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

АНДРІАНОВ Юрій Володимирович

Програмний модуль класифікації аномалій у промислових системах Інтернету речей / Software Module for Anomaly Classification in Industrial Internet of Things Systems

Спеціальність 122 – Комп'ютерні науки
Освітньо-професійна програма – Комп'ютерні науки

Кваліфікаційна робота

Виконав студент групи КН-42
Ю.В. Андріанов

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

Кваліфікаційну роботу допущено до захисту
«___»_____ 2025 р.

В.о. завідувача кафедри
_____ Н.М. Васильків

Тернопіль – 2025

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

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ Н.М. Васильків
«____» _____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
АНДРІАНОВ Юрій Володимирович
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: Програмний модуль класифікації аномалій у промислових системах Інтернету речей / Software Module for Anomaly Classification in Industrial Internet of Things Systems
керівник роботи Кочан В.В., к.т.н., професор
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом по університету від 20 грудня 2024 р. № 938.
2. Строк подання студентом закінченої кваліфікаційної роботи 25 травня 2025 р.
3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.
4. Основні питання, які потрібно розробити:

– провести огляд предметної області, визначити ключові аспекти промислових систем Інтернету речей та їх особливості у контексті класифікації аномалій;

– виконати аналіз відомих рішень щодо виявлення та класифікації аномалій у IIoT, визначити їх переваги та недоліки;

– сформулювати постановку задачі дослідження, визначити основні задачі, які необхідно вирішити для покращення класифікації аномалій у промислових системах IoT;

– розробити модель для класифікації аномалій у IIoT, пояснити її структуру та основні компоненти;

– описати вибір набору даних для навчання та тестування класифікатора, описати процес попередньої обробки даних, включаючи нормалізацію, видалення пропущених значень та вибір релевантних ознак;

– визначити метрики оцінювання ефективності розробленого класифікатора, обґрунтувати їх вибір та інтерпретацію результатів;

– провести експериментальні дослідження ефективності класифікатора аномалій у IIoT;

– реалізувати розгортання класифікатора аномалій у тестовому середовищі, перевірити його продуктивність та можливості інтеграції у реальні IIoT-системи.

5. Перелік графічного матеріалу в роботі:

- трирівненва модель IIoT для класифікації аномалій;
- схема роботи детектора аномалій на основі автокодера;
- схема роботи класифікатора, побудованого на основі Transformer;
- схема взаємодії між детектором аномалій та класифікатором.

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 01.02. 2025 р.	
3	Написання 2 розділу кваліфікаційної роботи	до 01.04.2025 р.	
4	Написання 3 розділу кваліфікаційної роботи	до 01.05. 2025 р.	
5	Представлення попереднього варіанту кваліфікаційної роботи, перевірка та внесення змін керівником	до 15.05.2025 р.	
6	Опрацювання зауважень та представлення завершеного варіанту кваліфікаційної роботи. Підготовка супроводжуючих документів	до 25.05.2025 р.	
7	Перевірка кваліфікаційної роботи на оригінальність тексту	до 30.05.2025 р.	
8	Оформлення кваліфікаційної роботи та отримання допуску до захисту	до 10.06.2025 р.	
9	Подання кваліфікаційної роботи до захисту на засіданні атестаційної комісії	до 10.06. 2025 р.	

Студент_____ Ю.В. Андріанов
(підпис) (прізвище та ініціали)

Керівник кваліфікаційної роботи_____ В.В. Кочан
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Програмний модуль класифікації аномалій у промислових системах Інтернету речей» на здобуття освітнього ступеня «бакалавр» зі спеціальності 122 «Комп'ютерні науки» освітньої програми «Комп'ютерні науки» написана обсягом в 62 сторінки і містить 14 ілюстрацій, 11 таблиць, 1 додаток та 40 використаних джерел.

Метою кваліфікаційної роботи є розробка та дослідження ефективного підходу до виявлення та класифікації аномалій у IIoT на основі методів глибокого навчання.

Методи досліджень включають метод аналізу (для вивчення предметної області та виявлення недоліків сучасних рішень), метод моделювання (для побудови трирівневої архітектури системи та моделі взаємодії між детектором і класифікатором), метод добування даних (для формування набору ознак із різних джерел), метод експериментальних досліджень (для оцінки ефективності автокодера та трансформера), а також метод оптимізації (для вибору ключових характеристик, параметрів ковзного вікна та конфігурації моделі з урахуванням обмежень периферійних пристроїв).

Результати дослідження: запропоновано дворівневу архітектуру системи класифікації аномалій, яка поєднує автокодер для виявлення відхилень та модель Transformer для класифікації типу аномалії. Розроблено власний набір даних, що містить відмови та атаки у IIoT, реалізовано процес обробки, балансування та трансформації даних у формат часових послідовностей. Проведено валідацію на реальному тестовому стенді.

Результати роботи можуть бути використані для підвищення безпеки та стабільності у виробничих процесах, а також для побудови адаптивних систем моніторингу в інших сферах: енергетиці, транспорті, логістиці та критично важливих інфраструктурах.

Ключові слова: ПРОМИСЛОВИЙ ІНТЕРНЕТ РЕЧЕЙ, АНОМАЛІЇ, АВТОКОДЕР, ТРАНСФОРМЕР, ГЛИБОКЕ НАВЧАННЯ, КЛАСИФІКАЦІЯ, ПЕРИФЕРІЙНІ ОБЧИСЛЕННЯ.

ANNOTATION

Qualification work on the topic «Software Module for Anomaly Classification in Industrial Internet of Things Systems» for Bachelor's degree on speciality 122 «Computer Science» educational and professional program «Computer Science» is written on 62 pages and it contains 14 figures, 11 tables, 1 annex and 40 sources.

The purpose of this qualification work is to develop and investigate an effective approach for anomaly detection and classification in Industrial Internet of Things systems based on deep learning methods.

The research methods include analysis (to study the domain and identify the shortcomings of existing solutions), modeling (to design a three-level system architecture and the interaction model between the anomaly detector and classifier), data mining (to construct a feature set from multiple sources), experimental methods (to evaluate the performance of the autoencoder and Transformer), and optimization (to select key features, sliding window parameters, and model configurations considering the limitations of edge devices).

Research results: a two-level anomaly classification system architecture has been proposed, combining an autoencoder for anomaly detection and a Transformer model for anomaly classification. A custom dataset containing IIoT-related failures and cyberattacks has been developed, including data preprocessing, balancing, and transformation into time-series format. The proposed solution has been validated on a real testbed.

The results of this work can be applied to enhance safety and stability in industrial processes, as well as in the development of adaptive monitoring systems in other fields such as energy, transportation, logistics, and critical infrastructure.

Keywords: INDUSTRIAL INTERNET OF THINGS, ANOMALIES, AUTOENCODER, TRANSFORMER, DEEP LEARNING, CLASSIFICATION, EDGE COMPUTING.

ЗМІСТ

ВСТУП

Впровадження технології промислового Інтернету речей (Industrial Internet of Things, IIoT) суттєво змінює традиційні виробничі процеси, роблячи їх більш ефективними, автоматизованими та розумними [1–3]. Завдяки використанню сучасних датчиків, бездротового зв'язку та аналізу даних у реальному часі, IIoT допомагає підприємствам швидше реагувати на проблеми, прогнозувати несправності обладнання та покращувати продуктивність [4–6]. Але водночас зростає складність таких систем, що створює нові виклики, особливо у питаннях безпеки та надійності їхньої роботи [6].

Одна з головних проблем IIoT – виявлення незвичайних ситуацій (аномалій), які можуть бути спричинені як технічними збоями, так і кіберзагрозами [1, 7–9]. На відміну від звичайних IT-систем, IIoT поєднує цифрові технології з виробничими процесами, тому будь-який збій або атака можуть мати серйозні наслідки [10]. До того ж, через різноманіття пристроїв та способів їх підключення виявлення таких загроз стає складним завданням [11]. Для цього потрібні сучасні методи, які дозволять відрізняти звичайні коливання в роботі від реальних загроз [12].

Сучасні дослідження пропонують різні підходи для вирішення цієї проблеми, наприклад, на основі методів машинного навчання для аналізу великих обсягів даних у режимі реального часу [10, 13]. Але просто виявити проблему недостатньо – потрібно ще розуміти, що саме відбувається. Тому важливим завданням є класифікація аномалій, тобто автоматичне визначення, чи це технічна несправність, чи кібератака [14]. Необхідно створити систему, яка б самостійно розрізняла типи загроз і швидко надавала відповідну інформацію для їх усунення.

Мета роботи – розробка та дослідження ефективного підходу до виявлення та класифікації аномалій у IIoT на основі методів глибокого навчання.

Для досягнення поставленої мети необхідно виконати наступні завдання:

1. Провести огляд предметної області, визначити ключові аспекти промислових систем Інтернету речей та їх особливості у контексті класифікації аномалій.

2. Виконати аналіз відомих рішень щодо виявлення та класифікації аномалій

у IIoT, визначити їх переваги та недоліки.

3. Сформулювати постановку задачі дослідження, визначити основні задачі, які необхідно вирішити для покращення класифікації аномалій у промислових системах IoT.

4. Розробити модель для класифікації аномалій у IIoT, пояснити її структуру та основні компоненти.

5. Описати вибір набору даних для навчання та тестування класифікатора, описати процес попередньої обробки даних, включаючи нормалізацію, видалення пропущених значень та вибір релевантних ознак.

6. Визначити метрики оцінювання ефективності розробленого класифікатора, обґрунтувати їх вибір та інтерпретацію результатів.

7. Провести експериментальні дослідження ефективності класифікатора аномалій у IIoT.

8. Реалізувати розгортання класифікатора аномалій у тестовому середовищі, перевірити його продуктивність та можливості інтеграції у реальні IIoT-системи.

Об’єкт дослідження – процеси моніторингу та аналізу аномальних подій у IIoT, що включають сенсорні мережі, кіберфізичні системи (CPS) та периферійні обчислення.

Предмет дослідження – методи та моделі глибокого навчання для виявлення та класифікації аномалій у IIoT, зокрема використання автоенкодерів для детекції відхилень у часових рядах та трансформерних нейронних мереж для класифікації аномалій.

Результати кваліфікаційної роботи апробовані та опубліковані у матеріалах студентської науково-практичної конференції “Інтелектуальні інформаційні технології в прикладних дослідженнях” (IITAR – 2025), м. Тернопіль, Україна, 27-29 травня 2025 р. (додаток А).

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

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ ДОСЛІДЖЕННЯ

1.1 Опис предметної області

IIoT [1-3] є технологічною концепцією, що передбачає інтеграцію сенсорних пристроїв, мережевих технологій та аналітичних систем у виробничі процеси. Основна мета IIoT – забезпечити безперервний моніторинг, автоматизацію та оптимізацію виробництва шляхом збору та аналізу великих обсягів даних у реальному часі.

IIoT системи складаються з таких ключових компонентів [1-3]:

1. Пристрої збору даних – сенсори, лічильники, контролери, які реєструють фізичні параметри (температура, тиск, вібрації тощо).
2. Кіберфізичні системи (CPS) – взаємодія фізичного обладнання та цифрових технологій для управління виробничими процесами.
3. Мережеві технології – протоколи передачі даних, зокрема MQTT, MODBUS, Profinet, що забезпечують зв’язок між пристроями.
4. Аналітичні платформи – системи штучного інтелекту та машинного навчання, що аналізують отримані дані, виявляють аномалії та допомагають у прийнятті рішень.

Завдяки IIoT промислові підприємства можуть зменшувати витрати на обслуговування, передбачати можливі несправності та запобігати аваріям, забезпечуючи підвищену ефективність та безпеку.

Попри всі переваги, інтеграція IIoT створює ризики та складнощі, пов’язані з технічними відмовами та кібератаками. Виробничі аномалії можуть бути спричинені фізичними проблемами обладнання або цілеспрямованими кібератаками на сенсори та мережеві протоколи.

Основні типи аномалій в IIoT [6]:

– технічні несправності – перегрів двигунів, зношення механізмів, відмови сенсорів, розбалансування процесів;

– порушення технологічних процесів – відхилення від заданих параметрів, несвоєчасне виконання операцій;

– кібератаки – підміна даних, DDoS-атаки на контролери, спуфінг сенсорних сигналів.

Ідентифікація таких аномалій є складним завданням, оскільки різні типи аномалій можуть мати схожі ознаки (наприклад, зміну показників сенсора може викликати як фізична поломка, так і атака на систему).

Традиційні методи виявлення аномалій включають:

1. Статистичні методи – аналіз середніх значень, стандартних відхилень, контрольні графіки. Ці підходи ефективні лише для простих відхилень, але не враховують складну динаміку виробничих процесів.

2. Методи на основі порогових значень – встановлення граничних рівнів для сенсорних показників. Недолік цього підходу – неможливість адаптації до змін у середовищі.

3. Методи машинного навчання – нейронні мережі, автоенкодери, трансформерні моделі, що дозволяють автоматично виявляти відхилення без необхідності ручного налаштування.

Однією з найбільш перспективних технологій є глибокі нейронні мережі, які можуть ефективно аналізувати великі масиви даних та знаходити нелінійні взаємозв’язки між параметрами. Однак, існуючі алгоритми мають обмеження, зокрема:

– низьку адаптивність до нових типів аномалій;

– високу кількість хибнопозитивних результатів;

– затримки у виявленні через складність моделей та обмеженість обчислювальних ресурсів.

Для підвищення ефективності систем виявлення аномалій у IIoT необхідно розробити гнучкий та адаптивний фреймворк, що поєднує:

– автоенкодери для виявлення аномалій – дозволяють розпізнавати нові відхилення без попереднього навчання на аномальних даних;

– трансформерні моделі для класифікації аномалій – забезпечують глибоке розуміння патернів у часі та покращують точність розпізнавання;

– методи периферійних обчислень – знижують затримки в аналізі даних та підвищують швидкість реакції на аномальні ситуації;

– урахування контекстної інформації – інтеграція виробничих параметрів для точнішого аналізу відхилень.

Таким чином, предметна область дослідження включає поєднання промислових сенсорних мереж, штучного інтелекту та методів виявлення загроз для забезпечення стабільної та безпечної роботи промислових систем.

1.2 Аналіз відомих рішень

Попри сучасні технології, класифікація аномалій у промислових системах залишається складним завданням. Основна проблема – це схожість між різними типами аномалій. Наприклад, якщо показники сенсора раптово змінюються, це може бути:

– технічна несправність – сенсор вийшов з ладу;

– кібератака – зловмисник підмінив дані.

Існуючі методи часто не можуть точно визначити причину відхилень, що ускладнює боротьбу з проблемами [15, 16].

Дослідники Ян та його команда [15] розробили метод для виявлення несправностей двигунів та кібератак на виробництві. Він працює добре, але тільки для певного типу обладнання. Іншими словами, якщо змінити тип виробничої системи, цей метод може не дати точних результатів. Це показує, що нам потрібні більш гнучкі рішення, які можна застосовувати для різних типів IIoT-систем.

Інша робота, проведена Ганджхані та співавторами [17], ефективно виявляє проблеми в електромережах, але не може розпізнавати інші загрози, які можуть виникати в промисловості.

Ще один виклик – постійні зміни в промислових системах. На підприємствах регулярно додають нові пристрої, датчики та технології, і система виявлення аномалій повинна вміти адаптуватися до цих змін.

Типові проблеми, які можуть виникнути:

– поломки обладнання – наприклад, перегрів двигуна або зношування деталей;

– порушення технологічного процесу – неправильна робота верстатів або

порушення стандартів якості;

– кібератаки – підміна даних, втручання у роботу датчиків або злом системи.

Юнан та співавтори [18] та Труонг [12] зазначають, що більшість сучасних методів не можуть самостійно пристосовуватися до таких змін. Часто доводиться вручну налаштовувати алгоритми або повністю оновлювати систему, щоб вона змогла знаходити нові типи загроз.

На підприємствах важливо не лише знайти проблему, а й зробити це швидко, щоб запобігти аваріям та фінансовим втратам. Якщо система працює повільно, то до моменту, коли вона повідомить про проблему, вже можуть статися значні пошкодження або простої виробництва.

Нізам та його команда [9] запропонували рішення: периферійні обчислення. Це означає, що аномалії виявляються безпосередньо на заводському обладнанні, а не передаються у центральну систему для аналізу. Це зменшує затримку обробки, але також має недоліки:

– часто доводиться вибирати між швидкістю та точністю;

– зростає навантаження на пристрої, бо вони повинні не лише збирати дані, а й аналізувати їх;

– обмежена універсальність – такі рішення розробляються під конкретні виробничі процеси.

Багато підходів до класифікації аномалій працюють лише в певних умовах, що обмежує їхню користь у широкому застосуванні.

Наприклад, дослідження Чжана [16] дозволяє виявляти атаки на сенсори, які підміняють дані, але цей метод навряд чи підійде для виробничих ліній або складів. Дослідження Ляна [19] показує, як оптимізувати роботу пристроїв у розумних електромережах, але для інших промислових систем воно занадто складне та вимагає специфічного налаштування.

Отже, аналіз сучасних підходів до класифікації аномалій у промислових системах Інтернету речей показує, що, попри значний прогрес у цій сфері, існує низка невирішених проблем. Основна складність полягає у неоднозначності природи аномалій, оскільки схожі зміни в даних можуть бути спричинені як

технічними несправностями, так і цілеспрямованими кібератаками. Це значно ускладнює точну ідентифікацію причин відхилень та розробку ефективних заходів реагування.

Сучасні підходи до виявлення аномалій часто мають обмежену універсальність. Деякі методи працюють лише для конкретних типів обладнання або вузькоспеціалізованих промислових процесів. Наприклад, метод, запропонований Ян та його командою, добре працює для моніторингу несправностей двигунів, але не є адаптивним до інших виробничих систем. Аналогічно, рішення Ганджхані ефективне в електромережах, проте не може бути безпосередньо застосоване у широкому спектрі IIoT-додатків.

Ще одним викликом є постійна зміна виробничих умов. Нові пристрої, датчики та технології вимагають регулярного оновлення алгоритмів виявлення аномалій. Більшість існуючих рішень не мають механізмів автоматичної адаптації, що змушує операторів вручну коригувати параметри моделей або повністю оновлювати систему при зміні робочих умов.

Також важливою проблемою є оперативність виявлення аномалій. У виробничому середовищі рішення повинні працювати в реальному часі, оскільки затримки в ідентифікації проблем можуть спричинити аварії, фінансові втрати та зниження продуктивності. Одним із перспективних підходів для підвищення швидкості аналізу є периферійні обчислення, які дозволяють обробляти дані безпосередньо на виробничому обладнанні. Однак такі методи мають низку недоліків, включаючи підвищене навантаження на пристрої та необхідність пошуку компромісу між швидкістю та точністю.

Крім того, багато існуючих підходів орієнтовані на вузькоспеціалізовані сценарії, що ускладнює їхнє використання у промислових середовищах з різною архітектурою. Наприклад, методи Чжана ефективні для виявлення атак на сенсори, але не придатні для контролю за складними виробничими лініями. Аналогічно, рішення Ляна добре працює у сфері розумних електромереж, але його впровадження в інші галузі вимагає значних змін та налаштувань.

Таким чином, аналіз літератури демонструє потребу у створенні універсальних підходів до виявлення та класифікації аномалій у IIoT-системах.

Необхідні методи, що можуть адаптуватися до змін у промислових процесах, працювати в реальному часі та забезпечувати високу точність навіть за умов нестабільного середовища. Це підтверджує актуальність подальших досліджень у цій галузі та розробки гнучких алгоритмів, здатних функціонувати у динамічних промислових системах.

1.3 Постановка задачі дослідження

Швидка еволюція IIoT та його інтеграція з CPS проклали шлях до появи розумних фабрик [20]. Ці сучасні виробничі середовища використовують цифрові технології для підвищення операційної ефективності, продуктивності та гнучкості [10, 12, 21]. Однак складність і взаємопов'язаність цих систем створює значні виклики у моніторингу та забезпеченні безпеки промислових процесів [6–8, 18].

Одним із ключових завдань у промисловому середовищі є виявлення та класифікація аномалій, що можуть включати технічні відмови обладнання, помилки в роботі сенсорів та кібератаки. Існуючі методи виявлення аномалій часто мають обмежену здатність розрізняти різні типи аномальних ситуацій, що може призводити до хибних тривог або втрати критично важливих даних.

З огляду на це, основною проблемою дослідження є розробка ефективного та масштабованого підходу до виявлення та класифікації аномалій у системах IIoT, який враховує особливості промислових середовищ, забезпечує високу точність роботи та мінімізує кількість хибнопозитивних та хибнонегативних результатів.

Багато традиційних методів аналізу аномалій базуються на статистичних підходах, які не враховують складну динаміку даних у IIoT-системах. Водночас, методи машинного навчання та глибоких нейронних мереж відкривають нові можливості для автоматизованого виявлення та класифікації аномалій.

Серед основних проблем існуючих підходів можна виділити:

– низьку адаптивність до змінюваного середовища – більшість моделей не враховують контекстні особливості виробничого процесу;

– високий рівень хибнопозитивних спрацьовувань, що ускладнює роботу операторів і знижує довіру до системи;

– недостатню здатність класифікувати нові типи аномалій, особливо якщо вони раніше не зустрічалися у тренувальних даних;

– високі обчислювальні витрати, що обмежує можливості розгортання таких моделей на периферійних пристроях.

Таким чином, розробка ефективного, масштабованого та адаптивного підходу для виявлення та класифікації аномалій у промислових системах IIoT є надзвичайно актуальною. Запропоноване дослідження спрямоване на вирішення цих проблем шляхом інтеграції сучасних глибоких нейронних мереж, використання автоенкодерів для детекції аномалій та трансформерних моделей для їх класифікації.

Запропонований підхід дозволить значно підвищити ефективність роботи промислових IIoT-систем, забезпечити їхню надійність та безпеку, а також зменшити ймовірність простоїв та несанкціонованого втручання в технологічні процеси.

Під час навчання дані беруть з тестового стенда, готового набору даних або створюють штучно. Потім з них вибирають найважливіші характеристики, очищають і готують для роботи детектора аномалій. Перед навчанням класифікатора дані врівноважують, щоб уникнути перекосів у навчанні.

На етапі використання система отримує дані від CPS і IIoT, обробляє їх і передає детектору аномалій. Якщо детектор знаходить аномалію, він передає її класифікатору, який визначає, чи це відмова чи атака. Якщо ж система не впевнена у результаті, вона надсилає оператору сповіщення, щоб він міг самостійно перевірити і вирішити, що це за випадок.

1. Збір даних.

Для збору даних можуть використовуватись різні способи. Найпростіший спосіб – використовувати вже готові набори даних, які доступні у відкритих онлайн-джерелах. Це швидкий та недорогий варіант. Інший спосіб – використовувати спеціальні програми, які можуть імітувати збої та атаки, що реально можуть виникнути у IIoT. Завдяки цьому можна отримати багато прикладів аномалій для подальшого аналізу. Однак створення повноцінної комп'ютерної моделі (симуляції) реальної IIoT-системи з усіма деталями може бути складною

задачею. Також можна використовувати історичні дані про роботу виробничої системи, але таких даних часто недостатньо, і вони можуть не охоплювати всі типи збоїв, які нас цікавлять. Ще один метод – використання генеративних нейронних мереж. Це штучний інтелект, який вміє створювати нові, штучні дані, схожі на реальні. Але щоб навчити такі моделі, потрібно мати багато вихідних даних. Найбільш прямий спосіб – це створювати збої та атаки прямо на реальній системі IIoT, але це дуже ризиковано, бо може завдати шкоди виробничому процесу. Тому більш безпечний варіант – створити спеціальний тестовий стенд (тестове середовище), який буде дуже схожим на справжню систему, та вже на ньому безпечно імітувати різні збої та атаки. Якщо є додаткове обладнання, це може бути також економним рішенням.

2. Розумна фабрика.

У цьому випадку «розумна фабрика» означає підприємство, де CPS інтегровані з IIoT. CPS – це автоматизоване виробництво, яке управляється за допомогою спеціального програмного забезпечення (наприклад, SCADA) і пристроїв, які називаються програмованими логічними контролерами. CPS є центральною частиною роботи виробництва [10, 12, 21]. Система IIoT встановлюється для того, щоб через Інтернет і хмарні технології контролювати і покращувати роботу CPS. Перший важливий крок у цьому фреймворку – це вивчити, як працюють вже встановлені на виробництві CPS та IIoT-системи. Це необхідно, щоб ті, хто створює систему для виявлення аномалій, добре розуміли архітектуру IIoT, всі її рівні, можливості, правила взаємодії (протоколи), заходи безпеки, а також типи даних, які вона отримує та обробляє.

3. Збої та атаки.

Перед тим, як збирати дані, потрібно чітко визначити, від яких саме атак та збоїв необхідно захищати IIoT-систему. Це означає, що потрібно скласти список можливих проблем і вирішити, які з них важливі, а які можна не враховувати. Деякі атаки можуть бути дуже малоймовірними, а деякі – надто складними або дорогими для вирішення. Інколи простіше скористатися альтернативними варіантами, наприклад, придбати страховий поліс.

4. Контекстна інформація.

Це важливий аспект для будь-яких систем, особливо у промисловості. Простими словами, контекстна інформація – це додаткові дані з різних джерел, які допомагають краще зрозуміти умови роботи системи і надати послуги, що відповідають конкретним потребам і очікуванням користувача [22]. Наприклад, важливо визначити параметри, які можуть змінюватися в залежності від особливостей конкретного виробничого процесу, і це допоможе краще класифікувати аномалії в IIoT.

5. Обробка даних.

Це перетворення сирих, неструктурованих даних у зручний формат для подальшого аналізу. Завдяки цьому забезпечується висока якість, однорідність і точність аналізу даних, що робить їх зручними для застосування моделей машинного навчання [10]. На цьому етапі відбувається об'єднання даних з кількох джерел, заповнення пропущених значень, масштабування, видалення повторів, перетворення текстових даних у числовий формат, нормалізація та виявлення аномально великих або малих значень (викидів) [10].

6. Зменшення кількості ознак.

Це процес вибору тільки тих ознак (характеристик), які дійсно впливають на результат аналізу. Зайві ознаки створюють зайве навантаження на комп'ютер і можуть погіршити точність аналізу [10, 23]. Для цього використовують різні підходи, наприклад, аналіз даних для виявлення важливості змінних. Методи зменшення розмірності поділяють на два типи: витягування нових ознак, коли вихідні ознаки перетворюють на меншу кількість нових [10, 23], і вибір найважливіших ознак, які найкраще допомагають у класифікації.

7. Балансування даних.

Якщо даних одного типу дуже мало, а іншого – багато, виникає дисбаланс, який погіршує якість аналізу. Щоб вирішити цю проблему, використовують різні методи: додають нові штучні дані (генерують їх за допомогою спеціальних моделей), змінюють налаштування класифікаторів або застосовують спеціальні методики врахування помилок [24-29].

8. Виявлення аномалій.

Це процес пошуку незвичайних ситуацій або подій у часових рядах даних,

які відрізняються від нормальної поведінки системи [9]. В цьому фреймворку використовується підхід, коли модель навчається тільки на нормальних даних, а потім самостійно визначає будь-які відхилення.

9. Класифікація аномалій.

Цей підхід пропонує двоетапний підхід. На першому етапі визначаються аномалії, а на другому – їх класифікують. Якщо система не впевнена, що це саме за аномалія, вона повідомляє про це оператора для додаткової перевірки.

Отже, метою роботи є розробка та дослідження ефективного підходу до виявлення та класифікації аномалій у IIoT на основі методів глибокого навчання.

Для досягнення поставленої мети необхідно виконати наступні завдання:

1. Провести огляд предметної області, визначити ключові аспекти промислових систем Інтернету речей та їх особливості у контексті класифікації аномалій.

2. Виконати аналіз відомих рішень щодо виявлення та класифікації аномалій у IIoT, визначити їх переваги та недоліки.

3. Сформулювати постановку задачі дослідження, визначити основні задачі, які необхідно вирішити для покращення класифікації аномалій у промислових системах IoT.

4. Розробити модель для класифікації аномалій у IIoT, пояснити її структуру та основні компоненти.

5. Описати вибір набору даних для навчання та тестування класифікатора, описати процес попередньої обробки даних, включаючи нормалізацію, видалення пропущених значень та вибір релевантних ознак.

6. Визначити метрики оцінювання ефективності розробленого класифікатора, обґрунтувати їх вибір та інтерпретацію результатів.

7. Провести експериментальні дослідження ефективності класифікатора аномалій у IIoT.

8. Реалізувати розгортання класифікатора аномалій у тестовому середовищі, перевірити його продуктивність та можливості інтеграції у реальні IIoT-системи.

2 ПРОЕКТУВАННЯ КЛАСИФІКАТОРА АНОМАЛІЙ У ПРОМИСЛОВИХ СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ

2.1 Трирівненва модель IIoT для класифікації аномалій

Для моделювання роботи конвеєрної системи було використано чотири тестові стенди. Кожен тестовий стенд містить асинхронний електродвигун, перетворювач частоти, програмований логічний контролер S7-300 та людино-машинний інтерфейс. Всі чотири тестові стенди з'єднані між собою через Ethernet-мережу із використанням протоколу Profinet. Це дозволяє забезпечити швидку та надійну передачу даних між пристроями.

У тестовому середовищі також реалізовано систему IIoT. Вона забезпечує дистанційний моніторинг CPS через хмарну платформу. На рисунку 2.1 представлена спрощена структура CPS, що включає чотири двигуни та HMI.

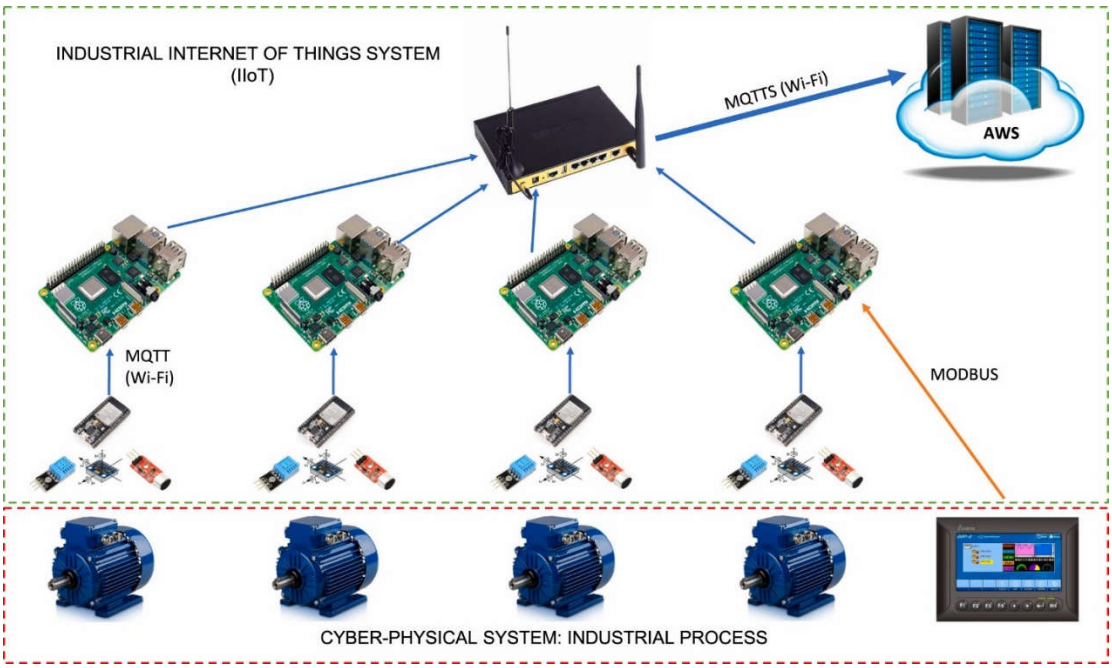

Рисунок 2.1 – Трирівненва модель IIoT для класифікації аномалій

На рисунку 2.1 представлена трирівнева модель IIoT, яка використовується для класифікації аномалій. Вона включає три основні рівні:

Рівень сприйняття – відповідає за збір даних із фізичних пристроїв. У цьому випадку він включає чотири трифазні електродвигуни та людино-машинний інтерфейс. На цьому рівні працюють датчики, що реєструють параметри роботи

двигунів, та мікроконтролери, які передають ці дані до наступного рівня.

Мережевий рівень – забезпечує передачу даних від сенсорів та пристроїв до системи моніторингу. Для цього використовуються Ethernet-мережа, протоколи Profinet, MQTT та MODBUS. Цей рівень відіграє критичну роль у забезпеченні стабільного обміну інформацією між компонентами системи.

Рівень застосування – виконує обробку отриманих даних та прийняття рішень. На цьому рівні працює хмарна система, яка аналізує отримані показники та визначає наявність аномалій у роботі CPS.

Завдяки цій трирівневій архітектурі система може ефективно збирати, передавати та обробляти дані в режимі реального часу, що підвищує точність виявлення та класифікації аномалій у промислових процесах.

У рамках IIoT-системи було використано чотири пристрої Raspberry Pi 3B, які виконують роль периферійних пристроїв. Кожен з них отримує дані від кількох датчиків, підключених до мікроконтролера ESP32. Цей мікроконтролер збирає показники сенсорів та передає їх на периферійні пристрої за допомогою протоколу MQTT.

Окрім цього, один із периферійних пристроїв взаємодіє з людино-машинним інтерфейсом через протокол MODBUS для отримання додаткової інформації про роботу електродвигунів.

Кожен периферійний пристрій виконує локальну обробку даних перед їхньою передачею у хмарну систему моніторингу та керування. Хмарна система розгорнута на платформі AWS.

Дана IIoT-система не лише здійснює моніторинг CPS у режимі реального часу, а й збирає та аналізує дані для виявлення та класифікації аномалій у роботі обладнання. Це дозволяє покращити контроль над виробничими процесами та своєчасно виявляти можливі збої або загрози.

2.2 Набір даних та обробка даних

2.2.1 Формування набору даних

Для реалізації цієї системи дані збиралися протягом десяти днів з інтервалом

чотири години. Дані з усіх двигунів у конвеєрній системі отримувалися через людино-машинний інтерфейс та передавалися на периферійний пристрій. Внутрішні дані кожного Raspberry Pi збиралися за допомогою додатку RPi-Monitor [5] та зберігалися у файлах CSV за допомогою Python-скрипта.

Додатково було проведено вимірювання відносної вологості та температури навколишнього середовища у двох різних місцях виробничого приміщення.

У цьому дослідженні основною метою було відокремлення збоїв від атак. Нижче описано типи несправностей і атак, які були змодельовані у тестовому середовищі.

Типи несправностей у тестовому середовищі

1. Перегрів (F1). Ця несправність була змодельована шляхом вимкнення вентилятора, який охолоджує периферійний пристрій. У тестовому середовищі використовувався 24-ватний вентилятор, розташований на відстані 20 см над Raspberry Pi.

2. Некоректне калібрування сенсора (F2). Щоб змоделювати неправильне калібрування сенсора звуку двигуна, значення вимірювання штучно збільшили на 20% у наборі даних. Оскільки калібрування сенсора безпосередньо змінити було неможливо, ця помилка реалізовувалася на етапі збору даних.

3. Відключення сенсора (F3). Ця несправність імітувалася шляхом відключення звукового сенсора та мікроконтролера ESP32, який ним керував. У наборі даних ця несправність відображається у вигляді нулів у відповідних стовпцях. Дана несправність не використовувалася під час оцінки моделі на раніше невідомих аномаліях під час крос-валідації.

Типи атак у тестовому середовищі:

1. Атака впровадження фальшивих даних (A1). Ця атака була змодельована шляхом підміни переданих даних від ESP32, підключених до сенсорів звуку двигунів на кожному периферійному пристрої. В результаті у MQTT-брокер надходили випадкові значення в межах від 0 до середнього значення звукового сигналу двигуна.

2. Атака "Відмова у обслуговуванні" (A2). Цей тип атаки спрямований на перевантаження MQTT-брокера, який працює на кожному периферійному

пристрої. Для цього на ноутбуці, підключеному до локальної мережі, запускали Python-скрипт, який підписував 1024 клієнти на тему “#” та надсилав короткі повідомлення на Mosquitto MQTT-брокер кожну секунду. Це призводило до насичення каналу зв’язку та порушення нормальної роботи системи.

Нижче наведено таблицю 2.1, яка описує деталі збору даних. Інформація була зібрана з різних джерел, з різними частотами вибірки та збережена у окремих файлах CSV.

Таблиця 2.1 – Структура зібраних даних

Джерело	Файл	Змінні	Частота збору	Опис
CPS	modbus.csv	Частота, напруга, струм, потужність, режим роботи	0.1 с	Дані про всі двигуни у конвеєрній системі
CPS	sound.csv	Звуковий сигнал двигуна	0.001 с	Акустичні параметри двигунів
Периферійний пристрій	internal.csv	Температура, частота процесора, завантаженість CPU (1, 5, 15 хв), напруга, вільна пам'ять, передача даних через Wi-Fi, струм	1-10 с	Внутрішні показники кожного Raspberry Pi
Будівля	mqtt_temp.csv	Вологість, температура	10 с	Дані про навколишнє середовище

Запропонований набір даних дозволяє аналізувати поведінку системи у нормальних та аномальних умовах. Він містить інформацію про фізичні показники двигунів, внутрішні параметри периферійних пристроїв та зовнішні фактори, що можуть впливати на роботу системи. Це дозволяє ефективно навчати та тестувати алгоритми виявлення та класифікації аномалій у промисловому середовищі.

2.2.2 Обробка даних

Сирі дані, зібрані під час експериментів, часто містять невідповідності, помилки або аномальні значення, які можуть негативно впливати на точність

роботи моделі. Тому перед використанням у класифікаційних моделях дані проходять етап попередньої обробки.

Ще однією важливою проблемою є те, що не всі джерела даних були доступні одночасно. Усі дані зберігалися у різних CSV-файлах, тому перед навчанням моделі необхідно було об'єднати змінні в єдиний набір даних. Для цього здійснювалося синхронізування міток часу, що означає вибір тільки тих моментів часу, для яких доступні всі змінні. Крім того, оскільки частота збору даних із різних сенсорів була неоднаковою, виконувалося переформатування, щоб всі змінні мали п'ять значень на секунду. Такий підхід дозволив зробити дані уніфікованими, що є критично важливим для якісного навчання моделей машинного навчання.

При роботі з виявленням аномалій важливо правильно обробляти відсутні дані, оскільки їхня некоректна обробка може суттєво знизити точність та надійність прогнозів моделі. Якщо в наборі даних бракувало лише кількох значень, використовувалася лінійна інтерполяція. Цей метод дозволяє заповнити відсутнє значення, обчислюючи середнє значення між двома сусідніми точками. У випадках, коли через затримку в зборі даних відсутні довші послідовності значень, застосовувався метод імпутації гарячого резерву. Він передбачає копіювання ділянки коректних даних з тієї ж серії у зону, де бракує значень.

На рисунку 2.2 показано приклад звукового сигналу двигуна, де було зібрано меншу кількість вибірок, ніж передбачено середньою частотою збору.

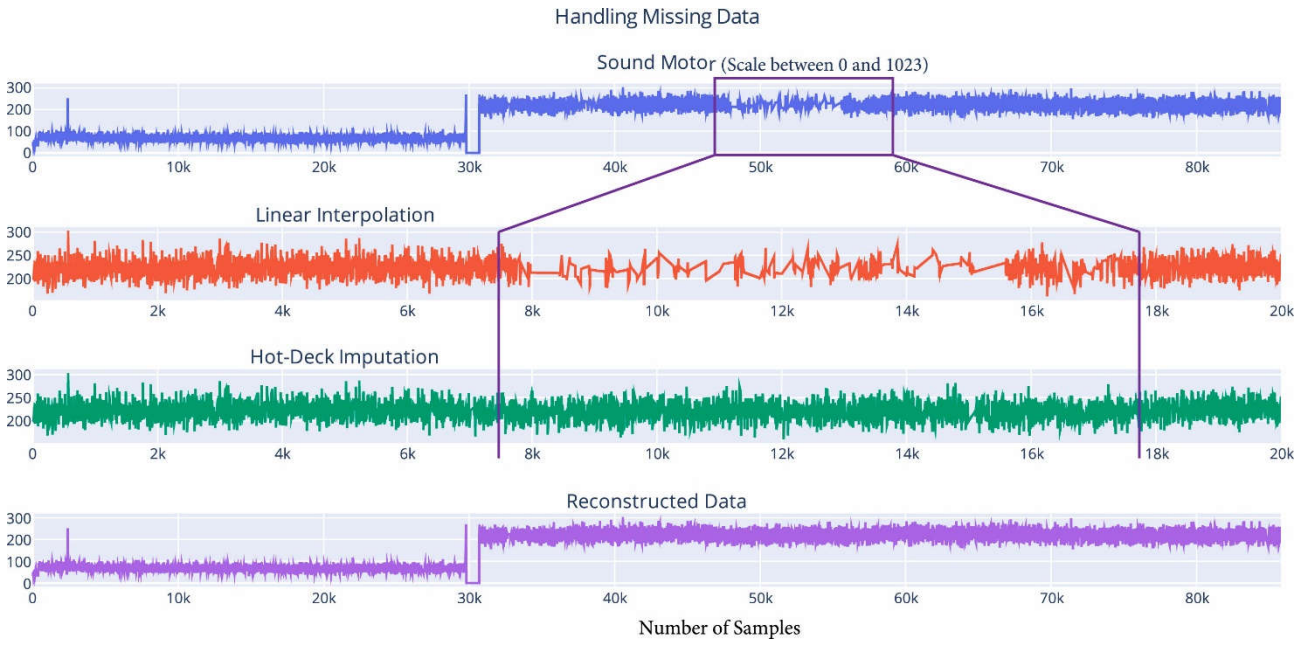

Рисунок 2.2 – Обробка відсутніх даних

Двома методами заміни відсутніх значень є лінійна інтерполяція, яка створює нове значення між двома вибірками, і гаряча імпутація, яка копіює діапазон даних із однієї серії.

Аналіз результатів показав, що для довгих інтервалів відсутніх даних імпутація гарячого резерву краще зберігає форму сигналу, ніж лінійна інтерполяція.

Формування характеристик.

Формування характеристик передбачає використання знань про предметну область для створення нових або модифікації існуючих ознак з метою покращення точності моделей машинного навчання.

У цьому дослідженні для усунення зростаючого тренду в обсязі переданих і отриманих даних через Wi-Fi було вирішено використовувати дельта-значення сигналів. Це означає, що кожне значення сигналу замінювалося різницею між поточним значенням та наступним значенням. Такий підхід дозволяє унеможливити накопичувальні зміни та зосередитися на реальних відхиленнях у сигналі.

Масштабування даних.

Набори даних часто містять змінні, які мають різні одиниці виміру та шкали, що може призводити до перекосу моделі на користь ознак з вищими числовими значеннями. Щоб уникнути цього, всі дані необхідно привести до однакового діапазону значень.

Для цього було застосовано метод мін-макс нормалізації за формулою:

$$x' = a + \frac{(x - \min(x))(b - a)}{\max(x) - \min(x)}, \tag{2.1}$$

де:

x' – нормалізоване значення;

x – початкове значення;

$\min(x)$ та $\max(x)$ – мінімальне та максимальне значення у вибірці відповідно;

a і b – нові мінімальне та максимальне значення після перемасштабування.

Ця техніка дозволяє привести всі значення до єдиного масштабу, що спрощує аналіз даних та робить модель більш стабільною.

Формування послідовностей.

При аналізі часових рядів використовується техніка ковзного вікна. Вона дозволяє перетворити набір даних із формату [n_samples, n_features] у формат [n_samples, timesteps, n_features], який краще підходить для алгоритмів глибокого навчання [11, 31, 32].

Перетворення даних у формат часових послідовностей важливе з кількох причин:

– покращує динаміку навчання моделі;

– дозволяє краще використовувати наявні дані;

– враховує темпоральну залежність, що є ключовим аспектом у виявленні аномалій.

На рисунку 2.3 представлено графічне зображення цього процесу. Кожна послідовність містить n_times вибірок і формується окремо для кожної ознаки.

Цей процес суттєво збільшує обсяг пам’яті, необхідний для збереження даних, проте дозволяє краще враховувати закономірності в часі. На рисунку 3.3 показано вибраний інтервал n_times на лівій частині та його розташування у новому форматі на правій частині.

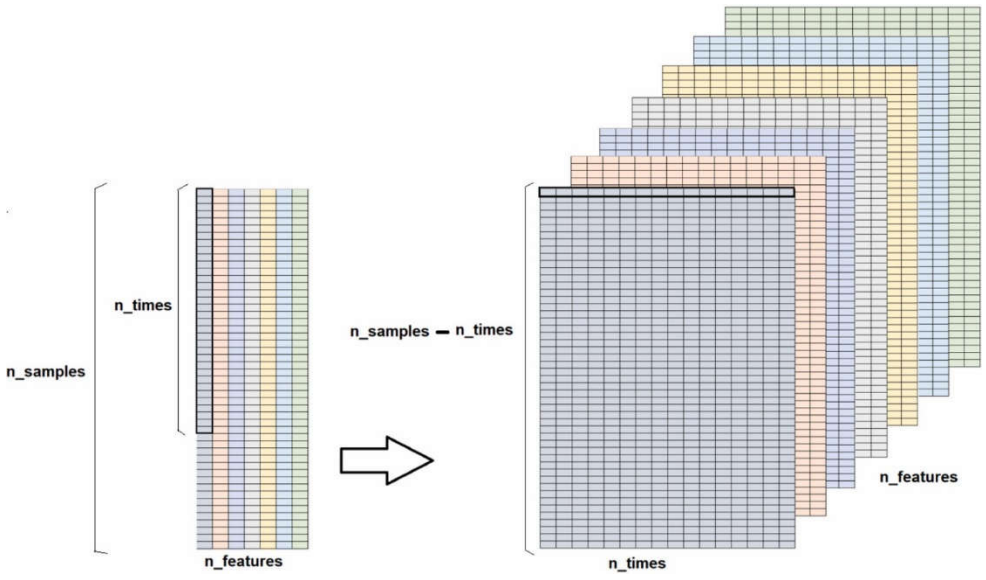

Рисунок 2.3 – Графічне представлення для перетворення даних часових рядів із [n_samples, n_features] у [n_samples, n_times, n_features]

Вибір розміру вікна є критично важливим етапом. Воно має бути достатньо великим, щоб охопити ключові закономірності, але не надто великим, щоб не "розмивати" аномалії.

Вибір оптимальної довжини послідовностей.

Для визначення найкращого розміру вікна було проведено тестування двох моделей класифікації аномалій: Transformers та LSTM. У таблиці 2.2 наведено результати тестування моделей при різних розмірах ковзного вікна, виміряні за F1-мірою.

Таблиця 2.2 – Вибір оптимальної довжини послідовностей

Розмір вікна	Модель Transformer	Модель LSTM
100	0.7992	0.7543
200	0.8123	0.7733
300	0.8339	0.7818
400	0.8043	0.6843
500	0.7781	0.6177

Аналіз результатів показав, що найкраща точність моделей досягалася при розмірі вікна у 300 вибірок. Це значення було обране для подальшого використання у навчанні та тестуванні моделі.

Завдяки правильному вибору розміру вікна вдалося знайти баланс між точністю та обчислювальною ефективністю, що є важливим фактором для промислових систем реального часу.

2.2.3 Вибір ключових ознак

Деякі алгоритми машинного навчання можуть бути обчислювально затратними, особливо якщо вони працюють з великими наборами даних, що містять велику кількість змінних. Тому для пришвидшення процесу навчання моделі було застосовано методи відбору ознак, які допомагають зменшити кількість вхідних параметрів, зберігаючи при цьому високу ефективність класифікації.

Для аналізу вибору ознак було проведено кореляційний аналіз за методом Спірмена. Цей аналіз виявив, що:

– завантаженість процесора за останні 5 хвилин (load_5) була сильно корельована із завантаженістю за 1 хвилину (load_1) та 15 хвилин (load_15).

– частота процесора (cpu_freq) та його напруга (cpu_volt) також мали високу кореляцію.

Хоча кореляція не означає причинно-наслідкового зв’язку, вона вказує на те, що load_5 та cpu_volt можуть бути видалені з набору даних, оскільки їхня інформація дублюється іншими параметрами.

Для підтвердження цього було проведено навчання моделі детектора аномалій із використанням усіх змінних, а потім модель навчали з видаленням окремих ознак.

Додатково було внесено такі зміни у набір ознак:

– замість загального обсягу переданих і отриманих даних через Wi-Fi використовувалися їхні дельта-значення (різниця між поточним і попереднім значенням).

– температура та відносна вологість у приміщенні були виключені, оскільки вони не мали безпосереднього зв’язку із роботою IIoT або CPS.

– доступна та вільна пам’ять процесора (memo_free, memo_avail) також були виключені, оскільки під час аналізу не було зафіксовано значних змін цих параметрів під час виникнення аномалій.

У кінцевому підсумку було проведено експериментальну перевірку, під час якої аномальна модель навчалася з різними комбінаціями змінних. В результаті, найкраща продуктивність моделі була досягнута при використанні восьми ключових характеристик:

– внутрішня температура пристрою;

– завантаженість CPU за 1 і 15 хвилин;

– дельта значення відправлених і отриманих даних по Wi-Fi;

– споживання струму процесором;

– звуковий сигнал двигуна;

– частота двигуна (як контекстна інформація).

У таблиці 2.3 представлено результати навчання моделі детектора аномалій з різними наборами ознак. Було поступово видалено менш значущі змінні, після чого модель перевірялася на точність, повноту та F1-міру.

Таблиця 2.3 – Результати навчання моделі детектора аномалій з різними наборами ознак

Кількість ознак	Виключені змінні	Причина виключення	Точність	Повнота	F1-міра
15	wifi_sent, wifi_receiv	Використано дельта-значення	0.5186	0.3275	0.4014
13	indoor_temp, %humidity	Не пов'язані з IIoT та CPS	0.9126	0.5223	0.6643
10	cpu_freq, memo_free, memo_avail	Не змінюються при аномаліях	0.9332	0.5296	0.6757
8	load5, cpu_volt	Сильна кореляція з іншими змінними	0.9226	0.6305	0.7491

Видалення зайвих ознак призвело до значного покращення точності класифікації аномалій. Після остаточного відбору змінних модель продемонструвала найкращі показники продуктивності, що підтверджує ефективність застосованого підходу.

Таким чином, вибір ключових характеристик дозволив суттєво скоротити обсяг даних для обробки та підвищити точність класифікації аномалій у IIoT-системах.

2.2.4 Балансування даних

Однією з ключових проблем у побудові моделей класифікації є незбалансованість набору даних, яка може суттєво впливати на точність роботи алгоритмів. Ця проблема виникає тоді, коли розподіл класів у вибірці є нерівномірним, що спричиняє зміщення моделі у бік найбільш представленого класу.

Якщо модель навчається на незбалансованих даних, вона може віддавати перевагу більшості і погано розпізнавати рідкісні події. Це є критичною проблемою

у задачах виявлення аномалій, оскільки саме менш поширені класи (аномальні випадки) є найбільш значущими [24, 28, 33].

У багатокласовій класифікації існує кілька підходів для вирішення проблеми незбалансованості класів:

1. Ресемплінг:

– Оверсемплінг – збільшення кількості зразків малочисельного класу шляхом дублювання або генерації нових даних;

– Андерсемплінг – зменшення кількості зразків переважаючого класу для вирівнювання розподілу.

2. Адаптація класифікатора: модифікація границі прийняття рішень алгоритму класифікації для кращого врахування менш поширених класів.

3. Ансамблеві методи: поєднання кількох алгоритмів класифікації для покращення точності.

4. Методи чутливості до вартості: використання штрафів за неправильну класифікацію рідкісних класів для стимулювання моделі точніше визначати аномалії [24, 25].

Ще одним підходом до боротьби з дисбалансом є розширення вибірки даних. Це особливо корисно для глибоких нейронних мереж, оскільки допомагає уникнути перенавчання [27].

Одним з найбільш ефективних методів генерації нових зразків даних є використання генеративних змагальних мереж (GANs – Generative Adversarial Networks). Вони особливо корисні у випадках, коли реальних даних недостатньо, їх важко отримати або вони потребують додаткової варіативності.

GANs складаються з двох нейромереж – генератора та дискримінатора, які тренуються в умовах змагання між собою. Генератор створює штучні зразки даних. Дискримінатор намагається відрізнити реальні дані від згенерованих.

Тренування відбувається за принципом нульової суми, де генератор намагається створювати все більш реалістичні дані, а дискримінатор покращується у визначенні підробок. Процес триває, поки дискримінатор не зможе більше легко відрізнити реальні дані від згенерованих, що означає, що генератор навчився створювати максимально реалістичні дані [31, 34].

У межах даної реалізації було застосовано андерсемплінг класу нормальних подій.

Після формування послідовностей у форматі [n_samples, n_times, n_features], частина зразків нормального класу була випадково видалена. Це дозволило зробити розподіл даних більш рівномірним, зменшити перевагу моделі у бік нормальних подій і покращити здатність класифікатора розпізнавати аномалії.

Такий підхід сприяв поліпшенню продуктивності моделі, дозволяючи їй точніше виявляти як несправності, так і потенційні кібератаки у IIoT-системах.

2.2.5 Виявлення аномалій

У цій роботі для виявлення аномалій використовується автокодер – це один із найефективніших підходів для неконтрольованого виявлення аномалій. Автокодери є моделями машинного навчання, які складаються з двох частин:

1. Енкодер – обробляє вхідні дані та стискає їх у латентне (приховане) представлення, що містить найважливішу інформацію.

2. Декодер – відновлює дані з цього стислого представлення, намагаючись отримати вихід, максимально наближений до початкових даних [35].

Основний принцип виявлення аномалій полягає у порівнянні вхідних та відновлених даних. Автокодер добре навчається на нормальних даних і може ефективно стискати та відновлювати їх. Проте, якщо на вхід надходять аномальні дані, модель не може їх коректно відтворити, і реконструкційна помилка значно зростає.

Щоб класифікувати дані як нормальні або аномальні, необхідно встановити порогове значення помилки реконструкції. Якщо помилка перевищує цей поріг, зразок вважається аномальним. Для вибору оптимального порогу використовуються баланс між чутливістю та специфічністю.

Під час тестування на нормальних даних максимальна різниця між вхідними та реконструйованими сигналами використовувалася як початковий поріг. Однак, слід враховувати, що навіть у нормальних наборах даних можуть бути викиди, які автокодер не відновлює. Це спричиняє підвищену помилку реконструкції, що може вплинути на продуктивність моделі у реальних умовах.

Для вирішення цієї проблеми викиди були видалені з нормальних даних за допомогою спеціального Python-скрипта. Всі значення, які перевищували середнє значення плюс три стандартних відхилення (μ+3σ\mu + 3\sigmaμ+3σ), замінювалися на відповідне порогове значення.

Також слід зазначити, що для кожної ознаки обчислюється власне порогове значення, оскільки різні змінні мають різні діапазони коливань.

На рисунку 2.4 представлено процес передбачення аномалій за допомогою автокодера.

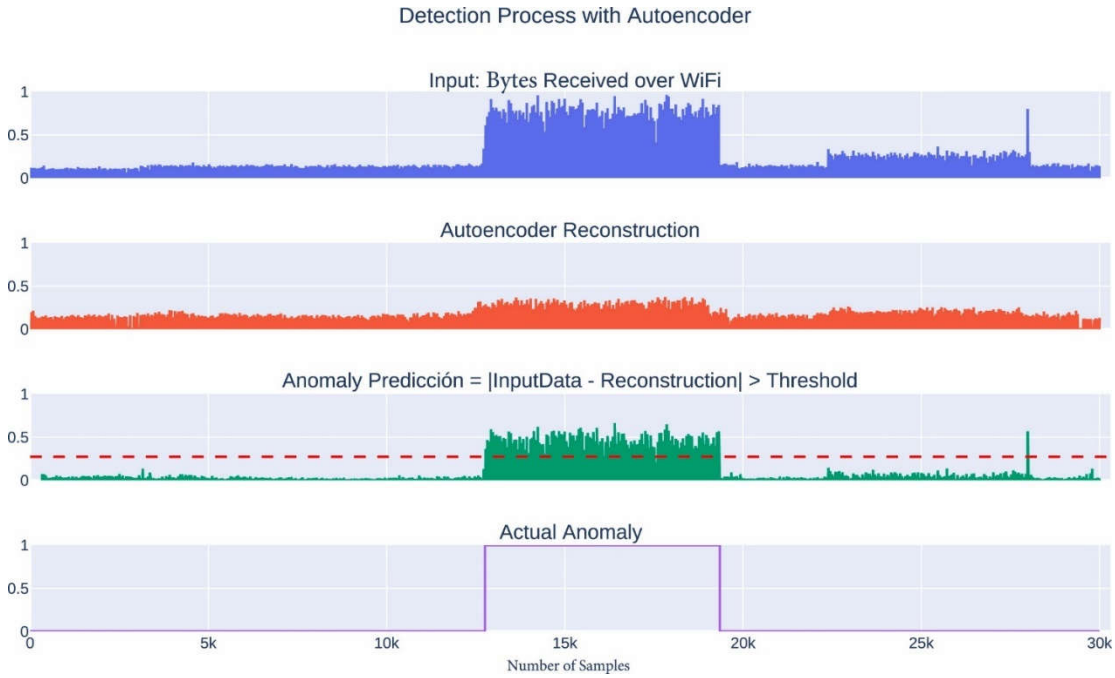

Рисунок 2.4 – Прогнозування аномалій за допомогою автокодера

Верхній графік відображає зміну дельта-сигналу отриманих даних Wi-Fi. Середній графік показує реконструкцію цього сигналу автокодером. Нижній графік демонструє різницю між вхідним та реконструйованим сигналами, а також порогове значення (пунктирна лінія).

Усі значення, що перевищують цей поріг, позначаються як аномальні.

У цій системі для енкодера та декодера використовувалися одно-вимірні згорткові шари (1D Convolutional Layers, Conv1D), які чергуються із шарами Dropout.

Одновимірні згорткові шари Conv1D спеціально розроблені для аналізу послідовних даних і широко застосовуються у часових рядах. Вони виконують

згорткову операцію, ковзаючи фільтром уздовж вхідних даних, що дозволяє виявляти локальні закономірності у послідовності.

Для декодера використовувалися транспоновані згорткові шари (Transposed Convolutional Layers) разом із Dropout, що допомагає уникнути перенавчання моделі.

На рисунку 2.5 показано схему роботи детектора аномалій на основі автокодера.

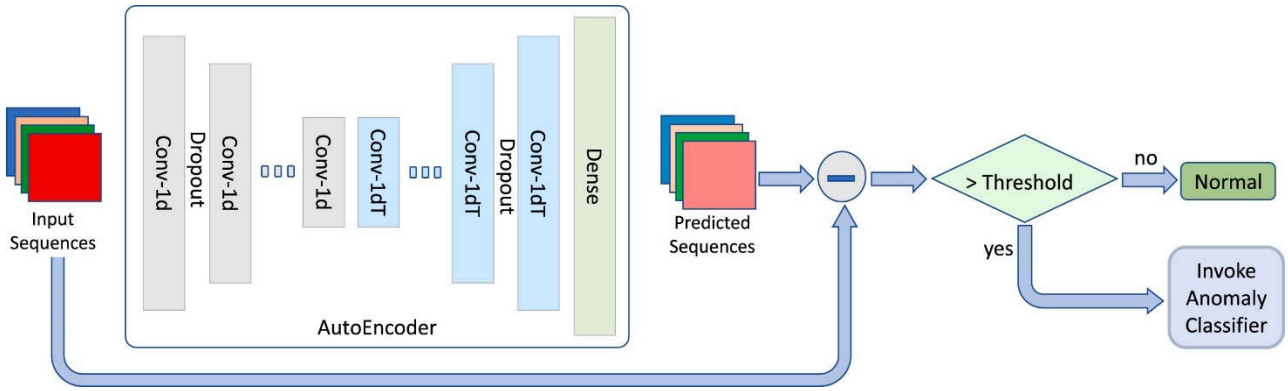

Рисунок 2.5 – Схема роботи детектора аномалій на основі автокодера

Якщо значення помилки реконструкції перевищує порогове значення, активується класифікатор аномалій. Якщо різниця не перевищує порогу, зразок класифікується як нормальний.

Запропонований автокодер на основі згорткових нейронних мереж (Conv1D) дозволяє ефективно знаходити аномалії у часових рядах IIoT-систем.

Використання реконструкційної помилки як критерію виявлення аномалій дозволяє працювати без міток аномальних подій. Оптимальний пороговий рівень розраховується окремо для кожної ознаки, що підвищує точність моделі. Видалення викидів з нормальних даних допомагає уникнути хибних спрацювань. Комбінація Conv1D та Dropout дозволяє детектору адаптуватися до різних типів аномалій без втрати узагальнюючої здатності.

Цей метод створює гнучку та ефективну систему для виявлення аномалій у промислових мережах IIoT.

2.2.6 Класифікація аномалій

Процес класифікації аномалій полягає в тому, щоб кожному вхідному зразку

призначити один із заздалегідь визначених класів. Це завдання належить до контрольованого навчання, оскільки модель навчається на розміченому наборі даних, а потім використовує отримані знання для класифікації нових прикладів.

Для виконання цієї задачі використано нейронну мережу Transformer, яка зазвичай застосовується для обробки природної мови (NLP). Однак ця архітектура також добре підходить для роботи з часовими рядами, оскільки може ефективно аналізувати послідовні залежності між даними.

Архітектура моделі базується на блоці енкодера, подібному до оригінальної реалізації Transformer. Ключовим компонентом цього підходу є механізм самоприділення уваги, який дозволяє моделі враховувати всю послідовність вхідних даних одночасно та визначати, які характеристики є найважливішими для виявлення аномалій.

Додатково використовується механізм мультиголової уваги, який дає змогу паралельно обробляти інформацію в кількох підпросторах. Це особливо корисно у виявленні аномалій, оскільки модель може виявляти різні типи відхилень у даних.

На відміну від класичних Transformer-моделей, у цій реалізації не використовуються вхідні вбудовування або позиційне кодування. Послідовності даних передаються безпосередньо в енкодер, що зменшує обчислювальну складність. Усі інші компоненти, такі як повнозв'язні шари та нормалізація, реалізовані відповідно до стандартної архітектури Transformer [36].

Рисунок 2.6 демонструє схему роботи класифікатора, побудованого на основі Transformer.

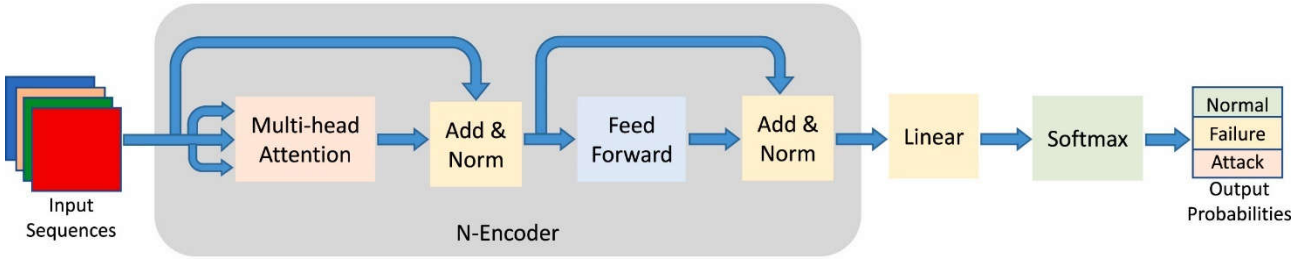

Рисунок 2.6 – Схема роботи класифікатора, побудованого на основі Transformer

2.2.7 Взаємодія детектора та класифікатора аномалій

Процес виявлення та класифікації аномалій відбувається у два етапи.

Спочатку детектор аномалій, побудований на основі автокодера, аналізує вхідні дані та визначає, чи є вони аномальними. Якщо рівень помилки реконструкції перевищує встановлений поріг, система вважає, що вхідний зразок є аномальним.

Після цього детектор передає знайдену аномалію в класифікатор, який визначає, чи є ця аномалія наслідком відмови в системі або результатом кібератаки.

Якщо класифікатор приходить до висновку, що зразок не є аномальним, а детектор помилково позначив його як аномальний, система присвоює цьому випадку мітку "подія". У такому разі відповідальність за остаточне рішення покладається на оператора, який може вручну перевірити цей зразок.

На рисунку 2.7 представлено схему взаємодії між детектором аномалій та класифікатором.

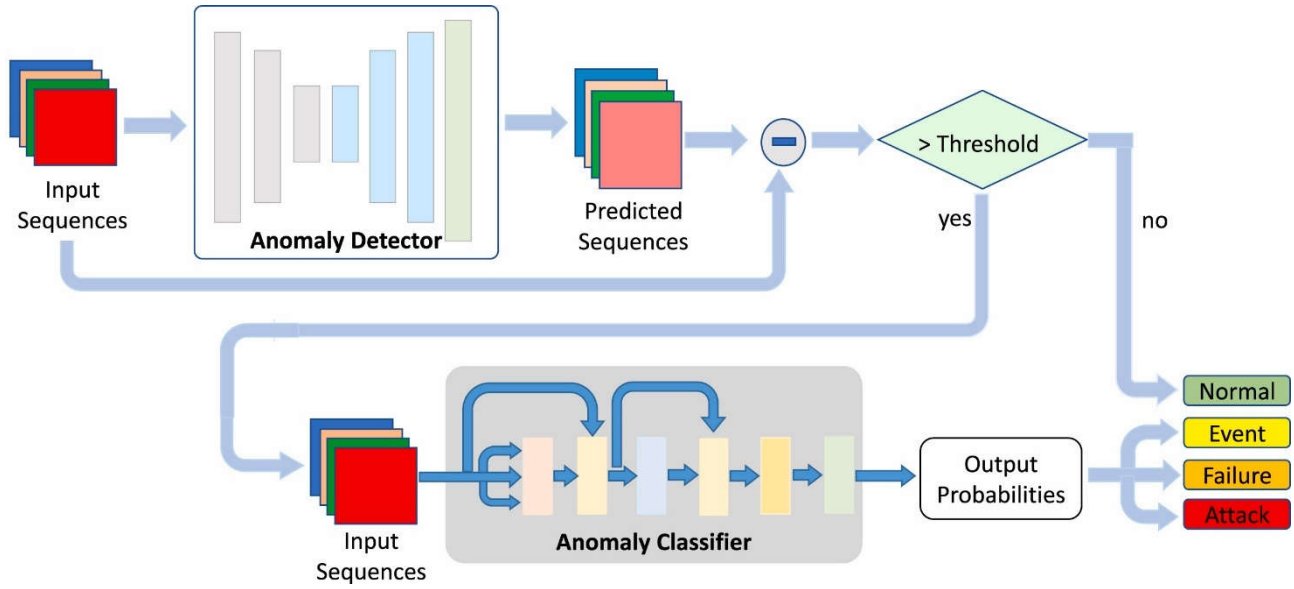

Рисунок 2.7 – Схема взаємодії між детектором аномалій та класифікатором

2.3 Метрики оцінювання ефективності моделі

Оцінювання ефективності машинного навчання зазвичай здійснюється за допомогою різних метрик. Однією з найпоширеніших є точність, яка визначає загальну кількість правильно класифікованих зразків. Однак у випадку незбалансованих наборів даних ця метрика може бути неінформативною.

Оскільки в даних міститься значно більше нормальних зразків, модель може демонструвати високу точність, навіть якщо насправді погано розпізнає аномалії. Для усунення цього ефекту слід використовувати метрики, які не залежать від

домінуючого класу.

До таких метрик належать:

1. Повнота – ця характеристика показує, скільки аномалій було правильно виявлено. Якщо модель не виявила достатньо аномалій, значення Recall буде низьким.

2. Прецизійність – ця метрика вказує, наскільки часто модель помилково ідентифікувала нормальні зразки як аномальні.

3. F1-міра – є балансом між точністю та повнотою і дозволяє отримати більш об’єктивну оцінку роботи моделі.

У таблиці 2.4 наведено формули для обчислення кожної з цих метрик.

Таблиця 2.4 – Формули для обчислення метрик

Метрика	Формула	Що оцінює
Accuracy (Точність)	$\frac{TP + TN}{TP + TN + FP + FN}$	Загальна точність моделі
Recall (Повнота)	$\frac{TP}{TP + FN}$	Кількість правильно виявлених аномалій
Precision (Прецизійність)	$\frac{TP}{TP + FP}$	Частка дійсно аномальних випадків серед усіх позначених як аномальні
F1-Score	$2 \times \frac{Precision \times Recall}{Precision + Recall}$	Баланс між Precision та Recall

TP (True Positive) – кількість аномалій, які були правильно виявлені.

TN (True Negative) – кількість нормально працюючих зразків, які були правильно класифіковані.

FP (False Positive) – кількість нормальних випадків, які були помилково позначені як аномалії.

FN (False Negative) – кількість аномалій, які модель не виявила.

Використання цих метрик дозволяє отримати об’єктивну оцінку ефективності моделі навіть у випадку незбалансованих наборів даних.

3 ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ КЛАСИФІКАТОРА АНОМАЛІЙ У ПРОМИСЛОВИХ СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ

3.1 Оцінки ефективності класифікатора аномалій у IIoT

3.1.1 Формування набору даних

Для ефективного виявлення та класифікації аномалій у IIoT важливо мати достатню кількість різноманітних даних, що включають відмови обладнання, кібератаки та інші порушення роботи системи [37]. Однак під час аналізу доступних ресурсів не було знайдено набору даних, який би містив окремо марковані відмови та атаки в промислових системах IIoT. Тому було прийнято рішення створити власний набір даних на основі тестової платформи.

Дані збиралися протягом 10 днів із періодичністю 4 години на день. Вся інформація зберігалася у 48 файлах. 31 файл містив дані про нормальну роботу системи. 13 файлів містили дані про відмови обладнання, зокрема: перегрів системи (F1), некоректне калібрування сенсорів (F2), відключення сенсора (F3). 4 файли містили дані про кібератаки, зокрема: атака шляхом ін’єкції даних (A1), атака типу "відмова в обслуговуванні" (A2). Структура зібраного набору даних: 2 105 134 записи нормальної роботи, 60 463 записи, що містять інформацію про відмови, 38 755 записів про кібератаки. Дані щодо відключення сенсора (F3) не використовувалися під час навчання моделі, а застосовувалися лише для оцінки її здатності виявляти нові невідомі аномалії. Цей набір даних доступний у відкритому репозиторії для подальшого використання в дослідженнях.

Таблиця 3.1 містить підсумкові дані про структуру набору даних.

Таблиця 3.1 – Загальна структура набору даних

Файли	Нормальні дані	Відмови	Атаки	F1	F2	F3	A1	A2
31	1 254 183	0	0	0	0	0	0	0
13	345 547	60 463	0	11	8	2	0	0
4	505 404	0	38 755	0	0	0	8	5
Усього	2 105 134	60 463	38 755	11	8	2	8	5

Цей набір даних усуває дефіцит високоякісних даних, необхідних для навчання моделей, що класифікують аномалії як відмови або атаки. Окрім цього, система дозволяє класифікувати конкретні типи відмов або атак, що є корисним для подальшого вдосконалення моделей машинного навчання.

3.1.2 Контекстна інформація

Робота системи IIoT значною мірою впливає на структуру даних CPS, що, у свою чергу, змінює певні змінні в процесі збору та аналізу даних. Одним із таких прикладів є сенсор звуку, показники якого безпосередньо залежать від частоти роботи найближчого двигуна. Оскільки звуковий сенсор може сприймати коливання, що не завжди є пов'язаними з аномаліями, для підвищення точності класифікації було вирішено використовувати частоту двигуна як контекстну змінну.

Рисунок 3.1 демонструє, що включення частоти двигуна до набору даних дозволяє краще розрізняти нормальну та аномальну поведінку сенсора звуку. Це стає особливо помітним у таких випадках:

1. Атака шляхом ін'єкції даних (A1) – коли рівень шуму сенсора змінюється без зміни частоти роботи двигуна (зображено ліворуч).

2. Відмова сенсора через відключення (F3) – коли показники звукового сенсора повністю відсутні, хоча двигун продовжує працювати (зображено праворуч).

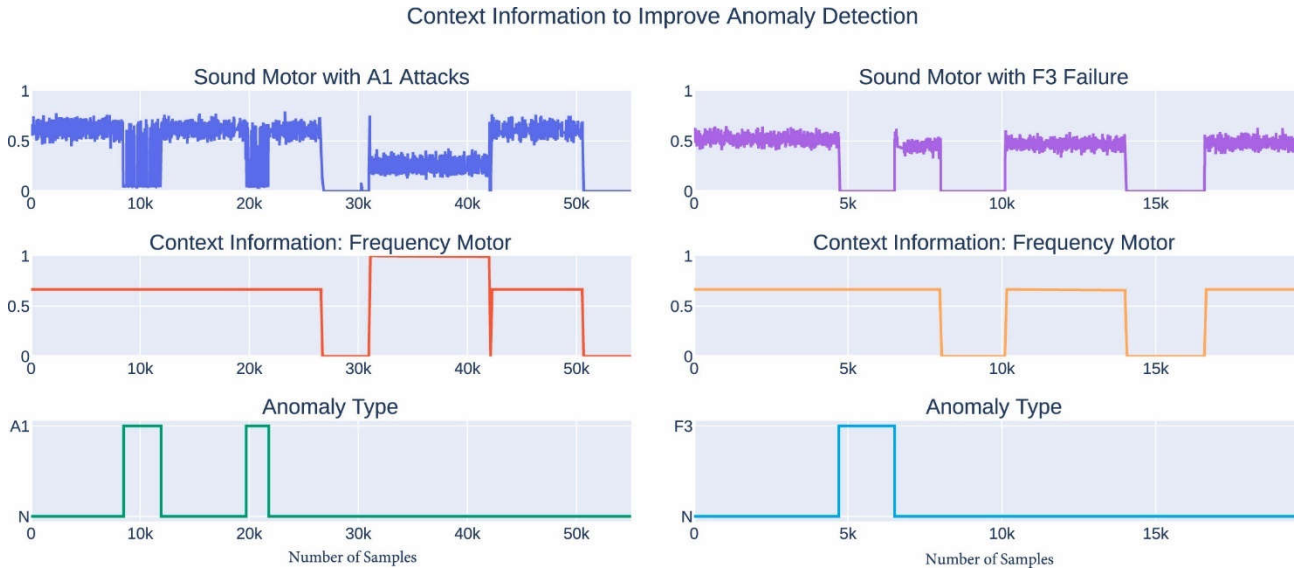

Рисунок 3.1 – Контекстна інформація

Таким чином, якщо рівень звуку коливається, а частота двигуна залишається незмінною, це є сигналом про можливу аномалію.

Для оцінки ефективності використання контекстної інформації було проведено тестування двох версій моделей:

1. Модель з урахуванням контекстних змінних, де використано додаткову інформацію про CPS.

2. Модель без контекстної інформації, яка базується виключно на даних із сенсорів IIoT.

Таблиця 3.2 містить порівняльний аналіз, який показує, що ігнорування контекстної інформації негативно впливає на точність виявлення та класифікації аномалій.

Зокрема, у випадку моделі без контекстної інформації:

– Детектор аномалій не зміг виявити відключення сенсора (F3);

– Класифікатор не зміг правильно визначити атаку шляхом ін’єкції даних (A1);

– Середнє значення F1-міри зменшилося з 0.9639 до 0.9262 для детектора аномалій і з 0.9004 до 0.8332 для класифікатора.

Ці результати вказують на те, що використання контекстної інформації значно покращує точність класифікації аномалій, що є критично важливим для забезпечення надійності систем IIoT.

Таблиця 3.2 – Вплив контекстної інформації на моделі виявлення та класифікації аномалій

Модель	Контекст	F1	F2	F3	A1	A2	F1-Score
Детектор	Так	✓	✓	✓	✓	✓	0.963900
	Ні	✓	✓	✗	✓	✓	0.926210
Класифікатор	Так	✓	✓	✓	✓	✓	0.900422
	Ні	✓	✓	✗	✗	✓	0.833197

Негативний вплив відсутності контекстної інформації на ефективність

детектора та класифікатора аномалій добре ілюструється на рисунку 3.2.

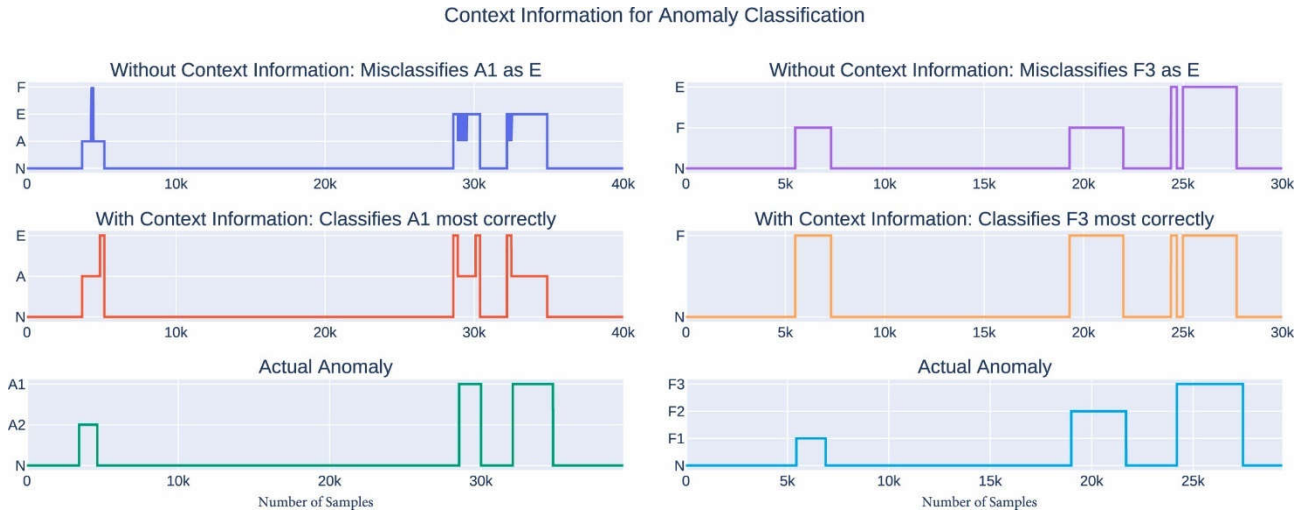

Рисунок 3.2 – Контекстна інформація допомагає правильно класифікувати атаки (A1)

На графіку зверху видно, що атаки типу A1 (ін’єкція даних) класифікуються як "події". Це означає, що класифікатор не зміг правильно визначити природу аномалії. У той же час, моделі, що враховують контекстну інформацію, правильно ідентифікують атаки (A1) як аномалії, що видно на середньому графіку. На нижньому графіку наведено фактичну класифікацію аномалій, що підтверджує покращення точності при використанні додаткових параметрів CPS.

3.1.3 Використання ковзного вікна для виявлення аномалій

У деяких випадках аномалії не виявляються стабільно, а зразки, які класифікуються як аномальні, чергуються з нормальними зразками. На рисунку 3.3 представлено приклад такої ситуації. На перший погляд може здатися, що аномалія виявлена правильно. Однак, якщо розрахувати матрицю невідповідностей та оцінити точність, повноту та F1-міру, показники продуктивності детектора будуть незадовільними.

Для вирішення цієї проблеми в детекторі та класифікаторі аномалій була реалізована стратегія, що використовує послідовності з 300 зразків. Якщо в послідовності вихідних даних принаймні 15 зразків перевищують порогове значення, уся послідовність позначається як аномальна. Завдяки цій стратегії:

– аномалії позначаються як безперервна область на графіку прогнозів

(зображено на середньому графіку рисунку 3.3);

– модель ігнорує випадкові викиди, що виникають у поодиноких зразках, та не створює хибних спрацьовувань;

– система активує сигнал про аномалію лише тоді, коли 15 або більше зразків класифікуються як аномальні, що зменшує ймовірність помилкових спрацьовувань;

– аномалії, які тривають менше трьох секунд, ігноруються, оскільки швидкість вибірки становить 0,2 секунди.

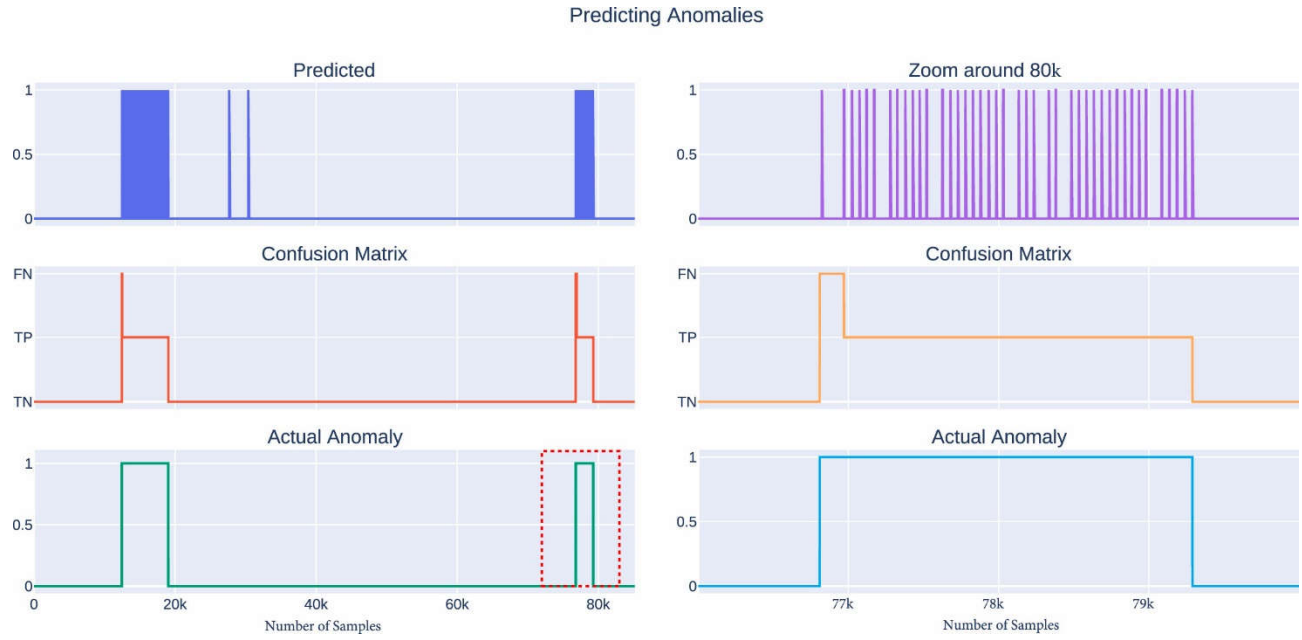

Рисунок 3.3 – Деякі аномалії виявляються періодично, чергуючись із нормальними зразками

Для оцінки ефективності цього підходу було проведено два експерименти:

1. Підрахунок точок аномалій без використання ковзного вікна – кожен окремий аномальний зразок розглядається як незалежний.

2. Використання ковзного вікна розміром 300 зразків, де аномалія реєструється лише в тому випадку, якщо в послідовності є принаймні 15 аномальних зразків.

Результати наведені у таблиці 3.3.

Як видно з таблиці, використання ковзного вікна значно покращує оцінку моделі:

– точність зросла з 0.9885 до 1.0000, що означає, що модель не генерує

хибних позитивних спрацьовувань;

– повнота покращилася з 0.0571 до 0.9745, що свідчить про правильне виявлення аномалій у всіх випадках;

– значення F1-міри збільшилося з 0.1079 до 0.9871, що підтверджує ефективність методу.

Таблиця 3.3 – Вплив ковзного вікна на продуктивність детектора аномалій

Метод оцінки аномалій	TN	TP	FN	FP	Accuracy	Precision	Recall	F1-Score
Послідовність 300 зразків	76 119	8 839	231	0	0.9973	1.0000	0.9745	0.9871
Підрахунок точок аномалій	76 113	518	8 552	6	0.8995	0.9885	0.0571	0.1079

На рисунку 3.3 представлено графічне порівняння роботи моделі без ковзного вікна (зліва) та з його використанням (справа).

Без використання ковзного вікна (верхній графік):

– аномальні зразки чергуються з нормальними;

– на ділянках аномалій можуть зустрічатися випадкові нормальні точки, що знижує показники продуктивності детектора.

З використанням ковзного вікна (середній графік):

– аномалії відображаються як безперервні області, що покращує стабільність роботи моделі.

– фактична аномалія (нижній графік) демонструє, що модель точно ідентифікує аномальні ділянки, використовуючи ковзне вікно.

3.1.4 Валідація класифікатора аномалій у IIoT

Для оцінки ефективності класифікатора аномалій у IIoT було використано метод перехресної валідації. Основною метою цієї методики є перевірка здатності моделі коректно працювати з новими, раніше невідомими даними.

Перехресна валідація передбачає розбиття даних на кілька підмножин,

навчання моделі на частині даних та перевірку її роботи на іншій частині. У класичному випадку набір даних ділиться на однакові за розміром підмножини. Однак у цьому дослідженні дані зберігалися у 15 окремих CSV-файлах, кожен із яких містив різні типи відмов та атак.

Результати перехресної валідації наведено у таблиці 3.4.

Таблиця 3.4 – Перехресна валідація класифікатора аномалій у IIoT

Файл	Тип аномалії	Precision	Recall	F1-міра
edge1_11.csv	F1, F2	0.96	0.82	0.89
edge1_12.csv	F1, F1	1.00	0.80	0.89
edge1_13.csv	F2, F2	0.81	0.92	0.86
edge1_14.csv	A2	0.90	0.74	0.81
edge2_9.csv	F2, F1	0.89	0.97	0.93
edge2_10.csv	F1, F1	0.99	0.75	0.85
edge2_11.csv	F2	1.00	1.00	1.00
edge2_12.csv	A2, A1, A1, A1, A1	0.91	0.88	0.89
edge3_8.csv	F1, F2	0.97	0.99	0.98
edge3_9.csv	F1, F1	1.00	0.81	0.90
edge3_10.csv	F2	1.00	1.00	1.00
edge3_12.csv	A2, A1, A1, A1, A1	0.97	0.85	0.91
edge4_10.csv	F1	0.88	1.00	0.94
edge4_11.csv	F1, F2	1.00	0.93	0.96
edge4_12.csv	A2, A2	1.00	0.72	0.84
Середнє значення	-	0.95	0.88	0.91

Основні показники продуктивності:

Середня точність (precision) = 0.952. Це означає, що система дуже рідко генерує хибнопозитивні (FP) спрацьовування. FP-спрацьовування зазвичай пов’язані з тим, що ефекти аномалії продовжуються після того, як першопричина вже усунена.

Середня повнота (recall) = 0.878. Вищий рівень хибнонегативних (FN)

спрацьовувань, ніж хибнопозитивних. FN-помилки виникають у початковій фазі аномалії, коли система ще не адаптувалася до змін. Деякі FN також з'являються у середині аномалії, коли окремі зразки помилково позначаються як нормальні.

Середня F1-міра = 0.91. Висока F1-міра свідчить про баланс між precision та recall, що вказує на загальну ефективність моделі.

Додатково було розраховано окремі значення precision, recall та F1-міри для різних типів аномалій:

Для атак: precision = 0.945, recall = 0.797, F1-міра = 0.862.

Для відмов обладнання: precision = 0.954, recall = 0.908, F1-міра = 0.927.

Це свідчить про те, що система точніше виявляє відмови, ніж атаки.

На рисунку 3.4 представлено графічне відображення результатів перехресної валідації для пристрою edge1.

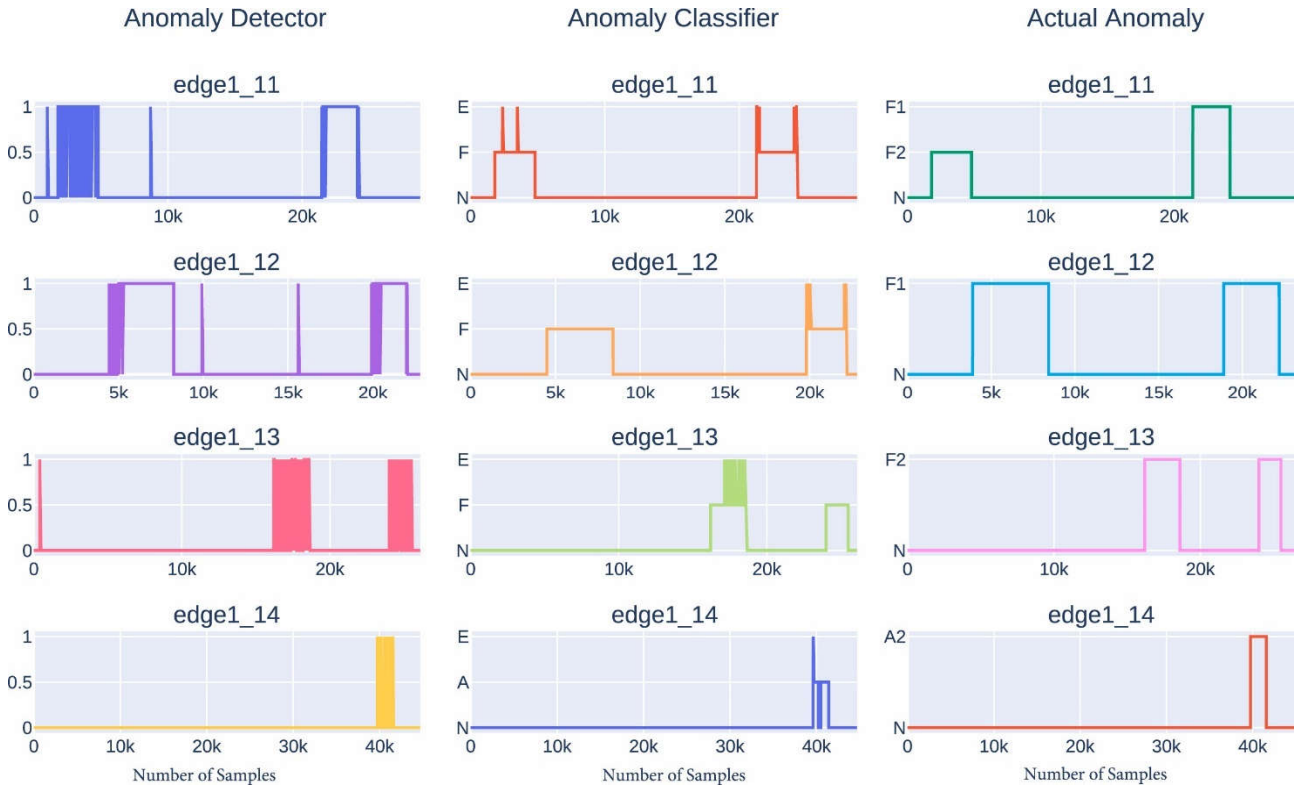

Рисунок 3.4 – графічне відображення результатів перехресної валідації для пристрою edge1

Всі аномалії були виявлені, хоча в деяких випадках невелика кількість зразків була позначена як події. У наборі даних edge1_13 кількість помилково класифікованих подій дещо збільшилася. Після аналізу 15 послідовних зразків у ковзному вікні (3 секунди), класифікатор усуває хибнопозитивні спрацьовування,

які не пов’язані з реальними аномаліями. Графіки справа відображають фактичні аномалії, що дозволяє порівняти коректність класифікації.

На рисунку 3.5 показано, як різниця між оригінальними та реконструйованими сигналами перевищує порогове значення (пунктирна лінія) під час відмови через підвищення температури в процесорі пристрою edge. Таким чином, користувач може перевірити, які вхідні дані впливають на виявлення аномалій автоенкодером.

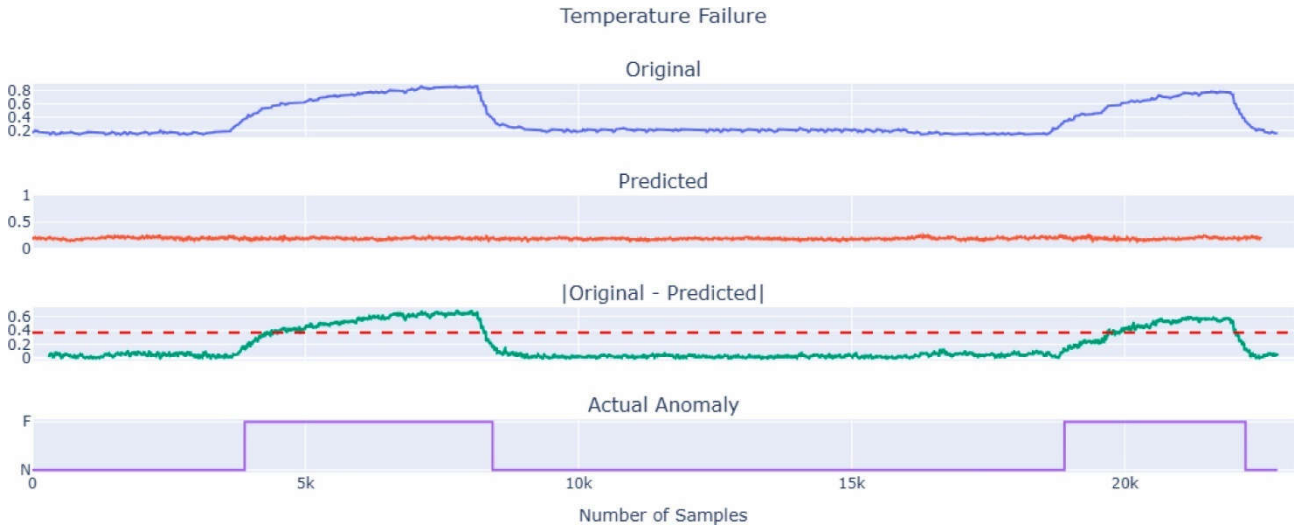

Рисунок 3.5 – Графічна інтерпретація моделі

3.1.5 Порівняння з іншими моделями

Для порівняння продуктивності з реалізованими в рамках класифікації аномалій були навчені нові моделі виявлення та класифікації аномалій на основі шарів LSTM. Автоенкодер було реалізовано з використанням LSTM у поєднанні з шарами випадкового відключення як для енкодера, так і для декодера. Вихід обгорнуто шаром TimeDistributed, який застосовує щільний шар до кожного тимчасового кроку вхідного тензора окремо. LSTM є типом рекурентної нейронної мережі (RNN), яка ідеально підходить для обробки послідовних даних, таких як часові ряди, завдяки своїй спеціалізованій архітектурі, яка особливо ефективна для захоплення довгострокових залежностей у послідовних даних. Енкодер LSTM відповідає за стиснення вхідної послідовності у вектор фіксованого розміру, який представляє основні характеристики вхідних даних. У той же час декодер намагається реконструювати оригінальну вхідну послідовність. Шар TimeDistributed обгортає інший шар, наприклад, щільний шар, і застосовує його до

кожного тимчасового кроку вхідного тензора незалежно. Це означає, що для кожного тимчасового кроку використовуються ті самі ваги шару, але операція виконується окремо для кожного зрізу.

Класифікатор аномалій використовує шари LSTM, що чергуються з шарами випадкового відключення, щоб зменшити ризик перенавчання, та обгортання щільного шару за допомогою TimeDistributed. Мережа LSTM складається з серії блоків LSTM, кожен з яких відповідає за підтримку комірки пам'яті, яка може зберігати інформацію протягом тимчасових кроків. У таблиці 3.5 показано здатність кожної моделі уникати хибнонегативних (recall) та хибнопозитивних (precision) результатів, а також гармонійне середнє обох показників (F1). Хоча моделі на основі LSTM також показали хороші результати, автоенкодер на основі згорткової нейронної мережі є найкращим детектором, тоді як класифікатор на основі трансформера демонструє найкращі результати за всіма трьома метриками.

Таблиця 3.5 – Порівняння між моделями детектора та класифікатора аномалій

Блок	Модель	Точність	Повнота	F1-міра
Детектор	Conv1d	0.973610	0.913190	0.942433
	LSTM	0.962211	0.870235	0.913915
Класифікатор	Трансформер	0.893578	0.944319	0.918198
	LSTM	0.880367	0.894792	0.887471

Автоенкодер на основі Conv1d та класифікатор на основі трансформера показують кращі показники точності, повноти та F1-міри.

3.1.6 Валідація моделі з новими аномаліями

У попередньому параграфі було детально проаналізовано результати перехресної валідації. Запропонована система успішно ідентифікувала всі аномалії і не створювала хибнопозитивних спрацьовувань, які могли б викликати помилкові тривоги для неіснуючих аномалій. У цьому параграфі розглянуто ефективність класифікатора у виявленні нових типів аномалій, які не входили до навчального

набору даних.

Для оцінки продуктивності моделі було використано два файли, що містять відмови через відключення датчика (F3). Аномалії типу F3 були виявлені детектором, що свідчить про ефективну роботу алгоритму аномального виявлення. Однак класифікатор відніс ці аномалії до "звичайних подій" (events), а не до відмов. Як наслідок, система згенерувала сигнал для оператора, який мав вручну перевірити природу аномалії.

Хоча цей результат не є ідеальним, він свідчить про те, що система все ж таки успішно виявляє виникнення нової аномалії, навіть якщо не може її правильно класифікувати без попереднього навчання.

На рисунку 3.6 представлено графічну валідацію моделі з новими даними. Як видно, аномалії F3 були розпізнані, але класифіковані як "події" (E), а не як відмови (F).

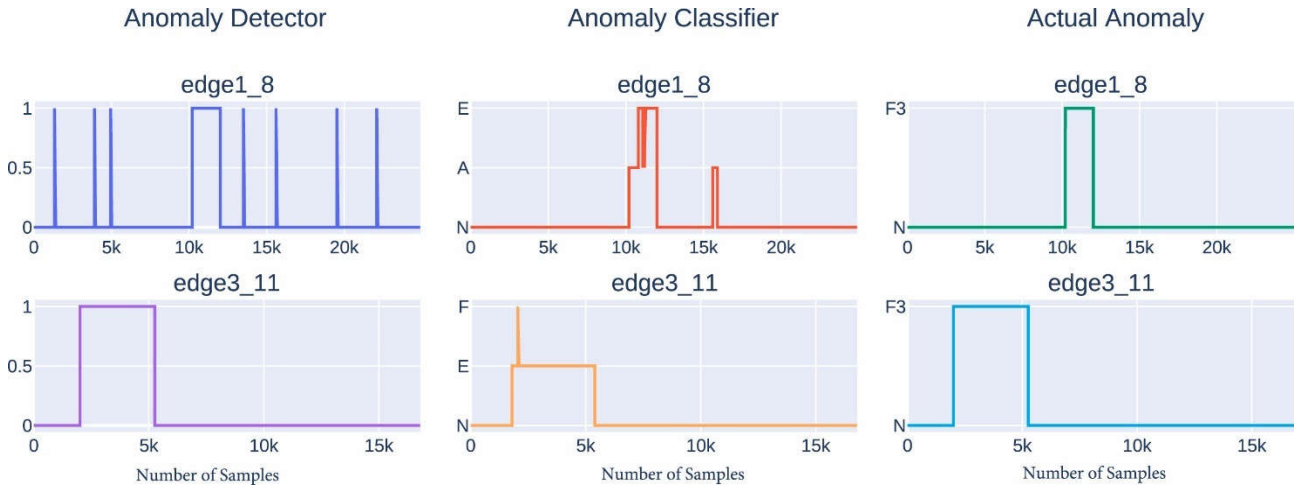

Рисунок 3.6 – Перевірка моделі з новими даними

3.2 Розгортання класифікатора аномалій IIoT у тестовому середовищі

Щоб забезпечити своєчасне виявлення аномалій, класифікатор рекомендується запускати безпосередньо на кожному периферійному пристрої. У цьому параграфі розглянуто результати розгортання системи в тестовому середовищі. Для зменшення навантаження на обчислювальні ресурси було використано функцію TFLiteConverter із бібліотеки TensorFlow, яка дозволяє створювати легковагові версії моделей детектора та класифікатора. Отримані

полегшені моделі були розгорнуті та запущені на пристрої Raspberry Pi 3, що дозволило мінімізувати витрати на обчислення.

Перевірка працездатності моделі здійснювалася на тому ж наборі даних, що використовувався для її навчання. Метою тестування було визначення ефективності роботи класифікатора та детектора аномалій у спрощеній версії, запущеній безпосередньо на периферійному пристрої.

На рисунку 3.7 показано оцінку роботи класифікатора аномалій у тестовому середовищі.

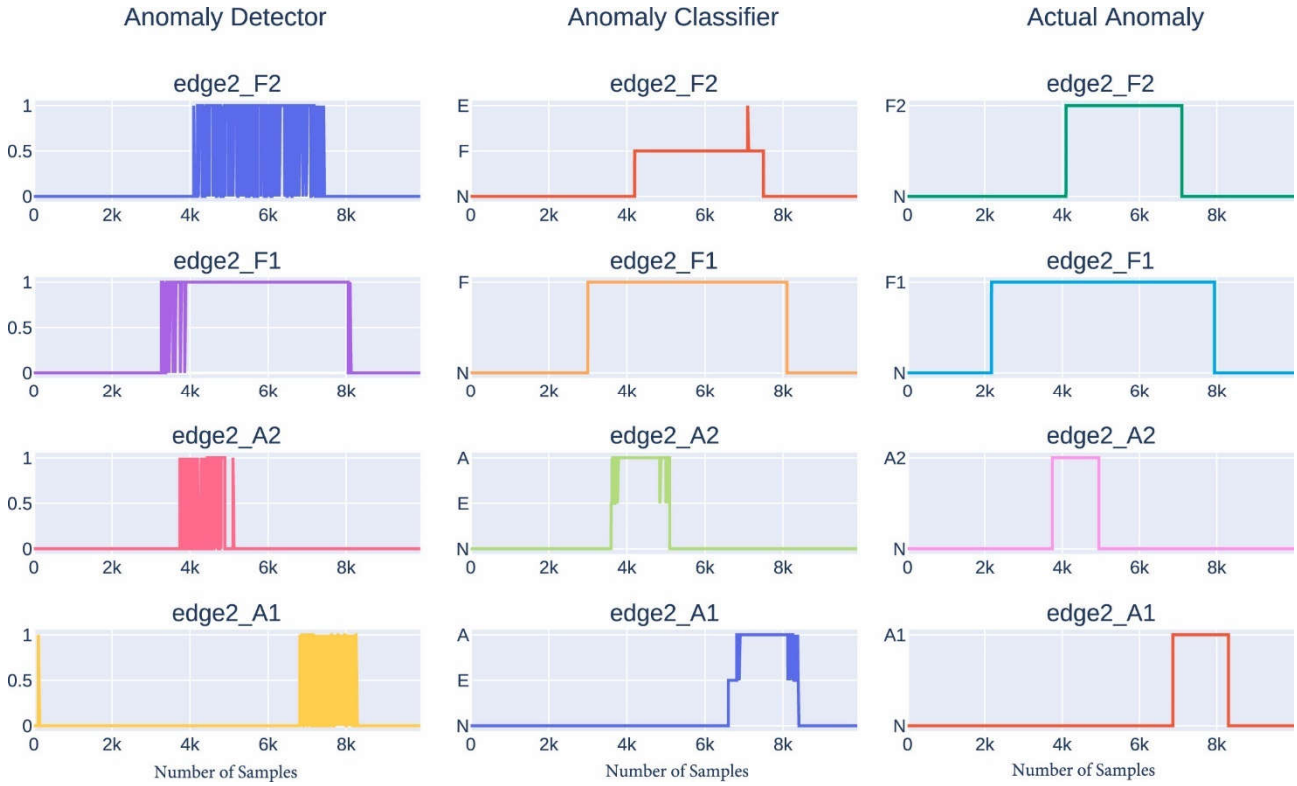

Рисунок 3.7 – Оцінка класифікатора аномалій IIoT у тестовому стенді

Детектор аномалій позначає кожен зразок як нормальний (0) або аномальний (1).

Класифікатор аномалій призначає зразкам одну з категорій:

N – нормальний стан;

E – подія (не визначена аномалія);

F – відмова;

A – атака.

У ході експерименту було оцінено здатність моделі розпізнавати різні типи аномалій. Як показано на рисунку 3.7, жодного разу не було зафіксовано

хибнопозитивних спрацьовувань, що могли б викликати непотрібні сигнали тривоги. У деяких випадках окремі зразки були класифіковані як "події", що означає, що детектор позначив їх як аномалії, а класифікатор визначив, що ці аномалії не є точними відмовами чи атаками. Проте кількість таких випадків була мінімальною у порівнянні з правильно класифікованими аномаліями, тому оператор міг легко визначити природу виявлених порушень.

На графіку, що ілюструє роботу моделі з набором даних edge2_F1, спостерігається затримка у виявленні аномалії. Система почала фіксувати проблему лише після приблизно 3000-го зразка, хоча фактична аномалія розпочалася ближче до 2000-го зразка. Це явище було передбачуваним, оскільки подібна поведінка спостерігалася і в попередніх тестах із виявленням перегріву процесора (аномалія F1).

Щоб оцінити якість роботи моделей, було розраховано показники точності, повноти та F1-міри. Як показано в таблиці 3.6, середнє значення F1-міри становило 0.90, що вказує на баланс між точністю та здатністю системи виявляти справжні аномалії. Виявлено, що система дещо краще ідентифікує відмови обладнання, ніж атаки, що узгоджується з результатами попередніх експериментів.

Таблиця 3.6 – Оцінка класифікатора аномалій IIoT у тестовому стенді

Файл	Тип аномалії	Точність	Повнота	F1-міра
edge2_F2	Неправильне налаштування (F2)	0.88	0.97	0.92
edge2_F1	Відмова через температуру (F1)	1.00	0.84	0.91
edge2_A1	Атака ін'єкції даних (A1)	0.86	0.93	0.89
edge2_A2	DoS-атака (A2)	0.91	0.88	0.89
Середнє значення	-	0.91	0.90	0.90

Оцінка швидкості виконання моделей на пристрої Raspberry Pi 3.

Для аналізу продуктивності було виміряно розмір файлів із моделями у спрощеному форматі та середній час виконання одного передбачення для послідовності з 300 зразків. Як показано в таблиці 3.7, розміри моделей є досить малими, а час виконання – мінімальним.

Таблиця 3.7 – Час виконання моделей на стенді для послідовності 300 зразків

Модель	Розмір (кБ)	Час виконання (с)
Детектор (автоенкодер)	361 кБ	0.06799 с
Класифікатор (трансформер)	116 кБ	0.074955 с

Отримані результати підтверджують, що навіть на малопотужному периферійному пристрої моделі працюють достатньо швидко для використання в реальних промислових умовах.

ВИСНОВКИ

1. У процесі дослідження предметної області встановлено, що IIoT є технологічною концепцією, що інтегрує сенсорні пристрої, кіберфізичні системи, мережеві технології та аналітичні платформи для забезпечення безперервного моніторингу та автоматизації виробничих процесів. Визначено, що головною проблемою є своєчасне виявлення аномалій, які можуть бути спричинені технічними несправностями або кібератаками.

2. Виконаний аналіз відомих рішень показав, що сучасні підходи до виявлення аномалій у IIoT базуються на машинному навчанні та глибоких нейронних мережах. Встановлено, що більшість сучасних методів мають низьку універсальність, оскільки вони адаптовані до конкретних типів виробничого обладнання та не враховують контекстні зміни у виробничих процесах. Крім того, методи виявлення аномалій часто страждають від високої кількості хибнопозитивних спрацьовувань та обмеженої здатності розрізняти технічні несправності від кібератак.

3. Враховуючи виявлені недоліки існуючих рішень, сформульовано основну задачу дослідження – розробку ефективного та адаптивного підходу для виявлення та класифікації аномалій у промислових системах IIoT. Такий підхід має поєднувати методи автоенкодерів для виявлення нових типів аномалій, трансформерні моделі для класифікації, а також використання периферійних обчислень для зниження затримок у виявленні.

4. У процесі проектування було розроблено трирівневу модель IIoT для класифікації аномалій у промислових системах. Вона складається з рівня сприйняття, мережевого рівня та рівня застосування. Така архітектура дозволяє ефективно збирати дані з фізичних пристроїв, передавати їх через надійні комунікаційні протоколи та обробляти в хмарному середовищі. Використання периферійних пристроїв та мікроконтролерів для попередньої обробки даних сприяє зменшенню затримок і підвищенню швидкості реакції на виявлення аномалій у режимі реального часу.

5. Створено детальний набір даних, що включає нормальні та аномальні

випадки, змодельовані у тестовому середовищі. До нього увійшли дані про несправності обладнання та кібератаки. Проведено комплексну обробку даних, яка включала синхронізацію часових міток, нормалізацію, балансування класів, обробку відсутніх значень та вибір ключових ознак. Використання методів мін-макс нормалізації, дельта-значень для часових рядів та кореляційного аналізу дозволило значно покращити якість вхідних даних для моделювання.

6. Запропоновано дворівневу систему детекції та класифікації аномалій, що складається з автокодера для первинного виявлення аномальних ситуацій та класифікатора на основі трансформерної нейронної мережі. Автокодер дозволяє виявляти відхилення у нормальній поведінці системи, використовуючи помилку реконструкції, а модель Transformer ефективно класифікує тип аномалії (технічна несправність чи кібератака). Використання цих підходів дозволило досягти високої точності класифікації, а оптимізація структури мережі та правильний вибір ключових ознак сприяли зниженню рівня хибнопозитивних результатів та покращенню ефективності роботи системи у промислових умовах.

7. Запропонований підхід, що поєднує детектор аномалій на основі автоенкодера та класифікатор на основі трансформерної моделі, продемонстрував високу точність у розпізнаванні аномальних подій. Зокрема, використання контекстної інформації та застосування ковзного вікна дозволило підвищити точність і зменшити кількість хибнопозитивних та хибнонегативних спрацьовувань. В середньому, F1-міра класифікації аномалій досягла 0.91, що свідчить про баланс між точністю та повнотою.

8. Перевірка продуктивності класифікатора на тестовому стенді показала можливість його використання у реальних промислових умовах. Оптимізовані моделі, що були конвертовані у формат TensorFlow Lite, успішно працювали на периферійних пристроях Raspberry Pi 3 із мінімальними обчислювальними витратами. Час виконання одного передбачення для послідовності з 300 зразків не перевищував 0.075 секунди, що забезпечує можливість реального часу моніторингу та швидкого реагування на аномальні події.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дугінець Г. В. Концепція "Інтернет речей" у глобальному виробництві: досвід для України. *Економіка і регіон*. 2018. №3 1. С. 127-133.
2. Шматковська Т. О., Стащук О. В., Дзямулич М. І. Великі дані та бізнес-моделювання економічних систем. *Ефективна економіка*. 2021. №5. URL: http://www.economy.nayka.com.ua/?op=1&z=8906.
3. Дзямулич М.І. Фадєєва І. Г. Шматковська Т.О. Промисловий Інтернет речей та його застосування у бізнес-процесах. *Економічний форум*. 2021. № 1(3). С.54-59.
4. Benaddi, H., Jouhari, M., Ibrahimi, K., Ben Othman, J., Amhoud, E.M. Anomaly detection in industrial iot using distributional reinforcement learning and generative adversarial networks. Sensors. 2022. Vol. 22. Article 8085.
5. Berger, X. Rpi monitor. 2022. https://github.com/XavierBerger/RPi-Monitor.
6. Byabazaire, J., O'Hare, G., Delaney, D. Data quality and trust: Review of challenges and opportunities for data sharing in iot. Electronics. 2020. Vol. 9. Article 2083.
7. Saez-de Camara, X., Flores, J.L., Arellano, C., Urbieta, A., Zurutuza, U. Clustered federated learning architecture for network anomaly detection in large scale heterogeneous iot networks. Computers & Security. 2023. Vol. 131. Article 103299.
8. Chevrot, A., Vernotte, A., Legeard, B. Cae: Contextual auto-encoder for multivariate time-series anomaly detection in air transportation. Computers & Security. 2022. Vol. 116. Article 102652.
9. Cui, L., Dong, Z., Xu, H., Zhao, D. Triplet attention-enhanced residual tree-inspired decision network: A hierarchical fault diagnosis model for unbalanced bearing datasets. Advanced Engineering Informatics. 2024. Vol. 59. Article 102322.
10. Ding, C., Zhao, J., Sun, S. Concept drift adaptation for time series anomaly detection via transformer. Neural Processing Letters. 2023. Vol. 55. Pp. 2081–2101.
11. Du, G., Zhang, J., Zhang, N., Wu, H., Wu, P., Li, S. Semi-supervised imbalanced multi-label classification with label propagation. Pattern Recognition. 2024. Article 110358.

12. Fang, Y., Yao, Y., Lin, X., Wang, J., Zhai, H. A feature selection based on genetic algorithm for intrusion detection of industrial control systems. Computers & Security. 2024. Vol. 139. Article 103675.

13. Ganjkhani, M., Gilanifar, M., Giraldo, J., Parvania, M. Integrated cyber and physical anomaly location and classification in power distribution systems. IEEE Transactions on Industrial Informatics. 2021. Vol. 17. Pp. 7040–7049.

14. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., Bengio, Y. Generative adversarial networks. Communications of the ACM. 2020. Vol. 63. Pp. 139–144.

15. Jiang, R., Xue, Y., Zou, D. Interpretability-aware industrial anomaly detection using autoencoders. IEEE Access. 2023. Vol. 11. Pp. 60490–60500.

16. Jithish, J., Alangot, B., Mahalingam, N., Yeo, K.S. Distributed anomaly detection in smart grids: a federated learning-based approach. IEEE Access. 2023. Vol. 11. Pp. 7157–7179.

17. Karkouch, A., Mousannif, H., Al Moatassime, H., Noel, T. Data quality in internet of things: A state-of-the-art survey. Journal of Network and Computer Applications. 2016. Vol. 73. Pp. 57–81.

18. Kim, J., Kang, H., Kang, P. Time-series anomaly detection with stacked transformer representations and 1d convolutional network. Engineering Applications of Artificial Intelligence. 2023. Vol. 120. Article 105964.

19. Ko, J.U., Na, K., Oh, J.S., Kim, J., Youn, B.D. A new auto-encoder-based dynamic threshold to reduce false alarm rate for anomaly detection of steam turbines. Expert Systems with Applications. 2022. Vol. 189. Article 116094.

20. Li, J., Othman, M.S., Chen, H., Yusuf, L.M. Optimizing iot intrusion detection system: feature selection versus feature extraction in machine learning. Journal of Big Data. 2024. Vol. 11. Article 36.

21. Li, Y., Peng, X., Zhang, J., Li, Z., Wen, M. Dct-gan: dilated convolutional transformer-based gan for time series anomaly detection. IEEE Transactions on Knowledge and Data Engineering. 2021. Vol. 35. Pp. 3632–3644.

22. Liang, L., Liu, S. Event-triggered distributed attack detection and fault diagnosis. IEEE Transactions on Instrumentation and Measurement. 2022. Vol. 72. Pp.

1–11.

23. Linardatos, P., Papastefanopoulos, V., Kotsiantis, S. Explainable ai: A review of machine learning interpretability methods. Entropy. 2020. Vol. 23. Article 18.

24. Liu, X., Du, Y. Towards effective feature selection for iot botnet attack detection using a genetic algorithm. Electronics. 2023. Vol. 12. Article 1260.

25. Mane, D., Magar, A., Khode, O., Koli, S., Bhat, K., Korade, P. Unlocking machine learning model decisions: A comparative analysis of lime and shap for enhanced interpretability. Journal of Electrical Systems. 2024. Vol. 20. Pp. 1252–1267.

26. Mantha, A.A., Hussain, A., Ravikumar, G. Hil testbed-based auto feature extraction and data generation framework for ml/dl-based anomaly detection and classification. IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). 2024. Pp. 1–5.

27. de Matos, E., Tiburski, R.T., Moratelli, C.R., Johann Filho, S., Amaral, L.A., Ramachandran, G., Krishnamachari, B., Hessel, F. Context information sharing for the internet of things: A survey. Computer Networks. 2020. Vol. 166. Article 106988.

28. Mazarbhuiya, F.A., Shenify, M. A mixed clustering approach for real-time anomaly detection. Applied Sciences. 2023. Vol. 13. Article 4151.

29. Mirani, A.A., Velasco-Hernandez, G., Awasthi, A., Walsh, J. Key challenges and emerging technologies in industrial iot architectures: A review. Sensors. 2022. Vol. 22. Article 5836.

30. Mooijman, P., Catal, C., Tekinerdogan, B., Lommen, A., Blokland, M. The effects of data balancing approaches: A case study. Applied Soft Computing. 2023. Vol. 132. Article 109853.

31. Niu, Z., Guo, W., Xue, J., Wang, Y., Kong, Z., Huang, L. A novel anomaly detection approach based on ensemble semi-supervised active learning (adessa). Computers & Security. 2023. Vol. 129. Article 103190.

32. Nizam, H., Zafar, S., Lv, Z., Wang, F., Hu, X. Real-time deep anomaly detection framework for multivariate time-series data in industrial iot. IEEE Sensors Journal. 2022. Vol. 22. Pp. 22836–22849.

33. Prasad, D., Hampapura Sripada, S. Neural network-based anomaly detection models and interpretability methods for multivariate time series data. 2023.

34. Qiu, T., Chi, J., Zhou, X., Ning, Z., Atiquzzaman, M., Wu, D.O. Edge computing in industrial internet of things: Architecture, advances and challenges. IEEE Communications Surveys & Tutorials. 2020. Vol. 22. Pp. 2462–2488.

35. Rodríguez, M., Tobón, D.P., Múnera, D. Anomaly classification in industrial internet of things: A review. Intelligent Systems with Applications. 2023. Article 200232.

36. Ryalat, M., ElMoaqet, H., AlFaouri, M. Design of a smart factory based on cyber-physical systems and internet of things towards industry 4.0. Applied Sciences. 2023. Vol. 13. Article 2156.

37. Shafiq, M., Tian, Z., Bashir, A.K., Du, X., Guizani, M. Corrauc: A malicious bot-iot traffic detection method in iot network using machine-learning techniques. IEEE Internet of Things Journal. 2020. Vol. 8. Pp. 3242–3254.

38. Андріанов Ю.В., Кочан В.В. Класифікації аномалій у промислових системах Інтернету Речей. Інтелектуальні інформаційні технології в прикладних дослідженнях : тези доп. студентської наук.-практ. конф. (м. Тернопіль, 27–29 травня 2025 р.). Тернопіль, 2025. С. 268-271.

39. 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.

40. Комар М.П., Саченко А.О., Васильків Н.М., Гладій Г.М., Коваль В.С., Ліп’яніна-Гончаренко Х.В. Методичні рекомендації до виконання кваліфікаційної роботи з освітньо-професійної програми «Комп’ютерні науки» спеціальності 122 «Комп’ютерні науки» за першим (бакалаврським) рівнем вищої освіти. Тернопіль: ЗУНУ, 2024. 52 с.

Додаток А

Апробація результатів роботи

Західноукраїнський національний університет

Факультет комп’ютерних інформаційних технологій

Кафедра інформаційно-обчислювальних систем і управління

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

Студентської науково-практичної конференції

ІНТЕЛЕКТУАЛЬНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ПРИКЛАДНИХ ДОСЛІДЖЕННЯХ

(IITAR-2025)

27-29 травня 2025 року

Тернопіль

2025

Збірник тез доповідей студентської науково-практичної конференції «Інтелектуальні інформаційні технології в прикладних дослідженнях» (IITAR-2025). (Тернопіль, 27-29 травня 2025 року). Тернопіль: ЗУНУ, 2025. 372 с.

До збірника увійшли тези доповідей учасників студентської науково-практичної конференції “Інтелектуальні інформаційні технології в прикладних дослідженнях” (IITAR – 2025), що відбувалась у рамках AI Week на базі кафедри інформаційно-обчислювальних систем і управління Західноукраїнського національного університету. Мета конференції — об’єднати науковців, освітян, представників IT-бізнесу та здобувачів освіти для обміну досвідом, презентації сучасних досліджень і впровадження інноваційних рішень у сфері комп’ютерних наук, штучного інтелекту та суміжних галузей.

За зміст наукових праць та достовірність наведених фактологічних і статистичних матеріалів відповідальність несуть автори публікацій та їхні наукові керівники. У збірнику зберігається стилістика та орфографія авторів матеріалів.

Склад організаційного комітету конференції

Керівництво оргкомітету

Мирослав Комар, д.т.н., професор, професор кафедри інформаційно-обчислювальних систем і управління

Христина Ліп’яніна-Гончаренко, д.т.н., доцент, доцент кафедри інформаційно-обчислювальних систем і управління

Надія Васильків, к.т.н., в.о. завідувача кафедри інформаційно-обчислювальних систем і управління

Члени програмного комітету

Василь Коваль, к.т.н., доцент, доцент кафедри інформаційно-обчислювальних систем і управління, заступник декана факультету комп’ютерних інформаційних технологій

Олександр Осолінський, к.т.н., доцент, доцент кафедри інформаційно-обчислювальних систем і управління

Павло Биковий, к.т.н., доцент, доцент кафедри інформаційно-обчислювальних систем і управління

Діана Загородня, к.т.н., доцент, доцент кафедри інформаційно-обчислювальних систем і управління

Ігор Майків, к.т.н., доцент кафедри інформаційно-обчислювальних систем і управління

Члени оргкомітету

Андрій Івасечко, викладач кафедри інформаційно-обчислювальних систем і управління

Дмитро Дюг, викладач кафедри інформаційно-обчислювальних систем і управління

Христина Юрків, студентка ФКІТ ЗУНУ, технік лабораторії з проблем інформаційних технологій

Мар’яна Соя, студентка ФКІТ ЗУНУ, лаборант кафедри інформаційно-обчислювальних систем і управління

Микола Телька, студент ФКІТ ЗУНУ, лаборант кафедри інформаційно-обчислювальних систем і управління, студентський декан факультету комп’ютерних інформаційних технологій

Секція 3. AIoT (Штучний інтелект речей)

Андріанов Юрій
студент групи КН-42
andrianov.yuriy.new@gmail.com
Кочан Володимир
к.т.н., професор
vk@wunu.edu.ua
Західноукраїнський національний університет
Тернопіль, Україна

КЛАСИФІКАЦІЇ АНОМАЛІЙ У ПРОМИСЛОВИХ СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ

Швидка еволюція промислового Інтернету речей (IIoT) та його інтеграція з кіберфізичними системами (CPS) проклали шлях до появи розумних фабрик [1]. Ці сучасні виробничі середовища використовують цифрові технології для підвищення операційної ефективності, продуктивності та гнучкості [2]. Однак складність і взаємопов'язаність цих систем створює значні виклики у моніторингу та забезпеченні безпеки промислових процесів [3].

Одним з головних завдань у цьому середовищі є виявлення і класифікація аномалій, серед яких: технічні збої, помилки сенсорів і кібератаки. Існуючі методи мають обмежену здатність до диференціації типів аномалій, що призводить до хибних спрацювань або втрати даних.

Тому актуально розробити ефективний, масштабований та адаптивний підхід до виявлення та класифікації аномалій, який забезпечить високу точність і мінімальну кількість помилок. Запропоноване рішення базується на поєднанні глибоких нейронних мереж, автоенкодерів для детекції аномалій і трансформерних моделей для їх класифікації.

Розглянемо етапи побудови системи виявлення та класифікації аномалій у промислових IIoT-середовищах:

1. Збір даних. Для збору даних можуть використовуватись різні способи. Найпростіший спосіб – використовувати вже готові набори даних, які доступні у відкритих онлайн-джерелах. Це швидкий та недорогий варіант. Інший спосіб – використовувати спеціальні програми, які можуть імітувати збої та атаки, що реально можуть виникнути у IIoT. Завдяки цьому можна отримати багато прикладів аномалій для подальшого аналізу. Однак створення повноцінної комп'ютерної моделі (симуляції) реальної IIoT-системи з усіма деталями може бути складною задачею. Також можна використовувати історичні дані про роботу виробничої системи, але таких даних часто недостатньо, і вони можуть не охоплювати всі типи збоїв, які нас цікавлять. Ще один метод – використання генеративних нейронних мереж. Це штучний інтелект, який вміє створювати нові, штучні дані, схожі на реальні. Але щоб навчити такі моделі, потрібно мати

багато вихідних даних. Найбільш прямий спосіб – це створювати збої та атаки прямо на реальній системі IIoT, але це дуже ризиковано, бо може завдати шкоди виробничому процесу. Тому більш безпечний варіант – створити спеціальний тестовий стенд (тестове середовище), який буде дуже схожим на справжню систему, та вже на ньому безпечно імітувати різні збої та атаки. Якщо є додаткове обладнання, це може бути також економним рішенням.

2. Розумна фабрика. У цьому випадку «розумна фабрика» означає підприємство, де CPS інтегровані з IIoT. CPS – це автоматизоване виробництво, яке управляється за допомогою спеціального програмного забезпечення (наприклад, SCADA) і пристроїв, які називаються програмованими логічними контролерами. CPS є центральною частиною роботи виробництва [2]. Система IIoT встановлюється для того, щоб через Інтернет і хмарні технології контролювати і покращувати роботу CPS. Перший важливий крок у цьому фреймворку – це вивчити, як працюють вже встановлені на виробництві CPS та IIoT-системи. Це необхідно, щоб ті, хто створює систему для виявлення аномалій, добре розуміли архітектуру IIoT, всі її рівні, можливості, правила взаємодії (протоколи), заходи безпеки, а також типи даних, які вона отримує та обробляє.

3. Збої та атаки. Перед тим, як збирати дані, потрібно чітко визначити, від яких саме атак та збоїв необхідно захищати IIoT-систему. Це означає, що потрібно скласти список можливих проблем і вирішити, які з них важливі, а які можна не враховувати. Деякі атаки можуть бути дуже малоймовірними, а деякі – надто складними або дорогими для вирішення. Інколи простіше скористатися альтернативними варіантами, наприклад, придбати страховий поліс.

4. Контекстна інформація. Це важливий аспект для будь-яких систем, особливо у промисловості. Простими словами, контекстна інформація – це додаткові дані з різних джерел, які допомагають краще зрозуміти умови роботи системи і надати послуги, що відповідають конкретним потребам і очікуванням користувача [4]. Наприклад, важливо визначити параметри, які можуть змінюватися в залежності від особливостей конкретного виробничого процесу, і це допоможе краще класифікувати аномалії в IIoT.

5. Обробка даних. Це перетворення сирих, неструктурованих даних у зручний формат для подальшого аналізу. Завдяки цьому забезпечується висока якість, однорідність і точність аналізу даних, що робить їх зручними для застосування моделей машинного навчання [2]. На цьому етапі відбувається об'єднання даних з кількох джерел, заповнення пропущених значень, масштабування, видалення повторів, перетворення текстових даних у числовий формат, нормалізація та виявлення аномально великих або малих значень (викидів) [2].

6. Зменшення кількості ознак. Це процес вибору тільки тих ознак (характеристик), які дійсно впливають на результат аналізу. Зайві ознаки створюють зайве навантаження на комп'ютер і можуть погіршити точність аналізу [2]. Для цього використовують різні підходи, наприклад, аналіз даних для виявлення важливості змінних. Методи зменшення розмірності поділяють на

два типи: витягування нових ознак, коли вихідні ознаки перетворюють на меншу кількість нових [2], і вибір найважливіших ознак, які найкраще допомагають у класифікації.

7. Балансування даних. Якщо даних одного типу дуже мало, а іншого – багато, виникає дисбаланс, який погіршує якість аналізу. Щоб вирішити цю проблему, використовують різні методи: додають нові штучні дані (генерують їх за допомогою спеціальних моделей), змінюють налаштування класифікаторів або застосовують спеціальні методики врахування помилок [5].

8. Виявлення аномалій. Це процес пошуку незвичайних ситуацій або подій у часових рядах даних, які відрізняються від нормальної поведінки системи [6]. В цьому фреймворку використовується підхід, коли модель навчається тільки на нормальних даних, а потім самостійно визначає будь-які відхилення.

9. Класифікація аномалій. Цей підхід пропонує двоетапний підхід. На першому етапі визначаються аномалії, а на другому – їх класифікують. Якщо система не впевнена, що це саме за аномалія, вона повідомляє про це оператора для додаткової перевірки.

Отже, запропонований підхід поєднує масштабованість, високу точність та реальну здатність до самоадаптації. Це відкриває шлях до створення надійних IIoT-платформ, здатних мінімізувати дороговартісні простої, своєчасно локалізувати технічні збої й ефективно відбивати кібернетичні загрози. Перспективи подальших досліджень полягають у поглибленій персоналізації моделей під конкретні виробничі лінії, а також у розробці легких інкрементних механізмів навчання, що дозволять безперервно оновлювати знання системи в режимі реального часу без зупинки виробництва.

Список використаних джерел

1. Li, J., Othman, M.S., Chen, H., Yusuf, L.M. Optimizing iot intrusion detection system: feature selection versus feature extraction in machine learning. Journal of Big Data. 2024. Vol. 11. 36.
2. Ding, C., Zhao, J., Sun, S. Concept drift adaptation for time series anomaly detection via transformer. 2023. Neural Processing Letters. Vol. 55. Pp. 2081–2101.
3. Saez-de Camara, X., Flores, J.L., Arellano, C., Urbieta, A., Zurutuza, U. Clustered federated learning architecture for network anomaly detection in large scale heterogeneous iot networks. 2023. Computers & Security. Vol. 131. 103299.
4. Liang, L., Liu, S. Event-triggered distributed attack detection and fault diagnosis. IEEE Transactions on Instrumentation and Measurement. 2022. Vol. 72. Pp. 1–11.
5. Mane, D., Magar, A., Khode, O., Koli, S., Bhat, K., Korade, P. Unlocking machine learning model decisions: A comparative analysis of lime and shap for enhanced interpretability. Journal of Electrical Systems. 2024. Vol. 20. Pp. 1252–1267.

6. Cui, L., Dong, Z., Xu, H., Zhao, D. Triplet attention-enhanced residual tree-inspired decision network: A hierarchical fault diagnosis model for unbalanced bearing datasets. Advanced Engineering Informatics. 2024. Vol. 59. Article 102322.