International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

Review Paper on Imbalanced Network based Intrusion Detection System using Deep Learning Technique

Mithilesh Kumar Choudhary
M. Tech. Scholar
Department of Computer Science and Engineering, MITS, Bhopal
Prof. Atul Kumar Mishra
Head of Dept.
Department of Computer Science and Engineering , MITS, Bhopal

Abstract
Intrusion Detection Systems (IDS) play a critical role in safeguarding computer networks against evolving cyber threats; however, real-world network traffic is highly imbalanced, where malicious attacks constitute a small proportion compared to normal traffic. Traditional machine learning algorithms struggle to learn minority attack patterns due to skewed class distribution, resulting in high false negatives and poor generalization. Recent advancements in deep learning offer improved feature representation and anomaly detection capability, yet class imbalance remains a primary performance bottleneck in IDS research. This review paper investigates the impact of data imbalance on IDS performance, highlights recent deep learning architectures including CNN, RNN, LSTM, GRU, Autoencoders, and Transformers, and discusses imbalance mitigation approaches such as data resampling, cost-sensitive learning, hybrid models, GAN-based synthetic sample generation, and ensemble learning. The paper further evaluates publicly available benchmark datasets such as NSL-KDD, UNSW-NB15, CICIDS2017, and CSE-CIC-IDS2018 in terms of imbalance characteristics. Finally, challenges, research gaps, and future research directions are presented to guide the development of more robust and generalizable IDS frameworks.
Keywords: - Intrusion Detection Systems (IDS), Deep Learning, Imbalanced Network

1. INTRODUCTION

With the rapid expansion of digital communication, cloud computing, IoT devices, and high-speed networks, cyberattacks have increasingly become more sophisticated, frequent, and impactful. To safeguard critical infrastructures and prevent malicious intrusions, Intrusion Detection Systems (IDS) are widely deployed as a core security mechanism for detecting suspicious activities and unauthorized network access. Traditional IDS solutions, including signature-based and rule-based approaches, rely on predefined attack signatures and deterministic patterns; although effective for known attacks, they fail to detect zero-day threats, polymorphic malware, and evolving intrusion patterns.

The rise of machine learning and deep learning techniques has transformed IDS research by enabling data-driven, adaptive, and automated detection of complex attacks. Deep learning models can extract hidden correlations, learn complex network behaviors, and provide higher detection accuracy compared to classical methods. However, a critical challenge remains largely unresolved: network traffic data is inherently imbalanced, where normal traffic dominates and certain attack

types—such as User-to-Root (U2R), Remote-to-Local (R2L), and reconnaissance attacks—are extremely rare. This imbalance leads to biased learning, high false-negative rates, and poor performance in identifying minority attacks, which may cause severe security breaches if undetected.

Furthermore, widely used network datasets such as NSL-KDD, UNSW-NB15, CICIDS2017, and CSE-CIC-IDS2018 is exhibit significant class distribution variations, making model generalization more difficult. Deep learning-based IDS must therefore integrate specialized strategies such as oversampling, cost-sensitive learning, GAN-driven data augmentation, ensemble learning, and hybrid feature extraction to effectively address data imbalance in real network environments.

This review paper provides a comprehensive analysis of recent deep learning techniques applied to intrusion detection with a specific focus on the imbalanced nature of network traffic. It examines dataset characteristics, evaluates emerging architectures, compares imbalance mitigation strategies, highlights performance metrics relevant to skewed datasets, and identifies open research challenges. The goal is to guide the development of next-generation IDS frameworks capable of robust, reliable, and real-time attack detection in modern cyber ecosystems.

2. LITERATURE REVIEW

Intrusion Detection Systems (IDS) have evolved significantly with the adoption of machine learning and deep learning techniques, especially in modern IoT-driven and large-scale network environments. Recent research has focused on improving detection accuracy, reducing false alarms, and addressing challenges related to imbalanced network traffic.

Dhiaa Musleh et al. (2023) proposed a feature extraction-based IDS for IoT environments using machine learning classifiers. Their approach demonstrated improved detection accuracy by selecting optimal network features, yet performance degraded under highly skewed traffic conditions, highlighting the need for imbalance-focused models.

S. K. B Sangeetha et al. [2], in imbalanced organization traffic, pernicious digital assaults can regularly stow away in a lot of typical information. It displays a serious level of covertness and jumbling in the internet, making it hard for Network IDS to guarantee the precision and practicality of discovery. This paper explores AI and profound learning for interruption recognition in imbalanced organization traffic. It proposes an original Difficult Set Sampling Technique (DSSTE) calculation to handle the class awkwardness issue. To start with, utilize the Edited Nearest Neighbor (ENN) calculation to separate the imbalanced preparing set into the troublesome set and the simple set. Then, utilize the K Means calculation to pack the larger part tests in the troublesome set to diminish the larger part. Zoom in and out the minority tests' persistent characteristics in the troublesome set integrate new examples to expand the minority number.

Kezhou Ren et al. [3], network attacks pose significant threats to network services' security. Therefore, it is essential to make use of brand-new technical approaches in order to boost the effectiveness of intrusion detection systems. In recent years, a number of reinforcement learning algorithms for network intrusion systems, such as Markov and others, have been developed to meet the IDS's needs for both intelligent and unmanned systems. A deep feed-forward neural network approach is used in conjunction with a deep Q-learning-based network intrusion detection model that incorporates reinforcement learning to provide continuous automatic learning capability for network environments. To test the model's performance, experiments were carried out with the

CSE-CIC-IDS2018 dataset, which contains a comprehensive collection of actual network traffic. The results of the experiments show that the proposed model can successfully identify threats in the network, outperforms standard machine learning methods, and has promising potential as an unmanned IDS in complex network settings.

R. Ahsan et al. [4], the issue of anomaly detection in imbalanced datasets is examined in this work within the context of network intrusion detection. To deal with the class-imbalance issue, a novel anomaly detection solution that takes into account both data-level and algorithm-level approaches is proposed. The oversampling capabilities of a Conditional Generative Adversarial Network (CGAN) and the auto-learning capabilities of reinforcement learning are combined in this approach. To additionally explore the capability of a CGAN, in imbalanced order undertakings, the impact of CGAN-put together oversampling with respect to the accompanying classifiers is inspected: Logistic Regression, Multilayer Perceptron, Random Forest, and Naive Bayes The experimental results show that the proposed method and CGAN-based oversampling in general perform better than other oversampling methods like the Synthetic Minority Oversampling Technique and Adaptive Synthetic. The Authors in 2021 Cyber-Physical Systems from IET: Hypothesis and Applications distributed by John Wiley and Children Ltd for The Establishment of Designing and Innovation.

S. Dong et al. [5], our production life has been greatly improved by the rapid development of Internet technology, but as a result, security issues have become increasingly prevalent. Users' privacy is at risk, and many aspects of society, including politics, the economy, culture, and people's means of subsistence, face significant security risks as a result of these issues. The development of the data transmission rate grows the extent of assaults and gives a more assault climate to interlopers. Strange location is a compelling security assurance innovation that can screen network transmission continuously, really sense outside assaults, and give reaction choices to pertinent chiefs. A technology for detecting abnormal traffic has also emerged as a result of advances in machine learning. The objective has been to use powerful and quick learning algorithms to respond immediately to shifting threats. The vast majority of the flow unusual identification research depends on reproduction, utilizing public and notable datasets. From one viewpoint, the dataset contains high-layered enormous information, which customary AI strategies can't be handled. However, the labeling cost is extremely high because the dataset's labels are all manually labeled and the labeled data scale is far behind the application requirements. This paper proposes a semi-directed Twofold Profound Q-Organization (SSDDQN)- based improvement strategy for network strange traffic location, mostly founded on Twofold Profound Q-Organization (DDQN), a delegate of Profound Support Learning calculation. The current network in SSDDQN uses a deep neural network as a classifier before using the autoencoder to reconstruct the traffic features. K-Means clustering is used by the target network's unsupervised learning algorithm first, followed by deep neural network prediction. For training and testing, the experiment makes extensive use of the NSL-KDD and AWID datasets and compares them to existing machine learning models. The experimental results demonstrate that SSDDQN performed well in a variety of evaluation metrics and has some advantages in terms of time complexity.

Lau lin et al. [6], in imbalanced organization traffic, pernicious digital assaults can regularly stow away in a lot of typical information. It displays a serious level of covertness and jumbling in the

internet, making it hard for Network Intrusion Detection System(NIDS) to guarantee the precision and practicality of discovery. This paper explores AI and profound learning for interruption recognition in imbalanced organization traffic. It proposes an original Difficult Set Sampling Technique (DSSTE) calculation to handle the class awkwardness issue. To start with, utilize the Edited Nearest Neighbor(ENN) calculation to separate the imbalanced preparing set into the troublesome set and the simple set. Then, utilize the KMeans calculation to pack the larger part tests in the troublesome set to diminish the larger part. Zoom in and out the minority tests' persistent characteristics in the troublesome set integrate new examples to expand the minority number.

A. Raghavan et al. [7], successful and proficient malware recognition is at the bleeding edge of examination into building secure computerized frameworks. Similarly as with numerous different fields, malware location research has seen a sensational expansion in the utilization of AI calculations. One AI strategy that has been utilized broadly in the field of example matching overall—and malware identification specifically—is covered up Markov models (HMMs). Gee preparing depends on a slope climb, and thus we can frequently work on a model via preparing on numerous occasions with various beginning qualities. In this exploration, we think about helped HMMs (utilizing AdaBoost) to HMMs prepared with different arbitrary restarts, with regards to malware identification. These procedures are applied to an assortment of testing malware datasets. We observe that irregular restarts perform shockingly well in contrast with helping. Just in the most troublesome "cold beginning" situations (where preparing information is seriously restricted) does helping seem to offer adequate improvement to legitimize its higher computational expense in the scoring stage.

Zhiyou Zhang et al. [8], in this paper, aimed at detection of internal intruders in HIDS. Commonly used login ids and passwords may be shared along with co-workers for professional purposes, which can be tampered or used by the attackers as a means of intrusion into the system details. The user was monitored and System Calls (SC) was extracted and the habitual SC pattern based on the habits of the user was taken into account and the profile of the user was stabilized. The forensic technique and other data mining techniques were applied at SC level host IDS to spot the internal attacks. Along with the user login credentials the forensic technique was applied to investigate the computer usage fashion against the collected user profile pattern and thereby check the identity of the user.

Afreen Bhumgara et al. [9], in this paper, With the decision rate threshold of 0.9, the system was able to perform with an accuracy rate of 94%. Nokia Research Center researchers modeled HIDS for mobile devices. The limitation include that each protocol state consume resources for tracing and testing, and its inability to guess the attacks resembling benign protocol. Access control fills in as the cutting edge of resistance against interruptions, bolstering both confidentiality and integrity parameters. Intrusion detection is the process of progressively observing the events occurring in a PC or network, examining them for indications of conceivable episodes and often interdicting the unapproved access. A state transition diagram can be constructed for the sequence of events, but not for the complex forms and hence the attacks having complex behavior which cannot be modeled as the state transition diagram will go unnoticed by the system.

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

3. DEEP LEARNING

Deep learning (DL) is a subset of machine learning (ML) procedures zeroed in on order undertakings and transformative calculations [14]. There are three sorts of learning: supervised learning, semi-supervised and unsupervised. DL structures consolidating DL models, completely associated networks, repetitive brain organizations, and fake brain networks were utilized in fields including AI, man-made reasoning, PC vision, information examination, understood, virtual entertainment site separating, computational semantics, computational science, drug plan, data recovery, and clear outline, among others [15]. Information obtaining and decentralized authoritative foundation in natural frameworks impacted fake ANNs. ANNs change from the human mind in more ways than one. Specifically, brain networks are steady and emblematic, though most working substances' natural minds are dynamic and simple.

Profound gaining gets its name from the way that it utilizes many layers in the organization. Early exploration exhibited that a direct perceptron can't be utilized as an all inclusive classifier yet that an organization with a non-polynomial information layer and one unreasonable width stowed away layer may [59]. Profound learning is a later variation including many layers of limited size, considering practical application and improvement while keeping up with hypothetical subjectivity under gentle circumstances. For execution, teachability, and clarity, profound learning structures are additionally permitted to be different and wander away generally from deductively informed connectionist models, consequently the "coordinated" segment [16].

Most of new profound learning procedures center around AI, particularly CNNs. They may likewise incorporate propositional recipes or dormant factors organized layer-wise in profound generative models like profound conviction organizations and profound Boltzmann machines. Each degree of profound learning figures out how to transform the information it gets into a somewhat more conceptual and composite portrayal. The crude contribution to a picture acknowledgment program could be a grid of pixels; the main delegate layer could digest the pixels and encode edges; the subsequent layer could form and encode edge courses of action; the third layer could encode a nose and eyes, and the fourth layer could perceive that the picture contains a face. Significantly, a profound learning calculation might sort out which highlights have a place with which level all alone.

The expression "profound learning" alludes to the quantity of layers that the information is changed through. Profound learning frameworks, specifically, have a critical credit task way (CAP) profundity [5]. The CAP is the contribution to-yield progress chain. Covers are utilized to characterize conceivable causal connections among info and result. The profundity of the Covers in a feed forward brain network is equivalent to the organization's profundity in addition to the quantity of secret layers in addition to one. The CAP profundity in repetitive brain organizations, where a sign can engender through a layer on numerous occasions, is hypothetically limitless. Albeit no by and large settled upon profundity level isolates shallow and profound learning, most scientists concur that profound advancing necessities a CAP profundity more prominent than 2. As in it can impersonate any capability, CAP of profundity two is a widespread surmised [7].

More layers, then again, don't work on the organization's capacity to inexact capabilities. Additional layers help in learning the highlights successfully in light of the fact that profound models can separate preferable elements over shallow models. Profound convolutional layers can build

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

profound learning models in CNN. The DL can support the deconstruction of these reflections and the ID of which elements further develop results. Profound learning strategies wipe out include designing for managed learning undertakings by changing over information into minimal element vectors closely resembling factor stacking and creating layered structures that lessen overt repetitiveness. Solo gaining errands might profit from profound learning calculations. This is a critical benefit since unlabeled information is more copious than named information. ANN and profound conviction networks are the two fundamental brain network that works like solo learning approach. There are one or two sorts of profound learning calculations, which are referenced underneath [8].

4. Intrusion Detection System

An Intrusion Detection System (IDS) is a security mechanism designed to monitor network traffic or system activities to detect abnormal behavior, policy violations, or malicious attacks. It helps identify potential intrusions such as malware infections, Denial-of-Service (DoS) attempts, unauthorized access, probing, and privilege escalation. IDS serves as a critical layer in cybersecurity frameworks, functioning as an early warning system that alerts administrators before threats escalate into serious breaches.

IDS typically operates through data collection, feature analysis, pattern identification, and attack classification. Based on deployment and detection methodology, IDS can be categorized into Network-based IDS (NIDS) and Host-based IDS (HIDS). Additionally, detection techniques are broadly classified into signature-based detection, which identifies known threats using predefined patterns, and anomaly-based detection, which detects deviations from normal behavior to identify new or unknown attacks.

Modern IDS systems increasingly adopt machine learning and deep learning approaches to automatically extract features, handle high-dimensional network data, improve generalization for unseen threats, and enhance detection accuracy—especially for emerging attacks. Due to the highly imbalanced nature of real-world traffic, intelligent IDS models must incorporate strategies like oversampling, cost-sensitive learning, and hybrid feature learning to improve detection of minority attack classes.

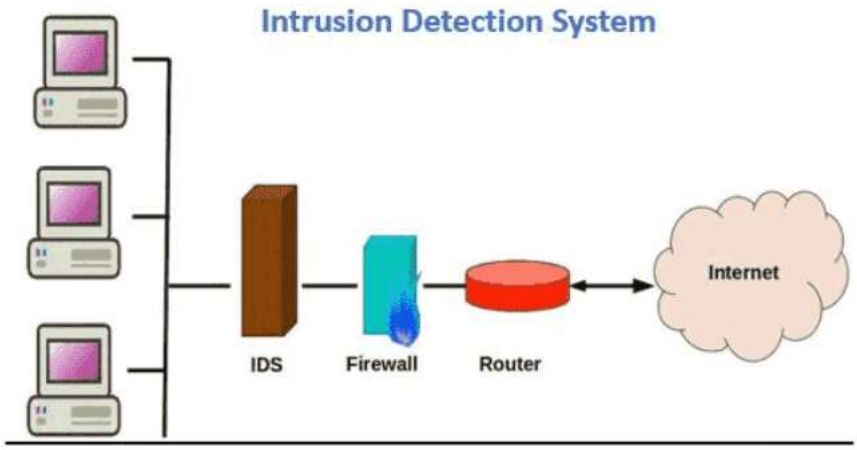

Figure 1: IDS System

5. CONCLUSION

The rapid evolution of cyber-attacks and the increasing complexity of network environments have necessitated the development of intelligent Intrusion Detection Systems capable of achieving high detection accuracy while addressing data imbalance challenges. This review analyzed various deep learning approaches, including CNN, LSTM, hybrid deep models, and autoencoder-based frameworks, which demonstrate superior feature-learning capability compared to traditional machine learning methods. While recent studies have improved intrusion detection performance, class imbalance remains a critical limitation, causing models to favor majority benign traffic and undermining accurate detection of minority attack classes. Techniques such as oversampling, cost-sensitive learning, ensemble architectures, and optimized loss functions have shown promising results in balancing detection performance across all attack categories. However, issues such as high training complexity, limited real-time applicability, dataset non-uniformity, and scalability challenges still persist. Therefore, future research should focus on developing lightweight, adaptive, and cost-efficient deep learning models, integrating real-time threat intelligence, and employing balanced learning strategies to enhance robustness and operational deployment in real-world network environments. Ultimately, addressing imbalance remains essential for building reliable IDS solutions that can safeguard modern digital infrastructures from emerging cyber threats.

References

[1] Dhiaa Musleh, Meera Alotaibi, Fahd Alhaidari, Atta Rahman, and Rami M. Mohammad, “Intrusion Detection System Using Feature Extraction with Machine Learning Algorithms in IoT,” Journal of Sensor and Actuator Networks, 12, 2023.

[2] S. K. B Sangeetha, Prasanna Mani, V. Maheshwari, Prabhu Jayagopal, M. Sandeep Kumar and Shaikh Muhammad Allayear, “Design and Analysis of Multilayered Neural Network-Based Intrusion Detection System in the Internet of Things Network”, Hindawi, 2022.

[3] Kezhou Ren, Maohuan Wang, Yifan Zeng and Yingchao Zhang, *“*An Unmanned Network Intrusion Detection Model Based on Deep Reinforcement Learning*”,* IEEE International Conference on Unmanned Systems (ICUS), IEEE 2022.

[4] R. Ahsan, W. Shi, X. Ma, and W. L. Croft, “A comparative analysis of CGAN-based oversampling for anomaly detection,” *IET* Cyberphysical Systems: Theory & Applications, vol. 7, no. 1, pp. 40–50, Mar. 2022.

[5] S. Dong, Y. Xia, and T. Peng, “Network Abnormal Traffic Detection Model Based on Semi-Supervised Deep Reinforcement Learning,” IEEE Transactions On Network And Service Management, vol. 18, no. 4, pp. 4197–4212, Dec. 2021.

[6] Lan Liu, Pengcheng Wang , Jun Lin, and Langzhou Liu, “Intrusion Detection of Imbalanced Network Traffic Based on Machine Learning and Deep Learning”, IEEE Access 2020.

[7] A. Raghavan, F. D. Troia, and M. Stamp, ``Hidden Markov models with random restarts versus boosting for malware detection," *J. Comput. Virol. Hacking Techn.*, vol. 15, no. 2, pp. 97107, Jun. 2019.

[8] Zhiyou Zhang and Peishang Pan “A hybrid intrusion detection method based on improved fuzzy C-Means and SVM”, IEEE International Conference on Communication Information System and Computer Engineer (CISCE), pp. no. 210-214, Haikou, China 2019.

[9] Afreen Bhumgara and Anand Pitale, "Detection of Network Intrusion Using Hybrid Intelligent System", IEEE International Conferences on Advances in Information Technology, pp. no. 167-172, Chikmagalur, India 2019.

[10] Ritumbhira Uikey and Dr. Manari Cyanchandani "Survey on Classification Techniques Applied to Intrusion Detection System and its Comparative Analysis", IEEE 4th International Conference on Communication $ Electronics System (ICCES), pp. no. 459-466, Coimbatore, India 2019.

[11] Aditya Phadke, Mohit Kulkarni, Pranav Bhawalkar and Rashmi Bhattad "A Review of Machine Learning Methodologies for Network Intrusion Detection", IEEE 3rd National Conference on Computing Methodologies and Communication (ICCMC), pp. no. 703-709, Erode, India 2019.

[12] S. Sivantham, R.Abirami and R.Gowsalya "Comapring in Anomaly Based Intrusion Detection System for Networks", IEEE International conference on Vision towards Emerging Trends in Communication and Networking (ViTECon), pp. no. 289-293, Coimbatore, India 2019.

[13] Azar Abid Salih and Maiwan Bahjat Abdulrazaq "Combining Best Features selection Using Three Classifiers in Intrusion Detection System", IEEE International Conference on Advanced science and Engineering (ICOASE), pp. no. 453-459, Zakho - Duhok, Iraq 2019.

[14] Lukman Hakim and Rahilla Fatma Novriandi "Influence Analysis of Feature Selection to Network Intrusion Detection System Performance Using NSL-KDD Dataset", IEEE International Conference on Computer Science, Information Technology, and Electrical Engineering (ICOMITEE), pp. no. 330-336, Jember, Indonesia 2019.

[15] T. Sree Kala and A. Christy, "An Intrusion Detection System Using Opposition Based Particle Swayam Optimization Algorithm and PNN", IEEE International Conference on Machine Learning, Big Data, Cloud and Parallel Computing, pp. no. 564-569, Coimbatore, India 2019.