УДК 621.391

О.О. Семенова
А.В. Джус
В.В. Мартинюк

РОЗПІЗНАВАННЯ КІБЕРАТАК У ІНТЕРНЕТІ РЕЧЕЙ ЗА ДОПОМОГОЮ НЕЙРОННИХ МЕРЕЖ

Вінницький національний технічний університет

Анотація

Робота присвячена дослідженню використання нейронних мереж для розпізнавання кібератак у системах Інтернету речей. У роботі аналізуються основні проблеми та загрози безпеки IoT, а також розглядається потенціал нейронних мереж для виявлення та запобігання кібератакам у реальному часі.

Ключові слова: Інтернет речей, кібератака, нейронна мережа.

Abstract

This paper is dedicated to the study of the use of neural networks for recognizing cyberattacks in Internet of Things systems. The work analyzes the main security issues and threats in IoT, as well as the potential of neural networks for detecting and preventing cyberattacks in real time..

Keywords: Internet of things, cyberattack, neural network.

Вступ

Інтернет речей (IoT) – це концепція, що передбачає підключення різноманітних пристроїв до Інтернету, що дозволяє здійснювати обмін даними між ними та з іншими системами. Зі швидким зростанням кількості IoT-пристроїв у таких сферах, як розумні будинки, промисловість, медицина та транспорт, важливість забезпечення їхньої безпеки стає дедалі більшою. Однак, через величезну кількість підключених пристроїв і їхню різноманітність, IoT-системи зазвичай виявляються уразливими до кібератак, що може призвести до серйозних наслідків, зокрема порушення конфіденційності, зниження працездатності мереж або навіть втрати контролю над критично важливими системами.

Однією з найбільших проблем у забезпеченні безпеки Інтернету речей є ефективне розпізнавання кібератак, оскільки традиційні методи захисту часто не здатні впоратися з такими великими обсягами даних і різноманітністю атак [1]. У цьому контексті все більш важливим стає використання новітніх технологій, зокрема штучного інтелекту, для аналізу мережевого трафіку та виявлення аномалій.

Одним із найперспективніших підходів до розпізнавання кібератак у IoT є застосування нейронних мереж. Завдяки своїй здатності навчатися на великих обсягах даних, нейронні мережі можуть ефективно ідентифікувати потенційні загрози в режимі реального часу. Метою цієї роботи є дослідити методи розпізнавання кібератак у системах Інтернету речей за допомогою нейронних мереж, оцінити їх ефективність та визначити перспективи їхнього використання в сучасних IoT-мережах.

Результати дослідження

Інтернет речей, з його різноманітністю пристроїв і технологій, є вразливим до різних типів кібератак. Ці атаки можуть бути спрямовані на порушення функціонування систем або на здобуття конфіденційної інформації [2]. Кібератаки на IoT-пристрої можуть мати різні форми, і це є ще однією причиною, чому забезпечення безпеки у цих мережах є таким складним. Основні види атак включають: DDoS-атаки (розподілені атаки на відмову в обслуговуванні), атаки на конфіденційність, фізичні атаки, атаки на мережеві протоколи, ін'єкція зловмисного програмного забезпечення.

Нейронні мережі — це підмножина штучного інтелекту, що імітує структуру і функції біологічних нейронних мереж мозку для вирішення складних завдань, таких як класифікація, регресія, розпізнавання образів та виявлення аномалій. Нейронні мережі мають здатність автоматично виявляти патерни та аномалії в даних, що робить їх потужним інструментом для розпізнавання кібератак у реальному часі. Вони використовуються для аналізу великих обсягів даних, що генеруються IoT-пристроями, і для виявлення відхилень від нормальної поведінки, що може свідчити про кібератаку [3].

Розпізнавання кібератак у системах IoT за допомогою нейронних мереж є потужним напрямком у галузі кібербезпеки, що здатне значно підвищити ефективність захисту від численних загроз, характерних для цієї технології. Враховуючи масштабне поширення IoT-пристроїв та їх вразливості, необхідність у надійних системах захисту стає дедалі більш актуальною.

Процес застосування нейронних мереж для виявлення атак зазвичай включає такі етапи: збір і попередня обробка даних, навчання моделі нейронної мережі, виявлення аномалій, оцінка та класифікація. Це дозволяє системам приймати рішення про подальші дії, наприклад, блокувати підозрілі підключення або надсилати сповіщення адміністраторам.

Окрім виявлення атак, нейронні мережі можуть використовуватися для прогнозування загроз. Це дозволяє попередити про можливі атаки ще до того, як вони відбудуться, що є важливим для підвищення безпеки IoT-мереж.

Пропонована нейронна мережа для розпізнавання кібератак у IoT буде мати багатошарову архітектуру, яка включає кілька етапів обробки даних, навчання та класифікації аномалій. Для розпізнавання кібератак в IoT необхідно отримати різноманітні типи вхідних даних від пристроїв. Це можуть бути: мережевий трафік, логи систем (записи про події, відключення пристроїв, доступи до серверів), стан пристроїв IoT, інформація про підключення пристроїв. Всі ці дані можуть бути представлені у вигляді числових векторів, що дозволяє нейронній мережі ефективно обробляти їх.

В той же час, застосування нейронних мереж для виявлення кібератак може мати певні недоліки. Серед зазначених недоліків можна виділити великі вимоги до ресурсів, адже для тренування нейронних мереж потрібно велике число прикладів, що вимагає значних обчислювальних ресурсів. Окрім того, можливі проблеми з інтерпретацією результатів – нейронні мережі часто працюють як «чорні ящики», і складно пояснити, чому модель видала певне рішення. Також проблематичними можуть бути збір і обробка даних, так як для навчання моделей необхідно мати високоякісні та різноманітні дані, що не завжди є можливим, особливо для нових типів атак.

Висновки

У результаті дослідження було доведено, що нейронні мережі можуть бути ефективними інструментами для забезпечення безпеки в екосистемі Інтернету речей. Ці технології не тільки дозволяють своєчасно виявляти кіберзагрози, але й можуть адаптуватися до нових типів атак. Однак для забезпечення ефективного застосування нейронних мереж у сфері IoT необхідно подолати ряд технічних та етичних проблем, таких як обмеження обчислювальних ресурсів, забезпечення конфіденційності та прозорості моделей.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. A. Aldhaheri, F. Alwahedi, M. A. Ferrag, and A. Battah, “Deep learning for cyber threat detection in IoT networks: A review,” Internet of Things and Cyber-Physical Systems, vol. 4. Elsevier BV, pp. 110–128, 2024. doi: 10.1016/j.iotcps.2023.09.003.
2. V. Anitha, C. G. Naveen Kumar, R. Kuchipudi, K. Sharma, J. Muralidharan, and R. Rajagopal, “Cybersecurity in Internet of Things Networks using Deep Learning Models,” 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS). IEEE, pp. 1090–1095, Mar. 23, 2023. doi: 10.1109/icscds56580.2023.10104851.
3. Mrunal K. Pathak, “Detecting Cyber-attacks in the Industrial Internet of Things using a Hybrid Deep Random Neural Network,” Journal of Electrical Systems, vol. 20, no. 1s. Science Research Society, pp. 165–174, Mar. 28, 2024. doi: 10.52783/jes.762.

Семенова Олена Олександрівна – канд. техн. наук, доцент кафедри інфокомунікаційних систем і технологій, Вінницький національний технічний університет, м. Вінниця, e-mail: semenova.o.o@vntu.edu.ua

Джус Андрій Васильович — аспірант групи 172-23а, факультет інформаційних електронних систем, Вінницький національний технічний університет, Вінниця, e-mail: dzhuz1988@gmail.com

Мартинюк Володимир В’ячеславович — аспірант групи 172-23а, факультет інформаційних електронних систем, Вінницький національний технічний університет, Вінниця, e-mail: vm4ukr@gmail.com

Semenova Olena O. – Cand. Sc. (Eng), Associate professor at the Department of Infocommunication systems and technologies, Vinnytsia National Technical University, Vinnytsia, e-mail: semenova.o.o@vntu.edu.ua

Dzhus Andrii V. – post-graduate student of 172-23a group, Faculty of Information Electronic Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: dzhuz1988@gmail.com

Martyniuk Volodymyr V. – post-graduate student of 172-23a group, Faculty of Information Electronic Systems, VinnytsiaNational Technical University, Vinnytsia, e-mail: vm4ukr@gmail.com