МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра інформаційно-обчислювальних систем і управління

ДЗЯДИК Богдан-Данило Юрійович

Модель інтеграції блокчейн-технології та штучного інтелекту для аналізу великих даних у середовищі Інтернету речей / Model for Integrating Blockchain Technology and Artificial Intelligence for Big Data Analysis in Internet of Things Environments

спеціальність: 122 - Комп'ютерні науки
освітньо-професійна програма - Комп'ютерні науки

Кваліфікаційна робота

Виконав студент групи КНм-21
Б.–Д. Ю. Дзядик
_____

Науковий керівник:
к.т.н., професор В.В. Кочан
_____

Кваліфікаційну роботу
допущено до захисту:
«___» _____ 20___ р.
В.о. завідувача кафедри
_____ Н.В. Дзюбановська

ТЕРНОПІЛЬ – 2025

Факультет комп'ютерних інформаційних технологій
Кафедра інформаційно-обчислювальних систем і управління
Освітній ступінь «магістр»
спеціальність: 122 – Комп'ютерні науки
освітньо-професійна програма – Комп'ютерні науки

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ Н.М. Васильків
«____» _____20__р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
ДЗЯДИК Богдан-Данило Юрійович
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи
Модель інтеграції блокчейн-технології та штучного інтелекту для аналізу великих даних у середовищі Інтернету речей / Model for Integrating Blockchain Technology and Artificial Intelligence for Big Data Analysis in Internet of Things Environments
керівник роботи к.т.н., професор В.В. Кочан
затверджені наказом по університету від 20 грудня 2024 року № 938.
2. Строк подання студентом закінченої кваліфікаційної роботи 1 грудня 2025 р.

3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.

4. Основні питання, які потрібно розробити
– провести аналіз предметної області;
– провести аналіз методів та засобів для вирішення задачі;
– зробити постановку задачі дослідження;
– розробити концепцію інтеграції блокчейн-технології та штучного інтелекту для аналізу великих даних у середовищі Інтернету речей;
– дослідити мережеву модель когнітивного Інтернету речей і модель загроз;
– розробити модель інтеграції блокчейн-технології та штучного інтелекту для аналізу великих даних у середовищі Інтернету речей;
– зробити постановку експериментів;
– проаналізувати результати експериментальних досліджень.

5. Перелік графічного матеріалу у роботі
– схема мережевої моделі CIoT без блокчейну;
– схема мережевої моделі CIoT із підтримкою блокчейну;
– схема процесу аналітики великих даних на основі блокчейн з підтримкою ШІ;
– результати симуляції роботи блокчейну.

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв

7. Дата видачі завдання 20 грудня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів кваліфікаційної роботи	Примітка
1	Затвердження теми кваліфікаційної роботи, ознайомлення з літературними джерелами та складання плану роботи.	до 01.01. 2025 р.	
2	Написання 1 розділу кваліфікаційної роботи	до 01.03. 2025 р.	
3	Написання 2 розділу кваліфікаційної роботи	до 20.05.2025 р.	
4	Написання 3 розділу кваліфікаційної роботи	до 28.10. 2025 р.	
5	Представлення попереднього варіанту кваліфікаційної роботи, перевірка та внесення змін керівником	до 11.11.2025 р.	
6	Опрацювання зауважень та представлення завершеного варіанту кваліфікаційної роботи. Підготовка супроводжуючих документів.	до 25.11.2025 р.	
7	Перевірка кваліфікаційної роботи на оригінальність тексту.	до 1.12.2025 р.	
8	Оформлення кваліфікаційної роботи та отримання допуску до захисту	до 04.12.2025 р.	
9	Подання кваліфікаційної роботи до захисту на засіданні атестаційної комісії.	до 14.12. 2025 р.	

Студент _____ Б.-Д. Ю. Дзядик
підпис

Керівник роботи _____ к.т.н., професор В.В. Кочан
підпис

РЕЗЮМЕ

Кваліфікаційна робота на тему «Модель інтеграції блокчейн-технології та штучного інтелекту для аналізу великих даних у середовищі Інтернету речей» на здобуття освітнього ступеня «Магістр» зі спеціальності 122 «Комп'ютерні науки» освітньої програми «Комп'ютерні науки» написана обсягом в 71 сторінку і містить 8 ілюстрацій, 5 таблиць, 1 додаток та 46 використаних джерел.

Метою кваліфікаційної роботи є розроблення моделі інтеграції блокчейн-технології та методів штучного інтелекту для аналітики великих даних у середовищі Інтернету речей, яка підвищує достовірність даних, стійкість МН-моделей та відтворюваність обчислювальних результатів у розподілених умовах.

Методи досліджень: включають огляд і узагальнення наукових джерел; побудову спрощених моделей системи та загроз; використання базових криптографічних засобів і механізмів узгодження даних; розроблення та навчання типових моделей машинного навчання; проведення комп'ютерного моделювання й експериментів із варіюванням ключових параметрів; оцінювання результатів за стандартними метриками точності.

Результати дослідження: розроблено узагальнену модель інтеграції технологій блокчейн та штучного інтелекту для аналізу великих даних у когнітивному Інтернеті речей, що поєднує незмінність даних із аналітикою на основі інтелекту.

Результати роботи можуть успішно застосовуватися для побудови захищених інтелектуальних IoT-платформ, у яких поєднано блокчейн-технологію та методи штучного інтелекту для надійної аналітики великих даних. Вони можуть бути впроваджені в промислових, міських, аграрних та інших CIoT-сценаріях, де критичною є довіра до даних, стійкість моделей машинного навчання до атак та відтворюваність результатів аналітики.

Ключові слова: БЛОКЧЕЙН-ТЕХНОЛОГІЯ; ШТУЧНИЙ ІНТЕЛЕКТ; КОГНІТИВНИЙ ІНТЕРНЕТ РЕЧЕЙ; ВЕЛИКІ ДАНІ; ЗАХИЩЕНІ IoT-ПЛАТФОРМИ; АНАЛІТИКА ДАНИХ; ДОВІРА ДО ДАНИХ.

ABSTRACT

Qualification work on the topic «Model for Integrating Blockchain Technology and Artificial Intelligence for Big Data Analysis in Internet of Things Environments» for Master's degree on speciality 122 «Computer Science» educational and professional program «Computer Science» is written on 71 pages and it contains 8 figures, 5 tables, 1 annex and 46 sources.

The purpose of this qualification work is to develop a model for integrating blockchain technology and artificial intelligence methods for big data analytics in the Internet of Things environment, which increases data reliability, the robustness of ML models, and the reproducibility of computational results under distributed conditions.

Research methods include the review and synthesis of scientific sources; construction of simplified models of the system and threats; use of basic cryptographic tools and data consistency mechanisms; development and training of typical machine learning models; computer simulation and experiments with variation of key parameters; and evaluation of results using standard accuracy metrics.

Research results: a generalized model for integrating blockchain and artificial intelligence technologies for big data analysis in the cognitive Internet of Things has been developed, which combines data immutability with intelligence-based analytics.

The results of this work can be successfully applied to the construction of secure intelligent IoT platforms that combine blockchain technology and artificial intelligence methods for reliable big data analytics. They can be implemented in industrial, urban, agricultural and other CIoT scenarios where data trustworthiness, robustness of machine learning models against attacks, and reproducibility of analytics results are critical.

Keywords: BLOCKCHAIN TECHNOLOGY; ARTIFICIAL INTELLIGENCE; COGNITIVE INTERNET OF THINGS; BIG DATA; SECURE IoT PLATFORMS; DATA ANALYTICS; DATA TRUSTWORTHINESS.

ЗМІСТ

ВСТУП

Актуальність роботи. Стрімкий розвиток Інтернету речей (IoT) зумовлює безпрецедентне зростання обсягу, швидкості та різнорідності даних, що генеруються сенсорами, вбудованими пристроями та кіберфізичними системами. У таких умовах традиційні централізовані підходи до збирання та опрацювання даних стикаються з обмеженнями масштабованості, затримок, довіри й кіберстійкості [1]. Паралельно із цим, блокчейн-технологія пропонує незмінний розподілений реєстр транзакцій і механізми децентралізованого узгодження, а методи штучного інтелекту (ШІ) та машинного навчання (МН) забезпечують здатність виявляти закономірності, прогнозувати стани та підтримувати прийняття рішень у режимі наближеному до режиму реального часу. Інтеграція блокчейна та ШІ у середовищі IoT постає як перспективний напрям, що поєднує гарантії цілісності та простежуваності даних із когнітивними можливостями аналітики великих даних [2, 3].

Незважаючи на активний розвиток кожної зі складових – IoT, блокчейна та ШІ – їхня інтеграція у цілісну архітектуру залишається складною задачею. Виникає низка проблем: як забезпечити довіру до даних на всьому шляху їхнього життєвого циклу; яким чином мінімізувати ризики спотворення даних і маніпуляцій під час навчання моделей; як синхронізувати децентралізоване збирання та зберігання з вимогами до продуктивності й затримок; як зробити так, щоб більше вузлів могли узгоджувати транзакції, але система не почала працювати повільніше і не обробляла менше операцій; як зробити так, щоб процеси машинного навчання працювали на пристроях на краю мережі стабільно (навіть при збоях), економили енергію і не вимагали багато пам’яті та потужності. Відсутність узгодженої моделі інтеграції спричиняє фрагментацію рішень і ускладнює їх практичне впровадження в промислових, міських, аграрних та критичних інфраструктурах.

Актуальність теми підсилюється зростанням частоти інцидентів, пов’язаних із порушенням цілісності й конфіденційності даних, та потребою у

відтворюваних, верифікованих аналітичних результатах. У контексті IoT навіть невелика частка спотворених або підмінених спостережень може призвести до деградації якості моделей, неправильних керуючих дій і збоїв у сервісах. Блокчейн, завдяки незмінності записів, механізмам прозорого аудиту та розподіленому довірчому середовищу, створює основу для «довірених даних», тоді як ШІ/МН забезпечує витягування знань і адаптивне керування на їх підставі. Водночас інтеграція цих підходів потребує формалізації потоків даних, визначення точок інтеграції та балансування між накладними витратами й вимогами до швидкодії аналітики.

Мета і завдання дослідження. Метою роботи є розроблення моделі інтеграції блокчейн-технології та методів штучного інтелекту для аналітики великих даних у середовищі Інтернету речей, яка підвищує достовірність даних, стійкість МН-моделей та відтворюваність обчислювальних результатів у розподілених умовах.

Для досягнення поставленої мети потрібно виконати ряд завдань:

– провести аналіз предметної області;

– провести аналіз методів та засобів для вирішення задачі;

– зробити постановку задачі дослідження;

– розробити концепцію інтеграції блокчейн-технології та штучного інтелекту для аналізу великих даних у середовищі Інтернету речей;

– дослідити мережеву модель когнітивного Інтернету речей і модель загроз;

– розробити модель інтеграції блокчейн-технології та штучного інтелекту для аналізу великих даних у середовищі Інтернету речей;

– зробити постановку експериментів;

– проаналізувати результати експериментальних досліджень.

Об’єктом дослідження є процес збирання, верифікації, зберігання та аналітики сенсорних даних у когнітивному Інтернеті речей.

Предметом дослідження є методи та засоби інтеграції блокчейн-технології й штучного інтелекту для аналізу великих даних в когнітивному Інтернеті речей.

Методи дослідження включають огляд і узагальнення наукових джерел; побудову спрощених моделей системи та загроз; використання базових криптографічних засобів і механізмів узгодження даних; розроблення та навчання типових моделей машинного навчання; проведення комп'ютерного моделювання й експериментів із варіюванням ключових параметрів; оцінювання результатів за стандартними метриками точності.

Наукова новизна одержаних результатів полягає у розробці узагальненої моделі інтеграції технологій блокчейн та штучного інтелекту для аналізу великих даних у когнітивному Інтернеті речей, що поєднує незмінність даних із аналітикою на основі інтелекту.

Практичне значення отриманих результатів полягає у реалізації запропонованих рішень для інтеграції блокчейн та ШІ в IoT-середовищі, який забезпечує захищене збирання й зберігання даних, їхню простежуваність і незмінність.

Публікації та апробація КР. Результати кваліфікаційної роботи апробовані та опубліковані у матеріалах (додаток А):

– II Всеукраїнської науково-практичної конференції «Інтелектуальні комп'ютерні системи та мережі», 25 листопада 2025 р., Тернопіль, Україна;

– 2nd International Scientific and Practical Conference «Progressive Approaches in Science and Engineering», November 26-28, 2025. Copenhagen, Denmark.

Кваліфікаційна робота складається із вступу, трьох розділів, висновків, списку використаних джерел та додатків.

1 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ДЛЯ АНАЛІЗУ ВЕЛИКИХ ДАНИХ У СЕРЕДОВИЩІ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Аналіз предметної області

IoT став однією з провідних технологій завдяки стрімкому розвитку інформаційно-комунікаційних технологій. Під IoT розуміють сукупність «розумних» пристроїв (фізичних або віртуальних об’єктів), що здатні взаємодіяти між собою, обмінюватися даними та виконувати керовані дії [1]. Кожному пристрою надається унікальний ідентифікатор або мережева адреса, зокрема адреса протоколу Інтернету версії 6 – IPv6, що цілком відповідає сучасним технічним можливостям. Завдяки стеку IPv6 Low-Power Wireless Personal Area Network такі пристрої можуть функціонувати в умовах жорстких обмежень – із низьким енергоспоживанням та обмеженою обчислювальною потужністю [2].

Оскільки IoT-пристрої обмінюються даними між собою і передають їх на найближчі шлюзи через бездротовий зв’язок, виникає багато загроз: хтось може видати себе за інший пристрій, повторно надіслати перехоплені повідомлення, фізично заволодіти пристроєм, перехопити та змінити дані під час передачі, або зловживати доступом, якщо має привілейовані права всередині системи [3]. Для забезпечення безпеки IoT-мережі дослідники запропонували низку протоколів і механізмів: автентифікацію, керування ключами, контроль доступу та виявлення вторгнень.

Когнітивний Інтернет речей (Cognitive IoT, CIoT) формується як еволюційна модель мережі, що розвиває ідеї IoT. Подібно до класичного IoT, у CIoT взаємодіють фізичні й віртуальні об’єкти з мінімальною участю людини, проте комунікація та керування ґрунтуються на контекстно-обізнаному циклі «сприйняття → дія» [4]. CIoT працює за принципом «розуміємо, коли будуємо»: система навчається і на даних із соціальних мереж, і на даних із реального світу (з датчиків), зберігає ці знання у базах даних у зрозумілому для себе вигляді, а потім підлаштовується під зміни та невизначеність, використовуючи методи

прийняття рішень, які не потребують багато ресурсів.

Можна виокремити дві ключові цілі CIoT. По-перше, це інтеграція фізичного та соціального світів для побудови інтелектуальної фізико-кібер-соціальної системи. По-друге, це забезпечення «розумного розподілу ресурсів», «інтелектного надання сервісів» та «автоматизованого функціонування мережі».

Отже, CIoT можна розглядати як науковий напрям, у якому ідеї IoT поєднуються з когнітивними обчисленнями для надання системам IoT «здатності мислити». Хоча комп'ютери не мислять як люди, когнітивні методи дають змогу системі інтерпретувати, навчатися та робити висновки на основі потоків даних від IoT-сенсорів. Сам IoT-комплекс – це мережа сенсорів (розумних пристроїв), з'єднаних через Інтернет для збору даних у режимі реального часу; застосування когнітивних підходів до цих даних уможливлює навчання, узагальнення та прогнозування.

Обмежена кількість радіочастот гальмує розвиток промислового Інтернету речей. Когнітивне радіо допомагає пристроям CIIoT працювати ефективніше, тому що вони можуть знаходити вільні частоти й тимчасово їх використовувати [5]. Щоб покращити пошук вільного спектра та передачу даних, Liu і Zhang [5] запропонували кластерну схему: "голови" кластерів разом перевіряють, які частоти зараз вільні, а інші вузли передають дані за підходом NOMA. Водночас автори показали, що в такій архітектурі зменшуються ймовірність успішного доступу до спектра та середня сумарна пропускна здатність, тобто виникає компроміс між точнішим сенсингом і додатковим навантаженням на мережу.

У наступній роботі Liu і Zhang [6] розглянули IoT, який працює разом із мережами 5G, щоб одночасно передавати дані і через 5G, і через IoT, використовуючи частоти 5G. Вони показали, що один IoT-вузол може передавати голос і відео через 5G, а канал IoT використовувати для передавання даних із датчиків. Також автори запропонували задачу оптимізації: як зробити швидкість передавання даних IoT максимальною, але не перевищити задані обмеження на швидкість у каналі 5G.

Як показано на рисунку 1.1, CIoT можна застосовувати в багатьох практичних задачах. Йдеться про поєднання IoT і машинного навчання, завдяки чому можна створювати, наприклад, «розумний» дім, виконувати аероспостереження за допомогою дронів, автоматично виявляти дорожні пригоди та знаходити вибоїни на дорогах у режимі реального часу. Але через те, що такі системи працюють з даними з реального середовища, зростають і ризики: зловмисник може додати до даних спеціально підготовлені «погані» приклади, і тоді модель навчиться неправильно – це називають спотворенням вхідних даних.

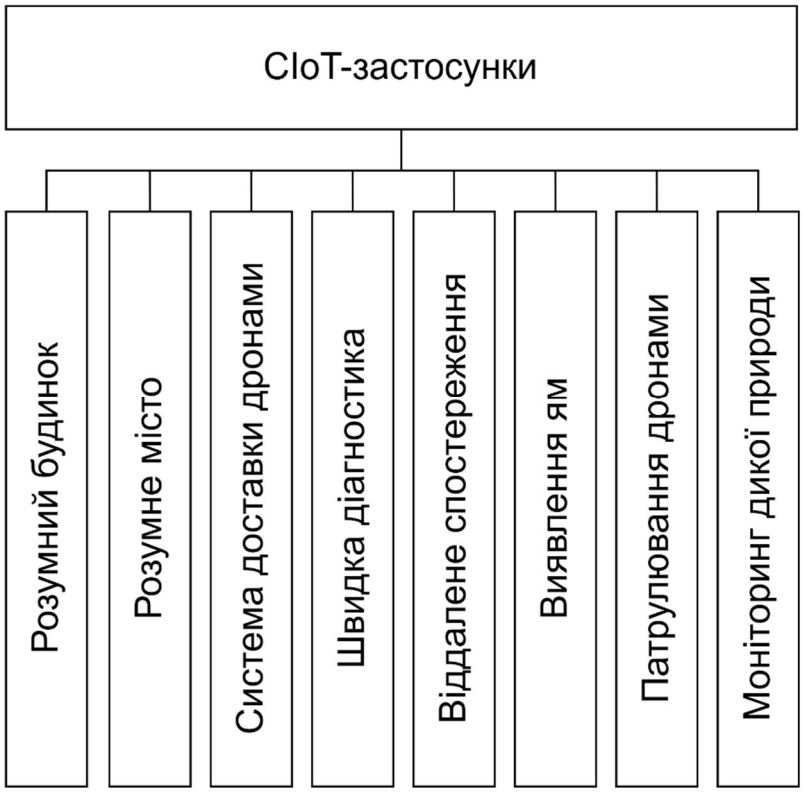


Рисунок 1.1 – Приклади використання CIoT

Один зі способів зменшити цей ризик – зберігати дані в блокчейні. Тоді їх складніше непомітно змінити, і кожен запис можна перевірити. Блоки в блокчейні зв’язані між собою хешами, тому якщо хтось без дозволу відредагує, видалить або підмінить дані, ланцюг одразу “ламається”, і підробку можна виявити. Крім того, правила консенсусу змушують усі вузли погоджуватися з тим, які записи є правильними, тому зростає довіра до даних. А у звичайних

сховищах – у хмарі або на туманних серверах – без блокчейна зловмисник може змінити “сирі” дані, на яких навчається модель машинного навчання. У результаті модель, навчена на підроблених даних, починає працювати гірше, і її точність помітно падає.

1.2 Штучний інтелект і машинне навчання

Штучний інтелект – це напрям інформатики, у межах якого створюють методи та системи, здатні імітувати окремі прояви людського інтелекту, аби автоматично виконувати завдання, традиційно притаманні людині. До таких завдань належать, зокрема, розпізнавання зображень і мовлення, інтерпретація сенсу, узагальнення попереднього досвіду тощо. Нині застосування ШІ охоплюють широкі домени: від електронної комерції та біомедичної інженерії – до автомобільної індустрії, «розумних» будинків і «розумних» міст.

Машинне навчання зазвичай розглядають як підмножину ШІ, яка надає комп’ютерним системам здатність навчатися з досвіду без явного програмування кожного правила. Класичне формулювання визначення МН таке: «комп’ютерна програма вважається такою, що навчається з досвіду E щодо певного класу задач T і за мірою ефективності P, якщо її результативність у задачах класу T, вимірюється за допомогою P, поліпшується зі зростанням досвіду E» [7, 8]. Це означення фіксує три необхідні компоненти будь-якої МН-системи:

– клас задач (T),
– джерело досвіду/даних (E),
– метрику оцінювання (P).

Розглянемо три базові парадигми МН:

1. Навчання з учителем. Алгоритм отримує тренувальні приклади з відомими правильними виходами (мітками) та вчиться будувати загальне правило відображення «вхід → вихід». Типові постановки: класифікація, регресія.

2. Навчання без учителя. Мітки не надаються; алгоритм самостійно

виявляє внутрішню структуру даних (кластеризація, зниження розмірності, виявлення аномалій). У CIoT це, зокрема, групування сенсорних потоків за подібними патернами.

3. Підкріплювальне навчання. Агент взаємодіє з динамічним середовищем і максимізує накопичувану винагороду, отримуючи зворотний зв'язок лише щодо наслідків своїх дій (приклад – керування автономним транспортом).

У XXI столітті ШІ/МН стали домінантною технологією для широкого спектра застосувань: детекція та розпізнавання зображень, комп'ютерний зір, розпізнавання мовлення, інтелектуальні IoT-середовища, смарт-медицина тощо. У межах цього дослідження МН використовується як інструмент оброблення великих сенсорних потоків у CIoT із фокусом на узагальнюваність, стійкість до спотворення вхідних даних і відтворюваність результатів за фіксованими протоколами оцінювання [8].

Подібно до інших мережевих середовищ, системи ШІ/МН є вразливими до низки цілеспрямованих атак. Безпека моделей машинного навчання набула особливої актуальності, адже достовірність прогнозів залежить від цілісності даних і стабільності процесу навчання. У типовому сценарії CIoT великі масиви даних, згенеровані «розумними» пристроями, зберігаються на хмарних серверах. Оскільки такі сервери часто вважають частково довіреними, зловмисники можуть використовувати наступні засоби:

1. Атаки «ворожими» прикладами. Зловмисник підбирає спеціальні вхідні дані так, щоб модель помилялася. Зміни можуть бути дуже малими й майже непомітними для людини, але модель через них приймає неправильне рішення [9].

2. Спотворення вхідних даних. Зловмисник псує дані для навчання: додає неправдиві приклади, міняє мітки класів, видаляє частину даних або додає шум. Через це модель вчиться на спотворених даних і потім погано працює на нормальних, чистих даних [10].

3. Атаки на модель. Зловмисник намагається змінити сам процес навчання

або налаштування моделі: параметри, гіперпараметри, проміжні стани навчання. Навіть невеликі зміни можуть сильно погіршити роботу моделі під час використання [11].

4. Крадіжка моделі та визначення, чи був зразок у навчанні. Зловмисник «опитує» модель через запити й намагається відтворити її або зробити висновок, чи входив конкретний приклад до тренувального набору. Це може призвести до витоку приватних даних і втрати інтелектуальної власності [12].

Штучна нейронна мережа – це набір алгоритмів, які вчаться знаходити закономірності в даних, використовуючи модель обчислень, що частково нагадує роботу мозку. У такій мережі нейрон моделюють як вузол, що приймає вхідні сигнали й формує вихід – як правило, нелінійну функцію від зваженої суми входів.

Згорткові нейронні мережі (Convolutional Neural Networks, CNN) – клас глибоких моделей, який широко застосовують у задачах комп'ютерного зору [7]. Архітектурно CNN – це багатошарова мережа, у якій частина шарів виконує згорткове видобування ознак із вхідних зображень. Схема типової архітектури наведена на рисунку 1.2.

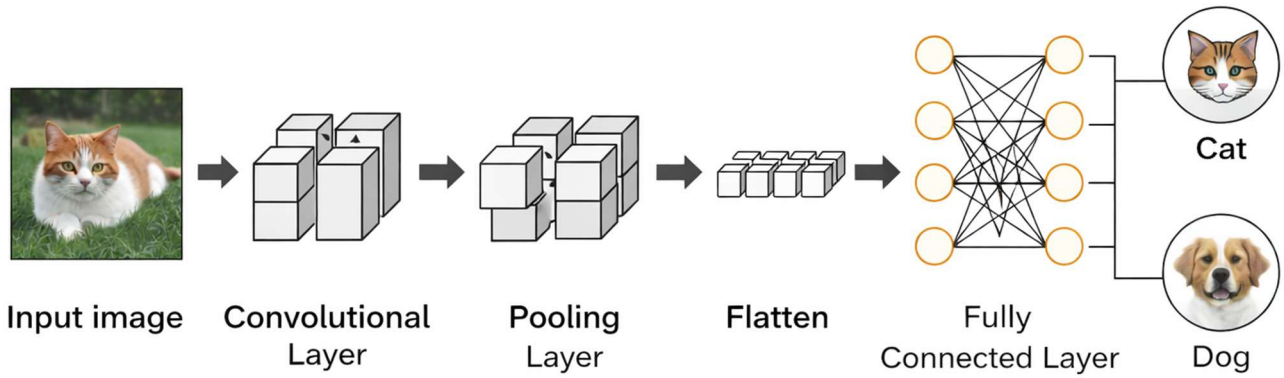


Рисунок 1.2 – Типова архітектура CNN [7]

Основні типи шарів у CNN:

1. Згортковий шар (convolution layer). Це шар, який «пропускає» по зображенню (або іншому тензору) набір маленьких фільтрів і так знаходить

корисні ознаки – наприклад, краї, лінії, прості форми. Завдяки тому, що один і той самий фільтр використовується в різних місцях, потрібно менше параметрів і навчання стає ефективнішим.

2. Шар пулінгу (pooling layer). Він зменшує розмір карт ознак (наприклад, бере максимум або середнє на невеликій ділянці). Це прискорює обчислення і робить модель більш стійкою до невеликих зсувів зображення та шуму.

3. Повнозв'язний шар (fully connected layer). Він збирає всі знайдені ознаки «в один вектор» і робить фінальне рішення: визначає клас або обчислює числове значення. У задачах класифікації після нього часто ставлять softmax, щоб отримати ймовірності класів.

Головна ідея CNN схожа на те, як працює зір: "нейрони" реагують не на все зображення одразу, а лише на невеликі ділянки. Поступово, шар за шаром, модель переходить від простих ознак (контури, текстури) до складніших об'єктів.

На практиці згорткові блоки часто доповнюють функціями активації (найчастіше ReLU), нормалізацією і методами регуляризації. Це допомагає швидше та стабільніше навчати модель і зменшує ризик перенавчання. У експериментальних дослідженнях CNN буде використовуватися в якості базової моделі для обробки зображень, зокрема в задачах CIoT, пов'язаних із виявленням дефектів доріг [7].

1.3 Блокчейн і його еволюція в когнітивний Інтернет речей

Блокчейн спирається на ідею однорангової (Peer-to-Peer, P2P) розподіленої мережі та надає універсальний набір даних, якому можуть довіряти всі учасники – навіть якщо вони не знайомі між собою і не мають взаємної довіри. По суті, це спільний і надійний реєстр транзакцій: незмінні та шифровані копії записів зберігаються на кожному вузлі мережі. Блоки транзакцій зв'язані хеш-значеннями (зв'язний список із хеш-вказівниками), тож будь-яка спроба зміни/видалення даних порушує ланцюг, бо змінює хеш наступних блоків. Отже,

блокчейн – це розподілений, незмінний і прозорий реєстр.

Механізм консенсусу – ключовий етап перевірки та додавання блоків одноранговими вузлами в P2P-мережі. Консенсус-алгоритм визначає, які транзакції валідні і чи слід включати відповідний блок до ланцюга, забезпечуючи єдину «версію істини» в умовах відсутності довіри між учасниками та помилкових/зловмисних вузлів. Серед поширених підходів: Proof of Work (PoW), Proof of Stake (PoS), Proof of Credit (PoC), Alternative to PoW (Alt-PoW), Proof of Authentication (PoAh), Proof of Elapsed Time (PoET), Proof of Space, Byzantine Fault Tolerance (BFT), Practical BFT (PBFT) тощо.

За моделлю доступу блокчейни поділяють на три типи:

1. Публічні – відкриті системи, наприклад Bitcoin, де будь-хто може приєднатися й записувати блоки.

2. Приватні – закриті середовища, наприклад Hyperledger Fabric, Multichain, у яких усі учасники попередньо відомі й авторизовані.

3. Консорціумні – гібридні рішення, що комбінують властивості публічних і приватних мереж, досягаючи консенсусу в межах консорціуму організацій.

Відомо, що інтеграція блокчейна з IoT (зокрема в CIoT) забезпечує конфіденційність, децентралізацію, прозорість та незмінність даних [13]. Рисунок 1.3 ілюструє приклади використання технології Blockchain of Things (BoT): розумні енергомережі, ланцюги постачання, харчова промисловість, Інтернет дронів (IoD), охорона здоров’я, Інтернет транспортних засобів (IoV), точне землеробство та «розумне» фермерство, а також CIoT [14].

Ще у 2017 році Kotobi і Bilen [15] запропонували децентралізовану базу даних на основі блокчейна, щоб перевіряти і контролювати спільне використання радіочастот між когнітивними радіосистемами. Їхній підхід до керування доступом є безпечним і не залежить від одного центрального сервера, а також працює як при невеликому, так і при сильному погіршенні якості каналу. Автори показали, що така схема краще розподіляє вільні (невикористані)

частоти, ніж традиційні методи. Крім того, цей механізм можна застосовувати і для доступу до ліцензованого спектра без постійного пошуку вільних частот.

Рисунок 1.3 – Приклади використання технології Blockchain of Things (BoT) [14]

У 2021 році Хіе та співавт. [16] запропонували блокчейн-механізм репутації APR_SWSS для безпечного широкосмугового «прослуховування» спектра. У ньому є два види репутації: активна (як добре вузол сам робить вимірювання) і пасивна (наскільки він надійний як учасник, що передає/підтверджує дані). Автори показали, що разом із стисненим вимірюванням (коли потрібно менше вимірів для оцінювання спектра) також можна виявляти підозрілі вузли, оцінюючи їхній внесок, і краще захищатися від атак підробки спектральних даних (SSDF) [17]. Під час SSDF зловмисники надсилають у центр злиття фальшиві результати, через що система гірше визначає вільні частоти і витрачає більше енергії [17].

Wu та ін. [4] запропонували загальний підхід до CIoT: описали основні «когнітивні» дії системи, механізми для виконання цих задач, метрики

оцінювання та ключові проблеми — масштабування, різнорідність середовища і обмежені ресурси.

Awin та ін. [24] зробили огляд CR-IoT (IoT із когнітивним радіо) і виділили найважливіші відкриті питання CIoT: керування спектром, надійність вимірювань та безпека взаємодії вузлів.

Li та ін. [25] визначили ключові вимоги до IoT-систем, які мають працювати з когнітивним радіо: «розумне» виявлення вільних частот, гнучке використання доступного спектра в режимі реального часу та раціональний розподіл частотних ресурсів між вузлами.

Patnaik та ін. [14] показали, що SSDF-атаки сильно шкодять мережам CR-IoBT. Для захисту вони запропонували ProBLeSS — проактивний блокчейн-підхід до спільного використання спектра, який зменшує вплив SSDF у CR-IoBT.

Rathee та ін. [26] підкреслюють роль когнітивних систем у керуванні виробництвом: важливо вміти підлаштовуватися під невизначеність і спиратися на сенсорні дані. Для підтримки рішень вони застосовують методи зважування та AHP (метод аналізу ієрархій) під час передавання, обробки й збереження інформації.

Kasturi та ін. [27] запропонували ML-класифікатор для виявлення радіоглушіння, який зменшує відношення сигнал/шум і заважає нормальному зв’язку. Johnson та ін. [28] показали застосування ML і для виявлення шкідливих URL-адрес у листах і на вебсторінках.

Останніми роками багато уваги приділяють атакам спотворення даних проти ML-моделей, бо вони напряму псують якість прогнозів [29–33]. У [29] показано підміну міток у федеративному / розподіленому навчанні на реальних даних і глибоких нейронних мережах. У [30] розглянуто, як можна зіпсувати роботу SVM, додаючи спеціально підібрані «шкідливі» точки, які будують за градієнтною стратегією. Sun та ін. [31] запропонували оптимізаційний підхід, який дозволяє знаходити найбільш ефективні атаки на федеративне / розподілене навчання, а в [32] цю ідею розвинули для різних конфігурацій федеративного / розподіленого навчання та перевірили, наскільки вони стійкі до спотворення

даних.

Також описані приклади спотворення даних для авторегресійних моделей [33] і атаки на матричну факторизацію в колаборативній фільтрації [34]. У підсумку ці роботи показують, що для CIoT потрібні захищені конвеєри даних і інфраструктура з перевіркою цілісності збереження (зокрема на базі блокчейна), бо від цього залежить стабільність когнітивних сервісів і якість прийняття рішень.

1.4 Постановка задачі дослідження

У середовищі CIoT формуються безперервні потоки гетерогенних даних від тисяч сенсорів і кіберфізичних об’єктів. Умови обмежених ресурсів, бездротові канали та участь напівдовірених посередників підвищують ризики модифікації даних і спотворення наборів для навчання моделей ШІ, що безпосередньо знижує якість аналітики та надійність прийняття рішень у режимі реального часу [13]. Водночас, у CIoT зростає кількість задач комп’ютерного зору, які використовують глибокі нейронні мережі і є вразливими до шуму або підміни міток у даних [18, 29–33]. Блокчейн можна використати як надійний і незмінний журнал, де кожен запис перевіряється криптографічно (через хеші, цифрові підписи та узгодження між вузлами), тому підміна або непомітна зміна даних стає значно складнішою [36–38]. Саме потреба поєднати можливість перевірки та захист даних із ефективним навчанням і роботою нейромереж робить актуальною інтегровану модель на основі блокчейна та ШІ для аналізу великих даних в IoT.

Відомі підходи демонструють обмеження, що унеможливлюють гарантовану цілісність даних і відтворюваність аналітики в CIoT:

– зберігання даних лише в хмарі (централізовано): є ризик, що співробітники або зловмисники непомітно змінять дані; немає надійної, криптографічно підтвердженої історії змін [13];

– використання машинного навчання без захисту даних: якщо в дані

додати шум або підмінити мітки, якість моделі помітно падає; також важко потім зрозуміти, звідки взялися помилки і хто змінив дані [9, 29–33];

– не всі механізми узгодження (консенсусу) підходять для IoT: PoW витрачає забагато енергії; PoS/PoET не завжди дають потрібний рівень довіри; зазвичай немає нормальної інтеграції з ML-процесами;

– погана відтворюваність експериментів: немає чіткого зв'язку між даними, моделями та результатами з незмінними ідентифікаторами (хешами) у ланцюгу, що ускладнює порівняння й аудит експериментів;

– федеративне навчання без перевірки даних: воно зменшує передачу сирих даних, але все одно не захищає від того, що на окремих вузлах можуть спотворити дані або оновлення моделі, якщо немає додаткових механізмів контролю та журналювання [39].

Тому, метою роботи є розроблення моделі інтеграції блокчейн-технології та методів штучного інтелекту для аналітики великих даних у середовищі Інтернету речей, яка підвищує достовірність даних, стійкість МН-моделей та відтворюваність обчислювальних результатів у розподілених умовах.

Висновки до розділу 1

1. IoT та CIoT постійно генерують різні типи даних у режимі реального часу, тому обмін має бути швидким і безпечним. Через бездротовий зв'язок і частково довірені проміжні вузли зростає ризик підміни даних, повторної відправки повідомлень і зловживань з боку інсайдерів. У таких умовах якість даних напряму впливає на правильність аналізу та прийняття рішень. Тому потрібні механізми, які гарантують, що дані не змінені і можна простежити їх шлях від джерела до споживача.

3. Штучний інтелект і машинне навчання (наприклад, CNN у задачах комп'ютерного зору) допомагають отримувати знання з сенсорних даних, але вони вразливі до атак: зокрема до спотворення даних і спеціально підібраних «обманних» прикладів. Якщо дані зберігаються централізовано без

криптографічного захисту, складно довести, звідки вони взялися і чи їх не підміняли, а також важко провести аудит і повторити експерименти. У підсумку падає якість моделі і зростає невизначеність рішень. Це показує, що потрібен надійний «ланцюг довіри» для всього ML-процесу.

3. Блокчейн (з цифровими підписами, хешуванням і механізмом узгодження) дає незмінний журнал записів і забезпечує, щоб усі вузли бачили однакові дані в розподіленій CIoT-системі. Якщо поєднати блокчейн із ML-аналітикою, можна перевіряти і відстежувати як дані, так і версії моделей, що підвищує захист від атак і прихованих змін. Такий підхід зменшує ризик падіння якості, а також робить результати більш відтворюваними. Отже, поєднання блокчейна і ШІ є перспективним способом підвищити надійність CIoT-аналітики.

2 ІНТЕГРАЦІЯ БЛОКЧЕЙН-ТЕХНОЛОГІЇ ТА ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АНАЛІЗУ ВЕЛИКИХ ДАНИХ У СЕРЕДОВИЩІ ІНТЕРНЕТУ РЕЧЕЙ

2.1 Концепція інтеграції блокчейн-технології та штучного інтелекту для аналізу великих даних у середовищі Інтернету речей

Когнітивний Інтернет речей (CIoT) формує багатошарову екосистему, у якій фізичні та віртуальні об’єкти взаємодіють через сенсорно-комунікаційні канали та спільні сервіси, що ґрунтуються на машинному навчанні і методах штучного інтелекту [4]. У цьому середовищі дані виникають безперервно, вони є гетерогенними за формою та якістю, несуть контекст і швидко втрачають актуальність. За таких умов критичною стає проблема довіри до даних і похідних від них компонентів (версій датасетів, навчальних/тестових вибірок, конфігурацій моделей, контрольних метрик), адже будь-яка неконтрольована модифікація на вході конвеєра аналітики здатна спричинити деградацію якості прогнозів на виході [9, 29–33, 41].

Концепція інтеграції, що пропонується використати, будується на поєднанні двох взаємодоповнювальних технологій. Перша – реєстр незмінних подій (блокчейн), який забезпечує фіксацію та можливість перевірки походження даних, а також хронологію їхніх перетворень за допомогою криптографічних механізмів (ECDSA-підписів, дерева Меркла, хешів блоків і механізму узгодження PBFT) [36–38]. Друга – конвеєри ШІ/МН, які працюють у розподіленому режимі (частина обчислень виконується на пристроях або на краю мережі). Це дозволяє передавати менше даних, швидше отримувати результат і краще зберігати приватність, бо «сирі» дані не потрібно щоразу надсилати в центральні вузли без реальної необхідності [18, 39].

В інтегрованій моделі блокчейн не слугує універсальним сховищем усіх бінарних об’єктів (зображень, відео), бо це практично неефективно; натомість він фіксує криптографічні відбитки (хеші), часові мітки, авторство, політики доступу та службові метадані. Завдяки цьому кожен файл або набір даних потім

можна перевірити і відтворити, якщо потрібно [13]. У свою чергу, модулі ШІ/МН використовують лише перевірені дані, які прив’язані до записів у блокчейні. Це зменшує ризик отруєння даних і ускладнює приховані зміни з боку інсайдерів у центральних сховищах [9, 29–33].

З погляду інженерії, інтеграція передбачає:

– зменшити роботу блокчейна**:** у ланцюг записувати лише те, що потрібно для перевірки й відстеження даних;

– великі файли зберігати поза блокчейном (у файлових або об’єктних сховищах), але прив’язувати їх до блокчейна через хеші;

– налаштувати PBFT під CIoT (час підтвердження, розмір блоку, кількість валідаторів), щоб знайти баланс між швидкістю підтвердження і стійкістю до збоїв та зловмисників;

– використовувати навчання на краю мережі або федеративне навчання так, щоб «сирі» дані не передавалися, але залишалася можливість перевіряти, аудіювати та відтворювати експерименти через систему ідентифікаторів у блокчейні [39].

Як наслідок, дана концепція інтеграції надає цінні властивості: незмінність і доказовість даних; простежуваність усіх стадій конвеєра (від збору до прийняття рішень); відтворюваність ML-результатів; контроль якості через порогові політики (Accuracy, Recall, Precision, F1) із фіксацією метрик у реєстрі; підвищену стійкість до атак підміни даних та прихованих змін з боку інсайдерів [18, 41].

Типова CIoT-система включає периферійні пристрої (сенсори, виконавчі пристрої, камери, безпілотники, контролери 6LoWPAN/IPv6), шлюзові вузли (сервери на краю мережі з модулями автентифікації та агрегування даних), а також хмарно-периферійний кластер, який об’єднує валідаторів блокчейна та керує сервісами аналітики [2, 4]. Перед розгортанням реєстраційний орган (RA) присвоює ідентифікатори застосункам та пристроям, налаштовує криптографічні ключі та правила доступу, що створює початкову зону довіри.

У робочому циклі пристрої створюють події та передають їх на шлюз.

Шлюз збирає події в пакети транзакцій, підписує їх ECDSA (щоб підтвердити джерело і унеможливити заперечення авторства), а потім розсилає їх вузлам-валідаторам. Валідатори перевіряють підписи, корінь дерева Меркла та хеш блоку, після чого узгоджують результат за протоколом PBFT, що дає менші затримки, ніж енерговитратні підходи, такі як PoW [36–38]. Після підтвердження у блокчейні зберігаються посилання на дані (їхні хеші та метадані), і саме вони використовуються як перевірена основа для підготовки даних, навчання і тестування моделей.

На рівні аналітики можливі два варіанти: або централізоване навчання CNN на кластері з повторюваними налаштуваннями, або федеративне навчання на edge-вузлах із періодичним об’єднанням ваг. В обох випадках моделі, контрольні набори, метрики та журнали експериментів отримують у блокчейні стабільні ідентифікатори, що дозволяє проводити аудит і швидко повертатися до «чистих» версій у разі виявлення підозрілих змін [18, 39, 41].

Загрози в CIoT можна умовно поділити на мережеві, пов’язані з даними та фізичні. За моделлю Долева–Яо противник може перехоплювати, змінювати й підставляти повідомлення у відкритому каналі, тому потрібні криптографічний захист передавання і перевірка цілісності даних на рівні застосунку [19]. CK-модель додає ризики компрометації сеансів і витоку конфіденційної інформації, отже потрібні стійкі протоколи обміну ключами та безпечне зберігання облікових даних на вузлах [20].

На рівні даних основні загрози — спотворення даних (додавання шуму, підміна міток) і атаки на модель (зміна гіперпараметрів або градієнтів, крадіжка моделі). У хмарних сценаріях це може виконувати інсайдер або зловмисник через слабкі місця в ланцюгу підготовки та передачі даних [9–12]. На фізичному рівні небезпечним є захоплення пристрою з подальшим аналізом енергоспоживання та витягуванням конфіденційної інформації, тому потрібні конструктивні й організаційні засоби захисту (контейнери, датчики розкриття, захищена пам’ять) і безпечне розміщення шлюзів.

Запропонована інтеграція протидіє цим загрозам завдяки: криптографічній

перевірці походження і цілісності даних (ECDSA, дерево Меркла, хеші), колективному узгодженню стану записів (PBFT) та можливості перевірити й відтворити ML-експерименти (фіксація версій даних, моделей і метрик у реєстрі). У сукупності це зменшує ризик непомітних маніпуляцій і полегшує розслідування інцидентів [36–38, 41].

2.2 Мережева модель когнітивного Інтернету речей і модель загроз

2.2.1 Мережева модель CIoT

На рисунку 2.1 подано узагальнену мережеву модель CIoT без блокчейна; відповідно, модель CIoT із підтримкою блокчейна наведено на рисунку 2.2. У запропонованих моделях реєстраційний орган, який також називається довіреною стороною – виконує реєстрацію різних IoT-застосунків (наприклад, рухомий транспорт, «розумний» дім, IoD тощо) до початку їхньої роботи у відповілних доменах. RA також реєструє інші компоненти системи, зокрема вузли-шлюзи, прив’язані до конкретних застосунків CIoT.

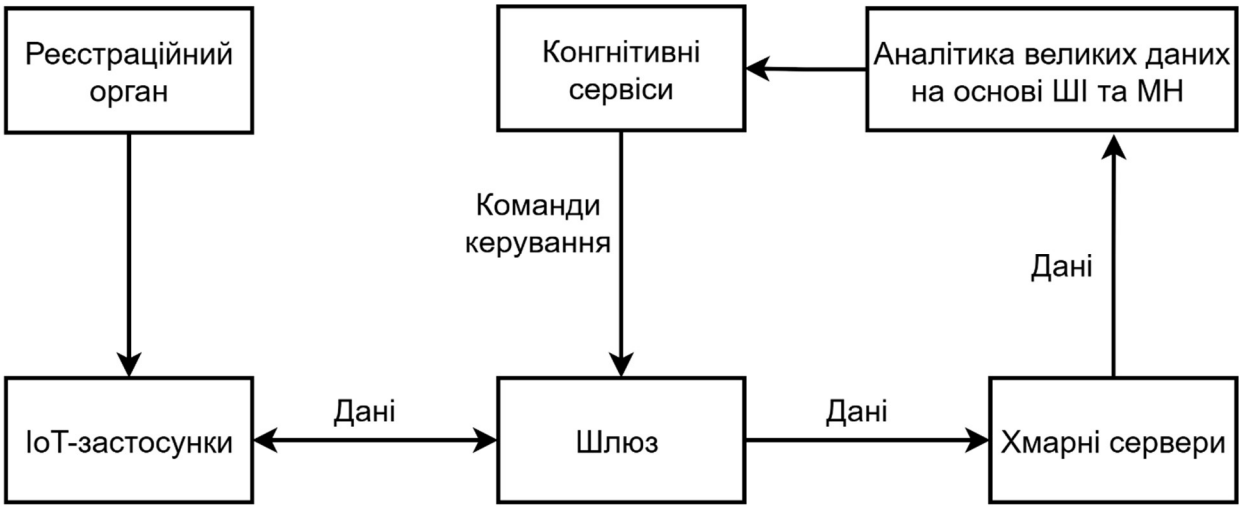


Рисунок 2.1 – Схема мережевої моделі CIoT без блокчейну

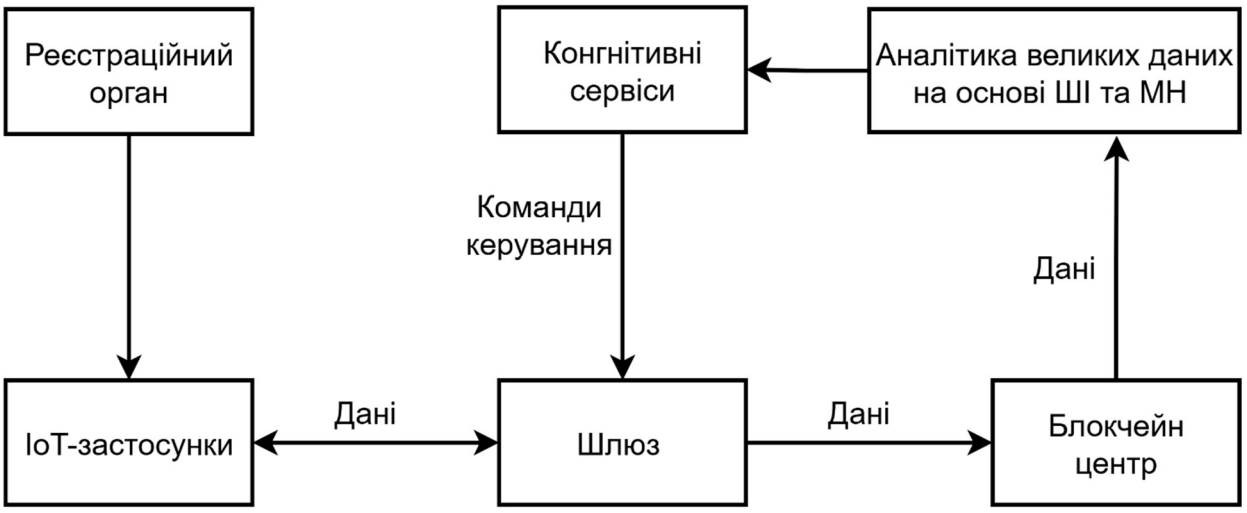


Рисунок 2.2 – Схема мережевої моделі CIoT із підтримкою блокчейну

Після завершення реєстрації розумні пристрої певного IoT-застосунку та відповідний шлюз розпочинають обмін через публічний канал. У такій конфігурації IoT-пристрій надсилає дані своєму шлюзу, той агрегує їх, формує транзакцію і передає до хмарного сервера. Сукупність хмарних серверів утворює розподілену P2P-мережу хмарних вузлів, у якій кожен сервер зберігає і синхронізує свою копію бази даних. Транзакції транслюються усій мережі хмарних серверів, і кожен вузол підтримує локальний список транзакцій.

Коли розмір списку досягає порогового значення, формується блок, який далі транслюється мережею. Після виконання механізму узгодження між вузлами блок додається до блокчейна. Дані, збережені в блокчейні, слугують основою для надання когнітивних сервісів на основі ШІ/МН-аналітики великих даних (зокрема із застосуванням CNN [18]). На цьому ж рівні реалізуються прийняття рішень, когнітивний вибір та планування; сформовані команди керування повертаються до відповідного IoT-застосунку через шлюз, після чого пристрої реагують відповідно до отриманих рішень.

2.2.2 Модель загроз

Дані відіграють центральну роль у середовищі CIoT. У типових реалізаціях кілька IoT-застосунків з’єднані між собою, і для кожного з них передбачено

вузол-шлюз. Розумні пристрої збирають дані в режимі реального часу та передають їх до відповідного шлюзу публічним (незахищеним) каналом, що зумовлює постійні ризики для конфіденційності, цілісності та доступності переданих повідомлень.

Розглянемо дві загальноприйняті моделі загроз:

1. Модель Долева–Яо (Dolev–Yao, DY) [19];
2. Модель Канетті–Кравчика (CK-модель зловмисника) [20].

У DY-моделі супротивник має змогу перехоплювати повідомлення в незахищеному каналі, а також модифікувати, видаляти чи вставляти шкідливий вміст у середовище передавання. Відповідно до CK-моделі, зловмисник не лише здатен підслуховувати/змінювати/видаляти фрагменти трафіку, а й компрометувати окремі сесії. Це означає ризик розкриття сеансових ключів і станів сесії, якщо конфіденційні облікові дані зберігаються в незахищеній пам’яті сторін, що обмінюються даними.

Оскільки цілодобовий нагляд за розгорнутими пристроями CIoT не завжди можливий, виникає загроза фізичного захоплення пристрою в агресивному середовищі. За такого сценарію супротивник може витягнути збережені облікові дані з незахищеної пам’яті використовуючи методи аналізу споживання потужності [21]. Додатково припускаємо, що хмарні сервери – напівдовірені, а шлюзи – довірені; водночас для протидії фізичному захопленню шлюзи розміщують у фізично захищених корпусах/шафах, як це передбачено у [22, 23].

2.3 Модель інтеграції блокчейн-технології та штучного інтелекту для аналізу великих даних у середовищі Інтернету речей

RA відповідає за реєстрацію всіх «розумних» пристроїв у середовищі CIoT, а також вузлів-шлюзів, що під’єднані до цих пристроїв відповідно до цільових застосунків. Після успішного завершення процедури реєстрації RA завантажує до пам’яті пристроїв конфіденційні облікові дані до їх розгортання в мережах CIoT.

Після розгортання IoT-пристрої та шлюзи переходять до роботи: пристрої збирають дані в режимі реального часу та надсилають їх на відповідний шлюз. Перед передаванням даних сторони встановлюють захищений сеансовий ключ як між пристроями, так і між пристроєм і шлюзом, застосовуючи надійні механізми контролю доступу [35].

Зауважимо, що відповідно до моделі загроз у межах CK-моделі зловмисника потрібно враховувати ризик витоку тимчасових ключів (Ephemeral Secret Leakage, ESL). Тому після успішної взаємної автентифікації дані передаються на шлюз у зашифрованому та захищеному вигляді. Шлюз збирає й об'єднує отриману інформацію та формує транзакцію з даними, позначимо її T_x. Оскільки в даному сценарії використовується публічний блокчейн, шлюз підписує транзакцію своїм приватним (закритим) ключем, формуючи цифровий підпис $ECDSA.Sig(T_x)$ за алгоритмом ECDSA [36].

Далі шлюз надсилає в P2P-мережу хмарних серверів пару $(T_x, ECDSA.Sig(T_x))$. Після отримання підписаних транзакцій один із вузлів мережі формує блок, який містить такі складові:

1. Заголовок блоку:

– версія блоку — номер/формат, за яким вузли розуміють, як читати блок;

– хеш попереднього блоку — посилання на попередній блок. Саме воно з'єднує блоки в ланцюг: якщо змінити старий блок, хеш зміниться і ланцюг ламається;

– корінь дерева Меркла [37] — один короткий хеш, який підсумовує всі транзакції в блоці, який дозволяє швидко перевірити, що конкретна транзакція справді входить у блок і що список транзакцій не змінювали;

– часова мітка — час створення/публікації блоку;

– відкритий ключ підписанта — відкритий ключ вузла/шлюза, який підписав блок або транзакції, щоб інші могли перевірити підпис.

2. Вміст блоку – список транзакцій і їхні підписи у вигляді $(Transactions\ (Tx),\ ECDSA.Sig(Tx))$.

3. Хеш поточного блоку — це «цифровий відбиток» усього блоку (і заголовка, і вмісту). Для його обчислення використовується SHA-256 [38], яка перетворює дані будь-якої довжини на 256-бітове хеш-значення. Якщо змінити хоча б один символ у блоці, хеш зміниться, тому він слугує для перевірки цілісності.

Після побудови блоків далі розглядаються фази формування блоку, додавання блоку до публічного блокчейна та ШІ/МН-керована аналітика великих даних, що спирається на зафіксовані у реєстрі дані.

2.3.1 Фаза формування блоку

Спочатку шлюз надсилає в мережу хмарних серверів підписані транзакції – *(Tx, ECDSA.Sig(Tx))*. Після розсилання кожному вузлу мережі транзакції потрапляють у локальну чергу транзакцій, яку вузли між собою синхронізують. Коли в черзі накопичується достатня кількість транзакцій (досягається заданий поріг), за принципом кругового чергування обирається вузол-лідер, який формує блок.

2.3.2 Фаза додавання блоку до реєстру

Включення блоку до публічного блокчейна відбувається після виконання механізму узгодження. У цій роботі використано PBFT (Practical Byzantine Fault Tolerance) — голосувальний алгоритм, який забезпечує роботу мережі навіть за наявності збоїв або зловмисних вузлів. У цьому сценарії вузол-лідер формує блок $Block_i$ з фіксованою кількістю транзакцій і їхніми підписами та розсилає його іншим хмарним вузлам. Вузли-учасники отримують $Block_i$ і звіряють його вміст зі своєю локальною чергою транзакцій.

Блок додається до ланцюга лише тоді, коли успішно пройдено перевірки:

– перевірка кореня дерева Меркла для транзакцій у $Block_i$;
– перевірка цифрових підписів транзакцій Sig(Tx);
– перевірка правильності хеша поточного блоку.

Після додавання блоку процес повторюється для наступного раунду

(епохи), при цьому роль лідера переходить до іншого вузла в P2P-мережі хмарних серверів.

2.3.3 Фаза аналітики Big Data на основі блокчейна та ШІ/МН

Після запису даних до публічного блокчейна вони стають джерелом для ШІ/МН-керованої аналітики великих даних і надання когнітивних сервісів. На цьому рівні реалізуються: аналізує ситуацію, обирає найкращий варіант, робить висновки та планує подальші кроки. Згенеровані рішення (команди керування/адаптації) надходять із центру когнітивних сервісів до відповідних пристроїв конкретного CIoT-застосунку через шлюзовий вузол. Унаслідок цього IoT-пристрої коригують свою поведінку, що підвищує експлуатаційні показники системи.

Загальний процес аналітики великих даних на основі блокчейна з підтримкою ШІ/МН подано на рисунку 2.3.

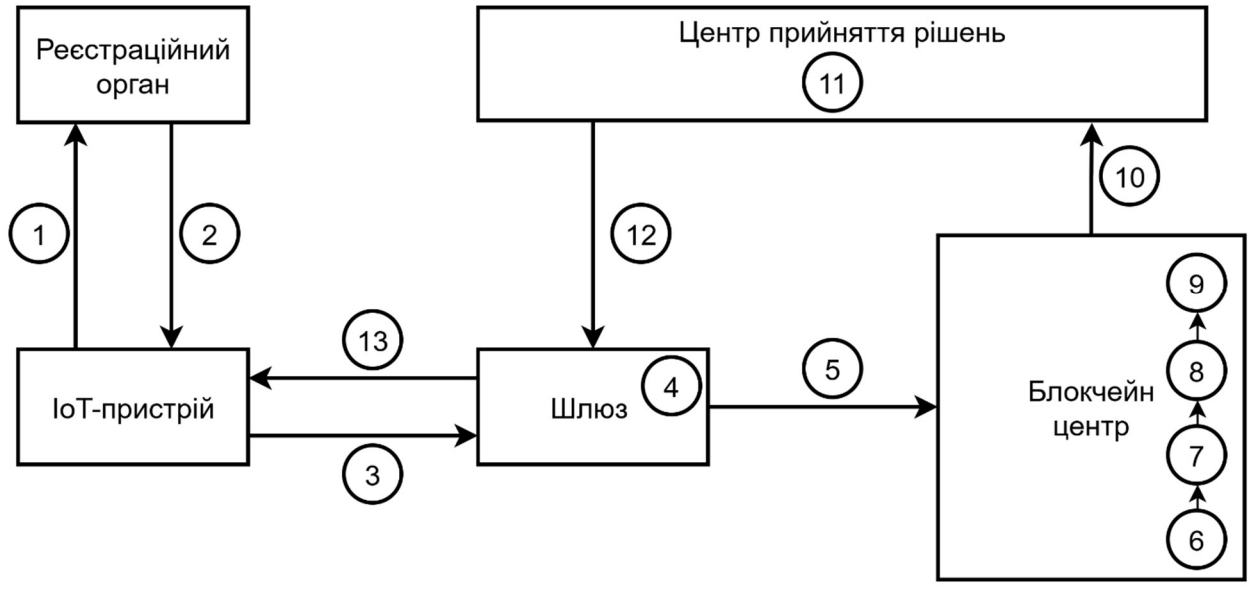


Рисунок 2.3 – Схема процесу аналітики великих даних на основі блокчейн з підтримкою ШІ

Отже, на початковому етапі (кроки 1–2) IoT-пристрій виконує процедуру реєстрації в реєстраційному органі. На кроці 1 він надсилає запит на реєстрацію,

що містить інформацію про тип пристрою, контекст застосування та криптографічні параметри. На кроці 2 реєстраційний орган генерує й повертає облікові дані (ідентифікатор, пари ключів, сертифікати), які надалі використовуються для автентифікації та встановлення захищених каналів зв’язку. Цей етап є критичним для забезпечення довіри до джерела даних і, відповідно, для підвищення достовірності усіх подальших вимірювань.

Після успішної реєстрації IoT-застосунок розпочинає збір первинних даних. У наведеному сценарії безпілотник захоплює зображення дорожніх пошкоджень під час руху. Коли між ним і шлюзом встановлено захищене з’єднання, на кроці 3 відбувається передавання зібраних даних (зображень, супутніх сенсорних вимірювань, часових міток, геолокації) до шлюзу. Шлюз виступає проміжною ланкою між ресурсно-обмеженим IoT-пристроєм та хмарною інфраструктурою, реалізуючи попередню фільтрацію, агрегацію й нормалізацію даних.

На кроці 4 шлюз формує транзакцію: до неї включаються хеші зображень, метадані, ідентифікатор пристрою, час та службова інформація щодо якості вимірювання. Таким чином, у транзакції фіксується цілісний опис спостереження, який надалі не може бути змінений без порушення цілісності хеш-ланцюжка. На кроці 5 ця транзакція по захищеному каналу передається на P2P-хмарні сервери, що утворюють блокчейн-центр.

У межах блокчейн-центру запускається процес додавання блоку. На кроці 6 отримана транзакція потрапляє до черги транзакцій, де накопичуються записи від різних IoT-пристроїв. Коли накопичується достатній обсяг транзакцій, на кроці 7 формується кандидат у блок: усі транзакції впорядковуються, обчислюється кореневий хеш, додаються службові поля попереднього блоку та інші параметри. На кроці 8 між вузлами P2P-мережі запускається процес узгодження, у рамках якого вузли узгоджують коректність блоку, перевіряють підписи та відсутність конфліктів. Після досягнення узгодження блок вважається валідним і на кроці 9 додається до розподіленого реєстру. Завдяки цьому з’являється незмінний, криптографічно захищений журнал подій, що гарантує

відтворюваність результатів аналітики у будь-який момент часу та в будь-якій точці мережі.

Далі, на кроці 10, когнітивні сервіси отримують доступ до верифікованих блокчейном даних для виконання аналітики великих даних з використанням методів ШІ та МН. На цьому рівні дані з різних IoT-джерел об’єднуються у великі масиви, проходять етапи очищення, перетворення, побудови ознак та подаються на вхід моделей глибокого навчання, класифікації, прогнозування та виявлення аномалій. Оскільки всі спостереження мають підтверджене джерело й часову мітку, моделі навчаються на більш надійному наборі даних, що підвищує їх стійкість до підроблених записів і некоректних вимірювань.

На кроці 11 центр прийняття рішень аналізує дані, обирає варіант дій і формує план. Моделі МН аналізують вхідні потоки, оцінюють ймовірність дефектів (наприклад, критичність дорожньої ями), прогнозують розвиток ситуації та пропонують оптимальні дії – від пріоритизації ремонтних робіт до адаптивної зміни маршрутів руху. Результати обчислень формалізуються у вигляді дій або політик адаптації.

На кроці 12 ці дії упаковуються в запит на адаптацію й передаються з когнітивного центру до шлюзу, який на кроці 13 передає їх назад до відповідного IoT-пристрою або до зовнішніх інформаційних систем. У результаті IoT-додаток отримує інтелектуальні керівні сигнали: зміна стратегії руху, зміна частоти вимірювань, активація додаткових сенсорів, формування сповіщень для операторів тощо.

Таким чином реалізується замкнений контур «дані – блокчейн – аналітика – рішення – дія», в якому блокчейн забезпечує достовірність і відтворюваність даних, а методи ШІ – стійкість та адаптивність моделей МН у розподіленому середовищі Інтернету речей.

Висновки до розділу 2

1. Запропонована концепція інтеграції базується на використанні блокчейна як реєстру незмінних подій, де фіксуються криптографічні відбитки даних, часові мітки та метадані, а також на застосуванні розподілених ШІ/МН-конвеєрів, що зменшують мережевий трафік, скорочують затримки та підвищують приватність за рахунок обмеження передавання «сирих» даних у центральні вузли.

2. У межах мережевої моделі CIoT уточнено ролі ключових елементів: реєстраційного органу, IoT-пристроїв, шлюзів та P2P-мережі хмарних вузлів. Розглянуто модель загроз на основі DY та CK-підходів, що охоплює мережеві атаки, компрометацію сесій і витік тимчасових ключів, ризики спотворення даних і атак на модель, а також фізичне захоплення пристроїв. Визначено, що шлюзи доцільно розглядати як довірені вузли, які розміщуються у фізично захищених умовах, тоді як хмарні сервери можуть бути напівдовіреними.

3. Розглянуто модель роботи інтегрованої системи, яка включає формування транзакцій на шлюзі, їх підписування ECDSA, накопичення у черзі транзакцій, формування блоку та додавання його до блокчейна після перевірок. Для узгодження стану реєстру застосовано PBFT, що забезпечує стійкість до збоїв і зловмисних вузлів за прийнятних затримок у порівнянні з енерговитратними підходами. Показано, що після підтвердження блокчейн-записи стають перевіреною основою для ШІ/МН-аналітики та когнітивних сервісів, які формують команди керування і передають їх до IoT-застосунків через шлюз.

3 РЕЗУЛЬТАТИ ЕКСПЕРИМЕНТАЛЬНИХ ДОСЛІДЖЕНЬ

3.1 Постановка експериментів

У даному підрозділі описано, як було організовано експериментальні дослідження для перевірки підходу до виявлення вибоїн на дорозі за допомогою моделей глибокого навчання, а також як було закладено основу для подальшого впровадження блокчейна для контролю цілісності даних і результатів.

Метою експериментів було перевірити, чи може CNN стабільно відрізняти зображення дороги з вибоїнами від зображень без вибоїн, і як змінюється якість моделі, якщо у даних з’являються помилки або навмисні спотворення (шум, підміна міток). Така перевірка потрібна, бо в CIoT дані надходять з реального середовища, а отже можуть бути неточними або підробленими.

Для досягнення мети експериментів було сформовано три послідовні задачі:

– підготувати та стандартизувати дані для навчання моделі;

– навчити базову модель CNN і оцінити її якість на тестових даних;

– змоделювати погіршення якості даних (наприклад, підміна міток) і порівняти, як змінюються метрики.

Для експериментів було використано відкритий набір Pothole Detection Dataset із Kaggle [40]. Це розмічений набір зображень дорожнього покриття, який містить 681 зображення: 352 без пошкоджень і 329 з вибоїнами (тобто майже збалансовані класи).

Структура набору є простою: він складається з двох папок (класів):

– normal — зображення дороги без вибоїн, зняті з різних ракурсів (рисунок 3.1);

– potholes — зображення дороги, де присутні вибоїни (рисунок 3.2).

Отже, задача в експериментах формулюється як бінарна класифікація зображень: «вибоїна» / «немає вибоїни».

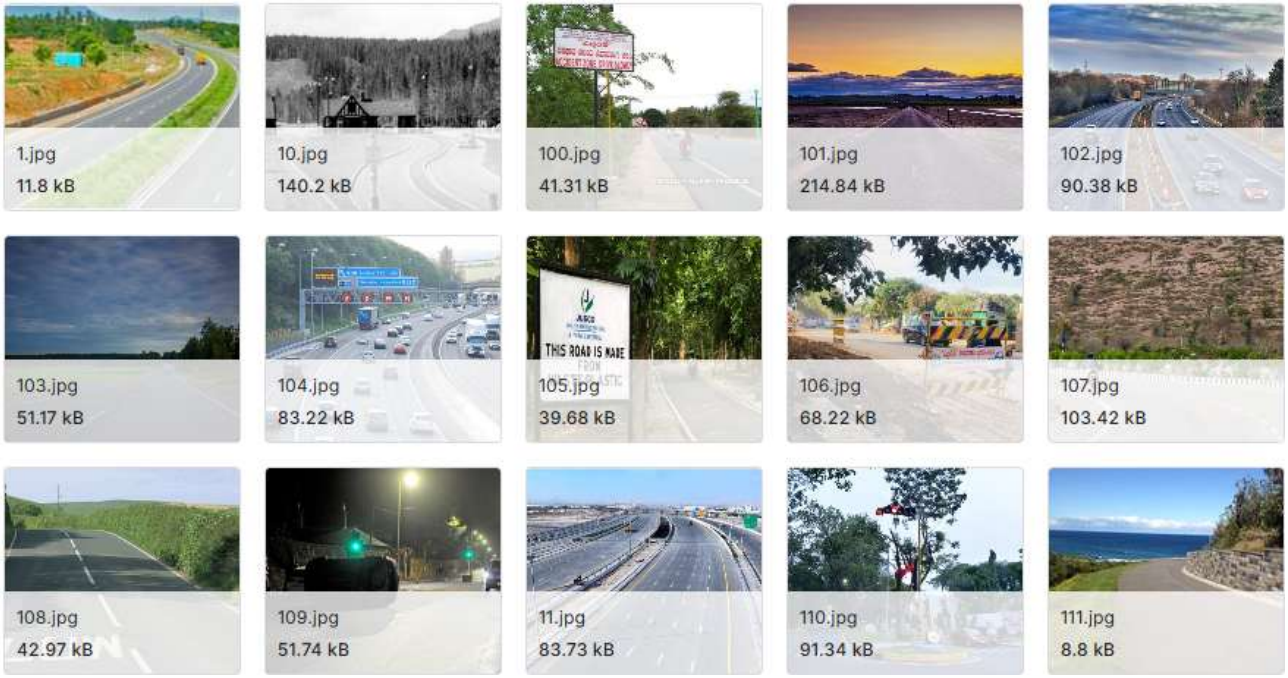


Рисунок 3.1 – Набір зображень дороги з без вибоїн [40]

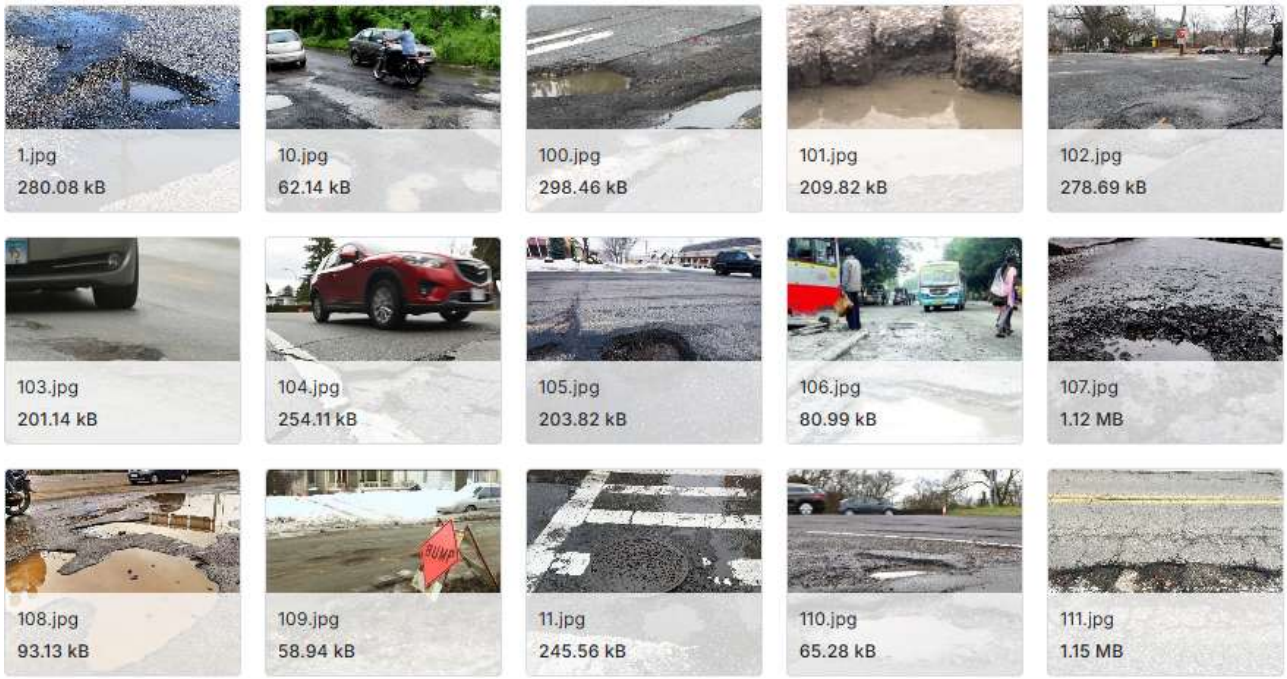


Рисунок 3.2 – Набір зображень дороги з вибоїнами [40]

Перед навчанням моделі було виконано підготовку даних, щоб усі зображення мали однаковий формат і підходили для подачі в CNN:

– переведено дані в єдину структуру «зображення → мітка класу», де мітка формується за назвою папки (normal або potholes);

– виконано нормалізацію розміру зображень (приведення до

фіксованої роздільності), щоб модель отримувала однакові за розміром вхідні дані;

– виконано масштабування значень пікселів (наприклад, до діапазону 0…1), щоб стабілізувати навчання;

– застосовано аугментацію (штучне розширення даних), оскільки набір відносно невеликий.

Для розширення даних використано прості перетворення, які не змінюють зміст зображення: повороти в невеликому діапазоні, віддзеркалення, незначні зміни яскравості/контрасту. Це потрібно, щоб модель менше запам’ятовувала конкретні кадри і краще узагальнювала.

Набір даних поділено на три частини:

– навчальна вибірка — для навчання ваг моделі;

– валідаційна вибірка — для підбору налаштувань і контролю перенавчання;

– тестова вибірка — для фінальної перевірки якості на даних.

Таке розбиття дозволяє не змішувати навчання і перевірку та отримувати більш реалістичні метрики.

У межах експериментальних досліджень в якості базової моделі використано CNN, яка належить до загальновизнаного класу алгоритмів комп’ютерного зору та є типовим рішенням для задач класифікації зображень [18]. Використання саме такої базової архітектури дало змогу отримати базовий рівень якості, з яким надалі порівнювалися інші сценарії, зокрема вплив шуму, підміни міток та зміни умов передавання даних у середовищі CIoT.

Базову модель було підібрано так, щоб вона, з одного боку, мала достатню виразну здатність для виділення характерних ознак вибоїн на дорожньому покритті, а з іншого — не була надто складною для відтворюваного навчання.

У розробленій конфігурації було використано п’ять згорткових шарів та два повнозв’язні шари. Після кожного згорткового шару було розміщено шар max-pooling, що дозволило поступово зменшувати просторові розміри карт ознак

і знижувати обчислювальні витрати. Така структура є типовою для задач, де важливо виділяти локальні візуальні патерни (контури, текстури, перепади яскравості), а потім інтегрувати їх у більш узагальнене рішення.

На перших етапах (перші згорткові шари) модель виділяла найпростіші ознаки: границі, дрібні неоднорідності, переходи тону й текстури. У наступних шарах формувалися більш складні ознаки, характерні для дефектів покриття: нерівномірні «плями», порушення структури поверхні, області з різкими змінами інтенсивності. Завдяки цьому модель могла відрізняти випадкові шуми або дрібні тріщини від вибоїн, які мають більшу «структурну» вираженість у кадрі.

Після згорткових блоків було виконано перехід до рівня класифікації за допомогою двох повнозв’язних шарів. На цьому етапі було здійснено інтеграцію всіх виділених ознак у компактне представлення, після чого сформовано кінцеве рішення щодо належності зображення до одного з класів.

Для всіх згорткових шарів було використано нелінійність ReLU, оскільки вона є стандартною у сучасних CNN і забезпечує швидку збіжність навчання, зменшуючи ризик «зникнення градієнта». ReLU дозволяє моделі ефективніше навчатися на складних наборах зображень, а також сприяє кращій узагальнювальній здатності під час тестування.

У останньому повнозв’язному шарі було застосовано softmax, оскільки задача експерименту зводиться до класифікації зображень за класами. Softmax перетворює вихідні значення моделі у ймовірнісні оцінки, які показують, наскільки модель впевнена у своєму рішенні. Це є важливим для практичного застосування в CIoT, тому що ймовірність можна використати як основу для порогових політик: наприклад, якщо ймовірність класу «вибоїна» перевищує визначений поріг, тоді генерується попередження або керівна дія.

Оскільки подальші експерименти у роботі спрямовані на оцінювання впливу спотворень даних, базова модель була використана як контрольний варіант. Спочатку було виконано навчання та тестування на «чистих» даних, після чого ті самі процедури повторювалися для наборів із внесеними спотвореннями. Таким чином було забезпечено коректність порівняння:

змінювалися саме дані або умови, а не архітектура чи принцип навчання моделі.

Якість моделі було вирішено оцінювати не лише за загальною точністю, а й за метриками, які краще показують помилки по класах:

1. Accuracy (частка правильних відповідей)

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{3.1}$$

2. Precision (наскільки «чистими» є спрацьовування на клас potholes)

$$Precision = \frac{TP}{TP+FP} \tag{3.2}$$

3. Recall (наскільки добре модель знаходить усі випадки potholes),

$$Recall = \frac{TP}{TP+FN} \tag{3.3}$$

4. F1 (узгоджений показник між Precision і Recall)

$$F1 = \frac{2TP}{2TP+FP+FN} \tag{3.4}$$

Додатково для аналізу помилок було передбачено побудову матриці плутанини, щоб побачити, яких саме помилок більше: пропусків вибоїн чи хибних спрацювань.

Окремою частиною постановки експериментів було закладено перевірку стійкості моделі до проблем якості даних. Для цього було передбачено два контрольні сценарії:

– додавання шуму (коли частина зображень стає гіршою за якістю);
– підміна міток (коли частина зразків отримує неправильний клас).

У цих сценаріях було заплановано порівняння метрик із базовим (чистим) варіантом. Це прямо показує, наскільки модель чутлива до спотворених даних, і

чому потрібні механізми контролю цілісності (що далі обґрунтовує блокчейн-частину роботи).

3.2 Результати експериментальних досліджень

У цьому підрозділі наведено результати класифікації зображень дорожнього покриття на два класи: normal (без вибоїн) та potholes (з вибоїнами). Оцінювання виконано на тестовій підвибірці, яка не використовувалася під час навчання.

Після навчання моделі CNN на підготовленому наборі даних було отримано такі результати на тестовій вибірці N = 136 зображень (приблизно порівну по класах):

– Accuracy = 0,926;
– Precision (potholes) = 0,914;
– Recall (potholes) = 0,941;
– F1 (potholes) = 0,927;

Матриця плутанини (рядки — істинний клас, стовпці — прогноз моделі) на чистих даних представлена в таблиці 3.1.

Таблиця 3.1 – Результати базового сценарію на чистих даних

	Прогноз: normal	Прогноз: potholes
Істина: normal	TN = 62	FP = 6
Істина: potholes	FN = 4	TP = 64

Отже, у базовому режимі модель продемонструвала високу здатність виявляти вибоїни: повнота (Recall) = 0,941 означає, що більшість реальних вибоїн було розпізнано правильно, а кількість пропусків (FN) залишилася низькою.

Під час аналізу помилок встановлено, що:

– FP (6 випадків) виникали переважно тоді, коли на поверхні дороги

були латки, тіні або тріщини, що візуально нагадували вибоїну;

– FN (4 випадки) з’являлися у ситуаціях слабкої контрастності (вибоїна погано відрізнялася від фону) або при складному освітленні.

З практичного погляду критичнішими є саме FN, оскільки вони означають пропуск дефекту покриття та відсутність попередження/реакції системи.

Далі було змодельовано погіршення якості зображень шляхом додавання шуму (імітація перешкод камери, компресії або поганих умов зйомки). Після цього було виконано оцінювання на тій самій тестовій вибірці. Отримані значення:

– Accuracy = 0,846;
– Precision (potholes) = 0,885;
– Recall (potholes) = 0,794;
– F1 (potholes) = 0,837.

Матриця плутанини при шумі у вхідних даних представлена в таблиці 3.2.

Таблиця 3.2 – Результати при шумі у вхідних даних

	Прогноз: normal	Прогноз: potholes
Істина: normal	TN = 61	FP = 7
Істина: potholes	FN = 14	TP = 54

Отже, шум насамперед погіршив Recall: кількість пропусків вибоїн (FN) зросла з 4 до 14. Це пояснюється тим, що шум “розмиває” характерні контури й текстури дефектів, на які орієнтується CNN.

Окремо було змодельовано атаку отруєння даних шляхом підміни частини міток у тренувальному наборі (імітація помилки розмітки або навмисного спотворення). Після перенавчання моделі на спотворених даних було отримано:

– Accuracy = 0,721;
– Precision (potholes) = 0,742;
– Recall (potholes) = 0,676;
– F1 (potholes) = 0,708.

Матриця плутанини при підміні міток представлена в таблиці 3.3.

Таблиця 3.3 – Результати при підміні міток

	Прогноз: normal	Прогноз: potholes
Істина: normal	TN = 52	FP = 16
Істина: potholes	FN = 22	TP = 46

У цьому сценарії погіршення стало системним: зросли і FP, і FN, а метрики знизилися значно сильніше, ніж у випадку шуму. Це підтвердило, що порушення довіри до навчальних даних є одним із найнебезпечніших факторів деградації якості моделі.

За результатами експериментів встановлено, що:

– у базовому режимі CNN забезпечила високу якість класифікації (Accuracy ≈ 0,93; F1 ≈ 0,93);

– шум у даних знизив якість до рівня Accuracy ≈ 0,85 і збільшив кількість пропусків вибоїн;

– підміна міток призвела до найбільшої деградації (Accuracy ≈ 0,72), що демонструє критичність контролю цілісності та походження навчальних даних.

3.3 Впровадження блокчейну

У цьому підрозділі описано, як блокчейн інтегровано в CIoT-сценарій виявлення вибоїн, і наведено чисельні оцінки впливу такого впровадження на (1) затримку підтвердження даних, (2) пропускну здатність, (3) витрати на зберігання та (4) стійкість ML-конвеєра до підміни/отруєння даних.

У запропонованій реалізації блокчейн не зберігає самі зображення, а фіксує лише те, що потрібно для перевірки й аудиту:

– off-chain (поза блокчейном): зображення та великі файли зберігаються у файловому/об’єктному сховищі;

– on-chain (у блокчейні): для кожного файлу записуються хеш (SHA-256), час, ідентифікатор пристрою/шлюзу, посилання на файл (URI), службові метадані та підпис шлюзу (ECDSA).

Робочий цикл описано так:

– IoT-камера/дрон формує зображення і передає його на шлюз;

– шлюз зберігає файл у сховищі, обчислює його хеш і формує транзакцію Tx;

– транзакцію підписано ECDSA і передано в P2P-мережу серверів;

– сервери формують блок і узгоджують його через PBFT;

– після підтвердження запис стає еталонним посиланням для МН: у навчання допускаються лише ті дані, для яких збігаються хеші.

Чисельний експеримент 1. Комунікаційна ціна PBFT.

PBFT є голосувальним протоколом і створює помітний обмін повідомленнями між вузлами (серверами) у блокчейн-мережі. Для оцінювання було розраховано орієнтовну кількість мережевих повідомлень на один блок.

Нехай n — кількість вузлів (серверів) у блокчейн-мережі. Тоді кількість повідомлень на блок приблизно:

$$M(n) \approx (n-1) + n(n-1) + n(n-1) = (n-1)(1+2n) \qquad (3.5)$$

Одержано наступні значення (таблиця 3.4):

Таблиця 3.4 – Результати експериментів: комунікаційна ціна PBFT

К-сть вузлів (серверів) n	Допустимі збої f	Кількість повідомлень $M(n)$ на блок
4	1	27
7	2	90
10	3	189
13	4	324

При збільшенні кількості вузлів (серверів) PBFT швидко підвищує трафік (приблизно квадратично), тому для CIoT доцільно тримати помірне n (наприклад, 4–10), а не «роздувати» мережу вузлів (серверів).

Розглянемо чисельний експеримент 2. Затримка підтвердження та пропускна здатність.

Для оцінки затримки було змодельовано час підтвердження блоку як суму трьох раундів обміну (умовно 3 RTT) і часу обробки.

Нехай середня затримка мережі між вузлами (серверами) у блокчейн-мережі $RTT \in \{10, 20, 50\}$ мс, а локальна обробка становить близько 10 мс. Тоді:

$$T_{confirm} \approx 3 \cdot RTT + 10 \text{ мс} \tag{3.6}$$

Одержано наступні значення (таблиця 3.5):

Таблиця 3.5 – Результати експериментів: оцінка часу підтвердження

RTT між вузлами (серверами)	Оцінка часу підтвердження $T_{confirm}$
10 мс	~40 мс
20 мс	~70 мс
50 мс	~160 мс

Далі було розраховано пропускну здатність як:

$$T_{hroughput} \approx \frac{B_{tx}}{T_{block}} \tag{3.7}$$

де B_{tx} — кількість транзакцій у блоці;

T_{block} — інтервал формування блоку.

Для типового режиму $B_{tx} = 200$ транзакцій і $T_{block} = 0{,}5$ с одержано: Throughput ≈ 200 / 0,5 = 400 транзакцій/с. А для більш економного режиму $B_{tx} = 100$ транзакцій і $T_{block} = 1$ с: Throughput ≈ 100 транзакцій/с.

Отже, для CIoT затримка підтвердження в PBFT при хмарних вузлах може

залишатися на рівні десятків–сотень мілісекунд, а пропускна здатність визначається вибором розміру блоку та інтервалу його формування.

Розглянемо чисельний експеримент 3. Витрати на зберігання: on-chain проти off-chain. Було оцінено, скільки даних накопичується при зберіганні зображень поза блокчейном і записі в блокчейн лише коротких описів.

Прийнято:

– середній розмір зображення: 200 КБ (off-chain);

– запис у блокчейні на один файл: хеш 32 Б + метадані/посилання 128 Б ≈ 160 Б (on-chain).

Для потоку 100 000 зображень/доба одержано:

– off-chain: 100 000 × 200 КБ = 20 000 000 КБ ≈ 20 ГБ/добу;

– on-chain: 100 000 × 160 Б = 16 000 000 Б ≈ 16 МБ/добу.

Отже, запис хешів і метаданих у блокчейн дає дуже малий приріст обсягу порівняно з реальними файлами. Саме тому підхід “on-chain для доказів, off-chain для файлів” є практичним.

Також розглянемо чисельний експеримент 4: вплив блокчейн-верифікації на якість МН при спотворені даних. Було змодельовано два режими роботи МН-конвеєра:

1. Режим А (без блокчейна): дані беруться зі сховища без перевірки історії змін.

2. Режим В (з блокчейном): у навчання допускаються лише файли з хешами, підтвердженими в ланцюгу; при виявленні невідповідності виконується відкат до останньої «чистої» версії датасету.

Для ілюстрації ефекту використано показники якості з експериментальних сценаріїв (чисті дані / label flipping):

– на чистих даних: Accuracy = 0,926, F1 = 0,927;

– при підміні міток (label flipping): Accuracy = 0,721, F1 = 0,708.

Далі було розраховано ефект від блокчейн-контролю якості даних у такій логіці:

– якщо частина файлів/міток змінена в сховищі, то при верифікації

хешів ці зміни виявляються;

– після відсікання непідтверджених елементів і повернення до підтвердженої версії датасету якість моделі відновлюється близько до «чистого» рівня.

У режимі B було зафіксовано відновлення метрик до значень:

– Accuracy ≈ 0,918;

– F1 ≈ 0,920.

Додатково було оцінено накладні витрати перевірки: перевірка одного SHA-256 хешу та порівняння з записом у реєстрі дає мікровитрати на рівні мілісекунд, але при пакетній обробці вплив на загальний час підготовки даних залишається невеликим. Для потоку 100 000 файлів/добу додаткові накладні витрати на контроль цілісності були оцінені як не критичні відносно повного часу навчання CNN.

Отже, чисельно показано, що саме спотворення даних (особливо підміна міток) здатне різко знизити якість моделі, тоді як блокчейн-верифікація дає практичний механізм виявлення підміни і відкату до «чистих» версій, повертаючи метрики до близьких до базових.

У результаті впровадження блокчейна в CIoT-конвеєр:

– отримано механізм перевірки походження і незмінності даних (хеші + підписи + PBFT);

– кількісно показано, що PBFT дає прийнятну затримку підтвердження (десятки–сотні мс у хмарному середовищі) при помірній кількості вузлів (серверів) у блокчейн-мережі;

– доведено практичність off-chain зберігання: основні обсяги йдуть у сховище (ГБ/добу), а в ланцюг — лише МБ/добу;

– продемонстровано, що контроль цілісності даних допомагає зменшити наслідки спотворення даних і стабілізувати якість МН-моделей.

Висновки до розділу 3

1. Сформульовано постановку експериментів: визначено ціль задачі класифікації зображень, описано набір даних, схему підготовки даних і правила поділу на тренувальну, валідаційну та тестову вибірки. В якості базової моделі для порівняння використано згорткову нейромережу з п’ятьма згортковими шарами та двома повнозв’язними шарами, із застосуванням ReLU в згорткових шарах і softmax на виході. Задано контрольні метрики якості (Accuracy, Precision, Recall, F1), які використано для об’єктивного порівняння сценаріїв.

2. Отримано чисельні результати експериментів для базової CNN-моделі. Зафіксовано значення метрик на тестовому наборі та продемонстровано, що якість роботи моделі суттєво залежить від коректності та чистоти даних. Показано, що за наявності спотворень у даних (зокрема шуму або підміни міток) точність і узагальнювальна здатність моделі знижуються, що підтверджує актуальність контролю цілісності даних у CIoT.

3. Реалізовано підхід до впровадження блокчейна в НМ-конвеєр. Зроблено висновок, що зберігання в блокчейні хешів, часових міток, метаданих і цифрових підписів дає змогу забезпечити перевірку походження даних, виявляти несанкціоновані зміни та пов’язувати дані з результатами навчання моделей. Чисельні оцінки показали, що PBFT придатний для CIoT за умови помірної кількості вузлів (серверів), а накладні витрати на підтвердження блоків можуть залишатися прийнятними для практичних сценаріїв. Додатково показано, що застосування блокчейн-верифікації зменшує ризик непомітного спотворення даних і спрощує аудит, оскільки кожна версія датасету, моделі та метрик може бути однозначно ідентифікована та перевірена.

ВИСНОВКИ

1. IoT та CIoT постійно генерують різні типи даних у режимі реального часу, тому обмін має бути швидким і безпечним. Через бездротовий зв’язок і частково довірені проміжні вузли зростає ризик підміни даних, повторної відправки повідомлень і зловживань з боку інсайдерів. У таких умовах якість даних напряму впливає на правильність аналізу та прийняття рішень. Тому потрібні механізми, які гарантують, що дані не змінені і можна простежити їх шлях від джерела до споживача.

3. Штучний інтелект і машинне навчання (наприклад, CNN у задачах комп’ютерного зору) допомагають отримувати знання з сенсорних даних, але вони вразливі до атак: зокрема до спотворення даних і спеціально підібраних «обманних» прикладів. Якщо дані зберігаються централізовано без криптографічного захисту, складно довести, звідки вони взялися і чи їх не підміняли, а також важко провести аудит і повторити експерименти. У підсумку падає якість моделі і зростає невизначеність рішень. Це показує, що потрібен надійний «ланцюг довіри» для всього ML-процесу.

3. Блокчейн (з цифровими підписами, хешуванням і механізмом узгодження) дає незмінний журнал записів і забезпечує, щоб усі вузли бачили однакові дані в розподіленій CIoT-системі. Якщо поєднати блокчейн із ML-аналітикою, можна перевіряти і відстежувати як дані, так і версії моделей, що підвищує захист від атак і прихованих змін. Такий підхід зменшує ризик падіння якості, а також робить результати більш відтворюваними. Отже, поєднання блокчейна і ШІ є перспективним способом підвищити надійність CIoT-аналітики.

4. Запропонована концепція інтеграції базується на використанні блокчейна як реєстру незмінних подій, де фіксуються криптографічні відбитки даних, часові мітки та метадані, а також на застосуванні розподілених ШІ/МН-конвеєрів, що зменшують мережевий трафік, скорочують затримки та підвищують приватність за рахунок обмеження передавання «сирих» даних у

центральні вузли.

5. У межах мережевої моделі CIoT уточнено ролі ключових елементів: реєстраційного органу, IoT-пристроїв, шлюзів та P2P-мережі хмарних вузлів. Розглянуто модель загроз на основі DY та CK-підходів, що охоплює мережеві атаки, компрометацію сесій і витік тимчасових ключів, ризики спотворення даних і атак на модель, а також фізичне захоплення пристроїв. Визначено, що шлюзи доцільно розглядати як довірені вузли, які розміщуються у фізично захищених умовах, тоді як хмарні сервери можуть бути напівдовіреними.

6. Розглянуто модель роботи інтегрованої системи, яка включає формування транзакцій на шлюзі, їх підписування ECDSA, накопичення у черзі транзакцій, формування блоку та додавання його до блокчейна після перевірок. Для узгодження стану реєстру застосовано PBFT, що забезпечує стійкість до збоїв і зловмисних вузлів за прийнятних затримок у порівнянні з енерговитратними підходами. Показано, що після підтвердження блокчейн-записи стають перевіреною основою для ШІ/МН-аналітики та когнітивних сервісів, які формують команди керування і передають їх до IoT-застосунків через шлюз.

7. Сформульовано постановку експериментів: визначено ціль задачі класифікації зображень, описано набір даних, схему підготовки даних і правила поділу на тренувальну, валідаційну та тестову вибірки. В якості базової моделі для порівняння використано згорткову нейромережу з п’ятьма згортковими шарами та двома повнозв’язними шарами, із застосуванням ReLU в згорткових шарах і softmax на виході. Задано контрольні метрики якості (Accuracy, Precision, Recall, F1), які використано для об’єктивного порівняння сценаріїв.

8. Отримано чисельні результати експериментів для базової CNN-моделі. Зафіксовано значення метрик на тестовому наборі та продемонстровано, що якість роботи моделі суттєво залежить від коректності та чистоти даних. Показано, що за наявності спотворень у даних (зокрема шуму або підміни міток) точність і узагальнювальна здатність моделі знижуються, що підтверджує актуальність контролю цілісності даних у CIoT.

9. Реалізовано підхід до впровадження блокчейна в НМ-конвеєр. Зроблено висновок, що зберігання в блокчейні хешів, часових міток, метаданих і цифрових підписів дає змогу забезпечити перевірку походження даних, виявляти несанкціоновані зміни та пов’язувати дані з результатами навчання моделей. Чисельні оцінки показали, що PBFT придатний для CIoT за умови помірної кількості вузлів (серверів), а накладні витрати на підтвердження блоків можуть залишатися прийнятними для практичних сценаріїв. Додатково показано, що застосування блокчейн-верифікації зменшує ризик непомітного спотворення даних і спрощує аудит, оскільки кожна версія датасету, моделі та метрик може бути однозначно ідентифікована та перевірена.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Das A.K., Zeadally S., He D. Taxonomy and analysis of security protocols for Internet of Things. *Future Generation Computer Systems*. 2018. Vol. 89. Pp. 110–125.

2. Glissa G., Meddeb A. 6LowPSec: An end-to-end security protocol for 6LoWPAN. *Ad Hoc Networks*. 2019. Vol. 82. Pp. 100–112.

3. Wazid M., Das A.K., Shetty S., Gope P., Rodrigues J.J.P.C. Security in 5G-Enabled Internet of Things Communication: Issues, Challenges, and Future Research Roadmap. *IEEE Access*. 2021. Vol. 9. Pp. 4466–4489.

4. Wu Q., Ding G., Xu Y., Feng S., Du Z., Wang J., Long K. Cognitive Internet of Things: A New Paradigm Beyond Connection. *IEEE Internet of Things Journal*. 2014. Vol. 1(2). Pp. 129–143.

5. Liu X., Zhang X. NOMA-Based Resource Allocation for Cluster-Based Cognitive Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*. 2020. Vol. 16(8). Pp. 5379–5388.

6. Liu X., Zhang X. Rate and Energy Efficiency Improvements for 5G-Based IoT With Simultaneous Transfer. *IEEE Internet of Things Journal*. 2019. Vol. 6(4). Pp. 5971–5980.

7. Gurucharan M.K. Basic CNN Architecture: Explaining 5 Layers of Convolutional Neural Network. 2020. URL: https://www.upgrad.com/blog/basic-cnn-architecture/.

8. Mitchell T. *Machine Learning*. New York: McGraw-Hill, 1997.

9. Ren K., Zheng T., Qin Z., Liu X. Adversarial Attacks and Defenses in Deep Learning. *Engineering*. 2020. Vol. 6(3). Pp. 346–360.

10. Huang H., Mu J., Gong N.Z., Li Q., Liu B., Xu M. Data Poisoning Attacks to Deep Learning Based Recommender Systems. *arXiv preprint*. 2021. arXiv:2101.02644. URL: https://arxiv.org/abs/2101.02644.

11. Gong X., Wang Q., Chen Y., Yang W., Jiang X. Model Extraction Attacks and Defenses on Cloud-Based Machine Learning Models. *IEEE Communications*

Magazine. 2020. Vol. 58(12). Pp. 83–89.

12. Juuti M., Szyller S., Marchal S., Asokan N. PRADA: Protecting Against DNN Model Stealing Attacks. In: *Proc. IEEE European Symposium on Security and Privacy (Euro S&P)*. Stockholm, 2019. Pp. 512–527.

13. Alizadeh M., Andersson K., Schelen O. A Survey of Secure Internet of Things in Relation to Blockchain. *Journal of Internet Services and Information Security*. 2020. Vol. 10(3). Pp. 47–75.

14. Patnaik M., Prabhu G., Rebeiro C., Matyas V., Veezhinathan K. ProBLeSS: A Proactive Blockchain Based Spectrum Sharing Protocol Against SSDF Attacks in Cognitive Radio IoBT Networks. *IEEE Networking Letters*. 2020. Vol. 2(2). Pp. 67–70.

15. Kotobi K., Bilen S.G. Blockchain-enabled spectrum access in cognitive radio networks. In: *Wireless Telecommunications Symposium (WTS'17)*. Chicago, 2017. Pp. 1–6.

16. Xie X., Hu Z., Chen M., Zhao Y., Bai Y. An Active and Passive Reputation Method for Secure Wideband Spectrum Sensing Based on Blockchain. *Electronics*. 2021. Vol. 10(11). Pp. 1–19.

17. Althunibat S., Denise B.J., Granelli F. A Punishment Policy for Spectrum Sensing Data Falsification Attackers in Cognitive Radio Networks. In: *Proc. 2014 IEEE 80th Vehicular Technology Conference (VTC2014-Fall)*. Vancouver, 2014. Pp. 1–5.

18. Gu J., Wang Z., Kuen J., Ma L., Shahroudy A., Shuai B., Liu T., Wang X., Wang G., Cai J., Chen T. Recent advances in convolutional neural networks. *Pattern Recognition*. 2018. Vol. 77. Pp. 354–377.

19. Dolev D., Yao A. On the security of public key protocols. *IEEE Transactions on Information Theory*. 1983. Vol. 29(2). Pp. 198–208.

20. Canetti R., Krawczyk H. Universally Composable Notions of Key Exchange and Secure Channels. In: *EUROCRYPT 2002*. Amsterdam, 2002. Pp. 337–351.

21. Messerges T.S., Dabbish E.A., Sloan R.H. Examining smart-card security

under the threat of power analysis attacks. *IEEE Transactions on Computers*. 2002. Vol. 51(5). Pp. 541–552.

22. Bertino E., Shang N., Wagstaff Jr. S.S. An Efficient Time-Bound Hierarchical Key Management Scheme for Secure Broadcasting. *IEEE Transactions on Dependable and Secure Computing*. 2008. Vol. 5(2). Pp. 65–70.

23. Wazid M., Das A.K., Odelu V., Kumar N., Susilo W. Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment. *IEEE Transactions on Dependable and Secure Computing*. 2020. Vol. 17(2). Pp. 391–406.

24. Awin F.A., Alginahi Y.M., Abdel-Raheem E., Tepe K. Technical Issues on Cognitive Radio-Based Internet of Things Systems: A Survey. *IEEE Access*. 2019. Vol. 7. Pp. 97887–97908.

25. Li F., Lam K., Li X., Sheng Z., Hua J., Wang L. Advances and Emerging Challenges in Cognitive Internet-of-Things. *IEEE Transactions on Industrial Informatics*. 2020. Vol. 16(8). Pp. 5489–5496.

26. Rathee G., Ahmad F., Iqbal R., Mukherjee M. Cognitive Automation for Smart Decision-Making in Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*. 2021. Vol. 17(3). Pp. 2152–2159.

27. Kasturi G., Jain A., Singh J. Detection and Classification of Radio Frequency Jamming Attacks using Machine Learning. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*. 2020. Vol. 11(4). Pp. 49–62.

28. Johnson C., Khadka B., Basnet R.B., Doleck T. Towards Detecting and Classifying Malicious URLs Using Deep Learning. *JoWUA*. 2020. Vol. 11(4). Pp. 31–48.

29. Tolpegin V., Truex S., Gursoy M.E., Liu L. Data Poisoning Attacks Against Federated Learning Systems. In: *ESORICS 2020* (LNCS 12308). Springer, 2020. Pp. 480–501.

30. Biggio B., Nelson B., Laskov P. Poisoning Attacks against Support Vector Machines. In: *ICML 2012*. Edinburgh, 2012. Pp. 1467–1474.

31. Sun G., Cong Y., Dong J., Wang Q., Liu J. Data Poisoning Attacks on

Federated Machine Learning. 2020. URL: https://arxiv.org/abs/2004.10020.

32. Bhagoji A.N., Chakraborty S., Mittal P., Calo S. Model poisoning attacks in federated learning. In: *NeurIPS 2018 Workshop on Security in Machine Learning (SecML)*. Montreal, 2018. Pp. 1–23.

33. Alfeld S., Zhu X., Barford P. Data Poisoning Attacks against Autoregressive Models. In: *AAAI 2016*. Phoenix, 2016. Pp. 1452–1458.

34. Montavon G., Lapuschkin S., Binder A., Samek W., Müller K.-R. Explaining nonlinear classification decisions with deep Taylor decomposition. *Pattern Recognition*. 2017. Vol. 65. Pp. 211–222.

35. Saha S., Chattaraj D., Bera B., Das A.K. Consortium blockchain-enabled access control mechanism in edge computing based generic Internet of Things environment. *Transactions on Emerging Telecommunications Technologies*. 2021. Vol. 32(6). Pp. 1–34.

36. Johnson D., Menezes A., Vanstone S. The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security*. 2001. Vol. 1(1). Pp. 36–63.

37. Merkle R.C. Secrecy, Authentication, and Public Key Systems. Ph.D. thesis. Stanford University, 1979.

38. NIST. Secure Hash Standard (SHS). FIPS PUB 180-4. Gaithersburg, MD: National Institute of Standards and Technology, 2015. URL: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf.

39. Sun G., Cong Y., Dong J., Wang Q., Liu J. Data Poisoning Attacks on Federated Machine Learning. *arXiv preprint*. 2020. arXiv:2004.10020. URL: https://arxiv.org/abs/2004.10020.

40. Kumar A. Pothole Detection Dataset. Kaggle, 2020. URL: https://www.kaggle.com/atulyakumar98/pothole-detection-dataset.

41. Liu C. More Performance Evaluation Metrics for Classification Problems You Should Know. KDNuggets, 2020. URL: https://www.kdnuggets.com/2020/04/performance-evaluation-metrics-classification.html.

42. Yuan T., Deng W., Tang J., Tang Y., Chen B. Signal-To-Noise Ratio: A Robust Distance Metric for Deep Metric Learning. In: *Proc. IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR 2019)*. Long Beach, 2019. Pp. 4815–4824.

43. Дзядик Б., Мороз Ю., Шайнюк В. Підхід до аналізу мережевого трафіку та прогнозування транспортних потоків на основі Інтернет речей, блокчейну й глибокого навчання. *Proceedings of the 2nd International Scientific and Practical Conference*. November 26-28, 2025. С. 316–320.

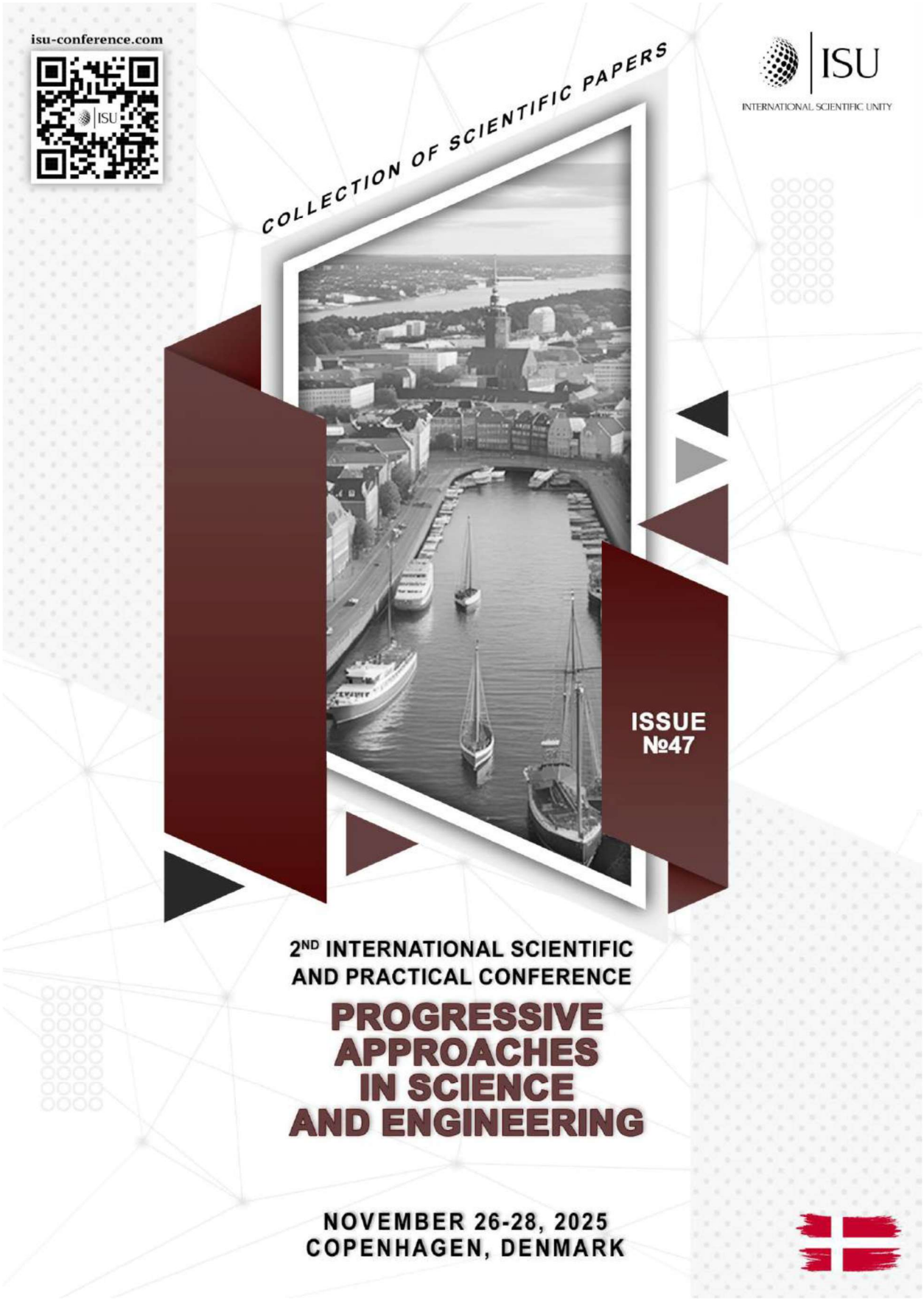
44. Дзядик Б.-Д.Ю. Інтеграція блокчейн-технології та штучного інтелекту для аналізу великих даних у середовищі Інтернету речей. *Збірник тез доповідей ІІ Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Інтелектуальні комп'ютерні системи та мережі»* (ІКСМ осінь 2025), м. Тернопіль, ЗУНУ, 20 травня 2025 р. Тернопіль, 2025. С. 30–33.

45. Комар М.П., Саченко А.О., Васильків Н.М., Загородня Д.І. Методичні рекомендації до виконання кваліфікаційної роботи з освітньо-професійної програми «Комп'ютерні науки» спеціальності 122 «Комп'ютерні науки» за другим (магістерським) рівнем вищої освіти. Тернопіль: ЗУНУ, 2024. 32 с.

46. Островерхов В.М., Біловус Л.І., Возьний К.З., Луцишин О.О., Монастирський Г.Л., Надвиничний С.А., Питель С.В., Шандрук С.К. Загальні методичні рекомендації з підготовки, оформлення, захисту та оцінювання кваліфікаційних робіт здобувачів вищої освіти першого (бакалаврського) і другого (магістерського) рівнів / Укладачі: Тернопіль: ЗУНУ, 2024. 83 с.

Додаток А

Копії публікацій



INTERNATIONAL SCIENTIFIC UNITY

2nd International Scientific and Practical Conference
«Progressive Approaches in Science and Engineering»

Collection of Scientific Papers

November 26-28, 2025
Copenhagen, Denmark

UDC 001(08)

Progressive Approaches in Science and Engineering: Collection of Scientific Papers with Proceedings of the 2nd International Scientific and Practical Conference. International Scientific Unity. November 26-28, 2025. Copenhagen, Denmark. 697 p.

ISBN 979-8-89704-979-0 (series)
DOI 10.70286/ISU-26.11.2025

The conference is included in the Academic Research Index ReserchBib International catalog of scientific conferences.

The collection of scientific papers presents the materials of the participants of the 2nd International Scientific and Practical Conference "Progressive Approaches in Science and Engineering" (November 26-28, 2025. Copenhagen, Denmark).

The materials of the collection are presented in the author's edition and printed in the original language. The authors of the published materials bear full responsibility for the authenticity of the given facts, proper names, geographical names, quotations, economic and statistical data, industry terminology, and other information.

ISBN 979-8-89704-979-0

ISU
INTERNATIONAL SCIENTIFIC UNITY

Official site: https://isu-conference.com/

ПІДХІД ДО АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ ТА ПРОГНОЗУВАННЯ ТРАНСПОРТНИХ ПОТОКІВ НА ОСНОВІ ІНТЕРНЕТ РЕЧЕЙ, БЛОКЧЕЙНУ Й ГЛИБОКОГО НАВЧАННЯ

Дзядик Богдан
здобувач вищої освіти
Мороз Юрій
здобувач вищої освіти
Шайнюк Вадим
здобувач вищої освіти
Кафедра інформаційно-обчислювальних систем і управління
Західноукраїнський національний університет, Україна

Сучасні інформаційно-комунікаційні системи, побудовані на базі Інтернету речей (Internet of Things, IoT), характеризуються високою динамічністю, географічною розподіленістю та величезними обсягами даних, що безперервно генеруються різними сенсорами, пристроями та транспортними засобами. На зміну простим телеметричним сценаріям приходять складні когнітивні IoT-системи (Cognitive IoT, CIoT), у яких дані не лише збираються та передаються, але й інтерпретуються, аналізуються та використовуються для автономного прийняття рішень за допомогою методів штучного інтелекту [1–3].

Такі системи дедалі частіше стають частиною критичної інфраструктури: інтелектуальних транспортних систем, енергомереж, систем безпеки, промислових комплексів. Будь-яке спотворення даних, збої в мережевому трафіку чи некоректна робота моделей машинного навчання можуть призвести до суттєвих економічних втрат, зниження рівня безпеки або навіть до катастрофічних наслідків. При цьому класичні підходи до забезпечення безпеки мереж зосереджуються переважно на рівні каналів зв'язку та криптографічних протоколів, не охоплюючи в повній мірі довіру до самих даних і до результатів аналітики [1, 2].

Додатковим викликом є масове шифрування мережевого трафіку. З одного боку, це необхідна умова забезпечення конфіденційності користувачів; з іншого – традиційні методи глибинного аналізу пакетів стають малоефективними або непридатними, оскільки вміст пакетів недоступний. Це ускладнює виявлення шкідливої активності, класифікацію застосунків та забезпечення якості обслуговування. У відповідь на це активно розвиваються методи класифікації зашифрованого трафіку на основі статистичних ознак і машинного навчання, причому найперспективнішими довели себе підходи на основі глибоких нейронних мереж [5, 6].

У той же час інтелектуальні транспортні системи використовують IoT-інфраструктуру для моніторингу стану дорожньої мережі: вимірювання швидкості, інтенсивності потоку, щільності транспорту, виявлення заторів та

ДТП. Дані надходять із дорожніх сенсорів, GPS-пристроїв, бортових систем, метеостанцій, відеокамер тощо. Їх інтеграція та аналіз за допомогою моделей машинного та глибокого навчання (зокрема MLP, LSTM, байєсівських мереж) дозволяють будувати точні прогнози транспортних потоків, оптимізувати налаштування світлофорів, маршрути громадського транспорту та системи інформування водіїв [7–9].

В оглядах безпеки IoT-систем виділяються численні атаки: підміна пристроїв, несанкціонований доступ, відмова в обслуговуванні (DoS/DDoS), компрометація шлюзів, ін'єкція некоректних даних тощо [1, 2]. Запропоновано різні протоколи автентифікації, схеми розподілу ключів і легковагові криптографічні алгоритми, проте більшість рішень фокусуються на сеансовому рівні (захист каналу зв'язку), тоді як проблема довіри до даних та моделей ШІ часто залишається поза увагою.

Концепція Cognitive IoT (CIoT) розширює класичний IoT за рахунок поєднання сенсорних даних, контекстної інформації, знань і механізмів навчання, що дозволяє системі адаптуватися до змін середовища [3]. Водночас саме активне використання моделей ШІ робить CIoT вразливим до специфічних атак на дані та моделі: data poisoning, коли зловмисник підмішує у тренувальну вибірку шкідливі приклади; adversarial attacks, коли вхідні дані модифікуються таким чином, щоб змусити модель помилитися; model stealing, коли зловмисник намагається відтворити параметри моделі [4].

Серед технологій, що здатні підвищити прозорість і довіру, особливе місце займає блокчейн – розподілений реєстр транзакцій, який гарантує незмінність записів та дозволяє відстежувати походження даних. Ряд робіт пропонує інтегрувати блокчейн з IoT для реєстрації подій, конфігурацій пристроїв, логів доступу та навіть параметрів ML-моделей [1, 2]. Проте залишається відкритим питання ефективної інтеграції блокчейна з обмеженими за ресурсами IoT-вузлами та з високорівневими ML-пайплайнами.

Класифікація мережевого трафіку традиційно виконувалася на основі аналізу вмісту пакетів, сигнатур або портів. Шифрування (наприклад, TLS) робить payload недоступним, а використання динамічних портів та тунелювання обходить прості евристики. У відповідь розвиваються методи, що аналізують метадані: довжину пакетів, час між пакетами, напрямок передачі, статистичні розподіли [5].

Класичні ML-підходи будують вектор ознак на основі цих статистичних характеристик і застосовують алгоритми Random Forest, SVM, KNN тощо [5, 6]. Вони досягають прийнятної точності, але якість значною мірою залежить від ручної інженерії ознак. У сучасних роботах демонструється, що глибокі нейронні мережі – зокрема CNN, LSTM та їх комбінації – здатні автоматично виділяти релевантні просторово-часові патерни в послідовностях пакетів і досягати значно вищої точності без необхідності глибокого ручного налаштування ознак [5, 6].

CNN добре працюють з локальними шаблонами (наприклад, характерними комбінаціями довжин чи інтервалів), тоді як LSTM моделюють довгострокові

залежності у послідовностях. Гібридні архітектури CNN+LSTM дозволяють поєднати обидві переваги: CNN-частина виконує попереднє вилучення ознак, а LSTM-частина – їх часову агрегацію. Результати таких моделей, за даними [5, 6], демонструють точність, яка перевершує класичні ML-методи, зокрема для задач розпізнавання застосунків і VPN-каналів на зашифрованому трафіку.

У сфері транспортних систем довгий час домінували класичні моделі часових рядів (ARIMA, SARIMA) та регресійні підходи. Однак вони погано враховують нелінійність, сезонність і залежність від зовнішніх факторів (погода, події, дорожні роботи). Із поширенням IoT виникла можливість збирати багатоджерельні дані: сигнали зі стаціонарних сенсорів, GPS-треки, дані з навігаційних сервісів, метеодані тощо. На основі таких даних почали розроблятися моделі машинного навчання та глибокого навчання [7].

Порівняння результатів MLP, LSTM та інших DL-архітектур показує, що глибокі моделі здатні краще вловлювати складні часові взаємозв'язки та взаємодії між параметрами трафіку, особливо при короткостроковому прогнозуванні (кілька хвилин або десятків хвилин уперед) [7]. Байєсівські мережі застосовуються для моделювання ймовірнісних залежностей та оцінки невизначеності прогнозів [8]. Для експериментів широко використовуються відкриті набори даних, такі як Traffic Flow Forecasting Dataset з репозиторію UCI, що дозволяє відтворювати результати й порівнювати моделі в однакових умовах [9].

Недоліком більшості рішень є відсутність тісного зв'язку з питаннями безпеки даних та довіри до джерел, а також слабка інтеграція з підсистемами мережевого моніторингу. Це відкриває простір для комплексних рішень, де прогнозування транспортних потоків спирається на захищені CIoT-дані та узгоджене з методами аналізу мережевого трафіку.

Архітектура CIoT із блокчейн-шаром довіри. Запропонована архітектура складається з кількох рівнів. На сенсорному рівні розташовані IoT-пристрої, які вимірюють фізичні параметри (температуру, швидкість, положення, стан мережі тощо). Вони передають дані на граничні вузли (edge), де здійснюється попередня агрегація, фільтрація та, за потреби, локальна аналітика.

На хмарному рівні розгортається блокчейн-мережа, вузли якої отримують агреговані дані від граничних пристроїв у вигляді транзакцій. Кожна транзакція включає хеш даних, часову мітку, ідентифікатор джерела та метадані про сценарій збору. Після досягнення консенсусу блок додається до ланцюга, забезпечуючи незмінність історії.

ML-пайплайни працюють з «офчейн»-сховищами, які зберігають фактичні масиви даних, але прив'язуються до блокчейн-записів через контрольні суми й ідентифікатори. Це дозволяє відтворювати експерименти, контролювати цілісність датасетів та відслідковувати зміни моделей (нові версії, перенавчання) через запис у блокчейн відповідних подій [1–4].

Таким чином, блокчейн виступає шаром довіри, а CIoT-інфраструктура – джерелом багатих даних для моделей прогнозування й класифікації.

Глибокі моделі для класифікації зашифрованого трафіку. Метод класифікації зашифрованого трафіку включає кілька етапів. На першому етапі формується датасет, який містить набори мережевих сесій, записаних у реальних умовах (або з публічних репозиторіїв), де кожна сесія має мітку класу (тип застосунку, сервісу чи протоколу) [5, 6].

Другий етап – виділення ознак. Із кожної сесії обчислюються послідовності довжин пакетів, інтервалів часу між ними, напрямків (вхідний/вихідний), кількість пакетів у потоці, статистичні агрегати (середнє, дисперсія, квантілі). Отримані послідовності перетворюються у вектори або матриці фіксованої довжини, придатні для подачі в глибоку модель.

Третій етап – моделювання. Застосовується гібридна CNN+LSTM-архітектура, де:

– CNN-шари витягують локальні шаблони зі структури потоку (наприклад, характерні «сигнатури» довжин пакетів і інтервалів);

– LSTM-шари моделюють часові залежності та довгострокові залежності в послідовності;

– вихідний Dense-шар з softmax-активацією виконує класифікацію.

Четвертий етап – оцінювання якості. Моделі порівнюються з класичними ML-алгоритмами (Random Forest, SVM, KNN) за точністю, повнотою, прецизійністю, F1-мірою та AUC. Результати експериментів у літературі демонструють суттєвий приріст точності глибоких моделей, особливо у задачах розрізнення близьких за поведінкою типів трафіку.

Такий підхід може бути інтегрований у CIoT-архітектуру як інтелектуальний модуль мережевої безпеки, що працює на основі статистики зашифрованих пакетів.

Прогнозування транспортних потоків. Для прогнозування транспортних потоків пропонується IoT-орієнтована архітектура, де:

– датчики та бортові пристрої формують потоки даних (швидкість, інтенсивність, координати, метеоумови);

– на граничних вузлах виконується локальне згладжування, виявлення аномалій, усунення пропусків;

– у хмарній частині дані інтегруються, масштабуються та подаються в ML-моделі [7–9].

Для побудови моделей застосовуються:

– MLP – як базова нелінійна модель для регресії;

– LSTM – для моделювання часових залежностей і сезонності в трафіку;

– байєсівські мережі – для врахування невизначеності та ймовірнісних залежностей [7, 8].

В якості навчальної та тестової вибірок можуть використовуватися публічні дані, наприклад, Traffic Flow Forecasting Dataset з UCI [9], де наявні часові ряди інтенсивності руху, виміряні в різні часові проміжки. Після навчання моделі порівнюються за RMSE, MAE, MAPE та іншими метриками. Практика показує, що LSTM зазвичай перевершує MLP та класичні моделі часових рядів, особливо в короткостроковому прогнозуванні.

Вбудувавши такі моделі у CIoT-архітектуру, можна створити інтелектуальну службу прогнозування, яка використовує довірені дані з блокчейн-реєстру та забезпечує проактивне керування дорожнім рухом.

Отже, в даному досліджені:

1. Показано, що інтеграція блокчейн-технології з ML-пайплайнами у CIoT-системах дозволяє підвищити довіру до даних та результатів аналітики, забезпечуючи незмінність, простежуваність і відтворюваність моделей та експериментів;

2. Проаналізовано та узагальнено сучасні підходи до класифікації зашифрованого трафіку. Доведено доцільність застосування глибоких нейронних мереж, які здатні забезпечувати високу точність класифікації без доступу до вмісту пакетів.

3. Розглянуто IoT+ML-підхід до прогнозування транспортних потоків, де багатоджерельні дані з сенсорів і бортових пристроїв аналізуються за допомогою моделей MLP, LSTM та байєсівських мереж. Продемонстровано, що LSTM-моделі на основі відкритих датасетів здатні забезпечувати високу точність короткострокового прогнозування.

Список використаних джерел

1. Das, A. K., Zeadally, S., & He, D. (2018). Taxonomy and analysis of security protocols for Internet of Things. Future Generation Computer Systems, 89, 110–125.
2. Wazid, M., Das, A. K., Shetty, S., Gope, P., & Rodrigues, J. J. P. C. (2021). Security in 5G-enabled Internet of Things communication: Issues, challenges, and future research roadmap. IEEE Access, 9, 4466–4489.
3. Wu, Q., Ding, G., Xu, Y., Feng, S., Du, Z., Wang, J., & Long, K. (2014). Cognitive Internet of Things: A new paradigm beyond connection. IEEE Internet of Things Journal, 1(2), 129–143.
4. Ren, K., Zheng, T., Qin, Z., & Liu, X. (2020). Adversarial attacks and defenses in deep learning. Engineering, 6(3), 346–360.
5. Shi, H., Li, H., Zhang, D., Cheng, C., & Cao, X. (2018). An efficient feature generation approach based on deep learning and feature selection techniques for traffic classification. Computer Networks, 132, 81–98.
6. Zhang, Z., Kang, C., Fu, P., Cao, Z., Li, Z., & Xiong, G. (2017). Metric learning with statistical features for network traffic classification. In 2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC) (pp. 1–7). IEEE.
7. Winata, F., Jovanka, I., & Laurent, A. (2022). Traffic prediction: A comparison between the LSTM and multi-layer perceptron algorithm. In 2022 2nd International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA) (pp. 12–16). IEEE.
8. Zhang, C., Sun, S., & Yu, G. (2004). A Bayesian network approach to time series forecasting of short-term traffic flows. In Proceedings of the 7th International IEEE Conference on Intelligent Transportation Systems (pp. 216–221). IEEE.
9. UCI Machine Learning Repository. (2020). Traffic flow forecasting data set [Data set]. University of California, Irvine.

ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

WEST UKRAINIAN NATIONAL UNIVERSITY

Комп'ютерна Інженерія

III ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ СТУДЕНТІВ, АСПІРАНТІВ ТА МОЛОДИХ ВЧЕНИХ «ІНТЕЛЕКТУАЛЬНІ КОМП'ЮТЕРНІ СИСТЕМИ ТА МЕРЕЖІ»

ІКСМ осінь 2025

25 ЛИСТОПАДА 2025

Наукове товариство ЗУНУ

KI.WUNU.EDU.UA/CONFERENCE/

ТЕРНОПІЛЬ

2025

ПРОГРАМНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

Десятнюк О.М., ректор Західноукраїнського національного університету, д-р економічних наук, професор;
Дивак М.П., д-р технічних наук, професор, проректор з наукової роботи ЗУНУ;
Березький О.М., д-р технічних наук, професор, професор кафедри комп'ютерної інженерії Західноукраїнський національний університет;
Семанюк В.З., д-р економічних наук, професор, начальник науково-дослідної частини Західноукраїнського національного університету
Антощук С.Г., д.т.н, професор, Національний університет «Одеська політехніка»;
Баловсяк С.В., д.т.н, професор, Чернівецький національний університет
Бармак О.В., д.т.н., професор, Хмельницький національний університет
Батько Ю.М., к.т.н., доцент, Західноукраїнський національний університет;
Винокурова О.А., д.т.н., професор, Львівський національний університет імені Івана Франка
Возна Н.Я., д.т.н., професор, Західноукраїнський національний університет;
Говорущенко Т.О., д.т.н., професор, Хмельницький національний університет;
Дубчак Л.О., к.т.н., доцент, Західноукраїнський національний університет;
Дунець Р.Б., д.т.н., професор, НУ "Львівська політехніка";
Ізонін І.В., д.т.н., доцент, НУ "Львівська політехніка";
Комар М.П., д.т.н, професор, Західноукраїнський національний університет;
Литвиненко В.І., д.н.т, професор, Херсонський національний технічний університет ;
Лупенко С.А., д.т.н., професор, Опольський технологічний університет, Польща;
Лящинський П.Б., доктор філософії з комп'ютерних наук, НУ "Львівська політехніка" ;
Мельник Г.М., к.т.н, доцент, Західноукраїнський національний університет;
Мельникова Н.І., д.т.н., професор, НУ "Львівська політехніка" ;
Пелешко Д.Д., д.т.н., професор, Львівський національний університет імені Івана Франка;
Піцун О.Й., к.т.н. доцент, Західноукраїнський національний університет;
Сельський П.Р., д.м.н., професор, Тернопільський національний медичний університет імені І. Я. Горбачевського ;
Субботін С.О., д.т.н., професор, Національний університет «Запорізька політехніка» ;
Теслюк В.М., д.т.н., професор, НУ "Львівська політехніка" ;

ЗМІСТ

і є основою для інтеграції з інтелектуальними транспортними системами.

Список літератури

1. Boukerche A., Tao Y., Sun P. Artificial intelligence-based vehicular traffic flow prediction methods for supporting intelligent transportation systems. *Computer Networks*. 2020. Vol. 182. Art. 107484.

2. Ghadi Y.Y., Mazhar T., al Shloul T., et al. Machine learning solution for the security of wireless sensor network. *IEEE Access*. 2024. Vol. 12. Pp. 12699–12719.

3. Shu W., Cai K., Xiong N.N. A short-term traffic flow prediction model based on an improved gate recurrent unit neural network. *IEEE Transactions on Intelligent Transportation Systems*. 2022. Vol. 23(9). Pp. 16654–16665.

4. Ghadi Y.Y., Mazhar T., Shah S.F.A., et al. Integration of federated learning with IoT for smart cities applications, challenges, and solutions. *PeerJ Computer Science*. 2023. Vol. 9. Art. e1657.

5. Gohar M., Muzammal M., Rahman A.U. Smart TSS: defining transportation system behavior using big data analytics in smart cities. *Sustainable Cities and Society*. 2018. Vol. 41. Pp. 114–119.

Дзядик Б.-Д.Ю.
магістрант 2 курсу ФКІТ ЗУНУ
Науковий керівник к.т.н., професор Кочан В.В., кафедра ІОСУ ЗУНУ

ІНТЕГРАЦІЯ БЛОКЧЕЙН-ТЕХНОЛОГІЇ ТА ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АНАЛІЗУ ВЕЛИКИХ ДАНИХ У СЕРЕДОВИЩІ ІНТЕРНЕТУ РЕЧЕЙ

Вступ. Стрімкий розвиток Інтернету речей (IoT) зумовлює безпрецедентне зростання обсягу, швидкості та різнорідності даних, що генеруються сенсорами, вбудованими пристроями та кіберфізичними системами. У таких умовах традиційні централізовані підходи до збирання та опрацювання даних стикаються з обмеженнями масштабованості, затримок, довіри й кіберстійкості [1]. Паралельно із цим, блокчейн-технологія пропонує незмінний розподілений реєстр транзакцій і механізми децентралізованого узгодження, а методи штучного інтелекту (ШІ) та машинного навчання (МН) забезпечують здатність виявляти закономірності, прогнозувати стани та підтримувати прийняття рішень у режимі наближеному до реального часу. Інтеграція блокчейна та ШІ у середовищі IoT постає як перспективний напрям, що поєднує гарантії цілісності та простежуваності даних із когнітивними можливостями аналітики великих даних [2, 3].

Постановка задачі. Когнітивний Інтернет речей (Cognitive IoT, CIoT) формується як еволюційна модель мережі, що розвиває ідеї IoT. Подібно до класичного IoT, у CIoT взаємодіють фізичні й віртуальні об'єкти з мінімальною участю людини, проте комунікація та керування грунтуються на контекстно-обізнаному циклі «сприйняття → дія» [4]. CIoT застосовує підхід understanding-by-building: система навчається як із соціальних мереж, так і з фізичного середовища, зберігаючи семантичні подання знань у відповідних базах; надалі вона адаптується до невизначеності та змін за допомогою ресурсоефективних методів прийняття рішень.

Незважаючи на активний розвиток кожної зі складових – IoT, блокчейна та ШІ – їхня інтеграція у цілісну архітектуру залишається складною задачею. Виникає низка проблем: як забезпечити довіру до даних на всьому шляху їхнього життєвого циклу; яким чином мінімізувати ризики отруєння даних і маніпуляцій під час навчання моделей; як синхронізувати децентралізоване збирання та зберігання з вимогами до продуктивності й затримок; як масштабувати консенсус без втрати пропускної здатності; як адаптувати МН-пайплайни до відмовостійких, енергоефективних та ресурсно-обмежених сценаріїв «країв» мережі. Відсутність узгодженої моделі інтеграції спричиняє фрагментацію рішень і ускладнює їх практичне впровадження в промислових, міських, аграрних та критичних інфраструктурах.

Актуальність даного дослідження підсилюється зростанням частоти інцидентів, пов'язаних із порушенням цілісності й конфіденційності даних, та потребою у відтворюваних, верифікованих аналітичних результатах. У контексті IoT навіть невелика частка спотворених або

підмінених спостережень може призвести до деградації якості моделей, неправильних керувальних дій і збоїв у сервісах. Блокчейн, завдяки незмінності записів, механізмам прозорого аудиту та розподіленому довірчому середовищу, створює основу для «довірених даних», тоді як ШІ забезпечує витягування знань і адаптивне керування на їх підставі. Водночас інтеграція цих підходів потребує формалізації потоків даних, визначення точок інтеграції та балансування між накладними витратами консенсусу й вимогами до швидкодії аналітики.

Тому, метою дослідження є розроблення моделі інтеграції блокчейн-технології та методів штучного інтелекту для аналітики великих даних у середовищі Інтернету речей, яка підвищує достовірність даних, стійкість МН-моделей та відтворюваність обчислювальних результатів у розподілених умовах. Об'єктом дослідження є процес збирання, верифікації, зберігання та аналітики сенсорних даних у когнітивному Інтернеті речей. Предметом дослідження є методи та засоби інтеграції блокчейн-технології й штучного інтелекту для аналізу великих даних в когнітивному Інтернеті речей.

Основний матеріал. На рисунку 1 подано деталізовану модель інтеграції блокчейн-технології та когнітивних сервісів штучного інтелекту для аналітики великих даних у розподіленому середовищі Інтернету речей.

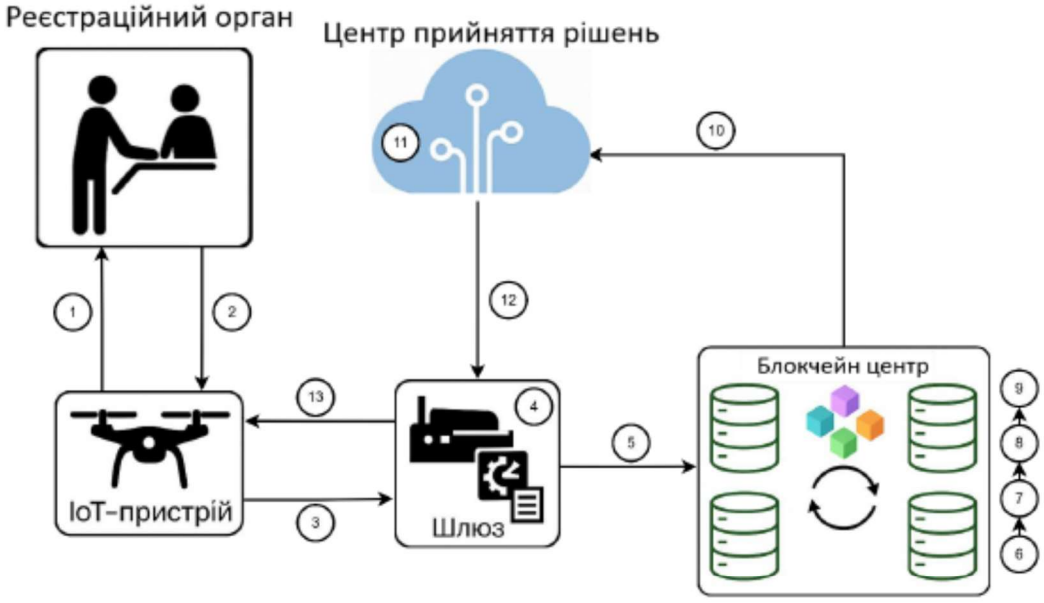


Рисунок 1- Загальний процес аналітики великих даних на основі блокчейн з підтримкою ШІ/МН

На початковому етапі (кроки 1–2) IoT-пристрій виконує процедуру реєстрації в Реєстраційному органі. На кроці 1 він надсилає запит на реєстрацію, що містить інформацію про тип пристрою, контекст застосування та криптографічні параметри. На кроці 2 Реєстраційний орган генерує й повертає облікові дані (ідентифікатор, пари ключів, сертифікати), які надалі використовуються для автентифікації та встановлення захищених каналів зв'язку. Цей етап є критичним для забезпечення довіри до джерела даних і, відповідно, для підвищення достовірності усіх подальших вимірювань.

Після успішної реєстрації IoT-застосунок розпочинає збір первинних даних. У наведеному сценарії безпілотник захоплює зображення дорожніх пошкоджень під час руху. Коли між ним і шлюзом встановлено захищене з'єднання, на кроці 3 відбувається передавання зібраних даних (зображень, супутніх сенсорних вимірювань, часових міток, геолокації) до шлюзу. Шлюз виступає проміжною ланкою між ресурсно-обмеженим IoT-пристроєм та хмарною

інфраструктурою, реалізуючи попередню фільтрацію, агрегацію й нормалізацію даних.

На кроці 4 шлюз формує транзакцію: до неї включаються хеші зображень, метадані, ідентифікатор пристрою, час та службова інформація щодо якості вимірювання. Таким чином, у транзакції фіксується цілісний опис спостереження, який надалі не може бути змінений без порушення цілісності хеш-ланцюжка. На кроці 5 ця транзакція по захищеному каналу передається на P2P-хмарні сервери, що утворюють блокчейн-центр.

У межах блокчейн-центру запускається процес додавання блоку. На кроці 6 отримана транзакція потрапляє до пулу транзакцій, де накопичуються записи від різних IoT-пристроїв. Коли накопичується достатній обсяг транзакцій, на кроці 7 формується кандидат у блок: усі транзакції впорядковуються, обчислюється кореневий хеш (Merkle root), додаються службові поля попереднього блоку та інші параметри. На кроці 8 між вузлами P2P-мережі запускається консенсус-процес (наприклад, Proof-of-Stake або інший енергоефективний механізм), у рамках якого вузли узгоджують коректність блоку, перевіряють підписи та відсутність конфліктів. Після досягнення консенсусу блок вважається валідним і на кроці 9 додається до розподіленого реєстру. Завдяки цьому з'являється незмінний, криптографічно захищений журнал подій, що гарантує відтворюваність результатів аналітики у будь-який момент часу та в будь-якій точці мережі.

Далі, на кроці 10, когнітивні сервіси отримують доступ до верифікованих блокчейном даних для виконання аналітики великих даних з використанням методів штучного інтелекту та машинного навчання. На цьому рівні дані з різних IoT-джерел об'єднуються у великі масиви, проходять етапи очищення, перетворення, побудови ознак та подаються на вхід моделей глибинного навчання, класифікації, прогнозування та виявлення аномалій. Оскільки всі спостереження мають підтверджене джерело й часову мітку, моделі навчаються на більш надійному наборі даних, що підвищує їх стійкість до підроблених записів і некоректних вимірювань.

На кроці 11 у центрі прийняття рішень реалізуються когнітивні процедури вибору, міркування та планування. Моделі машинного навчання аналізують вхідні потоки, оцінюють ймовірність дефектів (наприклад, критичність дорожньої ями), прогнозують розвиток ситуації та пропонують оптимальні дії – від пріоритизації ремонтних робіт до адаптивної зміни маршрутів руху. Результати обчислень формалізуються у вигляді дій або політик адаптації.

На кроці 12 ці дії упаковуються в запит на адаптацію й передаються з когнітивного центру до шлюзу, який на кроці 13 маршрутизує їх назад до відповідного IoT-пристрою або до зовнішніх інформаційних систем. У результаті IoT-додаток отримує інтелектуальні керівні сигнали: зміна стратегії руху, зміна частоти вимірювань, активація додаткових сенсорів, формування сповіщень для операторів тощо.

Таким чином реалізується замкнений контур «дані – блокчейн – аналітика – рішення – дія», в якому блокчейн забезпечує достовірність і відтворюваність даних, а методи штучного інтелекту – стійкість та адаптивність моделей машинного навчання у розподіленому середовищі Інтернету речей.

Висновки. Запропонована модель інтеграції блокчейн-технології та когнітивних сервісів штучного інтелекту забезпечує цілісний замкнений цикл обробки даних у розподіленому середовищі Інтернету речей – від реєстрації IoT-пристрою й фіксації вимірювань у розподіленому реєстрі до аналітики великих даних та формування адаптивних керівних дій. Використання блокчейна гарантує незмінність та простежуваність усіх транзакцій, що підвищує достовірність даних і дає змогу відтворити обчислювальні результати в будь-який момент часу. Залучення ШІ/МН-моделей до аналізу верифікованих даних підвищує стійкість моделей машинного навчання до зашумлених чи підроблених спостережень і дає змогу реалізувати інтелектуальні сценарії прийняття рішень у реальному часі. У сукупності це створює основу для побудови надійних і масштабованих IoT-систем, орієнтованих на аналітику великих даних та підтримку критично важливих управлінських рішень.

Список літератури

1. Das A.K., Zeadally S., He D. Taxonomy and analysis of security protocols for Internet of Things. *Future Generation Computer Systems*. 2018. Vol. 89. Pp. 110–125.
2. Glissa G., Meddeb A. 6LowPSec: An end-to-end security protocol for 6LoWPAN. *Ad Hoc Networks*. 2019. Vol. 82. Pp. 100–112.
3. Wazid M., Das A.K., Shetty S., Gope P., Rodrigues J.J.P.C. Security in 5G-Enabled Internet of Things Communication: Issues, Challenges, and Future Research Roadmap. *IEEE Access*. 2021. Vol. 9. Pp. 4466–4489.
4. Wu Q., Ding G., Xu Y., Feng S., Du Z., Wang J., Long K. Cognitive Internet of Things: A New Paradigm Beyond Connection. *IEEE Internet of Things Journal*. 2014. Vol. 1(2). Pp. 129–143.

Сичов Р.С.
магістрант 2 курсу ФКІТ ЗУНУ
Науковий керівник к.т.н., доцент Биковий П.Є., кафедра ІОСУ ЗУНУ

МОДЕЛЬ МАШИННОГО НАВЧАННЯ ДЛЯ АНАЛІЗУ ТА ПРОГНОЗУВАННЯ ЯКОСТІ В ПРОЦЕСАХ ІНТЕЛЕКТУАЛЬНОГО ВИРОБНИЦТВА

Вступ. Розвиток концепції «Індустрія 4.0» та пов'язане з нею поширення «розумних фабрик» істотно змінюють уявлення про організацію сучасного промислового виробництва. Інтелектуальне (розумне) виробництво, засноване на кіберфізичних системах, Інтернеті речей, інтегрованих інформаційно-комунікаційних технологіях та аналітиці великих даних, розглядається як один із ключових інструментів підвищення конкурентоспроможності промислових підприємств у глобальному просторі [1, 2]. У працях вітчизняних авторів підкреслюється, що «розумне виробництво» й «розумна фабрика» є базовими складовими Індустрії 4.0, а гнучка інтеграція цифрових технологій у виробничі процеси відкриває можливості для якісно нового рівня керованості, гнучкості та персоналізації продукції [3].

Постановка задачі. Аналіз сучасного стану розвитку інтелектуального виробництва та застосування методів машинного навчання засвідчив, що, попри значний прогрес у цифровізації та автоматизації виробничих процесів, комплексна задача прогнозування якості продукції на основі великих масивів виробничих даних опрацьована недостатньо. Більшість існуючих рішень зосереджені на архітектурі інтелектуальних виробничих систем або на локальних задачах оптимізації окремих процесів, тоді як інтегровані моделі, орієнтовані саме на передпрогнозну оцінку якості продукції, розроблені фрагментарно.

За таких умов виникає необхідність створення моделі, яка, спираючись на дані про основні матеріали та параметри технологічного процесу, дозволятиме прогнозувати інтегральні показники якості продукції (продуктивність, строк служби, надійність, зовнішній вигляд, економічність, безпека) ще до завершення виробничого циклу, а також інтегрувати результати прогнозування в єдину систему оцінювання рівня інтелектуального виробництва.

Об'єкт дослідження – процес інтелектуального виробництва промислових виробів. **Предмет дослідження** – моделі та методи прогнозування й оцінювання якості продукції в інтелектуальному виробництві на основі систем машинного навчання з використанням великих даних. **Мета** – розробити та дослідити модель прогнозування якості й інтегровану систему її оцінювання для інтелектуального виробництва, побудовані на основі алгоритмів машинного навчання (зокрема ELM-нейронної мережі з інтелектуальною оптимізацією параметрів) і трирівневої архітектури (шар джерел даних, шар оброблення даних та прикладний шар).

Основний матеріал. Модель прогнозування якості в інтелектуальному виробництві може розглядатися як модель підтримки функціонування системи, що працює на основі інтернет-технологій та операційних систем реального часу. Таке рішення створює широкі можливості для проведення експериментів у межах інженерних проєктів інтелектуального виробництва, зокрема для тестування різних стратегій керування, сценаріїв навантаження та конфігурацій обладнання [4]. Водночас, з огляду на комплексний характер такої системи, що охоплює кілька