Grenze International Journal of Engineering and Technology, January Issue

Deep Learning with Domain Adaptation for Cross-Dataset Generalization in Intrusion Detection Systems

Ms. Gowri S[1], Ms. Keerthikhaa K R[2], Ms. Jayasasirekha M[3], Ms. Madhupriya T[4] and Ms. Kavya R[5]
[1]Assistant Professor, Department of Artificial Intelligence and Data Science, Sri Eshwar College of Engineering (Autonomous) Coimbatore, India
Email: gowri.s@sece.ac.in
[2-5]Department of Artificial Intelligence and Data Science, Sri Eshwar College of Engineering (Autonomous) Coimbatore, India
Email: gugapriya05@gmail.com, jayasasirekha30032005@gmail.com, m38264309@gmail.com, kavyaramasamy80@gmail.com

***Abstract*— In order to defend networks against cyber attacks, we require intrusion detection systems - commonly referred to as IDS. While these systems function well with common datasets, artificial intelligence (AI) based intrusion detection systems tend to fail under different scenarios. The source of these failures is reliance on certain datasets and discrepancies in the distribution of the datasets. Therefore, availability of these datasets is problematic to relying on AI for false positive and accuracy metrics in real-world situations, where the patterns of attack and traffic can vary significantly. To address this issue, we present a deep learning-based IDS using domain adaptation to improve efficiency across diverse datasets. Utilizing convolutional and recurrent neural networks for traffic feature identification, we combine domain-adversarial training (DANN) with correlation alignment (CORAL) to reduce the differential between source and target domains. Experiments on ToN-IoT, UNSW-NB15, and CIC-IDS2017 show the performance of traditional deep models presented consistently lower results across categories in various datasets. Our approach provides 10-15% improvements in accuracy and reductions in false positive. This approach highlights the potential of domain adaptation for producing flexible and effective IDS for corporate, cloud, and Internet of Things settings. Regardless of parameters, the experiments demonstrate the need of domain adaptation for producing flexible and effective IDS for cloud, corporate, and IoT environments.Keywords— Intrusion Detection System (IDS), Deep Learning, Domain Adaptation, Cross-Dataset Generalization, CORAL, DANN, Cybersecurity, IoT Security.**

***Index Terms*— first term, second term, third term, fourth term, fifth term and sixth term.**

I. INTRODUCTION

Intrusion detection systems (IDS) play a crucial role in protecting today's digital environments in light of the increase of cyberthreats. IDS assists decision-makers in cloud, IoT, and enterprise networks by identifying unusual behavior and providing recommendations. How well they perform in a range of situations when aggressive conduct and traffic patterns are continuously changing will decide how effective they are.

Grenze ID: 01.GIJET.12.1.77_1

Typically, artificial intelligence-based intrusion detection systems (IDS) work well with normal datasets but struggle to operate with datasets with rare occurrences. Traditional models also have difficulty generalizing to many distributions of data, depending largely on the dataset. The proposed solution is to use a combination of convolutional and recurrent deep learning models and ways to help machines adapt to variations in data and unforeseen threats from data distributions or patterns in the future, such as using techniques like correlation alignment (CORAL) and domain adversarial neural networks (DANN). The machine adapts quickly to unforeseen traffic patterns in the datasets. Adaptive ability improves accuracy and lessens false positives. High-stakes domains can be anything from cloud services and incentivized delivery methods/internet of things ecosystems to hospitals/infrastructures and organizational infrastructures,this approach enables the development of effective, scalable, and user-centric IDS solutions. Additionally, it offers immediate benefits in cybersecurity. The use of generalized IDS that are cross-dataset will affect critical infrastructure, digital trust and national security, but also offer immediate value to cybersecurity. As we see in smart cities, healthcare, and industrial IoT, where many devices will generate traffic that is uniquely different, domain-adaptive deep learning can provide continuous and resilient security that does not require complete retraining for every new environment. More broadly, in a cloud and edge computing environment that will see different workloads, they can achieve similar scalable, yet resilient intrusion detection capabilities. This study describes a new technological development and it also supports a paradigm shift of sustainable cybersecurity. from models that are data dependent, to intelligent and adaptive IDS that can learn and adjust to new threats, thus laying a groundwork for more secure and dependable digital environments in multiple areas.

TABLE I. TYPE SIZES FOR CAMERA-READY PAPERS

Type size (pts.)	Appearance		
	Regular	Bold	Italic
8	Table captions,[a] table superscripts		
8	Section titles, tables, table names, first letters in table captions,figure captions, footnotes, text subscripts, and superscripts		
9	References, authors' biographies	Abstract	
9	Authors' affiliations, main text, equations, first letters in section titles		Subheading
10	Authors' names		
20	Paper title		

As always with a conversion to PDF, authors should very carefully check a printed copy.

II. HELPFUL HINTS

A. Figures

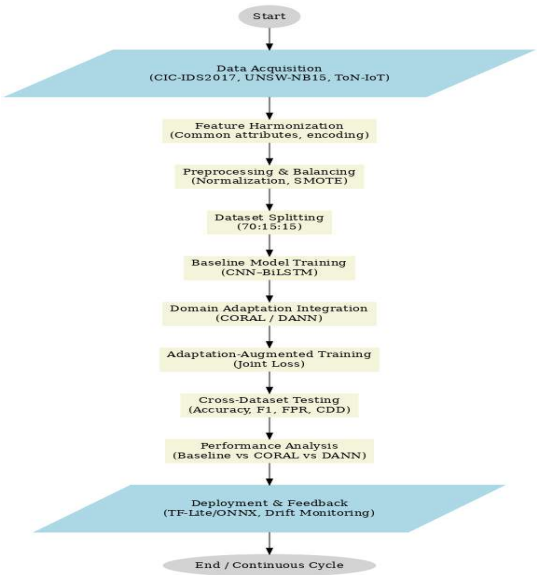

Figure 1 Workflow Diagram

The method used in this papesr combines domain adaption mechanisms with deep learning architectures to create a robust intrusion detection system that can generalize across datasets. Multi-source datasets, sophisticated preprocessing, hybrid CNN–BiLSTM feature extraction, and adaption modules like CORAL and DANN are all incorporated into the architecture. An IDS framework that remains resilient even when used in diverse and changing situations is the end product. Three benchmark datasets—CIC-IDS2017, UNSW-NB15, and ToN-IoT—form the foundation of this investigation. Because every dataset is gathered in a different setting, traffic numbers and attack patterns vary greatly. Overlapping characteristics including flow duration, packet length, inter-arrival intervals, and protocol identifiers are chosen in order to create a shared feature space.

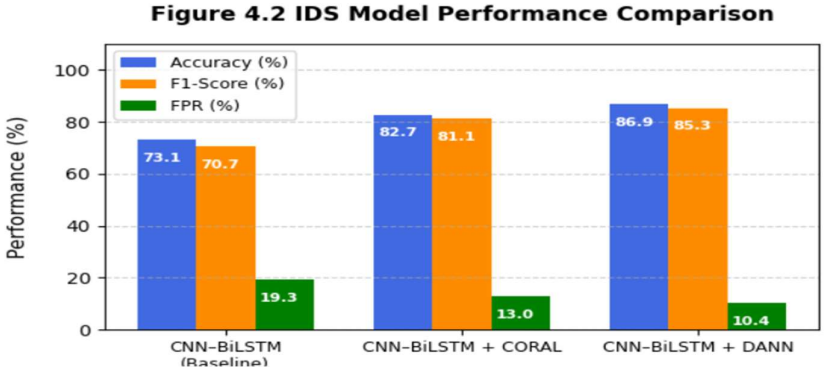

Figure 2 Model Performance Comparison

REFERENCES

[1] Ahmed, U., Nazir, M., Sarwar, A., Ali, T., Aggoune, E.M. (2025). Signature-based Intrusion Detection through Machine Learning and Deep Learning Techniques Enhanced with Fuzzy Clustering. Scientific Reports, 15:1726.

[2] Sajid, M., Malik, K.R., Almogren, A., Malik, T.S., Khan, A.H., Tanveer, J., Rehman, A.U. (2024). Improving Intrusion Detection: A Combined Machine and Deep Learning Method. Cloud Computing Journal, 13:123.

[3] Xiong, S., Chen, X., Zhang, H., Wang, M. (2024). Deep Learning Framework for Android Malware Detection Utilizing Domain Adaptation Across Varied Distributions. Artificial Intelligence Progress, 6(1):13–24.

[4] Zhang, J., Yu, L., Feng, Z., et al. (2024). Domain Adaptation-Based Network Intrusion Detection System for Industrial Control Systems. ResearchGate preliminary version.

[5] Team WDFT-DA (2025). Wasserstein Distance Driven Feature Tokenizer Transformer Domain Adaptation Method. Computers & Security, Elsevier.

[6] Sultana, S., Wahab, S.A., Tariq, N., Khan, J.A., Mujahid, M., Mylonas, A. (2025). A Deep Learning and Transformers-Based Multi-Class Intrusion Detection System for DDoS Attacks in IoT Networks. Sensors, 25(15):4845.

[7] Gupta, R., Liu, S., Zhang, R., Hu, X., Wang, X., Benkraouda, H., Kommaraju, P., Feamster, N., Nahrstedt, K. (2025). Generative Active Adaptation for Network Intrusion Detection with Imbalance and Drift. arXiv preprint.

[8] Kotb, H.M., Gaber, T., AlJanah, S., Zawbaa, H.M., Alkhathami, M. and others. (2025). A New Deep Synthesis Insider Intrusion Detection (DS-IID) Framework for Harmful Insiders and AI-Created Threats. Scientific Reports, 15:207.

[9] Alsubaei, F.S., et al. (2025). Intelligent Deep Learning Framework for Improved IoT Intrusion Identification. Scientific Reports, 15:20577.

[10] Kimanzi, R., et al. (2024). Deep Learning Techniques Applied in Intrusion Detection Systems: A Comprehensive Review. arXiv preprint arXiv:2402.17020.

[11] pFedCross Team (2025). Sturdy Intrusion Detection Utilizing a Customized Federated Cross Learning Model (pFedCross). Computers & Security, Elsevier.

[12] DIVA Research Team (2024). Neural Network Method for Network Intrusion Detection Utilizing Multi-Modal Learning and Domain Adaptation. DIVA-portal documentation.

[13] Wang, Y., Li, Q., Chen, Y. (2024). Survey of Network Intrusion Detection Systems Utilizing Deep Learning. ResearchGate.

[14] Singh, A., Kumar, V. (2025). Current Situation, Issues, and Upcoming Directions of Deep Learning for Intrusion Detection. Future Web, MDPI.

[15] Zhang, Y., Zhao, H., Li, W. (2024). Adaptive UAV Swarm Communication in Competitive Battlefields Through Deep Reinforcement Learning. IEEE Transactions on Vehicular Technology, 72(9):11032–11045.

[16] Huang, X., Chen, L. (2024). Covert Messaging in Military IoT Networks through Structured Audio. Defense Technology Journal, 19(2):231–244.