УДК 007.5:004.72:004.8

ОСОБЛИВОСТІ ЗАХИСТУ КІНЦЕВИХ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ

Чудо А.Р., Курдеча В.В.
Інститут телекомунікаційних систем,
КПІ ім. Ігоря Сікорського, Україна
E-mail: kyiv12@bigmir.net

FEATURES OF PROTECTION OF INTERNET OF THINGS DEVICES

The method for protecting IoT end devices has been modified, which differs in the data protection mechanism and allows to increase the security of the IoT network. The proposed solution can be implemented by the owners of IoT end devices to increase network security

За рахунок підключення різних пристроїв до Інтернету технологія Інтернету речей дає нові можливості для автоматизації, ефективності та прийняття продуманих рішень у різних сферах життєдіяльності. В зв'язку з цим особливо актуальною постає проблема захисту кінцевих пристроїв. А тому метою публікації є підвищення захищеності мережі Інтернету речей за рахунок модифікації захисту кінцевих пристроїв.

В роботі запропоновано модифікований метод захисту кінцевих пристроїв Інтернету речей(рис.1).

Рис.1. Модифікований метод захисту кінцевих пристроїв Інтернету речей.

Відмінністю запропонованого рішення є інтеграція навченої моделі в систему безпеки розумного будинку (рис.2). – що відповідає змінам в кроках 2 і 3 модифікованого методу (рис.1).

В першу чергу, щоб інтегрувати алгоритм машинного навчання, за допомогою якого відбувається відстеження аномального трафіку, потрібно зібрати дані з усіх датчиків.

Було взято набір даних з відкритим вихідним кодом трас трафіку зібраний з kaggle [1]. Дані були згенеровані в віртуальному середовищі, максимально наближеними до реальних. Загалом дані містять інформацію з різних датчиків розумного будинку. Ці набори даних містять зв'язок між різними вузлами IoT.

Набір цих даних в собі містять 347 935 нормальних даних та 10 017 аномальних. Також має відсутні значення в ознаках «Value» - 148 відсутніх

значень, «Source Type» має 2050 відсутніх даних. Класовий показник «Normality» розділений на 8 різних класів відповідно до нормальності.

Рис.2. Модель машинного навчання модифікованого методу.

У рамках попередньої обробки, виконується два основних кроки. По-перше, виявляються та обробляються пропущені значення. Це допомагає уникнути втрати цінних даних та зберегти структуру. Другим важливим кроком є обробка несподіваних значень.

Після того, як отримано дані, потрібно очистити їх від шуму, щодо кількості екземплярів кожного класу в даних після обробки даних та вилучення з неї необхідної інформації.

Для навчання моделей набір даних був розділений у співвідношенні 80% для навчання і 20% для тестування.

За допомогою отриманих результатів відображених на багатокласових матрицях помилок, можна виділити ефективний алгоритм для цих даних.

Результати натурно-імітаційного моделювання показали, що рішення «випадковий ліс» RF зміг правильно класифікувати кожен клас, лише 403 з 1178 зразка DoS відніс до ознаки Normality, тобто визначив аномальні пакети, як нормальні. А також помилково класифікував 18 нормальних значень, як DoS. DT має фактично таку ж ситуацію, як і RF. Не на багато гірші результати отримав алгоритм машинного навчання ANN. Він не зміг класифікувати 2 пакета SP та 1 MC. Інші ж алгоритми, дали значно гірші результати, вони не

змогли класифікувати точно аномальні дані. Крім KNN він класифікував все вірно, лише 444 нормальних значень визначив як DoS.

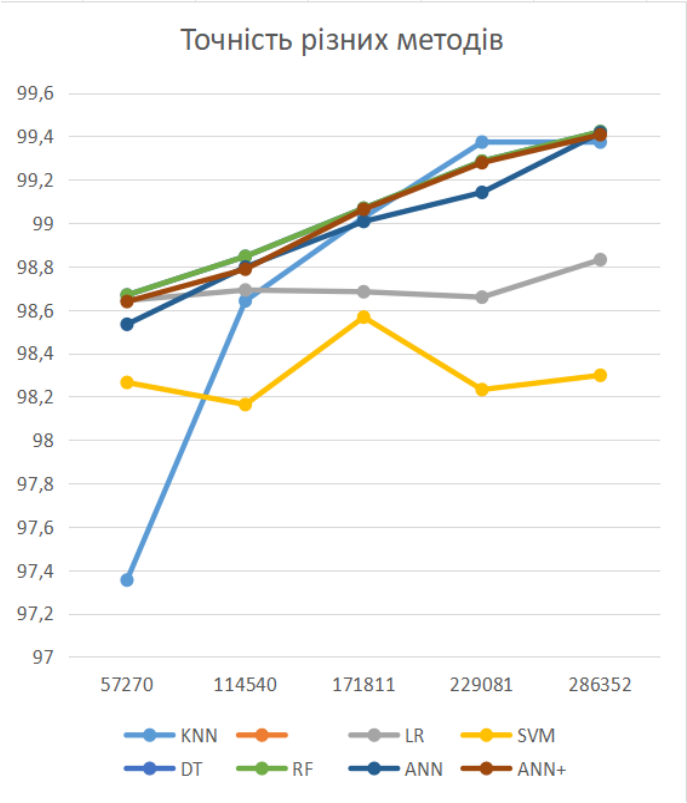

Рис. 3. Порівняння запропонованого рішення.

За результатами п'ятикратної перехресної перевірки можна дійти до таких самих висновків, як і за результатами отриманих з матриць. А саме алгоритми RF, DT та штучна нейронна мережа ANN показали майже однакові результати результати з точністю в 99.40%. Інші ж мають нижчий рівень точності.

Література

1. DS2OS traffic traces [Електронний ресурс] // Kaggle. – 2018. – Режим доступу до ресурсу: https://www.kaggle.com/datasets/francoisxa/ds2ostraffictraces.
2. Altulaihan E. Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms / E. Altulaihan, M. Almaiah, A. Aljughaiman // MDPI. – 2024. – https://doi.org/10.3390/s24020713.
3. Чудо А.Р. Курдеча В.В. Модифікований метод захисту кінцевих пристроїв інтернету речей // XVI Міжнародна науково-технічна конференція студентів та аспірантів «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем» ПРІТС 2024: Збірник тез конференції. К.: КПІ ім. Ігоря Сікорського, 2024. - с.305.
4. Globa, L., Kurdecha, V., Popenko, D., Bezvuhliak, M., Porolo, Y. (2022). Data Collection and Processing Method in the Networks of Industrial IOT. In: Perakovic, D., Knapcikova, L. (eds) Future Access Enablers for Ubiquitous and Intelligent Infrastructures. FABULOUS 2022. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 445. Springer, Cham. https://doi.org/10.1007/978-3-031-15101-9_11