УДК 004.4
Долинний І.С.[1], Тіменко А.В.[2] , Куликовська Н.А.[2]
[1] студ. гр. КНТ-513сп НУ «Запорізька Політехніка»
[2] старш.викл. НУ «Запорізька Політехніка»

ВИЯВЛЕННЯ АНОМАЛЬНИХ ДАНИХ В ІОТ-СИСТЕМАХ

Поява Інтернету речей (IoT) зробила революцію в багатьох галузях промисловості, впроваджуючи підключення та інтелект у повсякденні об’єкти. Однак це поширення також створило значні проблеми, зокрема щодо безпеки та надійності цих систем. Виявлення аномалій, яке визначає шаблони в даних, які не відповідають очікуваній поведінці, має вирішальне значення для підтримки цілісності та функціональності систем IoT. Враховуючи різноманітність і обсяг даних, створених пристроями Інтернету речей, традиційні методи виявлення аномалій часто не дають результатів. У цьому дослідженні досліджуються передові методи машинного навчання, які можуть врахувати унікальні характеристики даних IoT, такі як їх багатовимірність і динамічність. Основна увага зосереджена на оцінці ефективності трьох різних моделей: Isolation Forest, One Class SVM і Autoencoders, надаючи розуміння їх застосовності та продуктивності в реальних сценаріях. Це дослідження не лише висвітлює поточний стан виявлення аномалій в Інтернеті речей, але й закладає основу для майбутніх удосконалень у цій життєво важливій сфері.

Оскільки середовища IoT стають дедалі складнішими, зростає потенціал аномалій, які можуть вказувати на системні збої або порушення безпеки. Ефективне виявлення цих аномалій має першочергове значення для безпеки та ефективності роботи.

Рисунок 1 містить гістограми для трьох різних змінних: дощу, вітру і температури. Кожна гістограма показує розподіл частоти різних діапазонів значень цих змінних.

Гістограма дощу (синій колір), з великою кількістю значень зосереджених при нижчому діапазоні (наприклад, мало дощу), та набагато менша кількість значень при вищому діапазоні.

Гістограма вітру (жовтий колір), з менш рівномірним розподілом, що може вказувати на варіативність у швидкості вітру.

Гістограма температури (зелений колір) з дуже рівномірним розподілом значень, що свідчить про постійну температуру.

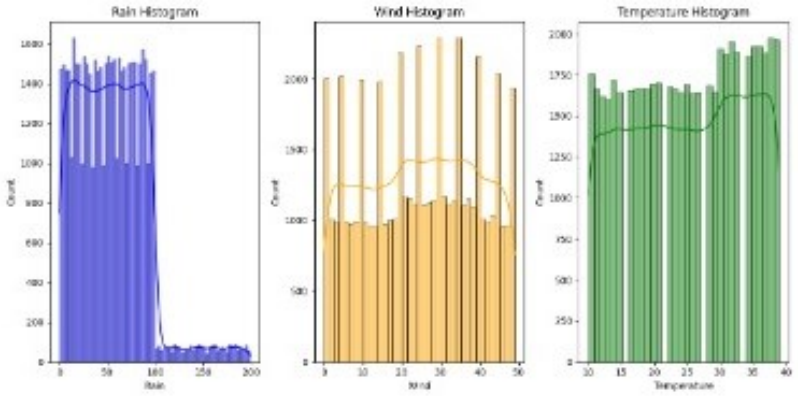

Рисунок 1 – Гістограми параметрів впливу

У цьому дослідженні реалізовано та порівняно три методи машинного навчання:

- ізольований лі;
- SVM;
- моделі автокодерів.

Ці методи були обрані через їх доречність у обробці багатовимірних і неоднорідних даних, типових для систем IoT.

Оцінка цих моделей на еталонному наборі даних IoT виявила різний ступінь ефективності, причому для оцінки продуктивності використовувалися такі показники, як точність, точність, запам’ятовування та

оцінка F1. Кожна модель має унікальні переваги та компроміси щодо можливостей виявлення аномалій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Elkhawaga G., Machine Learning-Based Anomaly Detection in IoT Networks: A Systematic Literature Review / G.Elkhawaga, A.Elragal // Journal of Big Data. 2021. – Vol. 8, No. 1. – P. 47. https://doi.org/10.1186/s40537-021-00433-2

2. Xiao G., Anomaly Detection for IoT Time Series Data Using Isolation Forest. / G.Xiao, J.Guo, V.Balasubramaniyan // IEEE 5th World Forum on Internet of Things (WF-IoT): 15-18 April 2019. – Limerick, Ireland, 2019 – P. 51-56. https://doi.org/10.1109/WF-IoT.2019.8767229

3. Narmada A., Anomaly Detection in IoT Networks Using Machine Learning / A.Narmada, S.Selvi // Internet of Things and Big Data Analytics for Smart Generation. – Springer, Cham, 2019. – P. 171-198. https://doi.org/10.1007/978-3-030-04203-5_8