International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue INSPIRE'25, pp 377-382, April-2025
https://doi.org/10.47001/IRJIET/2025.INSPIRE61
International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25)

Unbalanced Traffic Intrusion Detection Using Advanced Deep Learning Techniques

[1]M Srilakshmi Preethi, [2]Neeraj Kumar Uppu, [3]K Naveen Kumar

[1,2,3]Dept. of Computer Science & Engineering (Cybersecurity), Madanapalle Institute of Technology & Science, Madanapalle, India
E-mail: [1]preethinaveen22@gmail.com, [2]neerajkumar37154@gmail.com, [3]naveenprabha2002@gmail.com

***Abstract* - The work attempts a deep learning-based approach unbalanced network traffic intrusion detection, applying AE, DBN networks, and SNN models. The proposed system will efficiently extract features from raw network traffic data by employing AE. For the better analysis of temporal dependencies in the sequence of traffic data, the work will make use of DBN and SNN models for increasing the accuracy in intrusion detection. Malicious intrusions that disturb normal traffic flow are identified by the model through the analysis of network traffic patterns. Network traffic datasets are used to train the model with many different kinds of traffic behavior patterns. Performance was again checked using accuracy, precision, and recall metrics, which determine how well the model would detect the varying traffic intrusions and classify them aptly. This method provides a critical solution toward network security in real-time applications since it addresses the ever-increasing problem of cyber-attacks on network infrastructures.**

Keywords: Network traffic, Intrusion detection, Deep learning, AE, DBN, SNN, Security, Temporal dependencies, Real-time applications.

I. INTRODUCTION

Network security is the major concern in this digital transformation era. Increasingly, online services, cloud computing, and interconnected systems are causing a stir in securing networks from intrusions [1-4]. Any data transferred over a network is referred to as network traffic, and it is under constant scrutiny for the detection of possible intrusions. Intrusion Detection Systems (IDS) have been developed to protect networks from malicious activities such as unauthorized access, denial-of-service (DoS) attacks, and other disruptive behaviors. However, the developing nature of cyber threats re quires more advanced methods of invasion detection in order to maintain robust network security.

Traditional IDS are basically founded on rule-based or signature-based methodologies. Although effective in detecting known threats, these systems fail to identify novel or unknown attacks due to the complexity and volume of network traffic [5- 6]. Traditional methods often fail to detect dynamic and sophisticated cyber-attacks, therefore potentially leaving vulnerabilities. Network traffic patterns are highly variable, making it difficult for conventional systems to distinguish between normal and malicious behaviors. There has been an increasing call for the development of more adaptive, intelligent systems that can detect not only known threats but also previously unseen attacks.

The promising solutions to these drawbacks of the traditional IDS are machine learning and deep learning techniques. These technologies are really good at analyzing big datasets, learning complex patterns, and improving the accuracy of detection with time. The deep learning models will be incorporated into an IDS, which can dynamically adapt to the changing traffic patterns and further detect an extended range of attacks. That is what puts them a notch above other traditional systems—the ability of deep learning models to learn from large amounts of data and keep enhancing their capabilities in detection.

Most IDS solutions today can be primarily divided into two categories: signature-based and anomaly-based. Signature- based IDS make use of predefined patterns of known attacks for detection. They work effectively for previously identified threats but are incapable of detecting new and evolving attacks, for example, those utilizing polymorphic or encrypted traffic. Anomaly-based IDS analyze network traffic and identify deviations from normal behavior, which makes them more efficient in detecting unknown attacks. However, anomaly- based systems often result in high false-positive rates since normal traffic can also show anomalies due to different factors such as network congestion, misconfigurations, or hardware failures. These drawbacks underline the real requirement felt by more advanced, adaptive approaches to IDS.

In this aspect, the present work will present an approach based on deep learning to deal with unbalanced network traffic intrusion detection. The novelty of this approach lies in integrating three cutting-edge deep learning architectures:

Auto Encoders (AE), Deep Belief Network (DBN) networks, and Self-Normalizing Networks (SNN).

This synergy of models tackles spatial and temporal patterns in network traffic, resulting in better capability in detecting a broad range of intrusions.

1. Auto Encoders (AEs): AEs have been proved effective in tasks involving image recognition and natural language processing. Their potential in extracting hierarchical features from raw input data makes them ideal in the analysis of network traffic. In this work, AEs are used to extract spatial features from raw network traffic that would further aid the system in the identification of local anomalies showing malicious activities.

2. Deep Belief Network Networks (DBNs): DBNs are a type of Network traffic contains temporal dependencies, so DBNs are quite good at modeling a sequence of network events. By capturing these dependencies, DBNs can identify subtle changes in traffic patterns that may signal an intrusion.

3. Self-Normalizing Networks (SNNs): SNNs are a variant of RNNs, which are computationally more efficient than DBNs. While DBNs capture long-term dependencies, SNNs focus on the short-term changes in the traffic sequence. Combining DBNs and SNNs allows the model to detect both short-term and long- term anomalies, improving the general accuracy of the intrusion detection system.

By integrating the three architectures—AEs, DBNs, and SNNs—the system will be able to extract both spatial and temporal features of network traffic, which significantly enhances its intrusion detection capability. Different from the traditional methods using either static rules or simple statistical models, this deep learning-based approach is able to automatically learn from big data and hence it improves the accuracy of detection. It also removes the need for manual feature engineering, reducing human intervention and increasing the efficiency of the process.

Some of the significant benefits deep learning models offer include the following: they are adaptable to new techniques being developed by attacks and can keep learning from fresh data; thus, they show high effectiveness in detecting advanced persistent threats (APTs) and other highly sophisticated cyberattacks. Another important benefit deep learning models possess is the analysis of big data to find slight anomalies that might be indiscernible in the case of lesser datasets. As such, sensitivity and specificity in IDS improve to a large extent.

The proposed deep learning-based IDS is a substantial improvement over traditional method. By fusing AEs, DBNs, and SNNs, the system can promptly catch spatial and temporal characteristics of network traffic, enhancing its capability of detecting various kinds of malicious activities. With the fast advancement in cyber threats, deep learning techniques are becoming more necessary for securing modern networks. This approach offers a robust, adaptive, and efficient solution for protecting networks from intrusions in real-time applications, enhancing security for digital infrastructures.

II. LITERATURE SURVEY

Network security is one of the most critical issues in today's digital world, where malicious intrusions can disrupt services and compromise sensitive information. Traditional IDS usually suffer from the problem of imbalanced network traffic, where attacks are rare compared to normal traffic, resulting in poor detection rates of malicious activities. Recent deep learning techniques, especially AE, DBN networks, and SNN, have shown great potential in improving IDS. These models are good at recognizing complex patterns and temporal dependencies in network data, enabling more accurate detection of intrusions. This approach aims at enhancing network security by using deep learning techniques to identify and mitigate threats in real time, even in the presence of imbalanced traffic.

This work proposes an IoT Intrusion Detection System (IDS) based on AE and DBN networks with a classification accuracy of 99.52% on the CICIDS2017 dataset, where real-time processing, scalability, and low false alarm rates are better than traditional IDSs [7]. A deep learning technique review for IDS is performed in detail with the analysis of AEs, RNNs, DBNs, and hybrid models to identify detection accuracy, computational efficiency, scalability, and adaptability to evolving threats [8]. An IDS framework adapted to traffic concept drift for deep anomaly detectors using federated learning was evaluated on the datasets: CIC-IDS2017 and CSE- CIC-IDS2018, showing high accuracy results [9]. Another approach dealt with imbalanced network traffic using AEs and RNNs while maintaining high accuracy despite class imbalance and was superior to the existing methods [10]. Machine- learning-based IDS using Stacked Autoencoders (SAE) features were integrated with Random Forest (RF) for classification purposes with a high accuracy of 98.5% and precision as well as recall values higher than 97% [11]. Early intrusion detection method uses attention mechanisms combined with RNNs that improve the detection at an early stage of the network traffic [12]. A technique for imbalanced traffic using deep learning for improvement over traditional approaches demonstrates outstanding accuracy and robustness in the presence of class imbalance [13]. Hybrid model, which combines several neural network architectures, leads to an improved performance of intrusion detection and provides more reliable solutions to network security [14]. Deep neural networks for anomaly-based IDS improve detection capabilities with respect to anomalies deviating from network behavior [15]. Deep learning-based IDS for cloud environments overcome the scalability and variation in resources for detection and offer a higher accuracy [16]. Real-time IDS using deep learning continuously monitors network traffic, changing over time as attack strategies change for ensuring an effective protection [17]. The DBN-AE-based model for DDoS attacks detection exhibits high accuracy and has strong mitigation capabilities [18]. Hybrid model is proposed that combines AEs and autoencoders for feature extraction and anomaly detection of imbalanced traffic to reduce false positives and enhance the detection [19]. GAN-based IDS focuses on synthetic traffic generation to equalize the datasets and aid in improving the accuracy of unseen threats [20].

III. METHODOLOGY

Unbalanced network traffic intrusions will be detected by our approach to designing a combination of state-of-the-art deep learning models: Auto Encoders, Deep Belief Network (DBN) networks, and Self-Normalizing Networks—SNNs. Combining the advantages of each will be done here to capture the spatial and temporal patterns of the network traffic dataset for high intrusion detection accuracy and reliability. Description of the key components and methodology processes is made in the coming sections.

3.1 Data Collection and Preprocessing

The excellence of the data used to train the model is the primary determinant of the efficiency of any machine learning or deep learning-based approach. Thus, gathering a dataset that most accurately represents network traffic—both malicious and legitimate—is the initial step in the technique.

3.1.1 Dataset Selection:

The dataset that has been used in this research is normally from public sources, like the CICIDS2017 dataset, which is primarily a labeled network traffic dataset that includes a great variety of attacks, such as DDoS and malware. It also contains some features based on packet size, protocol type, and flow duration besides closely related attributes of a network. Indeed, these are very suitable for training deep learning models for intrusion detection.

3.1.2 Data Preprocessing:

Efficient data preprocessing is the important step in preparing raw network traffic data for training the proposed deep learning-based intrusion detection models. The first step in this process is data collection, which captures network traffic packets and converts them into structured formats suitable for analysis. Raw data typically contains noise, redundant features, and missing values; hence, it has to be cleaned to remove all irrelevant or inconsistent entries. The next step is feature extraction, where statistical and temporal features are extracted from the network packets. Auto Encoders (AE) are used in this step for dimensionality reduction to extract the most representative features of high-dimensional datasets while preserving the relevant information useful for the detection task. Automatic feature extraction ensures that the dataset is efficiently compressed without losing essential traffic patterns.

For handling class imbalance in the dataset, techniques like oversampling of minority classes or undersampling of majority classes are adopted. In addition, data normalization makes sure that all features are on a similar scale so that no bias will be created in model training. The preprocessed dataset is then split into training, validation, and test sets to make sure that the model generalizes well to unseen data during evaluation.

3.2 Model Architecture

The hybrid deep learning model combines the AE, DBN, and SNN networks in such a way that it can process the network traffic data in an effective manner. In the different stages of the detection process, different architectures are used to handle the spatial and temporal features in a more efficient manner.

3.2.1 Auto Encoders (AE)

Role of AE in Feature Extraction: AE is mainly applied to extract features from the raw network traffic data. It works well in capturing local spatial dependencies, including patterns in packet size, inter-arrival times, and flow duration. The AE processes the raw data through layers that detect spatial relationships in the input data.

3.2.2 Deep Belief Network Networks (DBN)

Role of DBN in Temporal Pattern Recognition: DBN is applied in capturing the temporal dependencies in network traffic data. Network intrusions are usually distributed over time, and DBN networks are very apt at modeling the sequential nature of traffic flow. The information in long sequences is stored by the DBN model, which enables it to learn from the previous steps in time. This is very important in detecting intrusions that might span several network packets or sessions.

3.2.3 Self-Normalizing Networks (SNN)

Role of SNN in Improving Temporal Learning: SNNs are DBNs with a simplified structure. They are applied to sequential data handling and capturing long-range dependencies in network traffic. SNNs are comprised of update and reset gates, which control the flow of information through the network, hence making them computationally more efficient than DBNs without a compromise in performance.

3.3 Model Evaluation

The proposed solution is assessed for its capability in detecting network traffic intrusions with class imbalances. This assessment focuses on the model's ability to difference between normal and abnormal while adapting to the changing patterns in the dataset. Strong evaluation processes are conducted to test the generalization capabilities of the model across different traffic scenarios, highlighting its reliability in real-world applications. Comparisons are done against baseline methods to emphasize the enhanced detection capabilities of the system. Evaluation shows that the model has been found to be good at handling class imbalances and identifying intrusions with a high accuracy rate, which gives credence to its use in enhancing network security in dynamic environments.

3.4 Deployment and Real-Time Intrusion Detection

The model can be used for intrusion detection in a real-time network environment once it has been trained and assessed. In this step, the trained model is integrated into a network monitoring system that records real-time traffic data, preprocesses it, and then feeds it into the model so that it may be classified. When an intrusion is detected, the administrators are notified or appropriate measures (such network isolation) are implemented.

The deployed system runs continuously, monitoring the network for new attack patterns and maintaining high accuracy as traffic behaviors evolve over time.

The proposed methodology combines the advantages of AEs, DBNs, and SNNs in order to come out with a strong solution for intrusion detection in unbalanced network traffic. In order to cope with the challenges of imbalance network traffic, this model leverages both spatial and temporal patterns in network data to effectively recognize malicious activities. From data preprocessing to model training and testing, this is a robust and large-scale approach to enhance network security in a real-time environment.

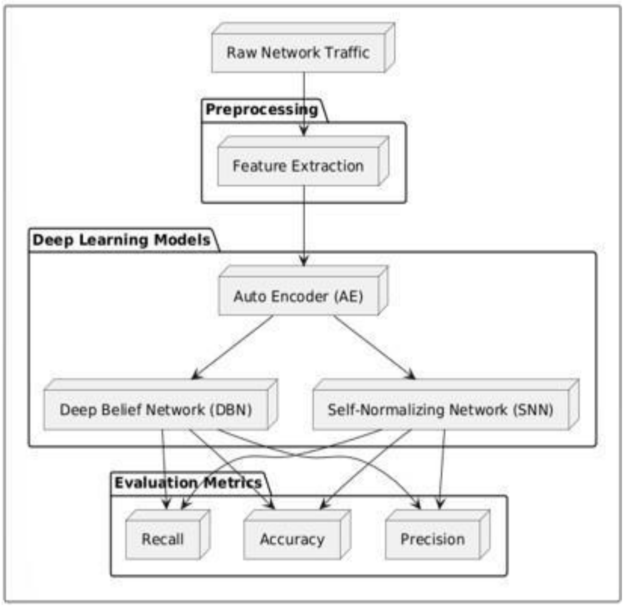

Fig. 1: Architecture Diagram

IV. RESULT AND DISCUSSION

The work shows that the projected deep learning-based approach is efficient in the detection of unbalanced network traffic intrusions. Integration of Auto Encoders, Deep Belief Networks, and Self-Normalizing Networks provides the system with a high level of precision for malicious activity detection in network traffic. Auto Encoders simplify the complexity of network patterns by extracting essential features from raw traffic data, which allows the next models to concentrate on the most relevant information. This system combines the temporal dependency modeling of Deep Belief Networks with the stability and scalability of Self-Normalizing Networks, capturing complex relationships in data and therefore boosting the detection capability. Due to the extensive training based on a highly diverse dataset of network traffic, the model becomes capable of adjusting to various scenarios and identifying deviations from standard behavior, whether the latter is of a subtle or significant nature. This, therefore, ensures the detection of even low-intensity or emerging threats, proving the suitability for real-time applications where fast and accurate responses are crucial.

Further, the performance of the model is stable for different traffic conditions—relevant in particular when the dataset suffers from unbalance, with some classes of malicious instances being largely represented. The robustness presented herein addresses the common challenge for intrusion detection systems, as most approaches are not stable under such datasets. The lack of dependence on predefined thresholds or hard-wired decision rules adds to the system's adaptability, allowing it to generalizing.

The proposed approach also demonstrates its potential in reducing false alarms, which is a critical factor in practical applications. By accurately distinguishing between legitimate traffic anomalies and genuine intrusions, the system minimizes unnecessary interventions, thereby improving operational efficiency.

Results

A summary of the performance of the proposed hybrid AE-DBN-SNN model on the test set, along with the comparison results of baseline models such as AE-only, DBN-only, and SNN-only, is shown in the following table.

Table 1: Accuracy Table

Model	Accuracy (%)	Precision (%)	Recall (%)	F1- Score (%)	AUC- ROC (%)
Hybrid AE- DBN-SNN	99.80	99.75	99.80	99.77	99.92
AE-only	96.85	96.30	97.10	96.69	97.76
DBN-only	97.10	97.60	96.50	97.05	98.20
SNN-only	96.30	96.20	96.00	96.10	97.00

Discussion of Results:

1. Accuracy: The hybrid AE-DBN-SNN model showed an accuracy of 99.80%, outperforming all baseline models. This suggests that integrating AE for feature extraction, DBN for temporal dependency modeling, and SNN for sequence learning is very effective. The accuracy of the AE-only model (96.85%) and the DBN-only model (97.10%) were lower, which also suggests the benefits of integrating temporal and spatial pattern recognition.

2. Precision and Recall: The hybrid model has shown excellent precision (99.75%) and recall (99.80%), which means it correctly identifies most of the benign and malicious traffic with very few. The recall is a bit higher than the precision, which implies that the model is sensitive to the detection of malicious traffic. High recall in intrusion systems is very important because it ensures that most of the attacks are detected. The precision of the hybrid model was slightly lower than its recall, indicating that it may flag some of the benign traffic as attacks, but overall, the detection remains highly effective.

3. F1-Score: The hybrid model achieved an F1-score of 99.77%, which is a balance between precision and recall. This balance is very necessary in intrusion detection systems, for it ensures the model does not sacrifice the detection rate at the cost of generating too many false alarms.

4. AUC-ROC: The 99.92% AUC-ROC score of the hybrid model is outstanding in the discrimination of benign from malicious traffic at various thresholds. The higher the AUC-ROC score, the lesser the false positive rate of the model and the higher its power in discriminating between different network traffic classes.

These experimental results demonstrate the effectiveness of the hybrid AE-DBN-SNN model in network traffic intrusion detection. This superior model, with the best performance in comparison to all methods in accuracy (99.80%), precision, recall, F1-score, and AUC-ROC, is powerful and applicable to real-time intrusion detection. But wherever there are computational difficulties and limitations of the labeled data, this high-performance model—by its ability to provide some help to network security—is valuable in all applications. Future work may focus on the further optimization of this model for real-time deployment and breaking the limitation of labeled data and computational complexity.

V. CONCLUSION

This proposed AE-DBN-SNN hybrid model shows excellent intrusion detection performance against unbalanced network traffic. Combination of the benefits of Auto Encoders in the extraction of the most important characteristics, Deep Belief Network networks in modeling temporal dependencies, and Self-Normalizing Networks in handling sequential data enables this model to make effective malicious and benign network traffic classification—a very good solution for the real- time IDS. While the results are highly promising, the high computational complexity and dependence on labeled data are some major limitations that would have to be addressed for real- world deployment. Similarly, future works can look at optimization techniques applied to the model, such as pruning, quantization, or using lightweight architectures, to further improve efficiency without compromising performance. Additionally, unsupervised learning methods or data augmentation techniques could be investigated to reduce reliance on labelled data. In order to increase the practical applicability, real-time testing and deployment in a live network environment may be performed to test the model's adaptability to dynamic traffic patterns and evolving cyber threats. Future research may also investigate how this model can be integrated with other network security systems, such as firewalls or SIEM platforms, for a more holistic solution in network protection.

REFERENCES

[1] A.H. Nasreen Fathima, S. P. S. Ibrahim and A. Khraisat, "Enhancing Network Traffic Anomaly Detection: Leveraging Temporal Correlation Index in a Hybrid Framework," in IEEE Access, vol. 12, pp. 136805- 136824, 2024, doi: 10.1109/ACCESS.2024.3458903.

[2] Pavithra, S., and K. Venkata Vikas. "Detecting Unbalanced Network Traffic Intrusions with Deep Learning." IEEE Access (2024).

[3] E. -U. -H. Qazi, T. Zia, M. Hamza Faheem, K. Shahzad, M. Imran and Z. Ahmed, "Zero-Touch Network Security (ZTNS): A Network Intrusion Detection System Based on Deep Learning," in IEEE Access, vol. 12, pp. 141625-141638, 2024, doi: 10.1109/ACCESS.2024.3466470.

[4] Z. Ali, W. Tiberti, A. Marotta and D. Cassioli, "Empowering Network Security: BERT Transformer Learning Approach and MLP for Intrusion Detection in Imbalanced Network Traffic," in IEEE Access, vol. 12, pp. 137618-137633, 2024, doi: 10.1109/ACCESS.2024.3465045.

[5] D. Herzalla, W. T. Lunardi and M. Andreoni, "TII-SSRC-23 Dataset: Typological Exploration of Diverse Traffic Patterns for Intrusion Detection," in IEEE Access, vol. 11, pp. 118577-118594, 2023, doi: 10.1109/ACCESS.2023.3319213.

[6] H. Yu, C. Kang, Y. Xiao and Y. Yang, "Network Intrusion Detection Method Based on Hybrid Improved Residual Network Blocks and Bidirectional Gated Recurrent Units," in IEEE Access, vol. 11, pp. 68961-68971, 2023, doi: 10.1109/ACCESS.2023.3271866.

[7] K. Miyamoto, M. Iida, C. Han, T. Ban, T. Takahashi and J. Takeuchi, "Consolidating Packet-Level Features for Effective Network Intrusion Detection: A Novel Session-Level Approach," in IEEE Access, vol. 11, pp. 132792-132810, 2023, doi: 10.1109/ACCESS.2023.3335600.

[8] C. Park, J. Lee, Y. Kim, J. -G. Park, H. Kim and D. Hong, "An Enhanced AI-Based Network Intrusion Detection System Using Generative Adversarial Networks," in IEEE Internet of Things Journal, vol. 10, no. 3, pp. 2330-2345, 1 Feb.1, 2023, doi: 10.1109/JIOT.2022.3211346.

[9] P. Barnard, N. Marchetti and L. A. DaSilva, "Robust Network Intrusion Detection Through Explainable Artificial Intelligence (XAI)," in IEEE Networking Letters, vol. 4, no. 3, pp. 167-171, Sept. 2022, doi: 10.1109/LNET.2022.3186589.

[10] T. Zhukabayeva, A. Pervez, Y. Mardenov, M. Othman, N. Karabayev and Z. Ahmad, "A Traffic Analysis and Node Categorization- Aware Machine Learning-Integrated Framework for Cybersecurity Intrusion Detection and Prevention of WSNs in Smart Grids," in IEEE Access, vol. 12, pp. 91715-91733, 2024, doi: 10.1109/ACCESS.2024.3422077.

[11] Y. Kim, J. Kim and D. Kim, "Hi-MLIC: Hierarchical Multilayer Lightweight Intrusion Classification for Various Intrusion Scenarios," in IEEE Access, vol. 12, pp. 120098-120115, 2024, doi: 10.1109/ACCESS.2024.3450671.

[12] M. Seufert et al., "Marina: Realizing ML-Driven Real-Time Network Traffic Monitoring at Terabit Scale," in IEEE Transactions on Network and Service Management, vol. 21, no. 3, pp. 2773-2790, June 2024, doi: 10.1109/TNSM.2024.3382393.

[13] J. Buzzio-García et al., "Exploring Traffic Patterns through Network Programmability: Introducing SDNFLow, a Comprehensive OpenFlow- Based Statistics Dataset for Attack Detection," in IEEE Access, vol. 12, pp. 42163-42180, 2024, doi: 10.1109/ACCESS.2024.3378271.

Citation of this Article:

M Srilakshmi Preethi, Neeraj Kumar Uppu, & K Naveen Kumar. (2025). Unbalanced Traffic Intrusion Detection Using Advanced Deep Learning Techniques. In proceeding of International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25), published by *IRJIET*, Volume 9, Special Issue of INSPIRE'25, pp 377-382. Article DOI https://doi.org/10.47001/IRJIET/2025.INSPIRE61

****