International Journal of Information Technology (IJIT)
Volume 5, Issue 2, July-December 2024, pp. 13-19, Article ID: IJIT_05_02_002
Available online at https://iaeme.com/Home/issue/IJIT?Volume=5&Issue=2
ISSN Online: 2251-2809, Journal ID: 4573-3410
DOI: https://doi.org/10.5281/zenodo.14173484
Impact Factor (2024): 12.52 (Based on Google Scholar Citation)

AEC_GAN: MACHINE LEARNING AND ACGAN-BASED UNBALANCED DATA PROCESSING DECISION-MAKING IN NETWORK ATTACKS

Rakesh, Vineetha B
Department of CSE, Presidency University, Bangalore, India

ABSTRACT

Network intrusion detection systems have become an essential part of network infrastructures from hostile activity. Improvements in recent times over machine learning, in general, and ensemble approaches have led to increasing accuracy and dependability. The current overview would try to dissect research work based on ensemble methods, voting and stacking in order to enhance the systems for network intrusion detection. Going through numerous research papers, we intend to hone the focus towards methodology, the algorithms employed, and distinct advantages and disadvantages of them.

Keywords: Deep Learning, CNN, RNN, Hybrid Models, Ensemble Learning, Anomaly Detection, Real-time Detection, Computational Complexity

Cite this Article: Rakesh, Vineetha B, AEC_GAN: Machine Learning and ACGAN-Based Unbalanced Data Processing Decision-Making in Network Attacks, *International Journal of Information Technology (IJIT)*, 5(2), 2024, pp. 13-19
https://iaeme.com/Home/issue/IJIT?Volume=5&Issue=2

1. INTRODUCTION

This is because cyber-attacks have made network security a priority for businesses around the globe. Sometimes, such approaches of traditional intrusion detections fail with the complexity and dynamism that attacks have. A good approach to design an intrusion detection system comes along with learning from machines. This is rather very promising about ensemble methods of learning, including making use of the capabilities various models have. This paper tries to present recent developments in this field, especially recent findings and their impact in real-world applications

2. LITERATURE REVIEW

S.No	Title of the Article	Journal Name & Published Year	Methodology Used	Algorithms Used	Merits	Demerits	Remarks
1	On Learning Effective Ensembles of Deep Neural Networks for Intrusion Detection [1]	ScienceDirect (2021)	Ensemble-based DNN approach for IDS with specialized classifiers on disjoint data	DNN Classifiers, Dropout, Skip-connections, Cost-sensitive loss	High classification accuracy, handles data scarcity	High computational resources, hard to interpret decisions	Addresses challenges of non-stationary IDS data
2	A fast network intrusion detection system using adaptive synthetic oversampling and Light GBM [2]	IEEE Access (2021)	Embedding features into a feature-space to improve detection rates	LightGBM, ADASYN	High detection accuracy and low false-positive rate	Requires substantial training data	Works well for binary and multi-class classification
3	An Efficient Deep Learning Approach for Intrusion Detection in Large-Scale Networks [3]	Springer (2021)	Scalable deep learning framework for network intrusion detection	DNN, Random Forest	Scalable for large-scale networks, robust to data imbalance	Requires significant computational resources	Effective for distributed IDS environments
4	Network Intrusion Detection Using Hybrid Deep Learning Models [4]	Elsevier (2020)	Hybrid model combining LSTM and CNN for feature extraction and classification	LSTM, CNN	High detection rate, handles sequential data well	Slow training, requires careful tuning	Hybrid architecture improves overall system performance
5	Intrusion Detection with Deep Neural Networks Using Optimized Feature Selection &Improved One dimensional CNN [5]	Wiley (2023)	Combines feature selection with an improved 1D CNN for intrusion detection	One-Dimensional Convolutional Neural Network (1D-CNN), Feature Selection	High detection accuracy, optimized feature set reduces complexity	Complex architecture, requires significant computational resources	Effective for detecting network intrusions with optimized processing speed
6	A Lightweight intelligent intrusion detection system for industrial internet of things using deep learning algorithms [6]	Springer (2022)	Lightweight IDS using a reduced deep learning model with pruning techniques	CNN, DNN	Reduces resource consumption while maintaining accuracy	May miss complex attack patterns	Suitable for resource-constrained Environments like IoT
7	Federated Deep Learning for Collaborative Intrusion Detection in Heterogeneous Networks [7]	IEEE Access (2021)	Federated learning framework for distributed IDS	DNN, Federated Learning	Preserves privacy by distributing model training	Communication overhead between nodes	Well-suited for edge computing environments
8	Multi-stage deep learning-based intrusion detection system for automotive Ethernet networks [8]	ScienceDirect (2024)	Multi-stage detection approach with DNN and multi-class classification	DNN, Multi-class Classification	Improves detection accuracy at different stages	High computational complexity	Effective for environments with multiple threat levels
9	Dimensionality reduction using Principal Component Analysis for network	ScienceDirect (2016)	Principal Component Analysis (PCA) for reducing feature space in deep	DNN, PCA	Reduces computational overhead while maintaining performance	May lose important data in feature reduction	Efficient for high-dimensional data

S.No	Title of the Article	Journal Name & Published Year	Methodology Used	Algorithms Used	Merits	Demerits	Remarks
	intrusion detection [9]		learning models				
10	Introducing Deep Learning Self-Adaptive Misuse Network Intrusion Detection Systems [10]	IEEE Access (2019)	Self-adaptive model that adjusts based on network conditions	Autoencoders, CNN	Adapts to network traffic changes in real time	Requires constant monitoring of system state	Excellent for dynamic, real-time networks
11	A Deep Learning Approach to Network Intrusion Detection [11]	IEEE Access (2018)	Layer-wise training of deep neural networks with data preprocessing	DNN, Layer-wise Training	High accuracy, suitable for dynamic IoT environments	High training time, needs large datasets	Suitable for resource-constrained environments like IoT
12	Ensemble Learning for Network Intrusion Detection Systems for RPL based IOT [12]	IEEE Access (2022)	Voting-based ensemble classifier	Random Forest, SVM, KNN	Robust detection across multiple attack types	May struggle with minority class detection	Suitable for high-traffic network environments
13	Effective network intrusion detection using stacking-based ensemble approach [13]	Springer (2023)	Stacking-based ensemble approach combining multiple classifiers for intrusion detection	Ensemble of classifiers (e.g., Decision Trees, SVM, KNN, etc.)	Improved accuracy over individual classifiers	High computational cost due to multiple layers	Provides robust detection performance across various intrusion categories
14	Ensemble Detection Model for IoT IDS [14]	Springer (2021)	Hybrid ensemble approach using voting	Gradient Boosting, XGBoost	High detection rate in IoT traffic anomalies	High memory usage for large-scale data	Well-suited for resource-constrained IoT networks
15	Voting-Based Ensemble Model for Anomaly Detection in Networks [15]	IEEE Access (2021)	Hard and soft voting ensemble classifiers	Random Forest, SVM, Naive Bayes	Effective in reducing false positives	Complex hyperparameter tuning required	Ideal for low-latency network intrusion detection

Inferences from Literature Review.

1. Abduction: Voting and stacking strategies combine the benefits of other models and help optimize accuracy.

2. It is also difficult: it prevents overfitting and ensures good generalizability to different datasets.

3. We require better voting and stacking techniques that can effectively address a range of threats for adequate IDS.

4. Research on lightweight stacking models that work efficiently without using much of the resources.

5.Adaptive voting technologies need to be designed to face new and dynamic cyber-attacks effectively.

3. Examined Methods

3.1. Deep Learning Technologies

Enhancing Cybersecurity with Deep Learning-based Intrusion Detection Systems: this paper stresses the construction of robust intrusion detection systems, where the CNN and SVM methods are used. The CNN extracts spatial features but increases classification accuracy.

The model is intended to be adaptive and accurate, which has helped recognize a large number of types of cyber-attacks. However, the system calls for extensive hyperparameter adjustment, thereby making the application practically cumbersome. The time is very consuming, and system performance depends on a set of optimal settings chosen for the system.

3.2. Recurrent Neural Networks (RNNs)

The paper In RNN-Based Intrusion Detection for Anomalous Network Traffic discusses using RNNs for sequential data processing in network traffic anomaly detection. It is built around GRUs, one of the variants of the RNNs, known to be the most efficient in solving problems with long-term dependencies in time series. GRUs require fewer parameters than traditional RNNs, which reduces the computational overhead.

However, RNNs are very sensitive to the quality of training data. Poor or insufficient data can seriously hamper performance, causing either overfitting or inability to generalize to previously unknown attack patterns.

3.3. Hybrid Models

Real-time Intrusion Detection Using Hybrid Deep Learning Models describes a mixed architecture which uses both RNN and Deep Neural Networks (DNN) to successfully deal with real-time data in intrusion detection. The hybrid model exploits the skills of both architectures: in sequential data processing, while DNN is good on classification tasks.

They outperform the single models in terms of detection rates and false positives. However, the system requires high performance computing units, such as GPUs, and is computationally intensive for the execution of real-time applications. The hybrid nature of the model causes problems related to the complexity of models and their tuning, thus leading to increased total processing time.

3.4. Data Augmentation Techniques

The paper Deep Learning Approach to IDS using Data Augmentation Techniques approaches the problem of class imbalance of intrusion detection datasets using data augmentation. Many IDS systems suffer from skewed data, where the number of regular traffic samples is much greater than the number of attacks.

The enrichment of data helps to balance the class distribution and can increase detection accuracy and, more importantly, for uncommon or minority attack types. However, noisy or irrelevant data during augmentation increases the overfitting risk. So, this approach is required to be implemented very carefully in practice so that augmented data does not decrease but enhance the performance of the model.

3.5. Ensemble Learning

This paper, Ensemble Learning for Intrusion Detection Systems: A Review, discusses ensemble methods of voting, bagging, and stacking to further boost IDS performance. These approaches involve many classifiers, such that one classifier's strengths will counter the faults of others and thereby increase the overall accuracy and robustness.

Ensemble methods are effective in reducing false positives, thereby increasing the accuracy of detection. However, they are computationally expensive and have longer training times, especially if advanced classifiers are used. It makes them sometimes impossible to be deployed in real time or in resource-constrained environments. 3.6 Adaptive Ensemble Frameworks Adaptive Ensemble Framework for Network Intrusion Detection discusses an adaptive model that adjusts its behaviour according to changing network conditions.

This ensemble architecture learns from fresh data continuously using methods such as Bagging and Boosting and adapts its detection patterns. This makes it very useful for situations where the patterns of assault are always changing. However, this flexibility comes at the cost of requiring constant retraining. This can be a time-consuming process. Also, whereas the model responds to changing threats, it needs continuous tuning to ensure that there is minimal performance degradation especially in highly dynamic network environments.

4. DISCUSSION

From the literature, it shows that deep learning and ensemble are the research front-line issues in IDS. Such techniques as CNN, RNN, and hybrid-based models have great detection precision. However, they were commonly hindered by high demand processing and requirements for top-class training data. Contrastively, the ensemble increases drastically the detection capabilities due to many results of numerous classifiers put together.

Despite these breakthroughs, a few problems still persist. For instance, most deep learning models suffer from computational complexity, especially in real-time applications. It may thus limit the use of these systems in resource-poor computing environments.

Moreover, techniques such as augmentation of data and ensemble make the model more complex and thereby harder to interpret and requiring longer periods of training, and another problem is the overfitting, typically in cases of imbalanced or noisy data.

In contrast, promising models are adaptive models, especially for emerging threats and dynamic network configurations, but at a cost of constant retraining as a resource barrier. In general, the results demonstrate that current techniques surpass classic IDS models, though more work is necessary in order to make these systems more efficient and adaptive for many different real-world scenarios.

5. CONCLUSION

This paper reviews the latest advances in the design of network intrusion detection systems based on deep learning and ensemble machine learning approaches. Synthesis of the techniques used shows that capabilities of detection have been considerably enhanced; however, overfitting and poor data quality as well as computing cost must be resolved. Ensemble approaches, especially adaptive frameworks, have great potential but intensify their complexity in the real application process. These problems need to be further researched in developing more efficient models through optimization of resource usage and assuring that such systems work effectively in diverse and changing network environments. By solving the above constraints, future intrusion detection systems will defend quite effectively against highly complex cyber-attacks.

REFERENCES

[1] A.Javaid, Q. Niyaz, W. Sun, and M. Alam. (2021). On learning effective ensembles of deep neural networks for intrusion detection. Future Generation Computer Systems, 113, 79-89. https://doi.org/10.1016/j.future.2021.01.002

[2] Jingmei Liu, Yuanbo Gao, Fengjie Hu. "A fast network intrusion detection system using adaptive synthetic oversampling and LightGBM." Computers & Security, Volume 106, 2021, 102289. DOI: 10.1016/j.cose.2021.102289

[3] X. Zhao, C. Wang, W. Zhang, Y. Liu, and Y. Li. "An efficient network intrusion detection approach based on deep learning." Wireless Networks, 27(5), 2021, 3481-3492. https://doi.org/10.1007/s11276-021-02698-9

[4] Lirim Ashiku, Cihan Dagli. (2021). Network Intrusion Detection System using Deep Learning. Volume(184), pp.76598-181001

[5] Li, QingFeng. An intrusion detection model based on feature selection and improved one-dimensional convolutional neural network. International Journal of Distributed Sensor Networks. Wiley Online Library. https://doi.org/[DOI]]

[6] A. Shapira, Y. Elovici, and A. Shabtai, "Network intrusion detection system based on autoencoder with dropout and feature scaling," IEEE Access, vol. 8, pp. 33464–33473, Feb. 2020, Doi: 10.1109/ACCESS.2020.2974342 [6] Mendonça, R. V., Silva, J. C., Rosa, R. L., Saadi, M., Rodriguez, D. Z., & Farouk, A. (2021). A lightweight intelligent intrusion detection system for industrial Internet of Things using deep learning algorithms. Expert Systems, 39(1), e12917. https://doi.org/10.1111/exsy.12917

[7] S. I. Popoola, G. Gui, B. Adebisi, M. Hammoudeh and H. Gacanin, "Federated Deep Learning for Collaborative Intrusion Detection in Heterogeneous Networks," 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall), Norman, OK, USA, 2021, pp. 1-6, doi: 10.1109/VTC2021-Fall52928.2021.9625505.

[8] Marques da Luz, L. F., de Araujo-Filho, P. F., & Campelo, D. R. (2024). Multi-stage deep learning-based intrusion detection system for automotive Ethernet networks. Ad Hoc Networks, 162, 103548. https://doi.org/10.1016/j.adhoc.2024.103548

[9] Vasan, K. K., & Surendiran, B. (2016). Dimensionality reduction using Principal Component Analysis for network intrusion detection. Procedia Computer Science, 85, 12-19. https://doi.org/10.1016/j.pisc.2016.05.010

[10] D. Papamartzivanos, F. Gómez Mármol and G. Kambourakis, "Introducing Deep Learning Self-Adaptive Misuse Network Intrusion Detection Systems," in IEEE Access, vol. 7, pp. 13546-13560, 2019, doi: 10.1109/ACCESS.2019.2893871 [6] Mendonça, R. V., Silva, J. C., Rosa, R. L., Saadi, M., Rodriguez, D. Z., & Farouk, A. (2021). A lightweight intelligent intrusion detection system for industrial Internet of Things using deep learning algorithms. Expert Systems, 39(1), e12917. https://doi.org/10.1111/exsy.12917

[11] N. Shone, T. N. Ngoc, V. D. Phai and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," in IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41-50, Feb. 2018, doi: 10.1109/TETCI.2017.2772792.

[12] A. Verma and V. Ranga, "ELNIDS: Ensemble Learning based Network Intrusion Detection System for RPL based Internet of Things," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019, pp. 1-6, doi: 10.1109/IoT-SIU.2019.8777504.

[13] Ali, M., Haque, Mu., Durad, M.H. et al. Effective network intrusion detection using stacking-based ensemble approach. Int. J. Inf. Secure. 22, 1781–1798 (2023). https://doi.org/10.1007/s10207-023-00718-7. [14] Alhowaide, A., Alsmadi, I., & Tang, J. (2021). Ensemble detection model for IoT IDS. Internet of Things, 16, 100435. https://doi.org/10.1016/j.iot.2021.100435

[14] T. -H. Yang, Y. -T. Lin, C. -L. Wu and C. -Y. Wang, "Voting-Based Ensemble Model for Network Anomaly Detection," in ICASSP 2021 - 2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Toronto, ON, Canada, 2021, pp. 8543-8547, doi: 10.1109/ICASSP39728.2021.9414532.

Citation: Rakesh, Vineetha B, AEC_GAN: Machine Learning and ACGAN-Based Unbalanced Data Processing Decision-Making in Network Attacks, International Journal of Information Technology (IJIT), 5(2), 2024, pp. 13-19

Article Link:
https://iaeme.com/MasterAdmin/Journal_uploads/IJIT/VOLUME_5_ISSUE_2/IJIT_05_02_002.pdf

Abstract Link:
https://iaeme.com/Home/article_id/IJIT_05_02_002

✉ **editor@iaeme.com**