;
- 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.
- 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.
- уперше розроблено модифікований спосіб побудови матриці переходу між поліноміальним та нормальним базисами скінченного поля, який полягає у використанні рекурентної формули $\alpha_{i+1} = t^{p^{i+1}} = t^{p^i \cdot p} = (\alpha_i)^p$ 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 $O\left(m^p\right)$.

Варто зауважити, що наукові результати отримані в дисертаційній роботі є достовірними та обґрунтованими. Це забезпечується чітко поставленими завданнями дослідження, застосуванням коректного математичного апарату, а також підтверджується експериментальними результатами проведених 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.

Текст дисертації логічно структурований, доступний для сприйняття та розуміння. Стиль мовлення дисертації – науковий. Автор послідовно й логічно викладає наукові положення з використанням загальноприйнятої термінології, а також таблиць, рисунків та фрагментів програмного коду, що полегшує сприйняття матеріалу.

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

У вступі обґрунтовано актуальність дослідження, сформульовано мету та задачі дослідження, а також наведено наукову новизну та практичне значення дисертаційного дослідження.

Перший розділ присвячено аналізу програмних систем захисту приватних наборів даних у машинному навчанні. Розглянуто етичні аспекти використання систем штучного інтелекту. Проаналізовано загрози приватності даних у системах аналізу даних та штучного інтелекту. Проведено комплексний порівняльний аналіз методів збереження приватності в машинному навчанні, на основі якого сформульовано вимоги до програмного забезпечення.

Другий розділ присвячено розробленню алгоритмічних методів міжбазисних перетворень елементів скінченних полів. Розглянуто використання полів Галуа в системах захисту та передачі інформації. Проаналізовано алгоритмічні методи виконання операцій над елементами поля $GF(p^m)$ у різних базисах. Розроблено метод пошуку нормальних поліномів, а також модифікований спосіб побудови матриці переходу між поліноміальним та нормальним базисами скінченного поля.

У третьому розділі дисертації проаналізовано математичне підґрунтя для розроблення методів шифрування даних, що використовують нейронні мережі. Запропоновано модифікацію моделі шифрування даних, яка дозволяє використовувати модель для зображень, представлених матрицею пікселів. Розроблено метод функціонального шифрування даних, характерною особливістю якого є можливість використання приватних наборів даних у програмних системах інтелектуального аналізу даних. Розглянуто й обрано метрики оцінки розроблених методів захисту приватних наборів даних.

Четвертий розділ присвячено розробленню програмного забезпечення захисту приватних наборів даних, а також проведенню експериментальних досліджень. Розроблено архітектуру програмної системи для вирішення задачі класифікації на основі приватних наборів даних. Розроблено програмну систему для виконання обчислень над елементами поля $GF(p^m)$ та виконання міжбазисних перетворень. Розроблено програмну систему вирішення задачі класифікації на основі приватних наборів даних, яка надає можливість здійснювати класифікацію оригінальних та зашифрованих даних. Проведено та проаналізовано експериментальні дослідження розроблених методів міжбазисних перетворень та методу функціонального шифрування. Розглянуто можливості інтеграції розроблених систем.

У висновках підсумовано отримані в дисертаційній роботі наукові та практичні результати.

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.

Також результати дисертації були апробовані на 3 наукових фахових конференціях.

Результати дисертаційної роботи достатньо повно висвітлені в представлених публікаціях здобувача. Публікації мають високий науковий рівень, а автор неухильно дотримується 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 першому розділі проведено комплексний порівняльний аналіз алгоритмічно-програмних методів збереження приватності в машинному навчанні за різними критеріями (складність, практичність, потреба у значній кількості даних, надійність, висока точність системи). Використані критерії є якісними, однак, краще було б використати й кількісні критерії. Крім цього, складність методів бажано було б оцінити за допомогою оцінки асимптотичної складності (нотація «*O*»).
2. Експериментальні дослідження розробленої системи вирішення задачі класифікації на приватних наборах даних проведено на наборі даних MNIST. Було б добре також провести відповідні дослідження й на інших наборах даних.
3. У підрозділі 4.3 вказано обрані параметри моделі шифрування даних з використанням нейронних мереж. Частину з них визначено експериментальним шляхом. З огляду на це, бажано було б докладніше описати, з якими саме значеннями параметрів моделі проводились експерименти й аргументувати чому обрані значення показують кращі результати.

Вважаю, що висловлені зауваження не є визначальними і 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 п.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:

завідувач кафедри програмних засобів
Національного університету
«Запорізька політехніка»,
доктор технічних наук, професор Сергій СУББОТІН

Підпис
ЗАСВІДЧУЮ
ВЧЕНИЙ СЕКРЕТАР
НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
"ЗАПОРІЗЬКА ПОЛІТЕХНІКА"