STT	Title	Year	Author	Link	Dataset	Contribution	Methodology	Metric	Result	Limitation/Futurework	Khai thác	Phương pháp hay
1	Intrusion Detection in Secure Network for Cybersecurity Systems using Machine Learning and Data Mining	22-23 thang 11, năm 2018	1 Hassan Azwar 2 Muhammad Murtaz 3 Mehwish Siddique 4 Saad Rehman	DOI: 10.1109 /ICETAS. 2018.8629 197 https: //ieeexplor e.ieee. org/docum ent/86291 97	CICIDS2017 dataset.	Đánh giá và so sánh nhiều thuật toán ML trên tập CICIDS2017 nhằm phát hiện tấn công mạng.	ML: Decision Tree, Random Forest, XGBoost, Neural Network (MLP, BP) **IDS**	Sử dụng Confusion Matrix để tính: Precision, Recall, F1-score, Accuracy	Accuracy ~92%. Tấn công phổ biến như DDoS/PortScan: độ chính xác >90%. Một số tấn công hiếm như XSS, SQLi: TP Rate gần 0.	Một số tấn công hiếm vẫn có độ chính xác thấp Chưa tích hợp phương pháp xử lý false positive nhiều Phân tích chủ yếu mang tính thống kê, chưa triển khai hệ thống thực tế (real-time)	ICETAS 2018	**IDS vẫn là một lĩnh vực nghiên cứu quan trọng trong an ninh mạng**
2	The Promise of Machine Learning in Cybersecurity	2017	James B. Fraley, Dr. James Cannady (Nova Southeastern University)	10.1109 /SECON. 2017.7925 283 https: //ieeexplor e.ieee. org/docum ent/79252 83/ ?bcId=bc	Private SOC dataset (>9M alerts)	Triển khai thực nghiệm mô hình DNN trong môi trường SOC thực tế để giảm tải phân tích sự kiện bảo mật	6 bước: Data prep → SME review → Model design → Training → TensorFlow/ DNN → Evaluation	Accuracy, Analyst time saved	Accuracy ~99% (test data), tiết kiệm ~78% thời gian cho các nhà phân tích SOC/NOC (từ 2.000h xuống còn ~455h/ngày)	Tiếp tục hỗ trợ tự động phân hồi nâng cao, kết hợp ngữ cảnh để ra quyết định nhanh và giảm false alerts	The Promise of Machine Learning in Cybersecurity	
3	Detecting Network Intrusion Beyond 1999: Applying Machine Learning Techniques to a Partially Labeled Cybersecurity Dataset	2018	Jan Klein, Sandjai Bhulai, Mark Hoogendoorn, Reb van der Mei, Raymond Hinfelaar	DOI: 10.1109 /WI. 2018.0001 7 https: //ieeexplor e.ieee. org/docum ent/86096 97/	Locked Shields 2017 (LS'17)	Áp dụng Autoencoder và Gradient Boosting Machine để phát hiện xâm nhập trên tập dữ liệu bán gán nhãn thực tế từ NATO (LS'17). So sánh với mô hình benchmark CS.0 và đánh giá thêm bằng chuyên gia an ninh.	- Autoencoder (unsupervised) - Gradient Boosting (supervised) - Benchmark CS.0	Accuracy, Precision, Recall, F1-score, nDCG, Expert Analysis	GBM đạt nDCG = 0.993, Precision = 1.0 nhưng Recall = 0.0727. Autoencoder: Recall = 0.982 nhưng Precision = 0.142. Expert xác nhận có 54 tấn công mới được phát hiện bằng Autoencoder.	Autoencoder nhiều false positives. GBM chính xác cao nhưng phát hiện ít. Đề xuất kết hợp kỹ thuật và trích xuất đặc trưng sâu hơn trong tương lai.	Detecting Network Intrusion beyond 1999: Applying Machine Learning Techniques to a Partially Labeled Cybersecurity Dataset	**Autoencoder có thể là công cụ hữu ích để phát hiện zero-day hoặc APT mới.**
4	When Machine Learning Meets Hardware Cybersecurity: Delving into Accurate Zero-Day Malware Detection	2021	Zhangying He et al.	DOI: 10.1109 /ISQED51 717. 2021.9424 330 https: //ieeexplor e.ieee. org/docum ent/94243 30/	Custom dataset (5000 benign + malware apps, HPC)	Đề xuất mô hình phát hiện malware zero-day dựa trên phần cứng (HPC) và ML. Dùng Boosted Random Forest để tăng hiệu quả	So sánh nhiều thuật toán ML (DT, RF, GNB, SGD, LR...) với AdaBoost. Chọn top 4 HPC bằng RFE. Đánh giá trên dữ liệu zero-day.	F1-Score, AUC, TPR, FPR, Latency	Boosted-RF đạt F1 = 92%, TPR = 95%, FPR = 2%. Vượt RF thường (F1 = 88%). Latency thấp (0.018s).	Các ML model chuẩn kém hiệu quả với zero-day. Cần Boosting để tăng khả năng nhận diện. Hạn chế do chỉ dùng 4 HPC và chưa xét tới adversarial evasion.	When Machine Learning Meets Hardware Cybersecurity: Delving into Accurate Zero-Day Malware Detection	Mô hình mạnh nhất là Boosted Random Forest (Boosted-RF)
5	Machine Learning and Deep Learning Methods for Cybersecurity	2018	Yang Xin, Lingshuang Kong, Zhi Liu, Yuling Chen, Yanmiao Li, Hongliang Zhu, Mingcheng Gao, Haixia Hou, Chunhua Wang	DOI: 10.1109 /ACCESS. 2018.2836 950 https: //ieeexplor e.ieee. org/docum ent/83592 87/	KDD Cup 99, NSL-KDD, CICIDS, ADFA	Tổng quan và đánh giá các phương pháp Machine Learning và Deep Learning ứng dụng trong phát hiện xâm nhập mạng và bảo mật hệ thống.	ML (SVM, KNN, Decision Tree, etc), DL (CNN, RNN, DBN, LSTM, etc)	Accuracy, Precision, Recall, F1-score, AUC, ROC	DL thường có độ chính xác cao hơn ML. Ví dụ, CNN đạt ~98.4%, DBN có thể đạt >99%, tùy theo cấu hình mô hình và tập dữ liệu.	Thiếu đánh giá thực nghiệm thực tế sâu, chủ yếu tổng hợp, chưa triển khai hệ thống thực tiễn; nhiều mô hình chỉ đánh giá bằng accuracy.	Machine Learning and Deep Learning Methods for Cybersecurity	Các thuật toán của ML và DL **Giảm false positives: Đặc biệt trong anomaly detection.** **Kết hợp nhiều mô hình (hybrid/ensemble).** **Tăng khả năng phát hiện zero-day attack**
6	Review: Deep Learning Methods for Cybersecurity and Intrusion Detection Systems	2020	Mayra Macas, Chunming Wu	https: //ieeexplor e.ieee. org/docum ent/92823 54/ ?bcId=Iw ZXh0gN bZWtCM TAAARI4 bCAAUzZ	KDD, NSL-KDD, CICIDS2017, ISCX2012	Tổng quan toàn diện về các kiến trúc học sâu (DL) dùng trong phát hiện xâm nhập. Đề xuất khung DL cho IDS.	Tổng quan CNN, RNN, DBN, AE, GAN, SDA, DBM, .; khảo sát nhiều nghiên cứu ứng dụng DL vào IDS	Accuracy, FPR, TPR, F1	RNN đạt 97.09%, AE+DBN tăng từ 89.75% lên 91.4%, GAN giảm FPR từ 19.19% xuống 15.59%, SDA vượt nhiều mô hình khác	Cần đánh giá độ tin cậy & độ bền của IDS DL-based. Còn hạn chế với dữ liệu giả mạo (adversarial). Cần nghiên cứu ứng dụng DL vào real-time IDS.	Review: Deep Learning Methods for Cybersecurity and Intrusion Detection Systems	**Tổng hợp các kiến trúc DL phổ biến: CNN, RNN, DBN, DBM, AE, GANs,..**
7	A Comprehensive Survey of Databases and Deep Learning Methods for Cybersecurity and Intrusion Detection Systems	2020	D. Gümüşbaş, T. Yıldırım, A. Genovese, F. Scotti	DOI: 10.1109 /JSYST. 2020.2992 966 https: //ieeexplor e.ieee. org/docum ent/90998 44/	KDD99, NSL-KDD, CICIDS2017, AWID2018, etc.	Tổng quan toàn diện các phương pháp Deep Learning dùng trong IDS và phân tích chi tiết các bộ dữ liệu benchmark thường dùng trong an ninh mạng.	So sánh các DL models: DBN, AE, CNN, LSTM, GAN; Phân tích chi tiết cách tiền xử lý dữ liệu, chuyển đổi định dạng, ưu/nhược của các kiến trúc DL	Accuracy, F1-Score, TPR, FPR	CNN, LSTM, và AE đạt hiệu quả cao trên nhiều tập dữ liệu; AE+GMM cải thiện phân lớp DoS/Probe; Hybrid CNN-LSTM có tiềm năng cao; GANs hỗ trợ tạo dữ liệu huấn luyện	Thiếu đánh giá về tính thời gian thực; nhiều DL models chưa được áp dụng thực tế; độ tin cậy dataset chưa được đảm bảo; cần nghiên cứu bias của dữ liệu benchmark	A Comprehensive Survey of Databases and Deep Learning Methods for Cybersecurity and Intrusion Detection Systems	Tổng quan toàn diện các phương pháp Deep Learning dùng trong IDS