ISSN 2219-9365

https://doi.org/10.31891/2219-9365-2025-83-21
УДК 621.396

СЕМЕНОВА Олена
Вінницький національний технічний університет
https://orcid.org/0000-0001-5312-9148
e-mail: semenova.o.o@vntu.edu.ua
ДЖУС Андрій
Вінницький національний технічний університет
https://orcid.org/0009-0005-3583-5766
e-mail: dzhuz1988@gmail.com
МАРТИНЮК Володимир
Вінницький національний технічний університет
https://orcid.org/0009-0006-8421-0348
e-mail: vm4ukr@gmail.com

ВИЯВЛЕННЯ ВТОРГНЕНЬ В ІНТЕРНЕТІ РЕЧЕЙ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЙ ОБЧИСЛЮВАНОГО ІНТЕЛЕКТУ

Наразі технологія Інтернету речей (Internet of Things, IoT) стрімко трансформує сучасні галузі індустрії, інтегруючи фізичні об'єкти з цифровими системами для забезпечення інтелектуальної взаємодії. Проте збільшення кількості підключених пристроїв і відкритість середовища можуть створюють певні проблеми виклики в області кібербезпеки. Традиційні системи виявлення вторгнень виявляються малоефективними в мережах IoT через обмежені ресурси пристроїв, динамічну топологію мереж і велику кількість нових, раніше невідомих атак. Для підвищення ефективності систем виявлення вторгнень доцільно використовувати підхід, заснований на використанні технологій обчислюваного інтелекту, зокрема методів машинного навчання, еволюційних моделей та алгоритмів обробки нечіткої інформації. У цій статті розглянуто застосування технологій обчислюваного інтелекту для підвищення ефективності систем виявлення вторгнень у середовищі IoT. У роботі обґрунтовано доцільність використання технологій обчислюваного інтелекту для підвищення ефективності виявлення аномальної поведінки та несанкціонованих дій у мережевому трафіку. Запропоновано підхід до побудови інтелектуальної системи виявлення вторгнень на основі нечіткого контролера, здатного адаптивно реагувати на змінні характеристики середовища та невизначеність у вхідних даних. У межах дослідження розроблено структуру нечіткого контролера типу Мамдані, визначено вхідні та вихідні змінні, сформовано базу нечітких правил та функцій належності. Здійснено моделювання роботи контролера в середовищі MATLAB. Розроблений нечіткий контролер може бути використаний як складова частина систем виявлення вторгнень. Отримані результати підтверджують доцільність застосування технологій обчислюваного інтелекту для підвищення надійності захисту IoT-мереж. Запропонований підхід може бути використаний як основа для побудови ефективних систем виявлення вторгнень нового покоління для підвищення стійкості IoT-інфраструктур.
Ключові слова: нечіткий контролер, Інтернет речей, виявлення вторгнень, кібератака, безпека, захист.

SEMENOVA Olena, DZHUS Andrii, MARTYNIUK Volodymyr
Vinnytsia National Technical University

DETECTION OF INTRUSIONS IN THE INTERNET OF THINGS USING COMPUTATIONAL INTELLIGENCE TECHNOLOGIES

Nowadays the technology of Internet of Things (IoT) is rapidly transforming modern industries by integrating physical objects with digital systems to enable intelligent interaction. However, the growing number of connected devices and the openness of IoT environments pose some cybersecurity issues. Traditional intrusion detection systems (IDS) are often ineffective in IoT networks due to limited device resources, dynamic network topologies, and the increasing number of novel, previously unseen attacks. To improve the efficiency of intrusion detection systems, it is advisable to use an approach based on the use of computational intelligence technologies, including machine learning methods, evolution models, and fuzzy logic algorithms. This paper explores the application of computational intelligence technologies to enhance the effectiveness of intrusion detection in IoT environments. The study substantiates the feasibility of applying computational intelligence technologies to enhance the efficiency of detecting anomalous behavior and unauthorized activities in network traffic. An approach is proposed for designing an intelligent intrusion detection system based on a fuzzy controller capable of adaptively responding to changing environmental conditions and uncertainty in input data. A Mamdani-type fuzzy inference system was developed, including the definition of input and output variables, the construction of a rule base, and the configuration of membership functions. The controller was modeled in the MATLAB environment. The developed fuzzy controller can serve as a component of intrusion detection systems. The obtained results confirm the feasibility of applying computational intelligence to enhance the reliability of IoT network security. The proposed approach can serve as a foundation for building effective next-generation intrusion detection systems systems to improve the resilience of IoT infrastructures.
Keywords: fuzzy controller, Internet of Things, intrusion detection, cyberattacks, security, protection.

Стаття надійшла до редакції / Received 01.06.2025
Прийнята до друку / Accepted 14.07.2025

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Інтернет речей (Internet of Things, IoT) виник як концепція об'єднання окремих фізичних об'єктів у одну єдину мережу з можливістю автоматичного обміну даними через мережу Інтернет. Фізичною базою цієї технології є сенсори, пристрої та засоби бездротового зв'язку, що виконують збір, передавання, приймання та аналіз інформації в реальному часі. Застосування технології IoT сприяє підвищенню ефективності управління, керування та моніторингу у різних сферах, зокрема в промисловості, енергетиці, транспорті та в галузі охорони здоров'я. Важливу роль у функціонуванні Інтернету речей відіграють хмарні обчислення, які забезпечують обробку великих обсягів даних. З огляду на стрімке зростання кількості підключених пристроїв, наразі актуальними є питання безпеки, масштабованості та енергоефективності IoT-систем [1].

Загрози безпеки в Інтернеті речей пов'язані з великою кількістю підключених пристроїв, що часто мають досить обмежені обчислювальні ресурси та недостатній рівень захисту. Окрім того, виникненню вразливостей сприяють слабкі механізми автентифікації та нерегулярне оновлення програмного забезпечення. Потенційні атаки, такі як, наприклад, DDoS-атаки, перехоплення даних та несанкціонований доступ, можуть призвести до втрати конфіденційності, порушення цілісності систем та зупинки роботи критичних сервісів. Особливу небезпеку становить компрометація пристроїв, що інтегрованих у медичні, транспортні або промислові системи, оскільки наслідки можуть бути небезпечними фізично [2]. Таким чином, розроблення та впровадження надійних протоколів захисту, шифрування даних і механізмів автентифікації є основними напрямками забезпечення безпеки пристроїв в IoT-середовищі.

Серйозну загрозу стабільного функціонування розподілених систем і цифрової інфраструктури в Інтернеті речей (IoT) становлять кібератаки. Найбільш поширеними є атаки типу «відмова в обслуговуванні» (DDoS), перехоплення даних, зловмисне перепрограмування пристроїв і несанкціонований контроль над ними. Через обмежені ресурси більшість IoT-пристроїв не мають вбудованих механізмів виявлення та запобігання вторгненням. Вразливості цих систем можуть використати зловмисники з метою створення спеціальних ботнетів, здатних паралізувати великі частини мережевої інфраструктури. Для протидії кібератакам у IoT необхідним є впровадження багаторівневих стратегій безпеки, що включають шифрування, аутентифікацію та безперервний моніторинг мережевої активності.

Важливу роль у забезпеченні безпеки мережевих з'єднань та захисті пристроїв від несанкціонованого доступу в Інтернеті речей відіграють системи виявлення вторгнень (Intrusion Detection Systems, IDS) [3]. Такі системи призначені для здійснення аналізу мережевого трафіку і поведінки пристроїв для виявлення аномалій, що можуть свідчити про наявні кібератаки або порушення політик безпеки. В той же час, при розробленні та впровадженні IDS у середовищі IoT необхідно особливу увагу приділяти вирішенню проблеми покращення ефективності їх функціонуванню в умовах обмежених обчислювальних ресурсів і гетерогенність пристроїв IoT.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Новітні підходи до реалізації IDS часто включають використання методів штучного інтелекту, зокрема машинного навчання та обчислювального інтелекту, з метою підвищення точності виявлення загроз [4]. Ефективність таких систем значною мірою залежить від їхньої здатності працювати в режимі реального часі з мінімальними затримками.

У порівняні із класичними структурами, системи виявлення вторгнень на основі машинного навчання здатні забезпечити більш точне розпізнавання аномальної поведінки пристроїв за рахунок здійснення аналізу великих обсягів даних. Такі системи можуть самостійно адаптуватися до нових типів атак, виявляючи такі типи закономірностей, які важко виявити традиційними методами [5, 6]. Використання алгоритмів класифікації, кластеризації та глибокого навчання дозволяє підвищити ефективність захисту IoT-мережі в умовах обмежених ресурсів [7].

Технології виявлення вторгнень на основі методу обчислювального інтелекту можна розділити на три основні категорії: виявлення вторгнень на основі штучних нейронних мереж, на основі генетичних та еволюційних алгритмів, на основі принципів нечіткої логіки [8]. Системи виявлення вторгнень в Інтернеті речей на основі нейронних мереж функціонують шляхом попереднього навчання моделей на зібраних даних про нормальну та аномальну поведінку мережевих вузлів. Після етапу навчання система аналізує в реальному часі поточний трафік або поведінкові характеристики пристроїв і класифікує їх як безпечні чи потенційно шкідливі [9, 10]. Завдяки здатності до автоматичного оновлення своїх даних, подібні системи характеризуються високою ефективність виявлення нових або змінених типів атак у середовищі Інтернету речей.

Системи виявлення вторгнень на основі генетичного алгоритму аналізують характеристики мережевого трафік пристроїв Інтернету речей та формують цифрові послідовності, які описують правила для класифікації трафіку як нормального або шкідливого. Найбільш точні правила зберігаються та використовуються в реальному часі [11, 12]. Таким чином можливо виявляти навіть невідомі раніше види атак.

В той же час, системи виявлення вторгнень на базі нечіткої логіки застосовують механізми нечіткого висновку для аналізу неоднозначних або частково визначених параметрів мережевої активності [13]. Такий підхід дозволяє ефективно обробляти нечіткі вхідні дані та приймати гнучкі рішення щодо аномальної поведінки пристроїв. Використовуючи правила нечіткої логіки, такі системи здатні із високою точністю виявляти загрози за умов невизначеності, що є характерним для IoT-середовища. Системи виявлення вторгнень на основі нечіткої логіки у Інтернеті речей перетворюють певні мережеві параметри, такі як частота з'єднань, обсяг трафіку або затримка, у нечіткі множини з використанням функцій належності. Далі застосовуються нечіткі правила виводу, які дозволяють оцінити ступінь підозрілості поточної активності з урахуванням нечіткої природи вхідних даних. На основі результатів нечіткого висновку система приймає рішення про наявність або відсутність потенційної загрози, забезпечуючи гнучкий і стійкий до похибок підхід до виявлення атак у мережі Інтернету речей [14].

Перевагою використання систем виявлення вторгнень на основі нечіткої логіки є їх здатність функціонувати в умовах обмеженої кількості попередніх даних, оскільки вони не потребують етапу навчання, характерного для методів машинного навчання [15]. Вони забезпечують високу гнучкість у прийнятті рішень і можуть ефективно працювати з неповною, нечіткою або суперечливою інформацією, що є типовим для середовища Інтернету речей. Нечіткі системи є менш чутливими до незначних змін у вхідних параметрах, що знижує кількість помилкових спрацювань порівняно з деякими алгоритмами машинного навчання. Крім того, вони характеризуються меншою обчислювальною складністю, що є важливою перевагою для застосування в пристроях з обмеженими ресурсами. В той же час, такі системи менш дослідженими, ніж системи на основі машинного навчання. Тому постає важлива задача розроблення та дослідження нечітких контролерів різної складності та з різними наборами вхідних величин, призначених для використання у якості ядра системи виявлення вторгнень у мережу Інтернету речей.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Таким чином, метою даної роботи є розроблення та дослідження нечіткого контролера для використання у системі виявлення вторгнень в мережу Інтернету речей.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Розроблений у рамках даного дослідження нечіткий контролер працює таким чином. На його вхід надходять три параметри, за якими можливо оцінити правильність функціонування пристрою Інтернету речей у рамках можливої наявності атаки на цей пристрій. Вхідні дані обробляються у контролері і на його виході з'являється вихідне значення, яке відповідає ймовірність, що цей досліджуваний пристрій зазнав атаки, тобто виявити вторгнення у мережу Інтернету речей.

Вхідними лінгвістичними змінними нечіткого контролеру, запропонованої в цьому дослідженні, є число переданих пакетів, швидкість передачі пакетів та коефіцієнт доставки пакетів. Вони були обрані виходячи із наступних міркувань.

Число переданих пакетів пристрою Інтернету речей є кількісним показником, що відображає загальну кількість інформаційних пакетів, які пристрій надіслав до інших вузлів мережі за певний проміжок часу. У контексті мережевих комунікацій це число характеризує обсяг мережевого трафіку, згенерованого пристроєм, і може слугувати індикатором його активності, навантаження або ж потенційної загрози. Цей показник є важливим параметром у задачах моніторингу та виявлення аномалій. Зокрема, різке зростання числа переданих пакетів може свідчити про спробу несанкціонованого вторгнення.

Швидкість передавання пакетів пристрою характеризує інтенсивність мережевої активності пристрою, і визначається як кількість пакетів даних, що передаються ним за одиницю часу. Також цей показник є критичним для своєчасного виявлення аномалій у мережевому трафіку.

Коефіцієнт доставки пакетів пристрою визначається як відношення кількості успішно отриманих пакетів до кількості пакетів, що були надіслані пристроєм. Високі значення цього коефіцієнта свідчать про надійність мережевих зв'язків і стабільність передачі даних, тоді як низький коефіцієнт доставки може вказувати на проблеми, пов'язані з несправністю пристроїв або атакою на мережу.

Вихідною змінною розробленого нечіткого контролеру є ймовірність вторгнення для конкретного пристрою Інтернету речей. Це є ймовірнісна метрика, що відображає ступінь ризику для пристрою з боку зовнішніх чи внутрішніх загроз. В даному випадку, це значення в інтервалі від 0 до 100, яке показує, наскільки імовірним є те, що пристрій буде об'єктом атаки або вже зазнав вторгнення. Ймовірність вторгнення виступає як інформативний показник поточної безпекової ситуації щодо окремого IoT-пристрою та загального стану кіберзахисту в мережі Інтернету речей.

Розроблений нечіткий контролер функціонує відповідно до 27 нечітких правил, які формалізують взаємозв'язки між вхідними параметрами та вихідним результатом. Така кількість правил забезпечує достатній рівень деталізації для адекватного моделювання складних залежностей у межах досліджуваної задачі.

Для дослідження функціонування розробленого нечіткого контролера нечіткого виводу було використано середовище MATLAB, яке забезпечує широкі можливості для моделювання, аналізу та візуалізації результатів роботи інтелектуальних систем. Застосування даного програмного забезпечення дозволило здійснити перевірку ефективності запропонованої моделі та оцінити її поведінку. Загальний вигляд розробленого нечіткого контролера системи виявлення вторгнень в програмі MATLAB подано на рис.1.

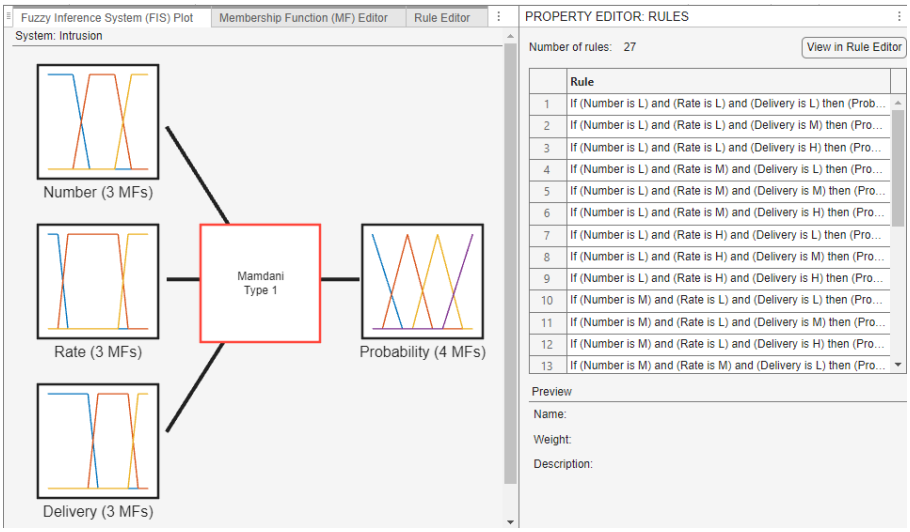

Рис. 1. Нечіткий контролер системи виявлення вторгнень в програмі MATLAB

У процесі розроблення нечіткого контролера у програмі MATLAB були введені вхідні та вихідні змінні з відповідним визначенням діапазонів значень та функцій належності для кожної терм-множини. Після цього була сформована база правил, що встановлює логічні зв'язки між вхідними параметрами та вихідною реакцією системи. Далі було виконане налаштування методів агрегування, імплікації та дефаззифікації відповідно до обраної моделі логічного висновку.

Симуляція роботи нечіткого контролера у програмному середовищі MATLAB виконується за допомогою вбудованих інструментів візуалізації та аналізу поведінки системи. Ці засоби дозволяють швидко перевірити коректність побудованої бази правил і функцій належності. Результат моделювання роботи нечіткого контролера системи виявлення вторгнень подано на рис.2.

Для перевірки здатності розробленого нечіткого контролера системи виявлення вторгнення адекватно приймати рішення здійснено його валідацію на основі тестових даних.

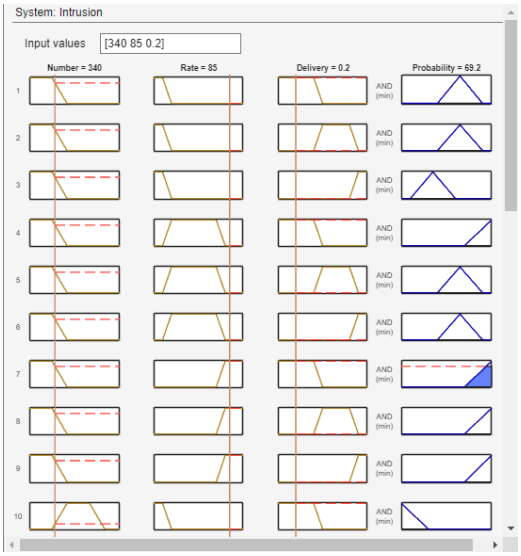

Рис. 2. Результати симуляції роботи нечіткого контролера

Результати валідації нечіткого контролера відображають відповідність між виходами розробленої моделі та еталонними значеннями, отриманими на основі тестових даних. Після подачі вхідних параметрів здійснюється обчислення вихідних значень за допомогою функції нечіткого висновку, і порівняння їх з

реальними результатами, що містяться у валідаційній вибірці. Отримано результати у вигляді графіків, де візуально зіставляються фактичні та змодельовані значення (рис.3). Так як на графіку відсутні значні відхилення результатів валідації, можна прийняти, що розроблений нечіткий контролер системи виявлення вторгнень у мережу Інтернету речей працює із прийнятною точністю.

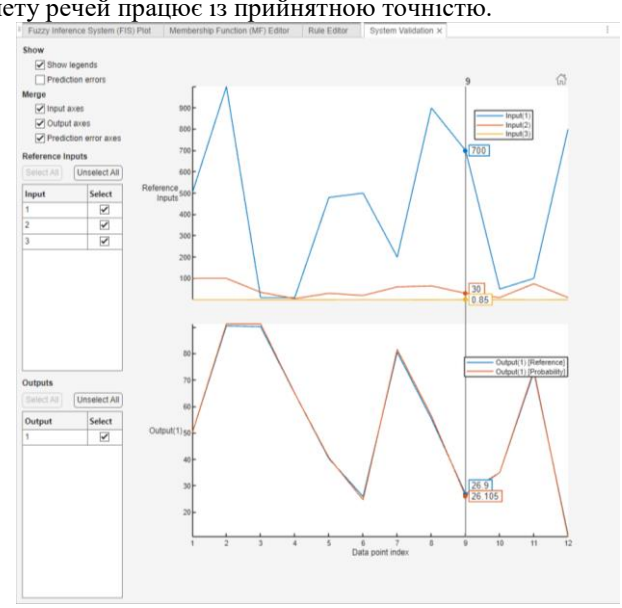

Рис. 3. Результати валідації роботи нечіткого контролера

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Стаття присвячена розгляду актуальної проблеми забезпечення безпеки в середовищі Інтернету речей (IoT) шляхом виявлення вторгнень із використанням технологій обчислюваного інтелекту. Здійснено аналіз можливостей та доцільності застосування технологій обчислюваного інтелекту для виявлення вторгнень у середовищі Інтернету речей. Проведене дослідження засвідчило, що традиційні підходи до виявлення атак є недостатньо ефективними в умовах динамічної та ресурсно-обмеженої IoT-інфраструктури. Натомість інтелектуальні методи демонструють високу здатність як до виявлення відомих атак, так і адаптації до нових. Запропонований у статті підхід спрямований на створення адаптивних і точних рішень для проактивного виявлення загроз в IoT, що є критично важливим для захисту сучасної кіберфізичної інфраструктури. Отримані результати підтверджують ефективність запропонованого підходу в умовах обмеженої інформації та демонструють високу точність.

Література

1. Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., & Stiller, B. (2022). Landscape of IoT security. Computer Science Review, 44, 100467. https://doi.org/10.1016/j.cosrev.2022.100467

2. Sarker, I. H., Khan, A. I., Abushark, Y. B., & Alsolami, F. (2022). Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions. Mobile Networks and Applications, 28(1), 296–312. https://doi.org/10.1007/s11036-022-01937-3

3. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity, 2(1). https://doi.org/10.1186/s42400-019-0038-7

4. Alsoufi, M. A., Razak, S., Siraj, M. M., Nafea, I., Ghaleb, F. A., Saeed, F., & Nasser, M. (2021). Anomaly-Based Intrusion Detection Systems in IoT Using Deep Learning: A Systematic Literature Review. Applied Sciences, 11(18), 8383. https://doi.org/10.3390/app11188383

5. Arunkumar, M., & Ashok Kumar, K. (2022). Malicious attack detection approach in cloud computing using machine learning techniques. Soft Computing, 26(23), 13097–13107. https://doi.org/10.1007/s00500-021-06679-0

6. Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2020). Machine Learning in IoT Security: Current Solutions and Future Challenges. IEEE Communications Surveys & Tutorials, 22(3), 1686–1721. https://doi.org/10.1109/comst.2020.2986444

7. Mittal, M., Kumar, K., & Behal, S. (2022). Deep learning approaches for detecting DDoS attacks: a systematic review. Soft Computing, 27(18), 13039–13075. https://doi.org/10.1007/s00500-021-06608-1

8. Wu, S. X., & Banzhaf, W. (2010). The use of computational intelligence in intrusion detection systems: A review. Applied Soft Computing, 10(1), 1–35. https://doi.org/10.1016/j.asoc.2009.06.019

9. Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P.-L., Iorkyase, E., Tachtatzis, C., & Atkinson, R.

(2016). Threat analysis of IoT networks using artificial neural network intrusion detection system. In 2016 International Symposium on Networks, Computers and Communications (ISNCC) (pp. 1–6). IEEE. https://doi.org/10.1109/isncc.2016.7746067

10. Chiba, Z., Abghour, N., Moussaid, K., omri, A. E., & Rida, M. (2016). A Cooperative and Hybrid Network Intrusion Detection Framework in Cloud Computing Based on Snort and Optimized Back Propagation Neural Network. Procedia Computer Science, 83, 1200–1206. https://doi.org/10.1016/j.procs.2016.04.249

11. Zhang, Y., Li, P., & Wang, X. (2019). Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network. IEEE Access, 7, 31711–31722. https://doi.org/10.1109/access.2019.2903723

12. Suhaimi, H., Suliman, S. I., Musirin, I., Harun, A. F., & Mohamad, R. (2019). Network intrusion detection system by using genetic algorithm. Indonesian Journal of Electrical Engineering and Computer Science, 16(3), 1593. https://doi.org/10.11591/ijeecs.v16.i3.pp1593-1599

13. Iyengar, N. Ch. S. N., Banerjee, A., & Ganapathy, G. (2022). A Fuzzy Logic Based Defense Mechanism against Distributed Denial of Services Attack in Cloud Environment. International Journal of Communication Networks and Information Security (IJCNIS), 6(3). https://doi.org/10.17762/ijcnis.v6i3.864.

14. Almseidin, M., Al-Sawwa, J., & Alkasassbeh, M. (2021). Anomaly-based Intrusion Detection System Using Fuzzy Logic. In 2021 International Conference on Information Technology (ICIT) (pp. 290–295). 2021 International Conference on Information Technology (ICIT). IEEE. https://doi.org/10.1109/icit52682.2021.9491742

15. Khraisat, A., Alazab, A. (2021). A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecurity, 4(1). https://doi.org/10.1186/s42400-021-00077-7

References

1. Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., & Stiller, B. (2022). Landscape of IoT security. Computer Science Review, 44, 100467. https://doi.org/10.1016/j.cosrev.2022.100467

2. Sarker, I. H., Khan, A. I., Abushark, Y. B., & Alsolami, F. (2022). Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions. Mobile Networks and Applications, 28(1), 296–312. https://doi.org/10.1007/s11036-022-01937-3

3. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity, 2(1). https://doi.org/10.1186/s42400-019-0038-7

4. Alsoufi, M. A., Razak, S., Siraj, M. M., Nafea, I., Ghaleb, F. A., Saeed, F., & Nasser, M. (2021). Anomaly-Based Intrusion Detection Systems in IoT Using Deep Learning: A Systematic Literature Review. Applied Sciences, 11(18), 8383. https://doi.org/10.3390/app11188383

5. Arunkumar, M., & Ashok Kumar, K. (2022). Malicious attack detection approach in cloud computing using machine learning techniques. Soft Computing, 26(23), 13097–13107. https://doi.org/10.1007/s00500-021-06679-0

6. Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2020). Machine Learning in IoT Security: Current Solutions and Future Challenges. IEEE Communications Surveys & Tutorials, 22(3), 1686–1721. https://doi.org/10.1109/comst.2020.2986444

7. Mittal, M., Kumar, K., & Behal, S. (2022). Deep learning approaches for detecting DDoS attacks: a systematic review. Soft Computing, 27(18), 13039–13075. https://doi.org/10.1007/s00500-021-06608-1

8. Wu, S. X., & Banzhaf, W. (2010). The use of computational intelligence in intrusion detection systems: A review. Applied Soft Computing, 10(1), 1–35. https://doi.org/10.1016/j.asoc.2009.06.019

9. Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P.-L., Iorkyase, E., Tachtatzis, C., & Atkinson, R. (2016). Threat analysis of IoT networks using artificial neural network intrusion detection system. In 2016 International Symposium on Networks, Computers and Communications (ISNCC) (pp. 1–6). IEEE. https://doi.org/10.1109/isncc.2016.7746067

10. Chiba, Z., Abghour, N., Moussaid, K., omri, A. E., & Rida, M. (2016). A Cooperative and Hybrid Network Intrusion Detection Framework in Cloud Computing Based on Snort and Optimized Back Propagation Neural Network. Procedia Computer Science, 83, 1200–1206. https://doi.org/10.1016/j.procs.2016.04.249

11. Zhang, Y., Li, P., & Wang, X. (2019). Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network. IEEE Access, 7, 31711–31722. https://doi.org/10.1109/access.2019.2903723

12. Suhaimi, H., Suliman, S. I., Musirin, I., Harun, A. F., & Mohamad, R. (2019). Network intrusion detection system by using genetic algorithm. Indonesian Journal of Electrical Engineering and Computer Science, 16(3), 1593. https://doi.org/10.11591/ijeecs.v16.i3.pp1593-1599

13. Iyengar, N. Ch. S. N., Banerjee, A., & Ganapathy, G. (2022). A Fuzzy Logic Based Defense Mechanism against Distributed Denial of Services Attack in Cloud Environment. International Journal of Communication Networks and Information Security (IJCNIS), 6(3). https://doi.org/10.17762/ijcnis.v6i3.864.

14. Almseidin, M., Al-Sawwa, J., & Alkasassbeh, M. (2021). Anomaly-based Intrusion Detection System Using Fuzzy Logic. In 2021 International Conference on Information Technology (ICIT) (pp. 290–295). 2021 International Conference on Information Technology (ICIT). IEEE. https://doi.org/10.1109/icit52682.2021.9491742

15. Khraisat, A., Alazab, A. (2021). A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecurity, 4(1). https://doi.org/10.1186/s42400-021-00077-7