Ceddi Journal of Information System and Technology (JST) *ISSN: 2829-808X (print)*
Vol. 4 No. 1 April (2025) *ISSN: 2829-6575 (online)*
https://doi.org/10.56134/jst.v4i1.114

A Review of Deep Belief Networks in Intrusion Detection Systems: Applications, Optimization Techniques, and Dataset Utilization

Sule Aishat A.[1*], Alhassan John K.[2], Ismaila Idris [3], Alabi Isiaq O.[4], Subairu Sikiru O.[5]

[1-5]*Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria*

Abstract

As reliance on the Internet and interconnected systems for essential services continues to grow, the need for strong cybersecurity defenses has become more pressing. Intrusion Detection Systems (IDS) are crucial in safeguarding these digital infrastructures. This paper investigates how Deep Belief Networks (DBNs) can enhance IDS capabilities, particularly in identifying advanced and dynamic threats such as Distributed Denial of Service (DDoS) attacks, SQL injections, and zero-day vulnerabilities. By reviewing recent research, we explore how DBNs have been applied in IDS contexts, examine optimization methods like layer-wise pre-training and dropout regularization that contribute to better detection performance, and evaluate commonly used benchmark datasets including UNSW-NB15, NSL-KDD, and CSE-CIC-IDS2018. This study compiles empirical evidence to assess DBNs' performance across varied network conditions and traffic types. Findings suggest that DBNs are effective in learning complex data patterns and improving the detection of anomalies. Nonetheless, challenges such as interpretability, high computational requirements, and the limitations of existing datasets continue to hinder widespread adoption. This work adds to the ongoing cybersecurity discourse by outlining major developments, constraints, and future directions for DBN-powered IDS. It ends by proposing strategic improvements, including the development of more efficient models, broader dataset coverage, and real-time, adaptive integration to support smarter and more responsive IDS solutions.

Keywords: Deep Belief Networks (DBN); Intrusion Detection Systems (IDS); Cybersecurity; Optimization Techniques; Benchmark Datasets.

Received: 2 January 2025 Revised: 19 March 2025 Accepted: 23 April 2025

Introduction

The increase in the sophistication and frequency of attacks has made it imperative for intrusion detection systems (IDS) to constantly improve their detection capability, as traditional IDS techniques, which usually rely on signature-based or heuristic-based detection algorithms, are inadequate for accurately detecting modern network traffic that is characterized by complexity and dynamism (Du et al., 2023). These traditional systems struggle to detect advanced persistent attacks, zero-day vulnerabilities, and other complicated incursions that defy recognized patterns or signatures (Maseer et al., 2024). These issues have increased interest in implementing deep learning (DL) approaches into IDS systems. Deep learning's increased utilization and remarkable performance in huge data processing can be used to handle large-scale, high-dimensional, and nonlinear data intrusion detection problems. Building a nonlinear network structure with several hidden layers can yield low-dimensional features that are easier to identify in the data, as well as boost intrusion detection accuracy (Asghar et al., 2019; Hwang et al., 2019; Khan et al., 2019; Yang et al., 2019; Yin et al., 2017).

According to research, Hinton et al.'s deep learning technique, known as the deep belief network, has sparked significant interest. The deep belief network may convert high-dimensional and nonlinear input characteristics into abstract features more suited for pattern categorization by extracting them layer by layer. DBNs are generative deep learning models that build hierarchical data representations using a layered design. They have sparked interest because of their ability to improve intrusion detection performance (Sajith & Nagarajan, 2022). Because of this structure, DBNs are better equipped to detect abnormalities and intrusions that conventional IDS techniques could miss by capturing intricate patterns and dependencies in network traffic (Ashiku & Dagli, 2021).

The effectiveness of Deep Belief Networks (DBNs) in Intrusion Detection Systems (IDS) is influenced by various factors, including the network environment, the type of network traffic, and the specific configuration of the DBN model. To optimize the performance of DBNs in IDS applications, researchers have adopted several strategies such as

*Corresponding author.
E-mail address: suleaishat990@gmail.com (Sule Aishat A.)

layer-wise pre-training, dropout regularization, and hyperparameter tuning. These techniques significantly contribute to enhancing the accuracy and efficiency of DBN models in practical, real-world scenarios. In addition, benchmark datasets play a crucial role in the evaluation of DBN-based IDS models, serving as standard references to assess and compare model performance objectively.

This study aims to provide a comprehensive review of recent research on the application of DBNs in IDS by addressing several key questions. First, it explores how DBNs are currently applied in IDS and evaluates their effectiveness across various network environments and attack scenarios. Second, it examines the optimization methods that have been used to improve DBN performance, analyzing their impact on detection accuracy and system reliability. Third, it investigates the benchmark datasets commonly used in DBN-based IDS research, highlighting their importance in model validation. Finally, it identifies major research gaps and discusses potential future directions that could advance the development of DBN-based intrusion detection systems. Through these discussions, this review seeks to offer a thorough understanding of DBN applications in IDS, uncover prevailing challenges and trends, and suggest valuable pathways for future research.

Method

This systematic review follows the PRISMA guidelines to ensure a comprehensive, transparent, and unbiased evaluation of the literature on Deep Belief Networks (DBNs) in Intrusion Detection Systems (IDS) (Page et al., 2021). The methodology involves systematically searching academic databases such as ACM Digital Library, IEEE Xplore, ScienceDirect, and SpringerLink using relevant keywords like "Deep Belief Networks," "Intrusion Detection Systems," "Optimization Techniques," and "Datasets," focusing on studies published between 2019 and 2024. The selection process adheres to defined inclusion and exclusion criteria, incorporating studies that explore DBN applications in IDS, optimization methods, and benchmark datasets while excluding those lacking empirical results or relevance. Data extraction captures key information on DBN applications, optimization techniques, dataset utilization, and performance metrics. The synthesis process thematically organizes findings to assess the effectiveness of DBNs in IDS, optimization strategies, and dataset challenges, highlighting trends, research gaps, and areas for future exploration. Through this structured approach, the review provides valuable insights into the advancements and challenges associated with DBNs in IDS.

Results and Discussion

Result

Research Question One: What are the current applications of DBNs in intrusion detection systems, and how effective are they in various network environments?

Deep Belief Networks (DBNs), a kind of deep learning model consisting of numerous layers, have received a lot of focus in the field of Intrusion Detection Systems (IDS) due to their capacity to learn hierarchical data structures. These models are very useful for IDS applications because they can detect complicated patterns in network traffic and distinguish between normal and malicious behavior. DBNs work by training multiple layers of Restricted Boltzmann Machines (RBMs), allowing them to learn from data representations at each level. This hierarchical learning mechanism gives DBNs the potential to simulate both known attack patterns and emergent threats in real-time network environments. The usage of DBNs in IDS is focused on anomaly identification and misuse detection, with the former detecting deviations from normal network behavior and the latter recognizing established attack patterns. DBNs have been deployed in a variety of network contexts, including enterprise networks, cloud infrastructures, Internet of Things (IoT) ecosystems, and wireless sensor networks.

Anomaly Detection in Enterprise Networks

DBNs are very useful for detecting anomalies in typical enterprise networks. These networks have predictable traffic patterns, and DBNs can be trained on previous traffic to detect anomalies that indicate probable intrusions. DBNs are effective at detecting enterprise-level assaults such as Distributed Denial of Service (DDoS), Denial of Service (DoS), and network probing. DBNs have been demonstrated in studies to achieve high detection rates and low false positives in these situations, especially when trained on balanced datasets that represent the range of attack types.

(Sathya et al., 2021) developed an anomaly-based intrusion detection approach known as DWU-ODBN, a deep belief network enhanced through a dual weight updating mechanism aimed at improving attack recognition capabilities. The evaluation of this model using the NSL-KDDCUP99 dataset demonstrated promising results, including a detection time of 77 seconds and an accuracy of 98.1%. The model also reported a false negative rate (FNR) of 8.39% and a false positive rate (FPR) of 11.04%. Performance tests across multiple benchmark datasets revealed that the system processed the KDD99 dataset in 77 seconds, NSL-KDDCUP99 in 78 seconds, CIDDS-001 in 71 seconds, and UNSW NB15 in 62 seconds. In a separate study (Wei et al., 2019) Introduced a hybrid DBN-based model that integrates fish swarm optimization, genetic algorithms, and particle swarm optimization to enhance IDS detection capabilities. Applied to the NSL-KDD dataset, the model showed a significant improvement in identifying rare attack types, particularly the R2L and U2R classes. Despite its effectiveness, the model's complex architecture was noted to increase training duration, presenting a trade-off between performance and computational efficiency.

(Malik et al., 2022) proposed a novel Intrusion Detection System (IDS) tailored for IoT environments, utilizing an enhanced Deep Belief Network (DBN) to effectively manage network traffic. In the data preprocessing stage, the TON-IoT dataset underwent several preparatory procedures, including sampling, data shuffling, label encoding, and normalization via min-max scaling. After dividing the dataset into training and testing subsets, the DBN model was applied to perform classification on the training data. To evaluate the system's effectiveness, the model's performance metrics were analyzed and compared against a range of conventional classifiers applied to the same dataset—such as Naive Bayes (NB), Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Classification and Regression Trees (CART), Random Forest (RF), and Linear Discriminant Analysis (LDA). Additionally, other deep learning models were benchmarked using different datasets, including DNN on Google Code Jam, LSTM+CNN on CICIDS, and DNN3 on the KDD dataset. The experimental results demonstrated that the proposed DBN-based system achieved superior performance, with an average accuracy reaching 86.3%, outperforming existing models.

Separately (Kim et al., 2020) s introduced an anomaly-based load balancing framework using reinforcement learning. Central to this approach is a specialized agent called DetectBot, which identifies anomalies and applies a reinforcement-based strategy to manage and distribute network loads efficiently. The model integrates a DBN to support intelligent decision-making during load balancing operations. DetectBot operates through four key stages: generating a structural representation of the network, monitoring traffic loads, forecasting future loads using neural-based predictions, and executing load distribution strategies.

In 2023 Rajarao and Sreenivasulu introduced two innovative methods for detecting anomalies in cloud computing environments by integrating Restricted Boltzmann Machines (RBM) with Logistic Regression (LR) and Support Vector Machines (SVM). These hybrid techniques utilize a two-stage process, an initial unsupervised learning phase for pre-training, followed by a supervised fine-tuning step. Performance was assessed using standard evaluation metrics, including accuracy, precision, recall, F1-score, and confusion matrix analysis. The experimental results demonstrated that the RBM-LR model achieved an impressive accuracy of 98.38%, while RBM-SVM reached 87.87%. These outcomes highlight the effectiveness of combining RBM with traditional classifiers in uncovering complex data patterns. The proposed methods offer valuable insights into future advancements in anomaly detection, system security, and real-time monitoring across diverse cloud-based applications.

Cloud and Virtualized Environments

The dynamic and distributed nature of cloud computing infrastructures presents distinct issues. DBNs have been used to monitor cloud infrastructures, detecting anomalous consumption patterns across virtual machines as well as threats, including resource abuse, hypervisor attacks, and data breaches. In cloud settings, DBNs use their deep learning skills to manage vast amounts of data and uncover patterns indicative of threats that may be difficult to detect using traditional methods. However, the scalability of DBNs in such dispersed systems is still an issue, with research concentrating on reducing training time and enhancing real-time detection.

A study carried out in 2020 by Velliangiri & Pandey investigated DDoS assaults in the field of cloud computing with optimization-based deep networks. The primary issues addressed are detecting attacks that are DDoS in cloud environments, enhancing cloud platform security against such attacks, and improving the detection technique's accuracy and efficiency. The solutions include developing a Taylor-Elephant Herd Optimization-based Deep Belief Network (TEHO-DBN) classifier for the detection of DDoS, utilizing deep learning for anomaly detection in clouds, and

employing an optimization-based technique to increase detection system performance. Simulating the TEHO-DBN classifier considers a number of evaluation parameters, including detection rate, accuracy, recall, computing time, and precision. However, when compared to existing methodologies, the proposed system outperformed the ones that existed.

(Dennis & Priya, 2021) carried out a study on identifying DDoS and economic denial of service (EDoS) assaults in a cloud computing environment using DBN and SVM technologies. It addressed issues such as effectively distinguishing between different types of EDoS and DDoS attacks, preventing attacks from traveling between Virtual Machines (VMs) and the hypervisor, and predicting attack percentages while determining sensitivity limits depending on system needs. Proposed solutions include developing a thorough strategy for identifying both EDoS and DDoS attacks, as well as implementing a global approach to increase threat detection. However, while detecting EDoS and DDoS attacks in cloud computing, some common performance indicators to consider are reporting time of the attack, request-response time, defensive cost/hour, victim service downtime, True Negative Rate (TNR), True Positive Rate (TPR), and accuracy. The findings produced from the fusion of DBN and SVM for identifying DDoS and EDoS assaults in the cloud show numerous important results. These include improved accuracy in detecting DDoS attack traffic, which leads to faster attack reporting and response times, as well as less downtime for victim services. Furthermore, the strategy reduces the costs involved with attack detection and mitigation. Notably, the categorization accuracy achieved is quite high, at 99.78%. Overall, these results highlighted how efficient the proposed method is in enhancing the security and resilience of cloud environments against DDoS and EDoS attacks.

(Samsu Aliar et al., 2024) developed a method to detect DDoS attacks in cloud systems using a hybrid Deep Belief Network and Gated Recurrent Unit (DBN-GRU) model, combined with optimal weighted features. This approach helps solve issues like slow system response and data privacy risks caused by DDoS attacks. The model was tested using performance metrics such as accuracy, precision, recall, F1-score, specificity, and error rates. Similarly (Agrawal et al., 2022) proposed a Modified Deep Belief Neural Network (M-DBNN) to detect and reduce DDoS attacks in digital environments. Their method aimed to protect users' data by detecting harmful behavior, improving feature preprocessing, and using the Chimp Optimization Algorithm to enhance classifier performance. The results showed that M-DBNN performed better than other existing models across several metrics, including accuracy, F1-score, and false positive rate.

IoT and Wireless Sensor Networks (WSNs)

DBNs have also found use in IoT ecosystems and wireless sensor networks (WSNs), which are particularly sensitive to security threats due to resource limits and limited processing capacity. DBNs, when tuned for low-power devices, have shown the ability to detect node capture, data injection, and routing attacks. In IoT applications, DBNs are used to analyze sensor traffic and detect anomalies that could indicate malicious behavior. One problem in these situations is striking a balance between the resource-intensive nature of DBNs and the energy efficiency and speed required for IoT installations. This research focuses on constructing lightweight DBN models that can identify intrusions without exhausting IoT devices' limited computational capabilities.

(Yang et al., 2019) introduced a fuzzy-based method to boost intrusion detection in IoT, cloud systems, and software-defined networks. They combined the Modified Density Peak Clustering Algorithm (MDPCA) with a Deep Belief Network (DBN) to handle large and complex datasets. MDPCA groups similar traffic features, making training easier, while DBN automatically learns and classifies hidden patterns. Tests on NSL-KDD and UNSW-NB15 datasets showed strong results in detection accuracy and low error rates. Compared to other models, MDPCA-DBN showed better overall performance, especially in multi-class classification, proving useful for modern network environments.

(Thamilarasu & Chawla, 2019) identified a security weakness in IoT networks due to their large attack surface, making them vulnerable to cyberattacks. To address this, they developed a secure and flexible Intrusion Detection System (IDS) for IoT environments. Their system uses a Deep Neural Network (DNN) built on a Deep Belief Network (DBN), which benefits from unsupervised learning, making it more efficient than supervised methods. The IDS detects unusual IoT traffic by combining network virtualization with a DNN binary classifier. Testing in both simulated and real-world environments showed that the model outperformed other methods, although it was less effective at detecting wormhole attacks in real tests. This IDS is one of the few tested with real IoT traffic, and it performed well, though the exact dataset used in simulations was not provided.

In (Zhang et al., 2019) introduced an Intrusion Detection System (IDS) for IoT environments based on a Deep Belief Network (DBN) that was tuned by a genetic algorithm (GA) to identify the optimal number of hidden layers and units in each layer. The DBN architecture incorporates an initial training phase with Restricted Boltzmann Machines (RBMs), followed by fine-tuning by back-propagation, as in previous models. This technique is unique in that it uses an 18-bit chromosome to record the number of units over up to three hidden levels, with each pair of six bits indicating one layer. Units in each layer are limited to be less than the input layer's features but greater than the output layer's units. The GA's fitness function strikes a compromise between detection rate, hidden layer count, and complexity standard deviation to improve detection while reducing complexity. Using the normalized NSL-KDD dataset, the study found 50 GA generations and optimal training epochs of 80 and 10 for back-propagation and RBM, respectively. The DBN's input and output layers were set at 41 and 2 units, respectively. For certain attack types, DoS, R2L, Probe, and U2R—the best structures were discovered to be 41-18-12-2, 41-31-2, 41-26-2, and 41-38-2, respectively. Each of these settings produced a detection rate of 99.45%, illustrating the GA-optimized IDS's efficiency against a variety of assaults.

(Dai et al., 2020) implemented a Deep Belief Network (DBN) to extract intricate features from spectral image data. Their method initiates by transforming raw inputs into a more representative feature space using unsupervised learning, specifically through Restricted Boltzmann Machines (RBMs). These RBMs are stacked hierarchically and trained one layer at a time using a greedy learning strategy. The study highlights how DBNs not only reduce dimensionality but also capture deep pixel-level information. When compared to conventional shallow feature extraction techniques, such as Principal Component Analysis (PCA), Minimum Noise Fraction (MNF), Factor Analysis (FA), and Independent Component Analysis (ICA), the DBN demonstrated superior classification performance.

(Otoum et al., 2019) proposed an Intrusion Detection System (IDS) for wireless sensor networks (WSNs) utilizing a DBN architecture. This model includes three hidden layers trained in a manner consistent with earlier DBN-based IDS approaches, although the exact size of each layer was not disclosed. To simulate WSN behavior, twenty sensors were configured to communicate through the Dynamic Source Routing (DSR) protocol within a hierarchical framework (H-DSR). Evaluated using the KDD Cup 1999 dataset, the IDS achieved a remarkable accuracy rate of 99.91% and a detection rate of 99.12%. In another study, (Coli et al., 2022) developed a deep learning framework tailored to identifying Distributed Denial of Service (DDoS) attacks in Internet of Things (IoT) environments. Their solution is based on a Deep Gaussian-Bernoulli Restricted Boltzmann Machine (DBM), which is capable of extracting advanced features without supervision and handling real-time input data, common in IoT contexts. The final classification layer employs Softmax regression. Tested on the NSL-KDD dataset, the model achieved an accuracy of 93.52%, demonstrating its effectiveness in identifying DDoS threats in IoT systems.

Applications in Mobile and Ad-Hoc Networks

Mobile and Ad-Hoc Networks (MANETs), known for their decentralized nature and unpredictable topology, are increasingly dependent on DBNs to identify network layer assaults. In these networks, DBNs are used to monitor real-time mobile device traffic and detect assaults such as packet dropping, selective forwarding, and Sybil attacks. DBNs are well-suited for MANETs due to their capacity to continuously learn and adapt to changing network conditions; yet, the high mobility and changeable configurations of these networks pose problems to DBN model stability. (Hanafi et al., 2023) proposed a novel method for detecting attacks in Mobile Ad Hoc Networks (MANETs) that combines Deep Belief Networks (DBN) and Long Short-Term Memory (LSTM) models. The study investigated many sorts of attacks, including probing, root-to-local, user-to-root, and denial of service (DoS). The results showed that the DBN had an accuracy of 99.46%, as well as a sensitivity and recall of 99.52%. In comparison, the LSTM model performed even better, with an accuracy of 99.75%, as well as sensitivity and recall rates of 99.79%.

(Dilipkumar & Durairaj, 2023) proposed the Centrality Epsilon Greedy Swarm and Gradient Deep Belief Classifier (CEGS-GDBC) as an Intrusion Detection System (IDS) approach for detecting multiple attacks in Mobile Ad Hoc Networks. This method uses a cluster head node election model, cluster construction, and a hybrid IDS. The system's performance was examined against a variety of multi-attack scenarios, including Denial of Service (DoS) and Zero-Day attacks, with an emphasis on metrics like as memory consumption, computation time, attack detection rate, and the Receiver Operating Characteristic (ROC) curve. The results showed that the CEGS-GDBC technique improves attack detection by 31% over earlier research. Furthermore, it incorporates a Gradient Deep Belief Network Classifier, which results in 39% less memory usage and 41% less calculation time than previous techniques.

(Vitalkar et al., 2023) proposed a DBN-based model for intrusion detection in Vehicular Ad Hoc Networks (VANETs). The authors argued that the Deep Belief Network (DBN) algorithm outperforms traditional network intrusion detection methods, including conventional machine learning and other deep learning algorithms. The model was trained, tested, and evaluated using the CICIDS2017 dataset, with experimental results demonstrating strong performance in both multi-class and binary classification tasks, achieving accuracies of 90% and 98%, respectively. In a related study, the authors also introduced an optimized deep learning-based model for cyber intrusion detection and secure communication in Mobile Ad Hoc Networks (MANETs). This model showed superior performance compared to previous approaches, achieving 94% accuracy, 93% precision, 93.45% recall, and an F1-score of 93.65%.

Research Question Two: What optimization strategies have been used to boost the performance of Deep Belief Networks in Intrusion Detection Systems?

Optimizing Deep Belief Networks (DBNs) for Intrusion Detection Systems (IDS) entails combining several strategies to improve detection accuracy, reduce false alarms, and shorten training time. The summary of the optimization techniques is presented in Table 1. (Wei et al., 2019) improved the structure of the Intrusion Detection System (IDS) for Deep Belief Networks (DBN) by experimenting with a hybrid optimization technique that combines the Particle Swarm Optimization (PSO) algorithm, the Artificial Fish Swarm Algorithm (AFSA), and the Genetic Algorithm. In this method, the PSO algorithm calculates the ideal number of hidden layers and units within each layer. The AFSA contributes to this process by recognizing initial particles, which improves the overall performance of the PSO-based DBN optimization.

In addition, the PSO technique, which was first enhanced with AFSA, now adds GA to accomplish global optimization. The combined AFSA-GA-PSO method's fitness criteria include the error rate, the number of DBN hidden layers, the maximum number of hidden layers, the number of units in the hidden layer, the total number of nodes in the hidden layers, the False Positive Rate (FPR), the False Negative Rate (FNR), and the Detection Rate. The performance of the proposed IDS model was evaluated with the KDDTest+ and KDDTest-21 datasets, with KDDTrain+ acting as the training dataset. The AFSA-GA-PSO optimization resulted in the model having four hidden layers with unit configurations of [75, 33, 18, 12] for each. Experimental results show that the proposed approach, AFSA-GA-PSO-DBN, achieved accuracy of 83.55%, 87.20%, 84.00%, and 80.40% for Probe, DoS, U2R, and R2L assaults, respectively. Similarly, the model reported an FPR of 0.77%, 5.64%, 0.17%, and 3.02% for Probe, DoS, U2R, and R2L assaults, respectively. In addition, the model attained an overall accuracy of 82.36% for KDDTest+ and 66.25% for KDDTest-20. The average training and detection times for KDDTest+ were 13358.32s and 1813.96s, respectively, whereas for KDDTest-20, they were 8201.29s and 1076.93s.

(Zhang et al., 2019) used a genetic algorithm (GA) to optimise the setup of hidden layers and units within each layer of the Deep Belief Network. Their suggested Intrusion Detection System (IDS) model, DBN-GA, was tested on the normalized NSL-KDD dataset. The study determined the appropriate parameters, setting the training epochs for back-propagation and Restricted Boltzmann Machines (RBM) to 80 and 10, respectively, and identifying the ideal number of GA generations to 50. The GA determined the most successful network configurations for certain attack types, yielding configurations of 41-18-12-2 for DoS, 41-31-2 for R2L, 41-26-2 for Probe, and 41-38-2 for U2R. The suggested IDS proved adaptable to multiple assaults, with detection rates of 99.45% for DoS, 97.78% for R2L, 99.37% for Probe, and 98.68% for U2R. Furthermore, the model achieved detection rates of 99.7%, 99.4%, 93.4%, and 98.2% for these attack types, with False Alarm Rates (FARs) of 0.8% for DoS, 0.7% for R2L, 7.3% for Probe, and 1.8% for U2R. Overall, these statistics show an average accuracy of 98.82% with a false alarm rate of 4.0%. Although it was indicated that the training time was lowered, no percentage was given, nor was the training duration of their model specified.

(Zhang et al., 2019) suggested a unique approach to detecting network threats that combines flow computation and deep learning approaches. The approach is made up of two main components: a real-time detection algorithm that uses flow calculations and frequent pattern analysis, and a classification algorithm that combines Deep Belief Networks and Support Vector Machines. The efficiency of the suggested Intrusion Detection System (IDS) model was evaluated using the CICIDS2017 dataset, which had a DBN structure configured as [41 30 20 10 5]. The experiments yielded precision and recall rates of 97.74% and 97.67%, respectively. Although the authors said that the model's training period was brief, they did not specify a particular timeframe.

(Wang et al., 2021) proposed a model that improves upon the classic deep belief network (DBN) technique. Unlike traditional methods, such as Back Propagation (BP), which can suffer from drawbacks such as local optima and long training periods due to set parameters, this model replaces BP with supervised learning within the DBN architecture. To improve classification performance, which can be hampered by KELM's random initialization of kernel parameters, the authors developed an improved grey wolf optimizer (EGWO) for parameter optimization. The suggested model, DBN-EGWO-KELM, was evaluated on a variety of datasets, including KDDCup99, UNSW-NB15, CICIDS2017, and NSL-KDD. The model outperforms existing intrusion detection models with an accuracy of 98.6% and detection time of 134s for the KDDCUP'99 dataset; 98.6% accuracy rate and 41s detection time for the NSL-KDD dataset; 93.42% accuracy and 214s detection time for the UNSW-NB15 dataset; 97.15% accuracy and 120s detection time for the CICIDS2017 dataset.

In another study on network intrusion detection systems (IDS), researchers proposed the use of Evaluated Bird Swarm Optimization (EBSO) in combination with a Deep Belief Network (DBN) to develop a lightweight IDS model, referred to as EBSO-DBN. The model's performance was critically evaluated using various metrics, including accuracy, precision, recall, F1-score, false alarm rate, and detection rate. The NSL-KDD benchmark dataset was employed to test and validate the effectiveness of the proposed model. (Elmasry et al., 2020) presented a unique Intrusion Detection System (IDS) model based on Deep Belief Networks (DBN) that includes a pre-training phase and a Particle Swarm Optimization (PSO) technique for hyperparameter tuning. Additionally, PSO was used for feature selection and dimensionality reduction. This dual PSO-based algorithm works on two levels: feature selection at the top and hyperparameter optimization at the bottom.

The performance of the IDS model was assessed using the NSL-KDD and CICIDS2017 datasets. The experimental results showed that the suggested IDS achieved binary classification accuracy and false alarm rates of 99.79% and 0.23%, respectively, on the NSL-KDD dataset, with training and testing times of 1552 seconds and 278 seconds. For the CICIDS2017 dataset, the model achieved an accuracy of 99.91% and a false alarm rate of 0.1%, with training and testing periods of 1617 and 915 seconds, respectively. Another notable study was undertaken by (Assiri & Ragab, 2023), who suggested the Honey Badger Algorithm with an Optimal Hybrid Deep Belief Network (HBA-OHDBN) technique for cyberattack detection. This method employs the Dung Beetle Optimization algorithm for hyperparameter adjustment. The HBA-OHDBN algorithm's performance was validated using the benchmark NSL-KDD dataset, which yielded 99.21% accuracy and a computational time of 0.95 seconds.

Table 1. Summary of DBN optimization techniques

S/N	Author	Year	Optimization Technique	Datasets Used	Performance Metrics	Key Findings
1	Wei et al	2019	Hybrid: Artificial Fish Swarm Algorithm (AFSA), Particle Swarm Optimization (PSO), Genetic Algorithm (GA)	KDDTest+, KDDTest-21, KDDTrain+	Accuracy: 82.36% (KDDTest+), 66.25% (KDDTest-20); FPR: 0.77%, 5.64%, 0.17%, 3.02% (Probe, DoS, U2R, R2L attacks)	AFSA-GA-PSO optimized DBN configuration with 4 hidden layers (units: [75 33 18 12]); improves accuracy and reduces FPR
2	Zhang et al	2019	Genetic Algorithm (GA)	NSL-KDD	Accuracy: 98.82%, FAR: 4.0%, DR: 99.45% (DoS), 97.78% (R2L), 99.37% (Probe), 98.68% (U2R)	GA optimized DBN configurations for attack types; improved detection rates across attacks with low false alarms
3	Zhang et al	2020	Support Vector Machine (SVM)	CICIDS2017	Precision: 97.74%, Recall: 97.67%	The DBN-SVM approach integrates flow calculation, achieving high precision and recall for real-time detection
4	Wang et al	2021	Enhanced Grey Wolf Optimizer (EGWO) Kernel-based Extreme Learning Machine (KELM)	KDDCup99, UNSW-NB15, CICIDS2017, NSL-KDD	Accuracy: 98.6% (KDDCup99, NSL-KDD), 93.42% (UNSW-NB15), 97.15% (CICIDS2017); Detection time: 134s (KDDCup99), 41s (NSL-KDD)	EGWO optimized kernel parameters for KELM, leading to improved accuracy and faster detection times

S/N	Author	Year	Optimization Technique	Datasets Used	Performance Metrics	Key Findings
5	Elmasry et al	2021	Dual PSO-based algorithm	NSL-KDD, CICIDS2017	Accuracy: 99.79% (NSL-KDD), 99.91% (CICIDS2017); False Alarm Rate: 0.23% (NSL-KDD), 0.1% (CICIDS2017); Training time: 1552s, 1617s,	PSO optimized both feature selection and hyperparameters, leading to superior accuracy and reduced false alarm rates.
6	Assiri & Ragab	2023	Dung Beetle Optimization (DBO) algorithm	NSL-KDD	Accuracy: 99.21%; Computational time: 0.95s	HBA-OHDBN combined with DBO for hyperparameter tuning showed excellent accuracy with minimal computational time for cyberattack detection.
7	Biju & Wilfred	2024	Evaluated Bird Swarm Optimization (EBSO)	NSL-KDD	Accuracy, Precision, Recall, F1-score, FAR, Detection Rate	EBSO-DBN is designed for lightweight IDS, evaluated on multiple performance metrics

In the realm of DBN-based Intrusion Detection Systems (IDS) research, several benchmark datasets have been widely adopted by researchers to assess the effectiveness of their proposed models. One of the most frequently used datasets is the KDD Cup 1999, which includes around 5 million training records and 2 million testing records, each containing 41 distinct features. These features are categorized into either "normal" or "attack" types, with attacks further divided into Denial of Service (DoS), Probe, Remote to Local (R2L), and User to Root (U2R). Another important dataset is the Kyoto 2006+, developed by Kyoto University, which spans network traffic from 2006 to 2015. It includes 24 features, of which 14 are from the KDD Cup 1999 dataset and 10 are original. The NSL-KDD dataset, a modified version of KDD Cup 1999, addresses several key issues from the original and contains 125,973 training samples and 22,544 testing samples, categorizing attacks into four types: DoS, R2L, U2R, and Probing.

The UNSW-NB15 dataset, created by the Australian Centre for Cyber Security, consists of about two million records with 49 attributes. It includes various attack types, such as worms, shellcode, reconnaissance, and DoS, and was collected using methods like Bro-IDS and Argus. The CIC-IDS2017 dataset, developed by the Canadian Institute of Cyber Security, provides network traffic data including both traditional flows and modern attack scenarios. This dataset incorporates various attacks such as brute force, Heartbleed, botnet, DoS, DDoS, and web attacks. Finally, the CSE-CIC-IDS2018 dataset offers a comprehensive view of current network traffic along with a variety of cyberattacks, including DoS and DDoS. This dataset has been especially useful for testing and designing IDS models in realistic network conditions. Each of these datasets plays a crucial role in developing and evaluating intrusion detection systems, providing valuable data for researchers to improve security measures in diverse network environments (Bay et al., 2000), (Song et al., 2011)**,** (Moustafa & Slay, 2015), (Sharafaldin et al., 2018), (Lashkari et al., 2017), (Abdulhammed et al., 2019), (Sharafaldin et al., 2018).

Research Question Four: **What are the primary research gaps in the application of DBNs in IDS, and what future directions could address these gaps?**

This subsection highlights the research gaps in the application of DBNs in IDS and what future directions could address these gaps.

i. **Lightweight IDS for IoT:** An Intrusion Detection System (IDS) is required to secure IoT networks and sensor nodes, which record and distribute massive volumes of crucial data via the internet. Given the limited computing power, storage capacity, and battery life of these sensor nodes, IDS can be deployed in two ways: at network entry points as a Network Intrusion Detection System (NIDS) to efficiently detect malicious activity, or throughout the sensor nodes themselves. The latter necessitates a lightweight IDS model that can function successfully under resource constraints. Developing a lightweight IDS that optimizes computational resources and training time while maintaining a high intrusion detection rate is a significant issue in this environment.

ii. **Low performance in real-world environment:** Another significant research challenge for Intrusion Detection Systems (IDS) is its performance in real-world environments. Most existing techniques have been evaluated and confirmed in laboratory settings using publicly available datasets, leaving their effectiveness in real-world scenarios largely unknown. As a result, it is unclear how these technologies will work outside of controlled situations. Furthermore, many of these approaches continue to rely on out-of-date datasets for testing, which may not adequately reflect current network threats and conditions, limiting their use in real applications.

iii. **Unavailability of a systematic dataset:** Recent research has revealed a huge gap in the availability of current datasets that appropriately reflect the latest attacks on modern networks. Many proposed Intrusion Detection System (IDS) systems fail to identify zero-day attacks due to insufficient training on different attack types and patterns. To create a successful IDS model, it is necessary to test and validate against a dataset that includes both historical and modern threats. A rich dataset with a wide range of attack definitions allows machine learning and deep learning models to discover more patterns, ultimately improving their ability to fight against various types of incursions. However, creating such datasets is resource-intensive and necessitates specialized skills, posing a significant hurdle for IDS development. As a result, there is an urgent need for a systematic strategy to developing and maintaining an up-to-date dataset with numerous samples of practically all attack types. Regular updates are required to capture the most recent intrusions, and making these datasets available will substantially help the research community.

iv. **Resources consumed by complex models:** Many Intrusion Detection System (IDS) approaches offered by researchers rely on complicated models that need significant processing power and computational resources, potentially resulting in additional overhead that can impair IDS performance. While using high-performance multi-core graphics processing units (GPUs) can speed up computations and minimize processing times, the cost is typically prohibitive. To reduce computational and processing overhead, an effective feature selection technique is required for intelligently recognizing the most important features and allowing faster processing. Although researchers are currently investigating various optimization strategies for feature selection, there is still tremendous room for improvement, necessitating additional research into developing more effective feature selection optimization algorithms.

Discussion

Deep Belief Networks (DBNs) have emerged as a promising deep learning technique for Intrusion Detection Systems (IDS) due to their ability to extract hierarchical and complex patterns from network traffic data. Unlike traditional IDS models that rely on signature-based or rule-based detection, DBNs leverage unsupervised pretraining and supervised fine-tuning to learn intricate attack patterns, making them highly effective in anomaly detection. However, despite their advantages, several challenges remain in their practical deployment for network security. One of the primary limitations of DBN-based IDS models is their high computational complexity as a DBN requires multiple layers of Restricted Boltzmann Machines (RBMs), which increases processing time and demands significant computational resources. This makes real-time intrusion detection challenging, particularly in environments where rapid response is critical. While high-performance GPUs can accelerate training and inference, their cost and energy consumption pose additional concerns, however, Cloud-based training solutions could mitigate some of these challenges by offering scalable computing power at a lower cost.

Another critical issue is the dependence of DBN models on high-quality datasets. Many existing IDS datasets suffer from class imbalances, outdated attack patterns, or insufficient diversity, limiting the generalization capability of DBN-based IDS. To improve detection accuracy and reduce false positives, IDS models must be trained on updated and well-balanced datasets. Furthermore, since cyber threats continuously evolve, DBNs should incorporate mechanisms for dynamic learning, allowing them to adapt to new attack vectors by regularly updating training data and retraining the model. Additionally, DBNs require careful feature selection to optimize performance. High-dimensional input data increases computational overhead and may introduce redundant or irrelevant features, negatively impacting detection efficiency. By selecting the most relevant features, it is possible to enhance detection accuracy while reducing processing costs. Hybrid approaches that combine DBNs with feature selection techniques, such as principal component analysis (PCA) or autoencoders, could improve model efficiency without sacrificing performance

Despite these challenges, DBN-based IDS models remain a promising solution for modern network security. Their ability to automatically learn deep representations of attack patterns offers a significant advantage over traditional IDS approaches. However, for widespread adoption, further research is needed to optimize model efficiency, reduce computational costs, and enhance adaptability to evolving cyber threats. By addressing these challenges, DBN-based IDS can become a more viable solution for real-time network intrusion detection.

Conclusions and Suggestions

Conclusions

Intrusion Detection Systems (IDS) are a critical defense mechanism against network intrusions. However, current IDS models face challenges such as high false alarm rates and difficulties in detecting zero-day attacks. Despite extensive research, there is still no comprehensive Network Intrusion Detection System (NIDS) capable of effectively protecting modern network environments, including the Internet of Things (IoT). Deep learning-based IDS models have demonstrated strong potential for improving detection accuracy, but their complexity and high computational requirements hinder real-time implementation. To enhance IDS performance, continuous updates to attack definitions and regular model retraining are necessary to keep pace with evolving cyber threats.

Suggestions

To address the limitations of IDS, future research should focus on developing an adaptive NIDS framework that integrates mechanisms for continuous learning and automatic updates. This approach will improve the system's ability to detect emerging threats while reducing false alarms. Additionally, leveraging high-speed GPUs can accelerate model training and inference, but their cost remains a concern. Exploring cloud-based GPU solutions can help mitigate this issue by providing scalable and cost-effective computational resources.

Furthermore, optimizing deep learning-based IDS models through efficient feature selection can reduce complexity while maintaining high detection accuracy. By selecting only the most relevant features, IDS models can achieve faster processing with lower computational overhead, making real-time implementation more feasible. Regular dataset updates and retraining should also be prioritized to ensure that AI-based IDS systems remain effective against evolving cyber threats. Finally, future research should explore lightweight deep learning techniques that balance performance and cost, enabling more efficient real-time intrusion detection.

Contribution: Sule: Content development, Formal analysis, investigation, methodology, writing original draft, review & editing. Alhassan: Conceptualization, quality assessment, review & editing, supervision. Ismaila: Quality assessment, review & editing, supervision. Alabi: Resources, quality assessment, supervision, review & editing. Subairu: Resources, quality assessment, supervision, review & editing.

References

Abdulhammed, R., Faezipour, M., Musa, S., Anuar, N. B., & Mostafa, S. A. (2019). A survey on deep learning techniques for network intrusion detection systems. *Electronics*, *8*(10), 1213. https://doi.org/10.3390/electronics8101213

Agrawal, A., Singh, R., Khari, M., Shanmuganathan, V., & Lim, S. (2022). Autoencoder for Design of Mitigation Model for DDOS Attacks via M-DBNN. *Wireless Communications and Mobile Computing*, *2022*, 1–14. https://doi.org/10.1155/2022/9855022

Asghar, M. Z., Abbas, M., Zeeshan, K., Kotilainen, P., & Hämäläinen, T. (2019). Assessment of deep learning methodology for self-organizing 5G networks. *Applied Sciences (Switzerland)*, *9*(15). https://doi.org/10.3390/app9152975

Ashiku, L., & Dagli, C. (2021). Network Intrusion Detection System using Deep Learning. *Procedia Computer Science*, *185*, 239–247. https://doi.org/10.1016/j.procs.2021.05.025

Assiri, F. Y., & Ragab, M. (2023). Optimal Deep-Learning-Based Cyberattack Detection in a Blockchain-Assisted IoT Environment. *Mathematics*, *11*(19). https://doi.org/10.3390/math11194080

Bay, S. D., Kibler, D., Pazzani, M. J., & Smyth, P. (2000). *The UCI KDD Archive of Large Data Sets for Data Mining Research and Experimentation**.

Coli, G. O., Aina, S., Okegbile, S. D., Lawal, A. R., & Oluwaranti, A. I. (2022). DDoS Attacks Detection in the IoT Using Deep Gaussian-Bernoulli Restricted Boltzmann Machine. *Modern Applied Science*, *16*(2), 12. https://doi.org/10.5539/mas.v16n2p12

Dai, X., Cheng, J., Gao, Y., Guo, S., Yang, X., Xu, X., & Cen, Y. (2020). Deep Belief Network for Feature Extraction of Urban Artificial Targets. *Mathematical Problems in Engineering*. https://doi.org/10.1155/2020/2387823

Dennis, J. B., & Priya, M. S. (2021). Deep belief network and support vector machine fusion for distributed denial of service and economical denial of service attack detection in cloud. *Concurrency and Computation: Practice and Experience*, *33*(1), e6543. https://doi.org/10.1002/cpe.6543

Dilipkumar, S., & Durairaj, M. (2023). Epilson Swarm Optimized Cluster Gradient and deep belief classifier for multi-attack intrusion detection in MANET. *Journal of Ambient Intelligence and Humanized Computing*, *14*(3). https://doi.org/10.1007/s12652-021-03169-x

Du, J., Yang, K., Hu, Y., & Jiang, L. (2023). NIDS-CNNLSTM: Network Intrusion Detection Classification Model Based on Deep Learning. *IEEE Access*, *11*, 24808–24821. https://doi.org/10.1109/ACCESS.2023.3254915

Elmasry, W., Akbulut, A., & Zaim, A. H. (2020). Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic. *Computer Networks*, *168*. https://doi.org/10.1016/j.comnet.2019.107042

Hanafi, A. S., Saheed, Y. K., & Arowolo, M. O. (2023). An Effective Intrusion Detection in Mobile Ad-hoc Network Using Deep Belief Networks and Long Short-Term Memory. *International Journal of Interactive Mobile Technologies*, *17*(19). https://doi.org/10.3991/ijim.v17i19.27663

Hwang, R. H., Peng, M. C., Nguyen, V. L., & Chang, Y. L. (2019). An LSTM-based deep learning approach for classifying malicious traffic at the packet level. *Applied Sciences (Switzerland)*, *9*(16). https://doi.org/10.3390/app9163414

Khan, M. A., Karim, M. R., & Kim, Y. (2019). A scalable and hybrid intrusion detection system based on the convolutional-LSTM network. *Symmetry*, *11*(4). https://doi.org/10.3390/sym11040583

Kim, J., Shim, M., Hong, S., Shin, Y., & Choi, E. (2020). Intelligent detection of iot botnets using machine learning and deep learning. *Applied Sciences (Switzerland)*, *10*(19). https://doi.org/10.3390/app10197009

Lashkari, A. H., Draper Gil, G., Mamun, M. A., & Ghorbani, A. A. (2017). Characterization of Tor Traffic Using Time Based Features. *Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP)*, 253–262. https://doi.org/10.5220/0006105602530262

Malik, R., Singh, Y., Sheikh, Z. A., Anand, P., Singh, P. K., & Workneh, T. C. (2022). An Improved Deep Belief Network IDS on IoT-Based Network for Traffic Systems. *Journal of Advanced Transportation*, *2022*. https://doi.org/10.1155/2022/7892130

Maseer, Z. K., Yusof, R., Al-Bander, B., Saif, A., & Kadhim, Q. K. (2024). *Meta-Analysis and Systematic Review for Anomaly Network Intrusion Detection Systems: Detection Methods, Dataset, Validation Methodology, and Challenges*.

Moustafa, N., & Slay, J. (2015). UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 Network Data Set). *2015 Military Communications and Information Systems Conference (MilCIS)*, 1–6. https://doi.org/10.1109/MILCIS.2015.7348942

Otoum, S., Kantarci, B., & Mouftah, H. T. (2019). On the Feasibility of Deep Learning in Sensor Network Intrusion Detection. *IEEE Networking Letters*, *1*(2), 68–71. https://doi.org/10.1109/lnet.2019.2901792

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., & Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *Systematic Reviews*, *10*(1). https://doi.org/10.1186/s13643-021-01626-4

Rajarao, B., & Sreenivasulu, M. (2023). A Hybridized- Logistic Regression and Deep Learning-based Approaches for Precise Anomaly Detection in Cloud. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*, 378–385. https://doi.org/10.17762/ijritcc.v11i9s.7433

Sajith, P. J., & Nagarajan, G. (2022). Intrusion Detection System Using Deep Belief Network & Particle Swarm Optimization. *Wireless Personal Communications*, *125*(2). https://doi.org/10.1007/s11277-022-09609-x

Samsu Aliar, A. A., Agoramoorthy, M., & Y, J. (2024). An Automated Detection of DDoS Attack in Cloud Using Optimized Weighted Fused Features and Hybrid DBN-GRU Architecture. *Cybernetics and Systems*, *55*(7). https://doi.org/10.1080/01969722.2022.2157603

Sathya, M., Jeyaselvi, M., Krishnasamy, L., Hazzazi, M. M., Shukla, P. K., Shukla, P. K., & Nuagah, S. J. (2021). A Novel, Efficient, and Secure Anomaly Detection Technique Using DWU-ODBN for IoT-Enabled Multimedia Communication Systems. *Wireless Communications and Mobile Computing*, *2021*. https://doi.org/10.1155/2021/4989410

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP)*, 108–116. https://doi.org/10.5220/0006639801080116

Song, J., Takakura, H., Okabe, Y., Eto, M., Inoue, D., & Nakao, K. (2011). *Statistical Analysis of Honeypot Data and Building of Kyoto 2006+ Dataset for NIDS Evaluation*.

Thamilarasu, G., & Chawla, S. (2019). Towards deep-learning-driven intrusion detection for the internet of things. *Sensors (Switzerland)*, *19*(9). https://doi.org/10.3390/s19091977

Velliangiri, S., & Pandey, H. M. (2020). Fuzzy-Taylor-elephant herd optimization inspired Deep Belief Network for DDoS attack detection and comparison with state-of-the-arts algorithms. *Future Generation Computer Systems*, *110*, 80–90. https://doi.org/10.1016/j.future.2020.03.049

Vitalkar, R., Thorat, S., Rojatkar, D., Vitalkar, R. S., & Rojatkar, D. V. (2023). *Intrusion Detection for Vehicular Ad-Hoc Network Based on Deep Learning*.

Wang, Z., Zeng, Y., Liu, Y., & Li, D. (2021). Deep Belief Network Integrating Improved Kernel-Based Extreme Learning Machine for Network Intrusion Detection. *IEEE Access*, *9*. https://doi.org/10.1109/ACCESS.2021.3051074

Wei, P., Li, Y., Zhang, Z., Hu, T., Li, Z., & Liu, D. (2019). An optimization method for intrusion detection classification model based on deep belief network. *IEEE Access*, *7*. https://doi.org/10.1109/ACCESS.2019.2925828

Yang, Y., Zheng, K., Wu, C., & Yang, Y. (2019). Improving the classification effectiveness of intrusion detection by using improved conditional variational autoencoder and deep neural network. *Sensors (Switzerland)*, *19*(11). https://doi.org/10.3390/s19112528

Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. *IEEE Access*, *5*, 21954–21961. https://doi.org/10.1109/ACCESS.2017.2762418

Zhang, Y., Li, P., & Wang, X. (2019). Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network. *IEEE Access*, *7*, 31711–31722. https://doi.org/10.1109/ACCESS.2019.2903723