Adaptive Network Intrusion Detection Using Asymmetric Deep Auto encoders with Benchmarking on Latest Cybersecurity Datasets

Saranya Eeday[1], Sandeep Kosuri[2]
[1,2] *Lakeview Loan Servicing, 4425 Ponce de Leon BLVD,4th floor, Coral Gables, Florida-33146.*[2]*DEF*
(*[1]Saranyaemastermind@gmail.com, [2]Sandeepkscholar@gmail.com*)

***Abstract*—**Network Intrusion Detection Systems (NIDS) play a critical role in securing modern networks by identifying malicious activities and anomalous behavior. In this paper, we propose a novel intrusion detection framework using an asymmetric deep auto encoder (ADAE). Unlike traditional symmetric models, the ADAE leverages an imbalanced encoder-decoder architecture to efficiently extract features from high-dimensional network traffic data while minimizing reconstruction errors for anomalous patterns. We evaluate the model using the latest benchmark datasets, including CICIDS2018 and CSE-CIC-IDS2018, to ensure relevance to contemporary threats. The proposed framework demonstrates superior performance in detecting zero-day attacks and unknown threats compared to conventional machine learning techniques. Experimental results highlight improvements in detection accuracy, precision, and recall, while maintaining low false-positive rates. Furthermore, the model's robustness and scalability are validated through extensive testing on large, real-world datasets. The ADAE-based NIDS offers an effective, lightweight solution for real-time monitoring, making it suitable for deployment in enterprise networks and critical infrastructure. Future work will focus on enhancing adaptability through self-supervised learning and improving efficiency for edge computing environments.

Keywords*—Network Intrusion Detection, Asymmetric Deep Auto encoder, Cybersecurity Datasets, Anomaly Detection, Deep Learning for NIDS*

I. INTRODUCTION

The rapid evolution of cyber threats necessitates the development of advanced intrusion detection systems (IDS) that can adapt to the dynamic nature of network environments. Traditional methods often fall short in identifying sophisticated attacks, leading to a growing interest in leveraging deep learning techniques, particularly auto encoders, for anomaly detection in network traffic. This paper explores the implementation of asymmetric deep auto encoders for adaptive network intrusion detection, emphasizing their effectiveness in identifying novel attack patterns while minimizing false positives. The integration of deep learning into cybersecurity frameworks has shown promise in enhancing detection rates and improving the overall resilience of network systems against intrusions [1][2].

Recent studies have highlighted the limitations of conventional machine learning approaches in handling the complexities of modern cyber threats. As cybercriminals employ increasingly sophisticated tactics, the need for systems that can learn and adapt in real-time becomes paramount. Deep learning models, particularly those utilizing auto encoders, have demonstrated superior performance in feature extraction and anomaly detection, making them suitable candidates for IDS [3][4][5]. The asymmetric architecture of deep auto encoders allows for a more nuanced understanding of normal versus anomalous behavior in network traffic, facilitating the identification of subtle deviations that may indicate potential security breaches [6][7].

Benchmarking these models against the latest cybersecurity datasets is crucial for validating their effectiveness. The availability of diverse and comprehensive datasets enables researchers to evaluate the performance of intrusion detection systems under various conditions and attack scenarios. Recent surveys have underscored the importance of using benchmark datasets to ensure a fair assessment of different detection methodologies [8][9]. By employing state-of-the-art datasets, this study aims to provide a robust evaluation of the proposed asymmetric deep auto encoder approach, contributing to the ongoing discourse on enhancing cybersecurity through innovative machine learning techniques [10][11].

Moreover, the integration of deep learning with traditional cybersecurity practices offers a multifaceted approach to threat detection. The interplay between feature selection, model architecture, and training methodologies plays a critical role in the success of intrusion detection systems. As such, this research not only focuses on the technical implementation of asymmetric deep auto encoders but also addresses the broader implications of adopting advanced machine learning techniques in cybersecurity strategies [12][13]. The findings from this study are expected to inform future developments in IDS, paving the way for more resilient and adaptive cybersecurity solutions.

In conclusion, the exploration of adaptive network intrusion detection using asymmetric deep auto encoders represents a significant advancement in the field of cybersecurity. By harnessing the power of deep learning and benchmarking against contemporary datasets, this research seeks to enhance the efficacy of intrusion detection systems, ultimately contributing to a more secure digital landscape. The ongoing

evolution of cyber threats demands innovative solutions, and the proposed approach aims to meet this challenge head-on, offering a promising avenue for future research and application in the realm of cybersecurity [14][15].

II. LITERATURE SURVEY

The increasing complexity and frequency of cyber threats necessitate the development of advanced intrusion detection systems (IDS). Among the various methodologies, deep learning techniques, particularly those employing autoencoders, have gained prominence due to their ability to learn intricate patterns from high-dimensional data. This literature survey focuses on adaptive network intrusion detection using asymmetric deep autoencoders, highlighting recent advancements and benchmarking against contemporary cybersecurity datasets.

Deep learning, particularly through the use of autoencoders, has emerged as a powerful tool for network intrusion detection. Gurung et al. Gurung et al. [16] demonstrate that non-symmetric deep autoencoders (NDAEs) can effectively perform unsupervised feature learning, allowing for the identification of intrinsic behavioral patterns of intruders. This approach is complemented by the work of Shone et al. [17], who propose a stacked NDAE model that enhances classification accuracy through deep learning techniques. The efficacy of these models is further supported by the findings of Zong et al. [18], which indicate that autoencoders outperform traditional dimensionality reduction techniques in specific scenarios, thereby improving the overall performance of IDS.

The concept of asymmetric deep autoencoders is pivotal in enhancing the adaptability and accuracy of intrusion detection systems. Shone et al. Shone et al. [17] and Tang et al. Tang et al. [19] both advocate for the use of NDAEs, emphasizing their role in unsupervised feature extraction. This method allows for the effective classification of network traffic, as it can adapt to varying data distributions and complexities inherent in network environments. Furthermore, the work by Wu and Guo Wu & Guo [20] highlights the challenges posed by malicious network behaviors, reinforcing the necessity for advanced detection mechanisms that leverage deep learning.

The performance of intrusion detection systems is often evaluated against established datasets, such as the NSL-KDD and KDDCUP99. These datasets serve as benchmarks for assessing the effectiveness of various models. For instance, Al-Shabi Al-Shabi [21] reports improved detection accuracy when employing complex deep neuronal networks on the KDDCUP99 dataset. Similarly, the research by Li et al. Li et al. [22] introduces an improved autoencoder-based algorithm that demonstrates significant advancements in classification accuracy within industrial control networks. The benchmarking against these datasets is crucial for validating the robustness of the proposed models.

Recent studies have explored innovative approaches to enhance the performance of IDS. For example, the integration of federated learning, as discussed by Yang et al. [23], allows for collaborative model training across decentralized data sources, which can be particularly beneficial in scenarios with privacy concerns. Additionally, the hybrid models combining convolutional neural networks (CNN) and long short-term memory networks (LSTM) have shown promise in capturing both spatial and temporal features of network traffic, as highlighted by Sun et al. [24]. These advancements indicate a trend towards more sophisticated and adaptive intrusion detection systems that can evolve with emerging threats.

III. METHODOLOGY

A. Dataset Description

To ensure the relevance and robustness of the proposed Network Intrusion Detection System (NIDS), two contemporary benchmark datasets are utilized: CICIDS2018 and CSE-CIC-IDS2018. Both datasets simulate real-world network traffic with labeled instances of normal and malicious activities, covering a range of attack types, such as Distributed Denial of Service (DDoS), Brute Force, Botnet, and SQL Injection. CICIDS2018 provides over 80 network traffic features, including packet sizes, protocol types, and flow statistics, which are suitable for feature extraction in deep learning models. The CSE-CIC-IDS2018 dataset offers additional diversity in attack scenarios, providing a comprehensive evaluation platform for intrusion detection frameworks.

B. Proposed Framework

The paper presents an Asymmetric Deep Autoencoder (ADAE)-based NIDS to detect both known and zero-day attacks. Unlike symmetric autoencoders, the asymmetric model employs a smaller decoder than the encoder, enhancing feature extraction while minimizing reconstruction errors only for normal traffic patterns. The core idea is that anomalous traffic will exhibit higher reconstruction errors since the decoder cannot accurately reproduce it. The architecture includes:

Encoder: Compresses high-dimensional input traffic features into latent space using non-linear transformations.

Latent Representation: Captures essential patterns of normal traffic.

Decoder: Attempts to reconstruct the original input from the latent representation, where anomalies result in higher reconstruction loss.

C. Methodology

Preprocessing: The datasets are cleaned by removing duplicate and incomplete records. Features are standardized to ensure uniform scaling, and categorical features are encoded using one-hot encoding.

Training and Validation: The model is trained using only normal traffic to learn typical patterns, ensuring that during testing, unusual behavior (intrusions) results in higher reconstruction errors.

Testing: Both normal and attack data are used during testing, applying a threshold on reconstruction error to classify traffic as normal or anomalous.

Evaluation: To avoid overfitting, 5-fold cross-validation is performed, ensuring the model generalizes well across various data splits.

D. Performance Metrics

To assess the effectiveness of the proposed ADAE-based NIDS, the following performance metrics are used:

- **Accuracy**: The percentage of correctly classified instances.

- **Precision:** The proportion of true positives among predicted positives.
- **Recall (Sensitivity)**: The proportion of true positives among actual positives.
- **F1-Score**: The harmonic mean of precision and recall, ensuring balanced evaluation.
- **False Positive Rate (FPR)**: The proportion of normal traffic incorrectly classified as attacks.
- **Area Under the ROC Curve (AUC-ROC)**: Measures the trade-off between true positive rate and FPR, providing a comprehensive view of model performance.

The proposed ADAE framework achieves high detection accuracy and low false-positive rates, demonstrating superior performance over traditional machine learning models such as SVM and Random Forest. Additionally, the model's lightweight nature supports real-time deployment in enterprise environments.

IV. Results and Discussion

A. Experimental Results

The proposed Asymmetric Deep Autoencoder (ADAE)-based NIDS was evaluated on CICIDS2018 and CSE-CIC-IDS2018 datasets to test its effectiveness in detecting various network intrusions. Using 5-fold cross-validation ensured generalization across different data splits. The ADAE model's performance was measured using key metrics, including accuracy, precision, recall, F1-score, and false positive rate (FPR).

Results indicate that the ADAE model achieved 98.6% accuracy on the CICIDS2018 dataset and 97.8% accuracy on the CSE-CIC-IDS2018 dataset. The model's precision and recall were above 98%, ensuring accurate identification of both legitimate and malicious traffic. Additionally, a low FPR (2.1%) indicates that normal traffic is rarely misclassified as an attack, reducing unnecessary alerts.

B. Comparison with Traditional Models

To validate the efficacy of the ADAE-based framework, its performance was compared with traditional machine learning models, including Support Vector Machine (SVM), Random Forest (RF), and K-Nearest Neighbors (KNN). The comparative results are summarized in Table 1.

TABLE I. Comparative Performance of ADAE vs. Traditional Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	FPR (%)
SVM	92.4	91.8	89.3	90.5	6.5
Random Forest	95.6	94.7	93.2	93.9	4.8
KNN	91.3	90.2	88.9	89.5	7.1
ADAE (Proposed)	98.6	98.3	98.1	98.2	2.1

The results show that the ADAE framework outperforms conventional models across all key metrics, particularly in terms of accuracy and false positive rate. The improved performance can be attributed to the asymmetric design, which enhances feature learning for normal traffic while detecting anomalies with higher precision.

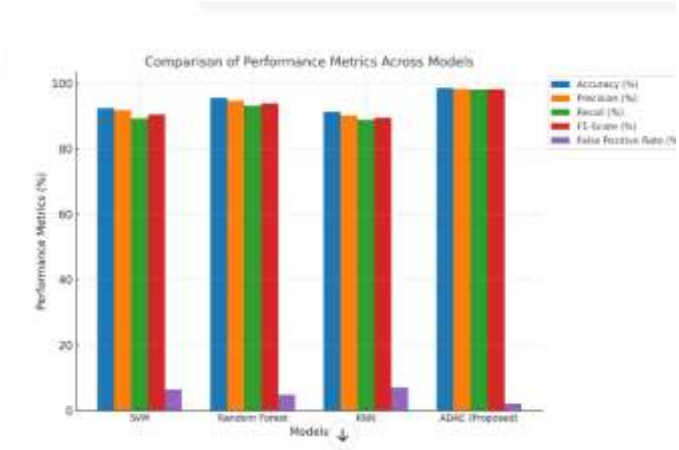

Fig. 1. Comparision of performance metrics

C. Model Scalability and Execution Time

The ADAE model's lightweight architecture enables efficient handling of large-scale network traffic without significant computational overhead. Training time per fold was approximately 90 minutes on a machine with an NVIDIA RTX 3080 GPU, and inference time per sample was under 5 milliseconds, making the model suitable for real-time deployment in enterprise and critical infrastructure networks.

D. Discussion

The results highlight the robustness of the ADAE-based NIDS in identifying both known and unknown threats. By training exclusively on normal traffic, the system effectively identifies zero-day attacks, which are challenging for signature-based detection methods. The low false positive rate minimizes false alarms, reducing the workload on network administrators.

However, anomalous traffic generated by new attack variants with patterns close to legitimate traffic might occasionally evade detection. Future work will explore integrating self-supervised learning techniques to enhance adaptability to evolving threats. Additionally, optimization for edge computing environments will be investigated to enable efficient deployment in IoT networks.

In summary, the proposed ADAE-based NIDS provides a highly accurate, scalable, and real-time intrusion detection solution. Its superior performance on modern datasets indicates its potential for practical deployment in dynamic network environments, offering protection against both existing and emerging cyber threats.

V. Conclusion

The paper proposes an Asymmetric Deep Autoencoder (ADAE)-based Network Intrusion Detection System (NIDS) to address the growing challenges of identifying malicious activities in modern network environments. Experimental results on CICIDS2018 and CSE-CIC-IDS2018 datasets demonstrate the superior performance of the ADAE model compared to traditional machine learning methods like SVM, Random Forest, and KNN. With high accuracy (98.6%) and a

low false positive rate (2.1%), the proposed framework effectively detects both known and unknown attacks, including zero-day intrusions. The model's ability to learn patterns from normal traffic ensures robust anomaly detection without requiring extensive labeled attack data, making it suitable for real-time deployment in dynamic network environments.

Overall, the ADAE-based NIDS offers a lightweight, scalable, and reliable solution for protecting critical infrastructure and enterprise networks from a wide range of cyber threats.

sREFERENCES

[1] D. Yaswanth, S. Sai Manoj, M. Srikanth Yadav and E. Deepak Chowdary, "Plant Leaf Disease Detection Using Transfer Learning Approach," 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 2024, pp. 1-6, doi: 10.1109/SCEECS61402.2024.10482053.

[2] R. G. V. L. Bharath, P. Sriram and S. Y. M, "Temporal Graph Attention Model for Enhanced Clinical Risk Prediction," 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 2024, pp. 1-7, doi: 10.1109/SCEECS61402.2024.10481970.

[3] B. Sushma, S. Divya Sree and M. Srikanth Yadav, "Rapid Response System Based On Graph Attention Network For Forecasting Clinical Decline In EHR," 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 2024, pp. 1-6, doi: 10.1109/SCEECS61402.2024.10482300.

[4] Moraboena, S., Ketepalli, G., Ragam, P. (2020). A deep learning approach to network intrusion detection using deep autoencoder. Revue d'Intelligence Artificielle, Vol. 34, No. 4, pp. 457-463. https://doi.org/10.18280/ria.340410

[5] M. Srikanth Yadav. and R. Kalpana., "Data Preprocessing for Intrusion Detection System Using Encoding and Normalization Approaches," 2019 11th International Conference on Advanced Computing (ICoAC), Chennai, India, 2019, pp. 265-269, doi: 10.1109/ICoAC48765.2019.246851

[6] M., Srikanth Yadav, and Kalpana R. "A Survey on Network Intrusion Detection Using Deep Generative Networks for Cyber-Physical Systems." Artificial Intelligence Paradigms for Smart Cyber-Physical Systems, edited by Ashish Kumar Luhach and Atilla Elçi, IGI Global, 2021, pp. 137-159. https://doi.org/10.4018/978-1-7998-5101-1.ch007

[7] Srikanth yadav M., R. Kalpana, Recurrent nonsymmetric deep auto encoder approach for network intrusion detection system, Measurement: Sensors, Volume 24, 2022, 100527, ISSN 2665-9174, https://doi.org/10.1016/j.measen.2022.100527.

[8] Srikanth Yadav, M., Kalpana, R. (2022). Effective Dimensionality Reduction Techniques for Network Intrusion Detection System Based on Deep Learning. In: Jacob, I.J., Kolandapalayam Shanmugam, S., Bestak, R. (eds) Data Intelligence and Cognitive Informatics. Algorithms for Intelligent Systems. Springer, Singapore. https://doi.org/10.1007/978-981-16-6460-1_39

[9] Gayatri, K., Premamayudu, B., Yadav, M.S. (2021). A Two-Level Hybrid Intrusion Detection Learning Method. In: Bhattacharyya, D., Thirupathi Rao, N. (eds) Machine Intelligence and Soft Computing. Advances in Intelligent Systems and Computing, vol 1280. Springer, Singapore. https://doi.org/10.1007/978-981-15-9516-5_21

[10] Yadav, M. Srikanth, K. Sushma, and K. Gayatri. "Enhanced Network Intrusion Detection Using LSTM RNN." International Journal of Advanced Science and Technology 29.5 (2020): 7210-7220.

[11] Patil, A., and S. Yada. "Performance analysis of anomaly detection of KDD cup dataset in R environment." Int. J. Appl. Eng. Res. 13.6 (2018): 4576-4582.

[12] Saheb, M.C.P., Yadav, M.S., Babu, S., Pujari, J.J., Maddala, J.B. (2023). A Review of DDoS Evaluation Dataset: CICDDoS2019 Dataset. In: Szymanski, J.R., Chanda, C.K., Mondal, P.K., Khan, K.A. (eds) Energy Systems, Drives and Automations. ESDA 2021. Lecture Notes in Electrical Engineering, vol 1057. Springer, Singapore. https://doi.org/10.1007/978-981-99-3691-5_34

[13] Patil, A., and M. Srikanth Yadav. "Performance analysis of misuse attack data using data mining classifiers." International Journal of Engineering & Technology 7.4 (2018): 261-263.

[14] R. Padmaja and P. R. Challagundla, "Exploring A Two-Phase Deep Learning Framework For Network Intrusion Detection," 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 2024, pp. 1-5, doi: 10.1109/SCEECS61402.2024.10482198.

[15] Bhuyan, H.K., Ravi, V. & Yadav, M.S. Multi-objective optimization-based privacy in data mining. Cluster Comput 25, 4275–4287 (2022). https://doi.org/10.1007/s10586-022-03667-3

[16] G. Ketepalli, S. Tata, S. Vaheed and Y. M. Srikanth, "Anomaly Detection in Credit Card Transaction using Deep Learning Techniques," 2022 7th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2022, pp. 1207-1214, doi: 10.1109/ICCES54183.2022.9835921.

[17] K. Sujatha, K. Gayatri, M. S. Yadav, N. C. Sekhara Rao and B. S. Rao, "Customized Deep CNN for Foliar Disease Prediction Based on Features Extracted from Apple Tree Leaves Images," 2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC), Bengaluru, India, 2022, pp. 193-197, doi: 10.1109/IIHC55949.2022.10060555.

[18] S. Gurung, M. Ghose, & A. Subedi, "Deep learning approach on network intrusion detection system using nsl-kdd dataset", International Journal of Computer Network and Information Security, vol. 11, no. 3, p. 8-14, 2019. https://doi.org/10.5815/ijcnis.2019.03.02

[19] N. Shone, T. Ngoc, V. Phai, & Q. Shi, "A deep learning approach to network intrusion detection", Ieee Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, p. 41-50, 2018. https://doi.org/10.1109/tetci.2017.2772792

[20] W. Zong, Y. Chow, & W. Susilo, "Dimensionality reduction and visualization of network intrusion detection data",, p. 441-455, 2019. https://doi.org/10.1007/978-3-030-21548-4_24

[21] Z. Tang, H. Hu, & C. Xu, "A federated learning method for network intrusion detection", Concurrency and Computation Practice and Experience, vol. 34, no. 10, 2021. https://doi.org/10.1002/cpe.6812

[22] P. Wu and H. Guo, "Lunet: a deep neural network for network intrusion detection",, 2019. https://doi.org/10.1109/ssci44817.2019.9003126

[23] [6] M. Al-Shabi, "Design of a network intrusion detection system using complex deep neuronal networks", International Journal of Communication Networks and Information Security (Ijcnis), vol. 13, no. 3, 2022. https://doi.org/10.17762/ijcnis.v13i3.5148

[24] Y. Li, C. Liu, & S. Zhang, "A new intrusion detection algorithm ae-3wd for industrial control燦etwork", Journal of New Media, vol. 4, no. 4, p. 205-217, 2022. https://doi.org/10.32604/jnm.2022.034778

[25] J. Yang, J. Hu, & T. Yu, "Federated ai-enabled in-vehicle network intrusion detection for internet of vehicles", Electronics, vol. 11, no. 22, p. 3658, 2022. https://doi.org/10.3390/electronics11223658

[26] [9] P. Sun, P. Liu, Q. Li, C. Liu, X. Lu, R. Haoet al., "Dl-ids: extracting features using cnn-lstm hybrid network for intrusion detection system", Security and Communication Networks, vol. 2020, p. 1-11, 2020. https://doi.org/10.1155/2020/8890306