IJIRIS: International Journal of Innovative Research in Information Security
Volume 10, Issue 04, May 2024
E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives

Boosting Network Security: A comparative Analysis of Deep Learning Techniques for Intrusion Detection

Dr.Heena Kousar,
Associate Professor, Department of CSE
East Point College of Engineering and Technology,
Bengaluru, Karnataka, INDIA
heena.k@eastpoint.ac.in
Adarsh Pawar,
Department of Computer Science Engineering
East Point College of Engineering and Technology,
Bengaluru, Karnataka, INDIA
adarshpawar2810@gmail.com
G Mohnish Reddy,
Department of Computer Science Engineering
East Point College of Engineering and Technology,
Bengaluru, Karnataka, INDIA
mohnishgundluri@gmail.com
Mukeshreddy Nagireddygari,
Department of Computer Science Engineering
East Point College of Engineering and Technology,
Bengaluru, Karnataka, INDIA
reddymukesh3101@gmail.com
Shaikh Athiq Rehman,
Department of Computer Science Engineering
East Point College of Engineering and Technology,
Bengaluru, Karnataka, INDIA
athiqrehamanattu@gmail.com

Publication History
Manuscript Reference No: IJIRIS/RS/Vol.10/Issue04/MYIS10083
Research Article | Open Access | Double-Blind Peer-Reviewed | Article ID: IJIRIS/RS/Vol.10/Issue04/MYIS10083
Received: 07, April 2024|Revised:16, April 2024 | Accepted: 27, April 2024 Published Online: 07, May 2024 Volume 2024 Article ID MYIS10083 http://www.ijiris.com/volumes/Vol10/iss-04/04.MYIS10083.pdf
Article Citation: Heena,Adarsh,Mohnish,Mukeshreddy,Shaikh(2024).Boosting Network Security: A comparative Analysis of Deep Learning Techniques for Intrusion Detection. International Journal of Innovative Research in Information Security, Volume 10, Issue 04, Pages 139-144
doi:> https://doi.org/10.26562/ijiris.2024.v1004.04
BibTex key: Heena@2024Boosting

Copyright: ©2024 This is an open access article distributed under the terms of the Creative Commons Attribution License; which Permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Abstract: This paper addresses demanding situations in Intrusion Detection Systems (IDS) by way of combining the Adaptive Synthetic Sampling (ADASYN) method with a break up-primarily based Resnet framework. ADASYN balances sample distribution, overcoming biases in the direction of large samples. Our method extracts multiscale functions, reduces interchannel redundancy, and enhances the version's capability using a smooth hobby operation. We recommend a Residual Neural Network (ResNN) version for intrusion detection, displaying massive enhancements in recognition accuracy and execution performance. Ongoing work targets to optimize performance further, highlighting the capacity for extra strong IDS solutions.

Keywords: IDS, Adaptive Synthetic Sampling (ADASYN), Residual Neural Network (ResNN), Multiscale Features, Interchannel Redundancy, Resnet Framework, Recognition Accuracy.

I. INTRODUCTION

The fast expansion of 5G generation has multiplied the complexity and scale of internet networks, making them more susceptible to attacks [1]. Traditional security measures like firewalls and encryption are crucial but can fall brief in preventing state-of-the-art assaults [2]. Intrusion Detection Systems (IDS) play a important role in detecting and classifying community attacks, assisting in early anomaly detection and response. Conventional gadget mastering methods are usually used for assault detection, focusing on characteristic selection and class [6]. Recent advancements encompass the use of Principal Component Analysis (PCA) for characteristic discount, combining classifiers like selection trees and aid vector machines, and exploring deep studying strategies together with Convolutional Neural Networks (CNNs) for greater accurate intrusion detection [7]. However, demanding situations stay, along with uneven sample distribution and facts redundancy, which impact version training and accuracy.

This look at objectives to cope with those challenges through featuring a unique attack popularity technique the use of a residual network and the ADASYN statistics augmentation set of rules. By leveraging these strategies, we aim to decorate the efficiency and accuracy of intrusion detection in dynamic community environments.

II. LITERATURE REVIEW

In the realm of Intrusion Detection, Wu and Shen delved into the realm of traditional pattern matching algorithms such as BM and AC. They explored enhanced versions like BMHS and AC-BM, which exhibited improved timeliness in IDS operations. Nevertheless, the adaptation of these algorithms to contemporary network threats poses a formidable challenge owing to the multifaceted nature of present-day threats [15]. Dagar et al., on the other hand, scrutinized Rabin Karp & Knuth Morris Pratt pattern-matched algorithms for intrusion detection but encountered obstacles in aligning them with today's complex network environments [16]. Shifting focus to Machine Learning-Based Intrusion Detection Algorithms, Thaseen and Kumar introduced a groundbreaking intrusion detection methodology utilizing multi-class Support Vector Machines (SVMs) coupled with least-squares feature selection. This innovative approach led to heightened model accuracy and performance levels [17].

Ingre et al., on a similar note, blazed a trail by creating an intrusion identification system that merges decision trees with pertinent aspect filtering techniques, thereby demonstrating dynamic iterative feature selection process [18]. When it comes to Deep Learning Approaches for Intrusion Detection, Lin et al. brought forth the CL-CNN model aimed at enhancing IDS detection accuracy down to the token level [5]. Etang and Wan harnessed a relational CNN framework to extract varied features, amplifying model expressiveness and effectiveness [19]. Seeking solutions for interchannel redundant information concerns, Zhang et al[20]. Put forward a split-based instantaneous processing (SPC) block. Inspired by this concept, our research introduces the SPC-CNN model customized specifically for attack detection tasks - surpassing conventional CNN models in overall performance metrics.

III. MODELS AND METHODS

ADASYN (Adaptive Synthetic Sampling Method)

ADASYN solves unbalanced classification problems in machine learning by generating artificial models for subclasses based on their distribution in the feature space Focuses on regions with low class density, making classification performance fly effective in situations where subclasses are spread across groups.

Over sampling and under sampling in ADASYN

ADASYN incorporates both over-sampling and under-sampling techniques to balance the class distribution. Oversampling results in artificial sampling for minority taxa, while under sampling selectively reduces the dominance of most taxa. This combined approach aims to improve model generalization and performance.

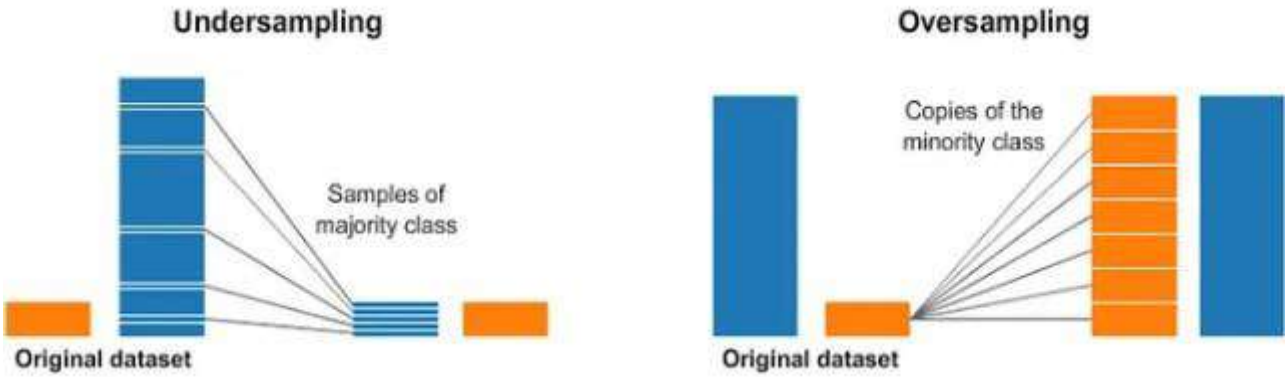

Fig.1 Under sampling and Oversampling referred from Google

Remaining networks

Residual networks (ResNets) use skip connections in residual blocks to solve the vanishing/explosive gradient problem in deep learning. These skip connections can learn the residual mapping of the network, for efficient deep network training and facilitate very deep architecture optimization

Network configuration of the remaining networks

The structure of Residual Networks consists of convolutional layers followed by skip connections that add input to the output of the layers. This allows the web browser to see remaining services and makes deeper architectures much more feasible.

Skip Connection diagram

Skip connection to the remaining networks bypasses one or more layers, so that the network can find the remaining mapping instead of the desired mapping directly. This helps to train deep networks that lack adverse effects of disappearance/explosion gradients.

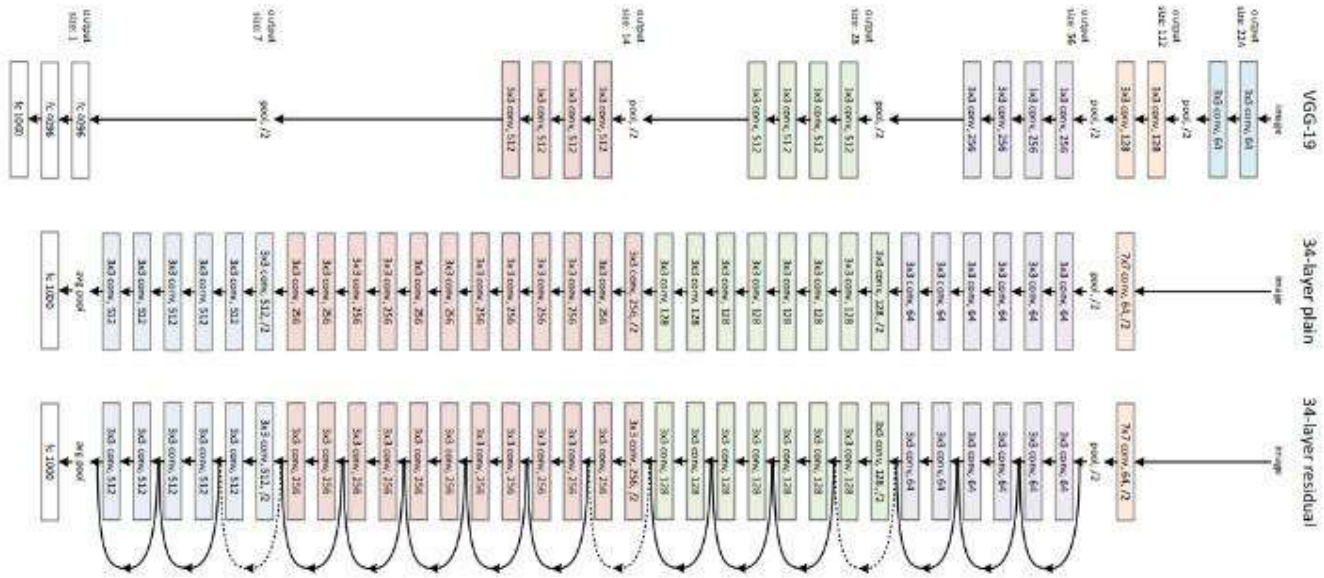

Fig. 2 Network Architecture of Residual Network referred from Google

IV. IMPLEMENTATION

Data Preprocessing

The preprocessing phase is important to ensure the quality and relevance of the data used in the analysis. Non-numeric features from the original flow data are converted to numeric properties based on the data type by methods such as one-hot encoding or label encoding followed by normalization methods such as min-max scaling or z-score normalization. The main step in data pre-processing is sampling, using a combined algorithm combining adaptive synthetic sampling (ADASYN) and repeated edited nearest neighbor (RENN) ADASYN focuses on creating synthetic samples for minority classes to track classes overcoming imbalance problems, while RENN Helps optimize data set by removing noisy patterns and improving the overall quality of the data Feature selection methods are then used to select the most suitable features that contribute most to the predictive power of the model. This helps reduce the size of the dataset and improves computational efficiency without compromising accuracy. Finally, the processed data is converted into a gray-scale map representation, which provides a visual and organizational framework for further analysis and observation Figure 1 shows the complete data preprocessing pipeline, highlighting the various steps a on the inside.

Hybrid Sampling Integrating RENN with ADASYN

The proposed hybrid sampling approach targets to create a balanced dataset via addressing both elegance imbalance and noisy facts problems. This strategy starts off evolved by keeping apart the dataset into sets one for almost all class and one for the minority magnificence. The DBSCAN clustering set of rules is then applied to discover and filter out noisy instances, making sure that simplest applicable and informative statistics factors are retained. Subsequently, the two datasets are merged to construct a balanced database.

Fig.3 Output

In this merging technique, the RENN method is applied to symbolize the majority magnificence efficaciously, while the ADASYN algorithm is hired to augment the minority class samples. This unique technique guarantees that the very last dataset maintains a balance among instructions even as also improving the overall nice of the records. The steps concerned on this hybrid sampling strategy consist of assessing the diploma of imbalance within the dataset, calculating proportions for artificial pattern technology based on ok-nearest pals, producing synthetic samples for each training, and refining the dataset through iterative procedures. Figure 2 affords an overview of the hybrid sampling technique.

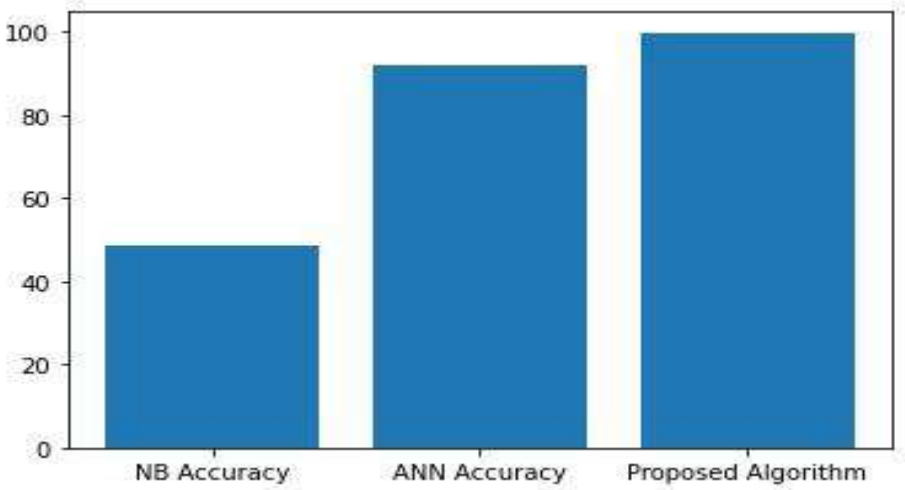

Fig.4 Comparison Graph

Algorithm

The algorithm used in this study is a multitask-based totally, two-stage alternating optimization approach designed to address the challenges of class imbalance and noisy records. The set of rules takes into account various parameters which includes the variety of artificial samples to generate, the target label, and the degree of imbalance within the dataset. The algorithmic steps involve retrieving minority and majority samples, locating k-nearest acquaintances for every minority sample, computing ratios for synthetic sample generation, randomly deciding on pals, generating synthetic samples based on pals and a parameter beta, and in the end outputting the synthetic samples. This iterative process enables in developing a balanced and consultant dataset for model education and assessment.

Remaining studies

Residual networks (ResNets) with skip connections are used to solve the common problem of missing or breaking gradients in deep neural networks. The main idea of ResNets is based on the identification of residual blocks that make it easier to learn residual mappings rather than the underlying mappings directly. These remaining parts have skip connections across one or more layers, facilitating the optimization and training of very deep networks. Skip connections enable the network to learn the remaining tasks, which are generally easier to optimize than direct mappings. This approach has been shown to effectively reduce the common decomposition problem and improve the overall accuracy of deep learning models. Network structures with residual blocks containing skip combinations consist of convolutional layers with skip combinations that add input to the output of the convolutional layers this structure enables deep networks to be trained by simplifying gradient flow and reducing optimization difficulties.

Research Analysis

Different parameters are considered to evaluate the performance of the proposed method, including true positive (TP), false negative (FN), true negative (TN), false positive (FP), precision, recall, precision, and F1-score these metrics are accurate sample classification, attack detection and provide insight into the model's ability to reduce false predictions. Accuracy measures the proportion of correctly classified samples, while recall measures the proportion of truly good samples correctly identified by the model Specificity refers to the proportion of truly accurate good predictions, and the F1-score represents the accuracy of matching and recall, providing a balanced evaluation metric for model performance.

Datasets

The data used in this study was the UNSW-NB15 database, developed by the Cyber Space Intelligence Laboratory at the Australian Cyber Security Centre. This dataset contains a wide range of objects categorized into normal and abnormal traffic, including various types of attacks such as backdoors, denial of service, shell code and worm's .The dataset is divided into training and testing sets, where each set contains examples of regular traffic and attacks. The distribution of samples across different attack types is visualized, providing insight into the class distribution of the dataset. Furthermore, Table I presents the types of attacks that affect the UNSW-NB15 data set, while Table 2 shows the order of the experimental conditions used for model training and evaluation.

V. CONCLUSION

In conclusion, our examine tackles critical challenges faced by means of intrusion detection systems (IDS), that specialize in records distribution imbalances and interchannel redundancy in current neural network (NN)-based fashions.

Our approach aims to reinforce IDS by means of leveraging superior strategies in information balancing, feature extraction, and model architecture. We stress the significance of records balance to save you model bias closer to massive samples even as neglecting smaller ones. The Adaptive Synthetic Sampling Method (ADASYN) correctly addresses this imbalance, making sure a truthful and consultant dataset for schooling. Our split-based ResNet framework introduces key advancements. It enables multiscale characteristic extraction thru more than one convolution phases, enriching network visitors statistics representation. It additionally mitigates interchannel redundancy, enhancing the model's capability to capture nuanced patterns. Furthermore, the incorporation of a soft hobby operation in ResNet enables sensible characteristic utilization, significantly boosting version expressiveness and performance in intrusion detection tasks. Our experimental effects, specifically with the hybrid ResNet model and ADASYN, display brilliant enhancements across diverse assessment criteria. Despite these improvements, optimization for execution efficiency and accuracy for smaller samples stays a focus. Moving forward, we goal to refine our method, that specialize in improving IDS identification skills thru a streamlined residual network structure with more desirable residual blocks. By innovating and integrating superior methodologies, we contribute notably to intrusion detection and cybersecurity.

FUTURE ENHANCEMENT

Analysing the statistics and research provided, several avenues for destiny enhancement in intrusion detection structures (IDS) and community security emerge. Firstly, exploring advanced sampling techniques past ADASYN and RENN may want to show fruitful. Techniques like SMOTE-NC or Borderline-SMOTE offer ability enhancements in dealing with imbalanced datasets and producing artificial samples more effectively. Secondly, endured advancements in deep getting to know architectures which include variations of ResNet, DenseNet, or EfficientNet can beautify function extraction and getting to know capabilities for complicated community visitors information. Thirdly, ensemble methods like Random Forests or Gradient Boosting Machines may be incorporated to improve version robustness and decrease fake positives. Additionally, growing adaptive characteristic choice algorithms, incorporating real-time stream processing frameworks, integrating explainable AI strategies, and discovering modern techniques for zero-day assault detection are promising areas for boosting IDS talents and addressing rising cybersecurity challenges efficiently. These avenues together goal to make IDS more adaptive, accurate, and responsive in mitigating evolving community threats.

REFERENCES

[1]. Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," Proc. IEEE, vol. 104, no. 9, pp. 1727–1765, Sep. 2016, https://doi:10.1109/JPROC. 2016.2558521
[2]. A.Kavianpour and M. C. Anderson, "An overview of wireless network security," in Proc. IEEE 4th Int. Conf. Cyber Secur. Cloud Comput. (CSCloud), New York, NY, USA, Jun. 2017, pp. 306–309, doi: 10.1109/ CSCloud.2017.45.
[3]. H.Sallay and S. Bourouis, "Intrusion detection alert management for highspeed networks: Current researches and applications," Secur. Commun. Netw., vol. 8, no. 18, pp. 4362–4372, Dec. 2015.
[4]. A.L.Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Commun. Surveys Tuts., vol. 18, no. 2, pp. 1153–1176, 2nd Quart., 2016, doi: 10.1109/ COMST.2015.2494502.
[5]. S.Z.Lin, Y. Shi, and Z. Xue, "Character-level intrusion detection based on convolutional neural networks," in Proc. Int. Joint Conf. Neural Netw. (IJCNN), Rio de Janeiro, Brazil, Jul. 2018, pp. 1–8, https://doi:10.1109/IJCNN.2018.8488987
[6]. B.Selvakumar and K. Muneeswaran, "Firefly algorithm based feature selection for network intrusion detection," Comput. Secur., vol. 81, pp. 148–155, Mar. 2019.
[7]. Y. Qi, M. Liu, and Y. Fu, "Research on SVM network intrusion detection based on PCA," Inf. Netw. Secur., vol. 2, pp. 15–18, Feb. 2015.
[8]. D.Zheng, Z. Hong, N. Wang, and P. Chen, "an improved LDA-based ELM classification for intrusion detection algorithm in IoT application," Sensors, vol. 20, no. 6, p. 1706, Mar. 2020.
[9]. C.Iwendi, S. Khan, J. H. Anajemba, M. Mittal, M. Alenezi, and M. Alazab, "the use of ensemble models for multiple class and binary class classification for improving intrusion detection systems," Sensors, vol. 20, no. 9, p. 2559, Apr. 2020.
[10]. H.Wang, J. Gu, and S. Wang, "An effective intrusion detection framework based on SVM with feature augmentation," Knowl.-Based Syst., vol. 136, pp. 130–139, Nov. 2017.
[11]. L.Xiao, Y. Chen, and C. K. Chang, "Bayesian model averaging of Bayesian network classifiers for intrusion detection," in Proc. IEEE 38th Int. Comput. Softw. Appl. Conf. Workshops, Västerås, Sweden, Jul. 2014, pp. 128–133, doi: 10.1109/COMPSACW.2014.25.
[12]. A.S.Eesa, Z. Orman, and A. M. A. Brifcani, "A novel feature-selection approach based on the cuttlefish optimization algorithm for intrusion detection systems," Expert Syst. Appl., vol. 42, no. 5, pp. 2670–2679, Apr. 2015.
[13]. S.S.Roy, A. Mallik, R. Gulati, M. S. Obaidat, and P. V. Krishna, "A deep learning based artificial neural network approach for intrusion detection," in Proc. Int. Conf. Math. Comput. (ICMC), Haldia, India, Jan. 2017, pp. 44–53.
[14]. S.M.H.Bamakan, H. Wang, T. Yingjie, and Y. Shi, "An effective intrusion detection framework based on MCLP/SVM optimized by timevarying chaos particle swarm optimization," Neurocomputing, vol. 199, pp. 90–102, Jul. 2016.

[15]. P.-F.Wu and H.-J. Shen, "The research and amelioration of patternmatching algorithm in intrusion detection system," in Proc. IEEE 14th Int. Conf. High Perform. Comput. Commun. IEEE 9th Int. Conf. Embedded Softw. Syst., Liverpool, U.K., Jun. 2012, pp. 1712–1715, https://doi:10.1109/HPCC.2012.256.

[16]. V.Dagar,V. Prakash, and T. Bhatia, "Analysis of pattern matching algorithms in network intrusion detection systems," in Proc. Int. Conf. Adv. Comput., 2016, pp. 1–5.

[17]. I.S.Thaseen and C. A. Kumar, "Intrusion detection model using fusion of chi-square feature selection and multi class SVM," J. King Saud Univ.- Comput. Inf. Sci., vol. 29, no. 4, pp. 462–472, Oct. 2017.

[18]. B. Ingre, A. Yadav, and A. K. Soni, "Decision tree based intrusion detection system for NSL-KDD dataset," in Proc. Int. Conf. Inf. Commun. Technol. Intell. Syst., Ahmedabad, India, 2017, pp. 207–218, https://doi:10.1007/978-3-319-63645-0_23.

[19]. H.Yang and F. Wang, "Wireless network intrusion detection based on improved convolutional neural network," IEEE Access, vol. 7, pp. 64366–64374, 2019, https://doi:10.1109/ACCESS.2019.2917299

[20]. Q.Zhang, Z. Jiang, Q. Lu, J. Han, Z. Zeng, S.-H. Gao, and A. Men, "Split to be slim: An overlooked redundancy in vanilla convolution," 2020, arXiv:2006.12085. http://arxiv.org/abs/2006.12085

IJIRIS © 2014-24, AM Publications -All Rights Reserved