Рудий Роман Олегович, аспірант,

Чернівецький національний університет

імені Юрія Федьковича, м. Чернівці

<https://orcid.org/0009-0002-5161-5032>

**ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ РЕКОНФІГУРОВНИХ АПАРАТНИХ ЗАСОБІВ У ТЕХНОЛОГІЯХ ІНТЕРНЕТУ РЕЧЕЙ З ПЕРСОНІФІКОВАНИМ ДОСТУПОМ**

Захист даних у сучасному світі має вирішальне значення, оскільки він забезпечує конфіденційність особистої інформації, запобігає маніпуляції фінансових та особистих даних третіми особами, забезпечує цілісність даних та підтримує довіру до підприємств та установ. Витік даних може мати значні наслідки - від фінансових втрат до шкоди репутації, що робить захист даних фундаментальною вимогою в нашу взаємопов'язану цифрову епоху.

На сьогоднішній день використання систем доступу до інформації стало звичною справою. Кожна зацікавлена особа може створити персональний обліковий запис та використовувати різноманітні сервіси у своїх цілях. Проте, чим більше людей використовують такі системи, тим більше з’являється кіберзагроз[1].

Однією з глобальною системою для збирання, обробки та маніпуляцією даними є Інтернет речі (IoT). IoT забезпечує платформу для з'єднання пристроїв через локальну або мережу Інтернет. За останні кілька років IoT набуло значної популярності як серед споживачів, так і в промисловості [2], а кількість підключених пристроїв вже перевищила 50 мільярдів до 2020 року. Завдяки великій кількості нових «розумних» послуг і продуктів, таких як розумна техніка, розумні будинки, розумні годинники, смарт-телевізори тощо, пристрої IoT швидко поширюються в усіх середовищах.

IoT включає в себе виробництво обладнання, розробку програмного забезпечення, радіозв'язок тощо. Очевидно, що всі ці компоненти повинні бути захищені. В останні роки все більша увага приділяється ризикам, пов’язаним з використанням простих пристроїв IoT у службах, які мають доступ до конфіденційної інформації або критично важливих засобів контролю, таких як відеозаписи з камер, система позиціювання в режимі реального часу, моніторинг, контроль доступу до будівель, промислові процеси, світлофори[3].

Одним із способів для забезпеченні захисту в IoT від деяких вразливостей є застосування програмованих логічних інтегральних схем (ПЛІС) на вентильній матриці. Ця інтегральна схема, призначена для програмування користувачем або розробником після виготовлення. Архітектура ПЛІС є унікальною, оскільки вона дозволяє користувачам визначати функціональні можливості та взаємозв’язки цифрової логіки всередині мікросхеми, що робить її надзвичайно універсальною та адаптованою для різних задач[4]. Таким чином, є можливість для побудови всередині ПЛІС від простого логічного вентилю до складної системи на кристалі. Схему стали використовувати для багатьох різних задач, таких як цифрова обробка сигналів, обробка зображень, криптографія[5], паралельна обробка, системи відмовостійкості, системи з низьким енергоспоживанням, моделювання, цифрове управління, штучний інтелект, мережеві технології, великі дані тощо[6]. Одним з підвиду ПЛІС є вбудована програмована логічна матриця (eFPGA), яку можна вбудувати безпосередньо в мікроконтролер. Вони часто використовуються для додавання можливостей програмованої логіки без необхідності окремого FPGA чіпа[7]. Впровадження FPGA в IoT можуть зробити системи більш безпечними за рахунок апаратної особливості чіпів, що дозволить забезпечити захисту від несанкціонованого доступу, виявлення загроз у реальному часі, безпечної ідентифікації, цілісності даних.

Використання реконфігурованих апаратних засобів може сприяти підвищенню безпеки даних у сучасних системах IoT, надаючи можливість захищати і забезпечувати цілісність даних в реальному часі. Це важливий крок у забезпеченні надійного функціонування та захисту великої кількості підключених пристроїв та послуг у взаємопов'язаному світі IoT.

**Література**

1. Altulaihan, E., Alismail, A., & Frikha, M. A survey on web application penetration testing. *Electronics*, 12(5), 1229 (2023). <https://doi.org/10.3390/electronics12051229>

2. Yadav, G., Paul, K., Allakany, A., & Okamura, K. IoT-PEN: an E2E Penetration Testing framework for IoT. *Journal of Information Processing*, 28, 633–642 (2020). <https://doi.org/10.2197/ipsjjip.28.633>

3. IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Journals & Magazine* (2019, October 1). <https://ieeexplore.ieee.org/abstract/document/8796409>

4. Soniya, T., Ragasudha, I., & Valli, P. N. Routing Architecture and Applications of FPGA: A survey. *Journal of Physics: Conference Series*, 1717, 012025 (2021). <https://doi.org/10.1088/1742-6596/1717/1/012025>

5. Kumar, K., Ramkumar, K., & Kaur, A. A lightweight AES algorithm implementation for encrypting voice messages using field programmable gate arrays. *Journal of King Saud University - Computer and Information Sciences*, 34(6), 3878–3885 (2022). <https://doi.org/10.1016/j.jksuci.2020.08.005>

6. Ruiz-Rosero, J., Ramirez-Gonzalez, G., & Khanna, R. Field Programmable Gate Array Applications—A Scientometric Review. *Computation*, 7(4), 63 (2019). <https://doi.org/10.3390/computation7040063>

7. Bouaziz, K. A review on embedded field programmable gate array architectures and configuration tools. *Turkish Journal of Electrical Engineering & Computer Sciences*, 28(1), 15–28 (2020). <https://journals.tubitak.gov.tr/elektrik/vol28/iss1/2/>