004.056.5:004.722 https://doi.org/10.30837/IYF.PCEIP.2024.153

ЗАХИСТ ДАНИХ ЗА ДОПОМОГОЮ БЛОКЧЕЙНУ ТА ШТУЧНОГО ІНТЕЛЕКТУ

Просолов В.В.
д.т.н. проф. Халімов Г.З.
Харківський національний університет радіоелектроніки, Харків, Україна
e-mail: vladyslav.prosolov@nure.ua

In this article, we will analyze SecNet, an architecture that can provide secure data storage, computation, and sharing in a large-scale Internet environment, aiming for a more secure cyberspace with true big data and thus advanced AI with a large number of data sources, through the integration of three key components: blockchain-based data sharing with a guarantee of ownership; a secure computing platform based on artificial intelligence; a trusted value exchange mechanism for purchasing a security service.

У доповіді розглядається можливість захистити дані шляхом поєднання блокчейну та штучного інтелекту, а також дослідити архітектуру захищеної мережі, щоб значно підвищити безпеку обміну даними та всієї мережі [1].

Щоб використовувати штучний інтелект (ШІ) і блокчейн для вирішення проблеми зловживання даними, а також розширити можливості штучного інтелекту за допомогою блокчейну для довіреного керування даними в недовіреному середовищі, пропонуємо SecNet, яка є новою мережевою парадигмою, зосередженою на безпечному зберіганню даних, обмін та обчислення замість спілкування.

SecNet гарантує право власності на дані за допомогою технологій блокчейну та безпечної обчислювальної платформи на основі ШІ, а також механізму стимулювання на основі блокчейну, пропонуючи парадигму та стимули для об’єднання даних і більш потужний ШІ для досягнення кращої безпеки мережі. Крім того, ми обговорюємо типовий сценарій використання SecNet у системі медичного обслуговування та надаємо альтернативні способи використання функції зберігання SecNet. Також, ми оцінюємо його покращення щодо вразливості мережі під час протидії DDoS-атакам і аналізуємо винахідницький аспект щодо заохочення користувачів до спільного використання правил безпеки для більш безпечної мережі.

Дані дуже важливі для їх власника, і різні типи даних можна створювати, змінюючи необроблені дані відповідно до різних вимог і сценаріїв. Наприклад, інформацію про здоров’я користувача, яка зберігається в PDC, можна витягти та реорганізувати, щоб стати структурованими медичними даними, що дуже зручно для покупців із лікарень, науково-дослідних інститутів і розробників програм [2].

Усі дані об’єкта в кіберпросторі зберігаються в PDC, тому їх безпека має велике значення для власника, оскільки дані фактично є цифровим клоном

об’єкта в реальному світі. Для захисту даних SecNet впроваджує компонент ASC в OSS у кожному PDC.

AI є однією з основних можливостей, інтегрованих у PDC. Для різних штучних інтелектів було винайдено різні методи машинного навчання, наприклад, зіставлення шаблонів, комп’ютерний зір і самостійне керування. Наразі досліджуються різні методи ШІ для обробки різних типів даних. Ці специфічні для даних функції штучного інтелекту можна розглядати як великий набір «острівців рішень»: наукові кола та індустрія створили численні ізольовані програмні компоненти та механізми, які мають справу з різними частинами інтелекту окремо. PDC працює як операційна платформа штучного інтелекту, об’єднуючи окремі компоненти штучного інтелекту в узгоджену інтелектуальну систему ширшого характеру. Різні функції штучного інтелекту взаємодіють одна з одною в PDC і діють як інтелектуальна система.

Для захищених обчислень на самому початковому етапі ASC може інтегрувати модуль Generative Adversarial Network (GAN) для генерації більш потужних правил безпеки, що розвиваються, і ввімкнення безпечного та інтелектуального OSS для PDC.

Модуль GAN ASC може вивчати поточні правила безпеки PDC, а потім генерувати зловмисні, але «схожі на законні» запити на доступ до деяких особистих даних, щоб заплутати OSS PDC, щоб змусити OSS втратити здатність класифікувати запит на доступ є незаконним чи ні. Після тривалого раунду генерації та класифікації за допомогою модуля GAN OSS PDC стане набагато розумнішим і потужнішим, а фальшиві запити доступу до даних матимуть мало шансів конкурувати з таким безпечним і інтелектуальним OSS цього PDC.

SecNet забезпечить величезну кількість додатків завдяки вбудованому штучному інтелекту та блокчейну. Одним із типових випадків розгортання та застосування SecNet є довірчий обмін медичними даними між недовіреними різними сторонами для підтримки інтелектуальної та безпечної екосистеми керування медичними даними, яка є ключем до глобальної системи охорони здоров’я.

У майбутній роботі ми дослідимо, як використовувати блокчейн для авторизації доступу до запитів на дані, а також розробимо безпечні та детальні смарт-контракти для обміну даними та обчислювальної служби на основі ШІ в SecNet. Крім того, ми змоделюємо SecNet і проаналізуємо його продуктивність за допомогою масштабних експериментів на основі передових платформ.

Список використаних джерел

1. H. Yin, D. Guo, K. Wang, Z. Jiang, Y. Lyu and J. Xing, "Hyperconnected network: A decentralized trusted computing and networking paradigm", IEEE Netw., vol. 32, pp. 112-117, Jan./Feb. 2018.

2. Y.-A. de Montjoye, E. Shmueli, S. S. Wang and A. S. Pentland, "openPDS: Protecting the privacy of metadata through SafeAnswers", PLoS ONE, vol. 9, no. 7, 2014.