RESEARCHING AND EVALUATION OF NETWORK-BASED INTRUSION DETECTION SYSTEM BASED ON SWARM LEARNING FOR IOT

Phạm Nguyễn Hải Anh - 21520586
Ngô Thanh Sang - 21522543

Tóm tắt

- Link Github của nhóm: https://github.com/PNg-HA/CS519.O21.KHTN
- Link YouTube video: https://youtu.be/CdB5sbcwIQ8

Phạm Nguyễn Hải Anh

Ngô Thanh Sang

Giới thiệu

- Hiện nay, nhu cầu sử dụng các thiết bị IoT ngày càng tăng nhanh.
- Sự phát triển chóng mặt kèm theo những thách thức về an ninh thông tin.
- Các hệ thống phát hiện xâm nhập mạng (NIDS) sử dụng mô hình Centralized Learning và Federated Learning chưa đảm bảo hoàn toàn tính bảo mật cũng như tính riêng tư của dữ liệu.

=> Sử dụng khung học bầy đàn (Swarm Learning Framework) tích hợp mã hóa đồng cấu để giải quyết những điểm yếu của các phương pháp trên.

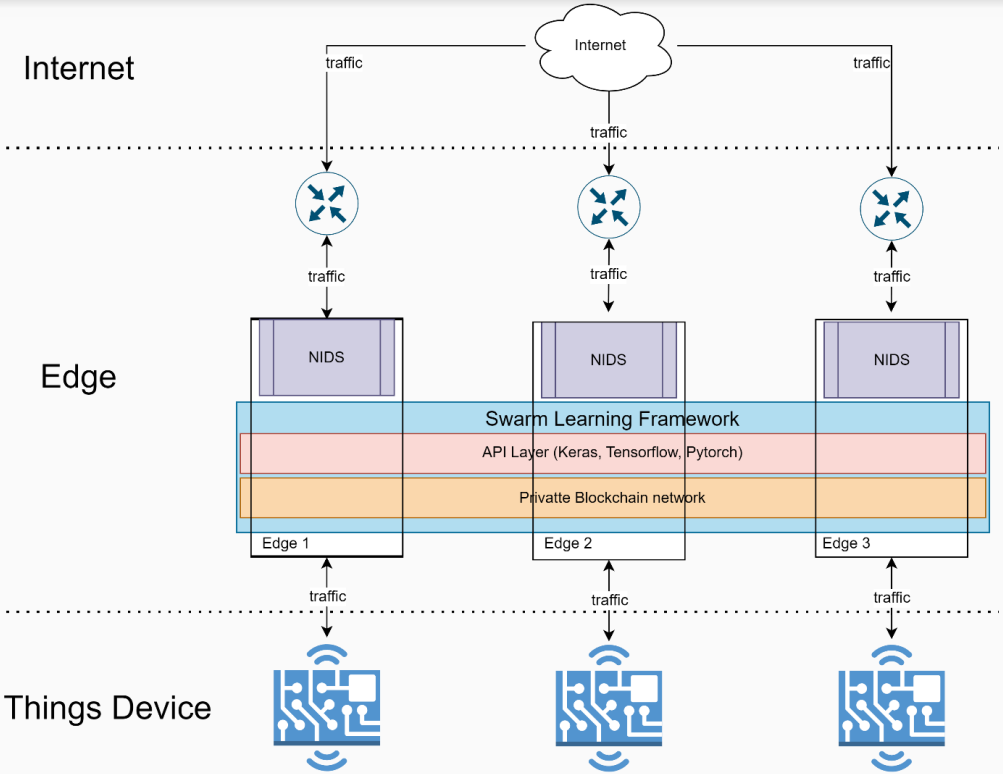
Mục tiêu

- Nghiên cứu triển khai framework học bầy đàn để đảm bảo tính an toàn trong mạng lưới cũng như quyền riêng tư dữ liệu của người dùng.

- Xây dựng mô hình học sâu tích hợp mã hóa đồng cấu cho hệ thống phát hiện xâm nhập mạng cho IoT trên framework học bầy đàn.

- Đánh giá hiệu suất của hệ thống NIDS được đề xuất.

Mục tiêu

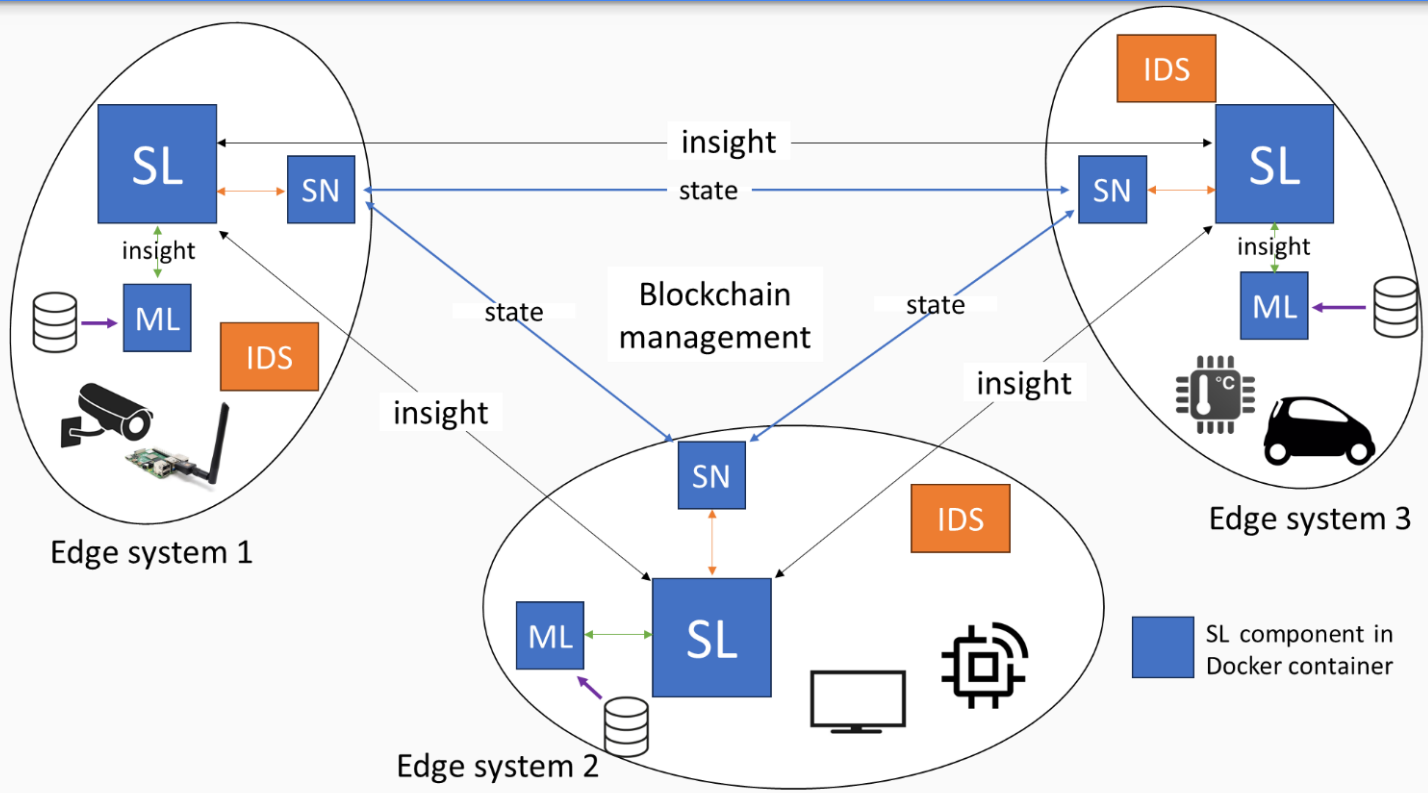


Hình 1: Mô hình triển khai

Nội dung và Phương pháp

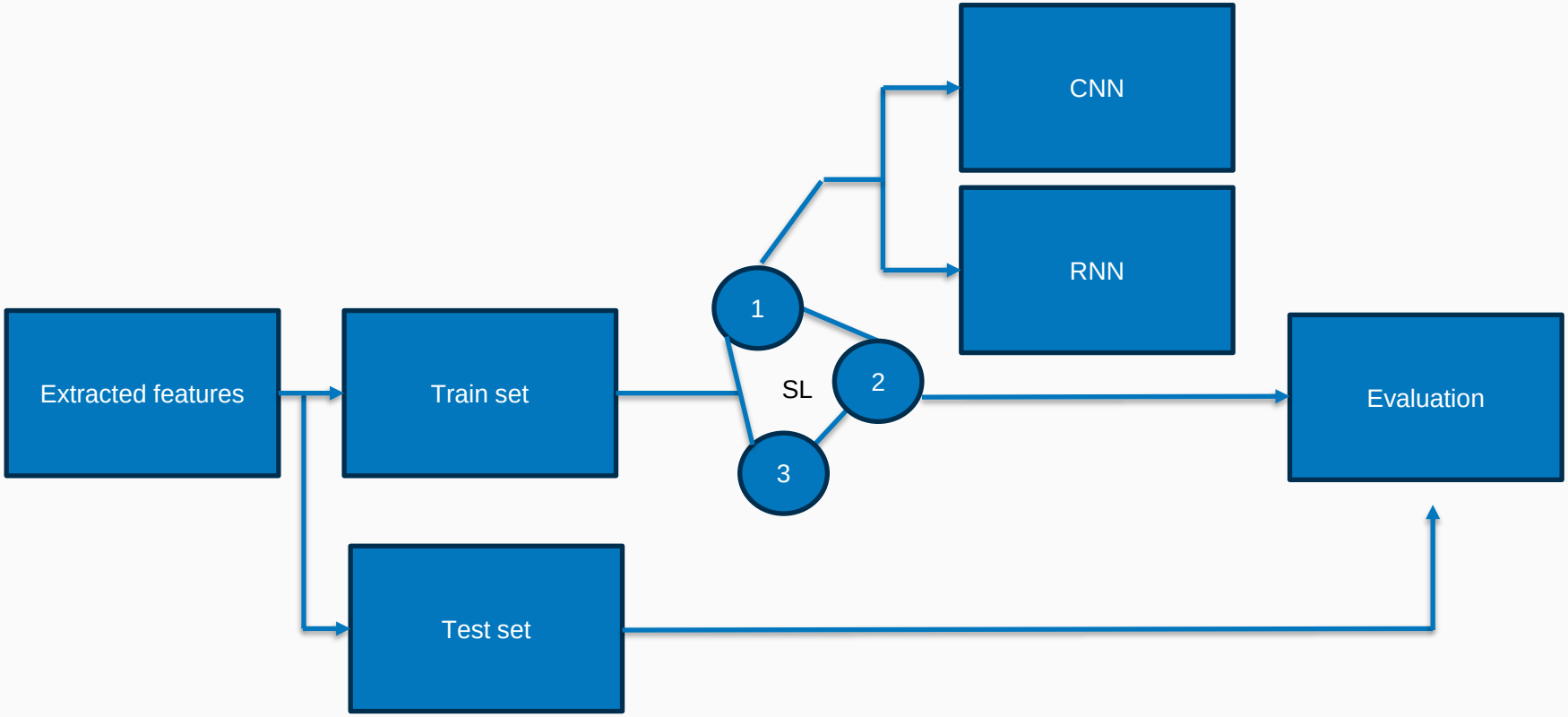
- Nghiên cứu và tìm hiểu các công nghệ liên quan (CNN, RNN trên FL, nghệ Blockchain trong framework học bầy đàn,...).
- Nghiên cứu, triển khai hệ thống trên framework học bầy đàn.
- Xây dựng mô hình học sâu tích hợp mã hóa đồng cấu trên trên khung học bầy đàn.
- Thực nghiệm, đánh giá hiệu suất.

Nội dung và Phương pháp



Hình 2: Mô hình hoạt động của khung học bầy đàn

Nội dung và Phương pháp



Kết quả dự kiến

- Đề xuất, triển khai hệ thống phát hiện xâm nhập mạng cho hạ tầng IoT cloud của khoa Mạng máy tính và Truyền thông – UIT trên nền học sâu phân tán với framework Swarm Learning. Qua đó đảm bảo tính bảo mật cho hệ thống IoT và đánh giá hiệu suất khi huấn luyện trên các tập dữ liệu lớn.

Tài liệu tham khảo

1. Li, Y., Chen, C., Liu, N., Huang, H., Zheng, Z., & Yan, Q: A blockchain-based decentralized federated learning framework with committee consensus. IEEE Network 2020: 234-241.
2. Sun, Y., Ochiai, H., & Esaki, H: Decentralized deep learning for multi-access edge computing: A survey on communication efficiency and trustworthiness. IEEE Transactions on Artificial Intelligence 2021: 963-972.
3. Warnat-Herresthal, S., Schultze, H., Shastry, K. L., Manamohan, S., Mukherjee, S., Garg, V., ... & Schultze, J. L.: Swarm learning for decentralized and confidential clinical machine learning. Nature 2021: 265-270.
4. Rashid, M. M., Khan, S. U., Eusufzai, F., Redwan, M. A., Sabuj, S. R., & Elsharief, M.: A Federated Learning-Based Approach for Improving Intrusion Detection in Industrial Internet of Things Networks. Network 2023: 158-179.
5. Moustafa, N.: A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets. Sustainable Cities and Society 2021: 102994.
6. Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B.: Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. Future Generation Computer Systems 2019: 779-796.