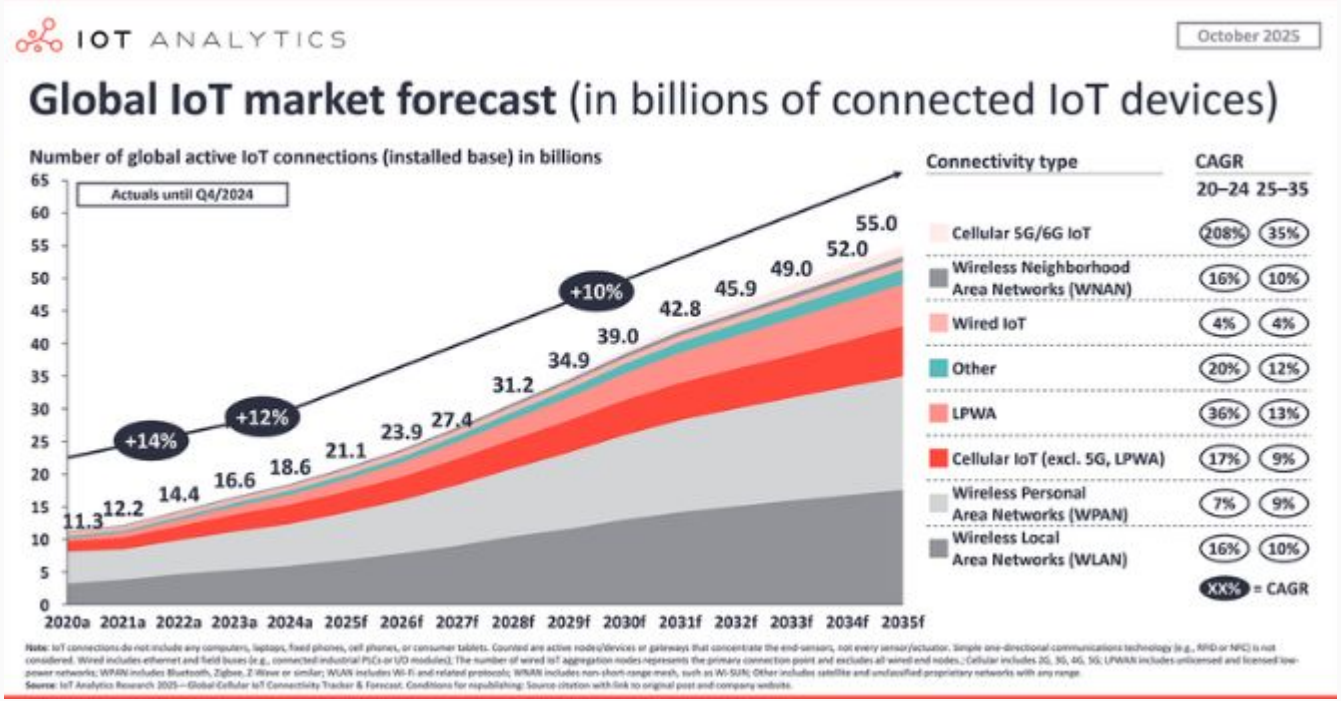
BUILDING AN INTELLIGENT EDGE SECURITY GATEWAY FOR IOT MALWARE DETECTION USING DEEP NEURAL NETWORKS

Tóm tắt

- Lớp: CS2205.CH201
- Link Github của nhóm: https://github.com/VanDo-27-2-2024/CS2205.CH201
- Link YouTube video: https://youtu.be/wCjZTluYy1c

- Họ và Tên: Đỗ Đình Vạn
- MSSV: 250202027

Bối cảnh


IOT ANALYTICS
October 2025
Global IoT market forecast (in billions of connected IoT devices)
Number of global active IoT connections (installed base) in billions
Actuals until Q4/2024
65
60
55
50
45
40
35
30
25
20
15
10
5
0
11.3
12.2
14.4
16.6
18.6
21.1
23.9
27.4
31.2
34.9
39.0
42.8
45.9
49.0
52.0
55.0
+14%
+12%
+10%
2020a 2021a 2022a 2023a 2024a 2025f 2026f 2027f 2028f 2029f 2030f 2031f 2032f 2033f 2034f 2035f
Connectivity type
CAGR
20–24 25–35
Cellular 5G/6G IoT 208% 35%
Wireless Neighborhood Area Networks (WNAN) 16% 10%
Wired IoT 4% 4%
Other 20% 12%
LPWA 36% 13%
Cellular IoT (excl. 5G, LPWA) 17% 9%
Wireless Personal Area Networks (WPAN) 7% 9%
Wireless Local Area Networks (WLAN) 16% 10%
XX% = CAGR

Bối cảnh

Lỗ hổng từ các thiết bị IOT

Bảo mật yếu kém từ thiết kế:

- Sử dụng mật khẩu mặc định (admin/admin, root/12345) và hardcoded credentials.
- Hệ điều hành cũ, ít được cập nhật bản vá (Unpatched Firmware).

Tài nguyên hạn chế:

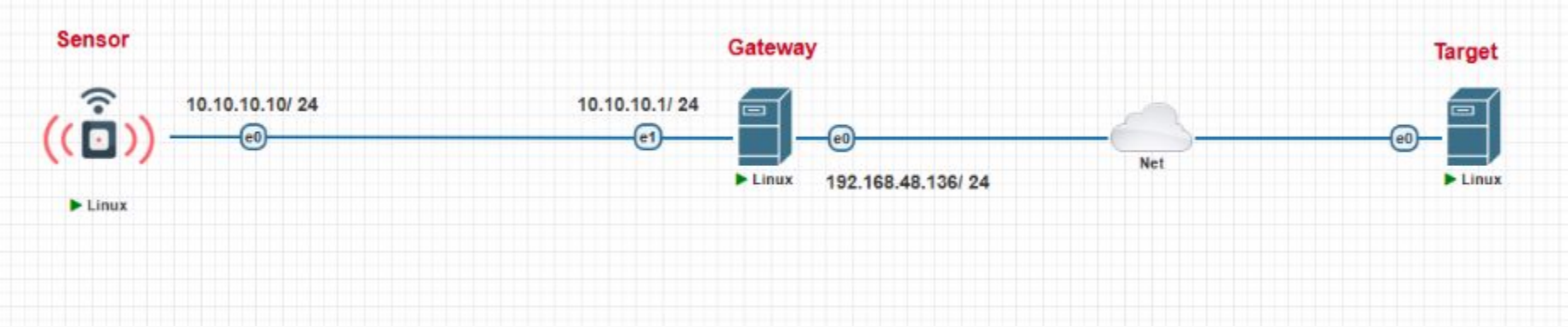
- CPU/RAM thấp → Không thể cài Antivirus hay Firewall cá nhân.
- Hoạt động 24/7 → Mục tiêu lý tưởng để hacker chiếm quyền điều khiển.

Mục tiêu

- **Xây dựng hệ thống giám sát và trích xuất dữ liệu tại biên:** Thiết lập Gateway trên nền tảng Raspberry Pi tích hợp công cụ Zeek để thu thập, phân tích và trích xuất các đặc trưng thống kê của luồng mạng (Flow statistics) theo thời gian thực.
- **Phát triển mô hình Deep Learning nhận diện tấn công:** Thiết kế, huấn luyện và tối ưu hóa mô hình Mạng nơ-ron sâu (DNN) trên bộ dữ liệu IoT-23 để phân loại chính xác lưu lượng bình thường và lưu lượng mã độc (DDoS, Scanning) dựa trên hành vi, không phụ thuộc vào địa chỉ IP.
- **Triển khai và đánh giá thực nghiệm:** Tích hợp mô hình vào Gateway, kiểm thử khả năng hoạt động trong môi trường thực tế với các kịch bản tấn công giả lập, đánh giá hiệu năng dựa trên độ chính xác, độ trễ và khả năng chịu tải.

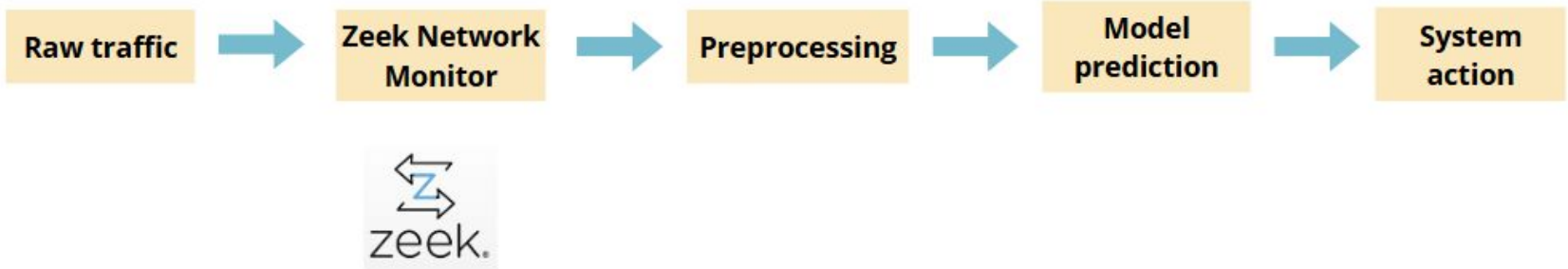
Nội dung và Phương pháp

Kiến trúc hệ thống



Nội dung và Phương pháp

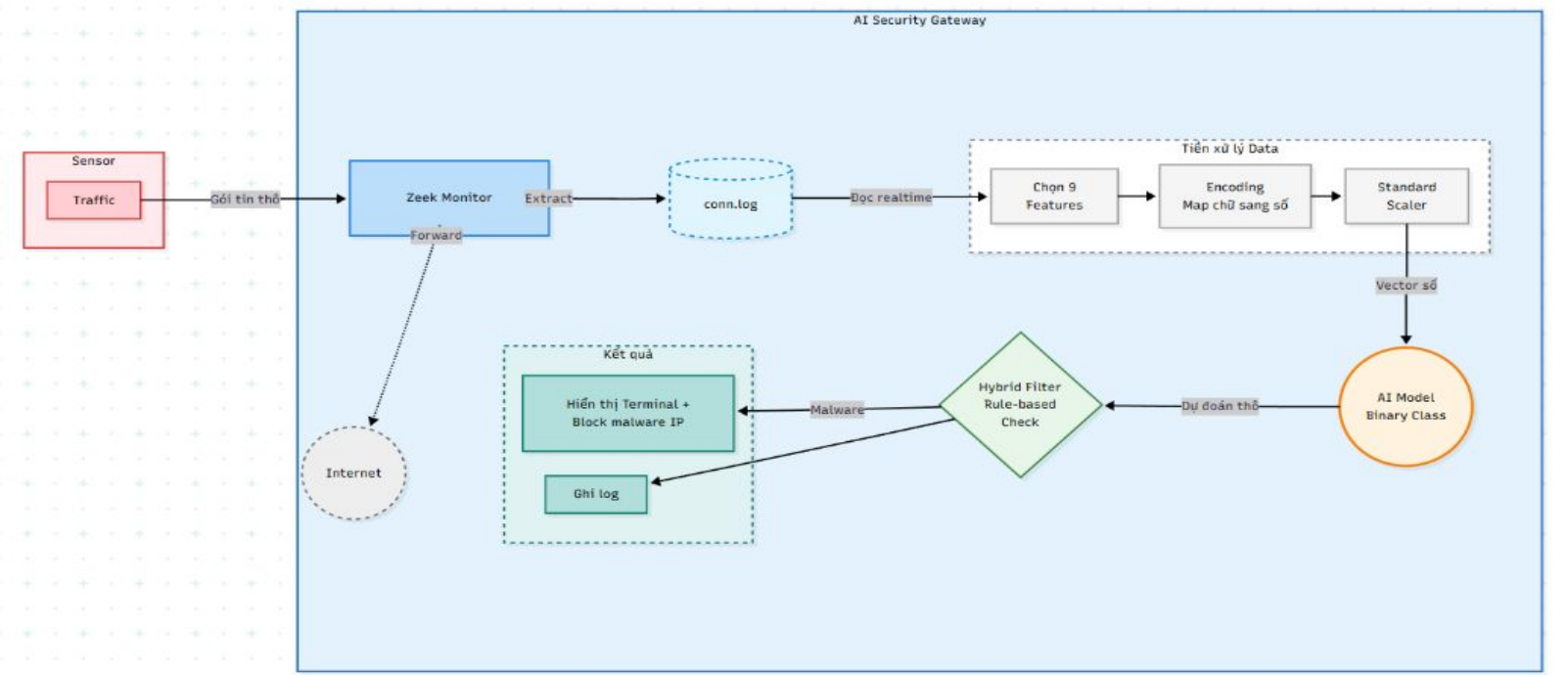
Gateway dataflow



1765760475.439792	CTxVgf107rP0moxTgj	10.10.10.10	50936	142.250.76.4	443	tcp	ssl	0.250443	888	4431	SF	T	F	0	ShADadFf	13	1428	1	4
4995	-	6																	
1765760475.397222	CC0qxGZQooqc8oEqk	10.10.10.10	50564	8.8.8.8	53	udp	dns	0.041677	43	59	SF	T	F	0	Dd	1	71	1	87	-	17
1765760475.397440	C2yoTb2jGU5hEW3hN	10.10.10.10	51627	8.8.8.8	53	udp	dns	0.033633	43	71	SF	T	F	0	Dd	1	71	1	99	-	17
1765760489.589851	CKRYJP1MCxELNHPvub	10.10.10.10	58498	192.168.48.135	80	tcp	http	0.003670	78	292	SF	T	T	0	ShADadFf	6	398	4	588	-	6
1765760499.320374	Cav4hX1GEYYghogIPd	10.10.10.10	42764	23.220.75.245	80	tcp	http	0.618947	136	798	SF	T	F	0	ShADadFf	6	396	5	1002	-	6

Nội dung và Phương pháp

Gateway dataflow



Kết quả dự kiến

- **Đóng góp về Lý thuyết:** Đề xuất kiến trúc cho bài toán gateway phát hiện malware trong IOT.
- **Đóng góp về Kỹ thuật:** Xây dựng thành công module phần mềm cho gateway tích hợp liền mạch cơ chế giám sát thời gian thực giữa công cụ Zeek và xử lý Deep Learning.

Tài liệu tham khảo

[1]. Sebastian Garcia, Agustin Parmisano, Maria Jose Erquiaga: **IoT-23: A labeled dataset with malicious and benign IoT network traffic.** Zenodo 2020.

[2]. Vern Paxson: **Bro: a system for detecting network intruders in real-time.** Computer Networks 31(23-24): 2435-2463 (1999).

[3]. Arnan Sae-Tang, M. L. Dennis Wong, Steven R. Weller: **NID-Net: A Deep Neural Network for Network Intrusion Detection.** ISCIT 2021: 271-276