КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.31.1072
УДК 004.89:004.852.5

Чугреєв Кирилл Олександрович
магістр
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID:0009-0005-6951-344X
Ch.kir.lev.2003@gmail.com

Волощук Олена Борисівна
кандидат технічних наук, доцент
Харківський національний університет радіоелектроніки, Харків, Україна
ORCID:0000-0002-5912-4126
Olena.voloshchuk@nure.ua

МЕТОД ПРОГНОЗУВАННЯ ЗБОЇВ ДЛЯ МЕРЕЖ ІНТЕРНЕТУ РЕЧЕЙ ЗА ДОПОМОГОЮ МАШИННОГО НАВЧАННЯ

Анотація. У статті розглядається проблема забезпечення надійності та безперебійного функціонування мереж Інтернету речей, що складаються з великої кількості сенсорних вузлів, шлюзів та розподілених обчислювальних елементів. Через високу гетерогенність пристроїв, швидку змінність топології та неоднорідність потоків даних такі мережі є вразливими до відмов різних типів - апаратних, мережевих та програмних. З огляду на це все більшої актуальності набувають методи прогнозування збоїв, здатні завчасно виявляти ризики дестабілізації системи. Обґрунтовано переваги використання гібридних підходів машинного навчання, що поєднують аналіз часових рядів та оцінку просторової взаємодії між вузлами мережі. Запропоновано метод прогнозування LGFP, побудований на поєднанні графових нейронних мереж (GNN) та архітектури LSTM, що забезпечує комплексну інтерпретацію даних. Метод дозволяє оцінювати ймовірність виникнення відмови на основі поточних і попередніх параметрів телеметрії, враховуючи взаємовплив елементів мережі. Проведено аналіз існуючих підходів, виконано порівняння моделей машинного навчання, а також описано процес формування вибірки для дослідження. Особливу увагу приділено проблемі балансування класів та фільтрації шумових структур у даних, що є критично важливими етапами для підвищення точності прогнозування. Отримані експериментальні результати демонструють перевагу запропонованого методу порівняно з традиційними моделями, такими як Random Forest, SVM та ізольовані LSTM-архітектури, що підтверджується підвищенням точності класифікації та F1-міри. Практичне застосування запропонованого підходу може забезпечити істотне підвищення стійкості IoT-систем у промислових, енергетичних та побутових умовах. Перспективи подальших досліджень включають розширення простору ознак, інтеграцію механізмів уваги для покращення інтерпретованості моделі та апробацію методу в реальних промислових умовах

Ключові слова: інтернет речей; машинне навчання; lstm; gnn; прогнозування збоїв; алгоритм; IoT; метрики.

ВСТУП

Постановка проблеми. Стрімке зростання кількості підключених пристроїв у мережах Інтернету речей призводить до збільшення навантаження на інфраструктуру, ускладнює керування розподіленими сенсорними вузлами та підвищує ймовірність виникнення відмов різного характеру. [1; 4; 11] У таких системах одночасно функціонують тисячі мікроконтролерів, що передають дані через різні протоколи та

мережеві шари, а будь-який локальний збій може спричинити каскадне поширення відмов.

Стан досліджень у цій галузі демонструє значний прогрес у використанні алгоритмів штучного інтелекту для обробки телеметрії, проте недостатньо уваги приділяється взаємодії між мережею як структурою та часовими закономірностями зміни параметрів. Переважна частина моделей аналізує пристрої ізольовано, ігноруючи міжвузлові залежності, що відіграють важливу роль у поширенні збоїв. [8; 11] Деякі дослідження застосовують графові нейронні мережі для аналізу IoT як структури, але ізольовано від часових залежностей, що обмежує точність прогнозу [8]. Значна кількість робіт фокусується на прогнозуванні відмов за часовими рядами та використанні LSTM чи подібних підходів [6; 7; 9; 10; 13], проте часто без урахування просторових взаємозв'язків.

Саме тому постає задача у створенні методу прогнозування відмов, який поєднує облік топології мережі та часових тенденцій у поведінці пристроїв. Впровадження проактивних гібридних моделей прогнозування дозволить підвищити стабільність функціонування IoT-мереж, скоротити витрати на технічне обслуговування та мінімізувати ризики аварійних ситуацій. [2; 6].

Аналіз останніх досліджень і публікацій . За останні роки було запропоновано численні підходи до прогнозування збоїв за допомогою машинного навчання, зокрема моделі класифікації, нейронні мережі та безнаглядові алгоритми виявлення аномалій [3; 5; 6]. Значна частина робіт фокусується на передбаченні збоїв на основі часових рядів, проте рідко враховує взаємний вплив мережевих вузлів [11; 12]. Деякі дослідження застосовують графові нейронні мережі для аналізу IoT як структури, але ізольовано від часових залежностей, що обмежує точність прогнозу [8]. Таким чином, залишається невирішеним питання побудови гібридних моделей, здатних одночасно обробляти просторові зв'язки та динаміку зміни параметрів. [2; 8].

Мета і задачі дослідження. Метою роботи є розроблення методу прогнозування збоїв у мережах Інтернету речей, що дозволяє завчасно виявляти ймовірність виникнення відмов шляхом об'єднання просторового та часовго аналізу телеметричних даних.

Для досягнення поставленої мети необхідно вирішити такі завдання:

- здійснити аналіз наявних підходів до прогнозування відмов у IoT [1; 3; 11];
- визначити ключові чинники, що впливають на деградацію сенсорних вузлів; [4; 6];
- сформувати вибірку даних та виконати її попередню обробку охоплюючи фільтрацію шумів і балансування класів [5; 7];
- розробити гібридну архітектуру машинного навчання на основі LSTM і GNN [2; 8];
- провести експериментальну оцінку запропонованого методу та порівняти його з базовими моделями [2; 6; 13].

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Вибір моделей машинного навчання, їх тренування та тестування

На першому етапі дослідження виконано відбір базових алгоритмів, що найчастіше застосовуються для задач прогнозування збоїв. Кожен алгоритм проходив однаковий цикл навчання на попередньо очищеній вибірці. Особливе значення мала якість

підготовки даних - було виконано нормалізацію, масштабування, видалення викидів, а також використано SMOTE-метод для корекції дисбалансу класів. Це забезпечило рівномірну представленість станів «норма» і «відмова», що позитивно вплинуло на показники точності.

Набір моделей тестувався із застосуванням стратегії k-fold cross-validation, що дозволило мінімізувати вплив випадковості на результати. Окремо вимірювалися метрики Accuracy, Precision, Recall та F1-score - саме вони були взяті за основу для подальнього порівняння.

Отримані значення(таб.1) показали, що класичні алгоритми, такі як Random Forest та SVM, здатні виявляти збої на рівні базової ефективності, проте суттєво поступаються нейронним моделям у випадках складних нелінійних залежностей. Найкращий результат серед одиночних моделей продемонструвала GNN, однак навіть вона інколи втрачала стабільність прогнозів у режимі високої змінності мережевих параметрів. Саме це стало підставою для переходу до гібридного підходу та побудови комплексної моделі LGFP.

Таблиця 1

Порівняльний аналіз моделей

Модель	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	Особливості
Logistic Regression	84,7	82,3	79,1	80,6	Базова модель, швидке навчання
Naive Bayes	82,9	80,6	78,4	79,5	Погано враховує нелінійності
SVM	89.8	88.5	85.6	86,9	Ефективна при лінійній сегментації
k-NN	88,1	87,3	83,7	85,0	Простий метод, низька масштабованість
Decision Tree	87,5	85,4	84,1	84,7	Інтерпретованість, схильність до перенавчання
Random Forest	93,6	91,8	90,9	91,3	Стійкість до шумів
XGBoost	94,2	92,7	91,9	92,2	Оптимізована ансамблева модель
MLP	92,1	90,5	89,7	90,1	Висока гнучкість, потребує багато даних
LSTM	96,3	95,7	95,1	95,4	Успішно моделює часові залежності
GNN	97,1	96,9	96,8	96,8	Найвища ефективність, врахування топології мережі

Модуль попередньої обробки даних включає нормалізацію показників та видалення статистичного шуму. Вхідні потоки телеметричних даних від розподілених сенсорних пристроїв поділяються на часові інтервали фіксованої тривалості. Кожен такий інтервал містить історичні заміри всіх моніторингових датчиків і репрезентується у вигляді набору характеристичних векторів X_t. Ці вектори включають низку технічних параметрів, серед яких температурні показники, рівень напруги живлення, завантаження обчислювальних ресурсів, інтенсивність сигналу та відсоток втрачених пакетів даних.

$$x_i' = \frac{x_i - \mu}{\sigma} \quad (1)$$

де μ - середнє значення ознаки, σ - стандартне відхилення

Модуль просторового кодування (GNN)

На даному етапі аналізу модель формує уявлення про кожен пристрій, інтегруючи не лише його власні показники, а й дані суміжних вузлів. Це досягається за рахунок використання модифікованої архітектури графової згорткової мережі (GCN), де сила впливу від сусіда визначається ваговим коефіцієнтом зв'язку.

$$H^{(l+1)} = \sigma(\tilde{D}^{-1/2}\tilde{A}\tilde{D}^{-1/2}H^{(l)}W^{(l)}) \quad (2)$$

де $\tilde{A} = A + I$ - матриця суміжності з одиничною діагоналлю, $\tilde{D}$ - діагональна матриця ступенів вузлів, $H^{(l)}$- матриця прихованих ознак на шарі l, $W^{(l)}$ – навчувані ваги.

В результаті для кожного вузла створюється просторово-контекстне уявлення, що агрегує інформацію від найближчих пристроїв у межах мережевої топології.

Модуль аналізу часових залежностей (LSTM)

Отримані після просторової обробки дані надходять до шару LSTM, основним завданням якого є моделювання часових змін у станах пристроїв. Завдяки спеціальній архітектурі, що включає комірки пам'яті з механізмами контролю інформаційного потоку, ця модель здатна динамічно оновлювати та фільтрувати відомості, визначаючи, які дані слід зберегти, а які ігнорувати.

$$f_t = \sigma(W_f[h_{t-1}, x_t] + b_f) \quad (3)$$

$$i_t = \sigma(W_i[h_{t-1}, x_t] + b_i) \quad (4)$$

$$C_t = f_t \odot C_{t-1} + i_t \odot \tanh(W_C[h_{t-1}, x_t] + b_C) \quad (5)$$

$$o_t = \sigma(W_o[h_{t-1}, x_t] + b_o) \quad (6)$$

$$h_t = o_t \odot \tanh(C_t) \quad (7)$$

де f_t, i_t, o_t - ворота забування, оновлення та виходу; C_t - стан пам’яті, h_t - прихований стан.

Такий підхід дає змогу виявляти часові кореляції між різними подіями, зокрема, встановлювати зв'язок між поступовим падінням напруги живлення та подальшим виходом вузла з ладу.

Фінальним етапом є модуль класифікації, який приймає згорткові часові представлення вузлів. Ці дані обробляються в повнозв'язному шарі нейронної мережі, де тип активації на виході вибирається відповідно до постановки завдання: сигмоїда - для бінарної класифікації (наприклад, «справний»/«несправний»), або софтмакс - для визначення одного з кількох можливих типів відмови.

$$\hat{y}_{t+1} = softmax(W_c h_t + b_c) \quad (8)$$

Модуль адаптивного навчання

Ключовою перевагою запропонованого підходу LGFP є його вбудована здатність до адаптації в реальному часі, що є критично важливим для нестабільного середовища IoT. Постійні зміни мережевої топології, рівня навантаження, характеру взаємодій та типів аномалій призводять до концептуального дрейфу даних (data drift), через який статичні моделі швидко втрачають ефективність. Для протидії цьому явищу архітектура системи включає механізм постійного оновлення, що регулює параметри GNN та LSTM-моделей відповідно до нових умов.(рис. 1)

Після кожного операційного циклу фіксуються всі нові випадки класифікації, включаючи коректні виявлення, пропущені інциденти та помилкові сповіщення. Ця інформація разом із сирими телеметричними даними надходить до централізованого сховища Data Lake, що функціонує як єдине джерело істини для подальшого вдосконалення моделей. За заданими інтервалами система автоматично обчислює ключові метрики ефективності - Accuracy, Precision, Recall та F1-score - у межах ковзного часового інтервалу.

На етапі підготовки до перетренування формується збалансований навчальний корпус даних шляхом об'єднання історичних записів із новими спостереженнями, що відображають поточні тенденції. Для подолання проблеми нерівномірного розподілу класів застосовуються спеціальні методи, такі як SMOTE для штучного збільшення рідкісних подій або андерсемплінг для скорочення перепредставлених категорій. Це забезпечує збалансоване представлення всіх типів подій і знижує ймовірність перенавчання на домінуючих класах.

Після підготовки датасету запускається паралельне навчання оновлених версій GNN та LSTM-моделей. GNN-компонент перебудовує векторні уявлення вузлів з урахуванням оновлених топологічних зв'язків, тоді як LSTM-модуль перенавчається на актуальних часових послідовностях. Обидві моделі проходять ретельну валідацію за стандартизованим набором метрик перед переходом до етапу тестування.

Фінальне тестування оновлених моделей відбувається в ізольованому середовищі staging, яке відтворює роботу продуктивної системи за допомогою копії реальних даних. Це дозволяє об'єктивно порівняти ефективність нової та поточної версій без втручання в роботу системи.

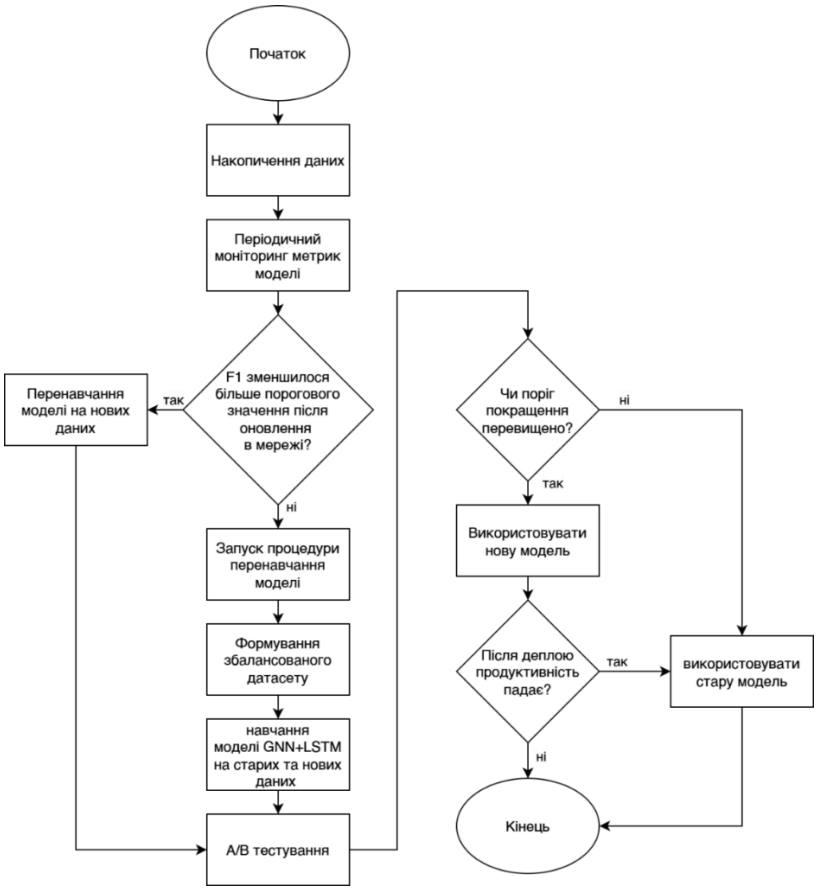

Рис 1. Алгоритм модулю адаптивного навчання

На блок-схемі(рис.2) представлено повний цикл роботи системи прогнозування відмов у мережі IoT, від отримання сирих даних до генерації класифікованих попереджень. Алгоритм реалізує багатоетапну обробку даних, що поєднує просторові та часові аналітичні модулі для підвищення точності виявлення аномалій. В таблиці 2 наведено види вихідних класифікацій

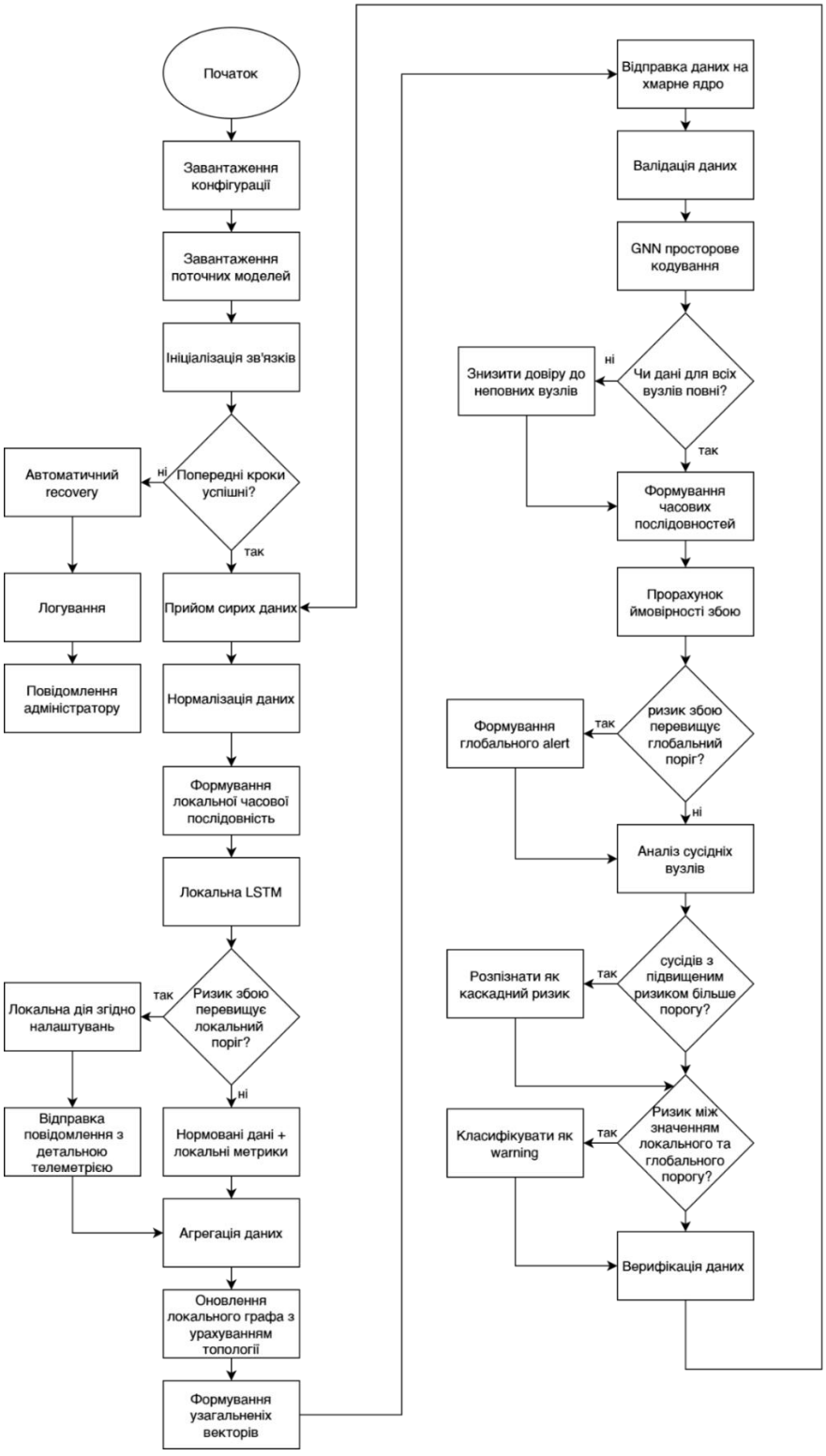

Рис 2. Алгоритм LGFP

Таблиця 2

Види класифікацій відмов

Тип попередження	Принцип функціонування	Ключове призначення	Ключові параметри та ефекти
Local Alert (Edge)	Миттєве спрацьовування на рівні окремого пристрою при низькому порозі сприйняття загрози	Оперативна нейтралізація локальних ризиків з мінімальним часом реагування	Швидкодія: Максимальна Результат: Автономна деактивація або сегментація проблемного вузла
Global Alert (Cloud)	Аналітична обробка агрегованих показників із просторово-часовим аналізом усієї інфраструктури	Координація стратегічного реагування для усунення системних загроз	Швидкодія: Помірна Результат: Перерозподіл ресурсів, профілактичні роботи, корегування політик безпеки
Cascade Detection	Ідентифікація каскадних відмов через моніторинг стану суміжних компонентів системи	Попередження лавиноподібного поширення аномалій по мережевій топології	Швидкодія: Критично висока Результат: Миттєва ізоляція цілих сегментів із сповіщенням оператора

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У ході науково-дослідної роботи було створено та емпірично підтверджено метод LGFP (LSTM-GNN Failure Prediction) для прогнозування відмов в IoT-системах. Дослідження охопило повний життєвий цикл розробки інтелектуальної системи - від аналізу предметної галузі та відбору алгоритмів машинного навчання до побудови архітектури, інтеграції в розподілене IoT-середовище та експериментального підтвердження ефективності.

На етапі аналітичного дослідження було проведено компаративне дослідження класичних та сучасних ML-моделей, включно з деревами рішень, методами найближчих сусідів, випадковими лісами, методами опорних векторів, лінійними класифікаторами, байєсовими моделями, градієнтними методами, багатошаровими перцептронами, бустингом та нейромережами LSTM і GNN. Експериментальні результати виявили обмежену ефективність традиційних алгоритмів при обробці багатовимірних часово-просторових даних IoT, тоді як нейромережеві підходи продемонстрували суттєво вищу точність та адаптивність.

На підставі отриманих даних було запропоновано гібридний підхід LGFP, що інтегрує переваги рекурентних мереж для аналізу часових залежностей та графових нейромереж для виявлення топологічних зв'язків між вузлами. Архітектура системи реалізує двоетапну обробку інформації: спочатку LSTM-модуль аналізує короткострокові тенденції та локальні аномалії в поведінці сенсорів, після чого GNN-компонент вивчає просторові залежності між пристроями, ідентифікуючи потенційні зони виникнення каскадних відмов. Таке поєднання часового та структурного аналізу забезпечує комплексне охоплення аспектів функціонування IoT-мереж, що підвищує точність прогнозування та операційну стабільність системи.

Проведене порівняльне дослідження метрик якості класифікації (accuracy, recall та F1-score) продемонструвало, що гібридна архітектура LGFP систематично перевершує показники окремо взятих LSTM та GNN моделей в середньому на 3-5%. У порівнянні з традиційними алгоритмами машинного навчання перевага становить 12-18%. Найбільш

значущим є підвищення стійкості моделі до обробки зашумлених та фрагментованих даних, що характерно для реальних IoT-систем.

Перспективи подальших досліджень включають розширення простору ознак, інтеграцію механізмів уваги для покращення інтерпретованості моделі та апробацію методу в реальних промислових умовах. Впровадження запропонованого рішення може закласти фундамент для створення адаптивних систем предикативного аналізу та автономного супроводу IoT-інфраструктур.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Chuhreiev, K. O. (2025). Comparison of machine learning methods for failure prediction in a smart home. In *Proceedings of the 6th Scientific and Technical Conference "Current State and Prospects of IoT Development"* (pp. 213–215). https://duikt.edu.ua/uploads/p_2779_40288420.pdf
2. Chuhreiev, K. O. (2025). A method based on a hybrid LSTM and GNN mechanism for failure prediction in Internet of Things networks. In *Proceedings of the 3rd International Scientific and Practical Conference "Modern Aspects of Digitalization and Informatization in Software and Computer Engineering"* (December 4–6, 2025).
3. Kilaru, M., et al. (2025). Adaptive learning systems: Integrating IoT sensors with machine learning for dynamic curriculum adjustment. In *2025 International Conference on Pervasive Computational Technologies (ICPCT)* (pp. 900–905). IEEE. https://doi.org/10.1109/ICPCT64145.2025.10939112
4. AlShehri, Y., & Ramaswamy, L. (2022). SECOE: Alleviating sensors failure in machine learning-coupled IoT systems. In *2022 21st IEEE International Conference on Machine Learning and Applications (ICMLA)*. IEEE. https://doi.org/10.1109/ICMLA55696.2022.00124
5. Ardito, S., Setiawan, W., & Wibisono, A. (2024). Enhancing predictive maintenance in manufacturing using deep learning-based anomaly detection. *International Journal of Technology and Modeling, 3*(1), 12–23. https://doi.org/10.63876/ijtm.v3i1.112
6. Aslam, S., et al. (2025). Machine learning-based predictive maintenance at smart ports using IoT sensor data. *Sensors, 25*(13), 3923. https://doi.org/10.3390/s25133923
7. Liu, Y., et al. (2020). Deep anomaly detection for time-series data in industrial IoT: A communication-efficient on-device federated learning approach. *IEEE Internet of Things Journal*, 1–11. https://doi.org/10.1109/JIOT.2020.3011726
8. Dong, G., et al. (2022). Graph neural networks in IoT: A survey. *ACM Transactions on Sensor Networks*. https://doi.org/10.1145/3565973
9. H, S., & Venkataraman, N. (2023). Proactive fault prediction of fog devices using LSTM-CRP conceptual framework for IoT applications. *Sensors, 23*(6), 2913. https://doi.org/10.3390/s23062913
10. Hajiaghayi, M., & Vahedi, E. (2019). Code failure prediction and pattern extraction using LSTM networks. In *2019 IEEE Fifth International Conference on Big Data Computing Service and Applications (BigDataService)*. IEEE. https://doi.org/10.1109/BigDataService.2019.00014
11. Khattach, O., Moussaoui, O., & Hassine, M. (2023). A survey on AI approaches for Internet of Things devices failure prediction. *E3S Web of Conferences, 469*, 00061. https://doi.org/10.1051/e3sconf/202346900061
12. Khan, W., et al. (2025). Machine learning-based optimal data retrieval and resource allocation scheme for edge mesh coupled information-centric IoT networks and disability support systems. *Internet of Things*, 101511. https://doi.org/10.1016/j.iot.2025.101511
13. Kwon, J.-H., & Kim, E.-J. (2020). Failure prediction model using iterative feature selection for industrial Internet of Things. *Symmetry, 12*(3), 454. https://doi.org/10.3390/sym12030454

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023

Kyryll Chuhreiev
Master's student
State university of information and communication technologies, Kyiv, Ukraine
ORCID:0009-0005-6951-344X
Ch.kir.lev.2003@gmail.com

Olena Voloshchuk
Candidate of Technical Sciences, Associate Professor
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID:0000-0002-5912-4126
Olena.voloshchuk@nure.ua

FAILURE PREDICTION METHOD FOR INTERNET OF THINGS NETWORKS USING MACHINE LEARNING

Abstract. The article addresses the problem of ensuring the reliability and uninterrupted operation of Internet of Things networks consisting of a large number of sensor nodes, gateways, and distributed computing elements. Due to the high heterogeneity of devices, rapid topology changes, and heterogeneity of data flows, such networks are vulnerable to various types of failures—hardware, network, and software. In view of this, fault prediction methods capable of detecting risks of system destabilization in advance are becoming increasingly relevant. The advantages of using hybrid machine learning approaches that combine time series analysis and the assessment of spatial interaction between network nodes are substantiated. A fault prediction method LGFP is proposed, built on the combination of graph neural networks (GNN) and LSTM architecture, which provides comprehensive data interpretation. The method allows estimating the probability of failure occurrence based on current and previous telemetry parameters while considering the mutual influence of network elements. An analysis of existing approaches is carried out, a comparison of machine learning models is performed, and the process of dataset formation for the study is described. Special attention is paid to the problem of class balancing and filtering of noise structures in the data, which are critically important stages for improving prediction accuracy. The obtained experimental results demonstrate the advantage of the proposed method compared to traditional models such as Random Forest, SVM, and isolated LSTM architectures, which is confirmed by increased classification accuracy and F1-score. The practical application of the proposed approach can provide a significant improvement in the robustness of IoT systems in industrial, energy, and household environments. Prospects for further research include the expansion of the feature space, the integration of attention mechanisms to improve model interpretability, and the testing of the method in real industrial conditions.

Keywords: internet of things; machine learning; lstm; gnn; fault prediction; algorithm; IoT; metrics.

1. Chuhreiev, K. O. (2025). Comparison of machine learning methods for failure prediction in a smart home. In *Proceedings of the 6th Scientific and Technical Conference "Current State and Prospects of IoT Development"* (pp. 213–215). https://duikt.edu.ua/uploads/p_2779_40288420.pdf
2. Chuhreiev, K. O. (2025). A method based on a hybrid LSTM and GNN mechanism for failure prediction in Internet of Things networks. In *Proceedings of the 3rd International Scientific and Practical Conference "Modern Aspects of Digitalization and Informatization in Software and Computer Engineering"* (December 4–6, 2025).
3. Kilaru, M., et al. (2025). Adaptive learning systems: Integrating IoT sensors with machine learning for dynamic curriculum adjustment. In *2025 International Conference on Pervasive Computational Technologies (ICPCT)* (pp. 900–905). IEEE. https://doi.org/10.1109/ICPCT64145.2025.10939112
4. AlShehri, Y., & Ramaswamy, L. (2022). SECOE: Alleviating sensors failure in machine learning-coupled IoT systems. In *2022 21st IEEE International Conference on Machine Learning and Applications (ICMLA)*. IEEE. https://doi.org/10.1109/ICMLA55696.2022.00124

5. Ardito, S., Setiawan, W., & Wibisono, A. (2024). Enhancing predictive maintenance in manufacturing using deep learning-based anomaly detection. *International Journal of Technology and Modeling*, *3*(1), 12–23. https://doi.org/10.63876/ijtm.v3i1.112
6. Aslam, S., et al. (2025). Machine learning-based predictive maintenance at smart ports using IoT sensor data. *Sensors*, *25*(13), 3923. https://doi.org/10.3390/s25133923
7. Liu, Y., et al. (2020). Deep anomaly detection for time-series data in industrial IoT: A communication-efficient on-device federated learning approach. *IEEE Internet of Things Journal*, 1–11. https://doi.org/10.1109/JIOT.2020.3011726
8. Dong, G., et al. (2022). Graph neural networks in IoT: A survey. *ACM Transactions on Sensor Networks*. https://doi.org/10.1145/3565973
9. H, S., & Venkataraman, N. (2023). Proactive fault prediction of fog devices using LSTM-CRP conceptual framework for IoT applications. *Sensors*, *23*(6), 2913. https://doi.org/10.3390/s23062913
10. Hajiaghayi, M., & Vahedi, E. (2019). Code failure prediction and pattern extraction using LSTM networks. In *2019 IEEE Fifth International Conference on Big Data Computing Service and Applications (BigDataService)*. IEEE. https://doi.org/10.1109/BigDataService.2019.00014
11. Khattach, O., Moussaoui, O., & Hassine, M. (2023). A survey on AI approaches for Internet of Things devices failure prediction. *E3S Web of Conferences*, *469*, 00061. https://doi.org/10.1051/e3sconf/202346900061
12. Khan, W., et al. (2025). Machine learning-based optimal data retrieval and resource allocation scheme for edge mesh coupled information-centric IoT networks and disability support systems. *Internet of Things*, 101511. https://doi.org/10.1016/j.iot.2025.101511
13. Kwon, J.-H., & Kim, E.-J. (2020). Failure prediction model using iterative feature selection for industrial Internet of Things. *Symmetry*, *12*(3), 454. https://doi.org/10.3390/sym12030454