Bima Journal of Science and Technology, Vol. 8(3) Sept, 2024 ISSN: 2536-6041

DOI: 10.56892/bima.v8i3.772

Review on the Network Intrusion Detection Systems (NIDS)

Farida Suleiman, Umar Iliyasu and Mukhtar Abubakar*

Department of Computer Science, Faculty of Computing Federal University Dutsinma

Katsima State, Nigeria.

Corresponding Author: mabubakar2@fudutsinma.edu.ng

ABSTRACT

In today's world, the rapid advancement of Information Technology has resulted in a large number of people accessing the internet globally. The COVID-19 pandemic has further sped up this trend, leading organizations and individuals to move towards online platforms for their daily activities and businesses. Consequently, these online activities have led to various cyber threats for users and networks. The paper analyzed the recent evaluation of Network Intrusion Detection System (NIDS) techniques, such as machine learning models like decision trees, support vector machines, logistic regression, and others, that have been effective in spotting cyber threats, but their effectiveness decreases when dealing with extensive and high-dimensional data. Deep learning models have demonstrated impressive performance in handling extensive and complex datasets. Moreover, ensembles and hybrid models have displayed potential for improved performance compared to stand-alone ML and DL techniques. The paper also included an analysis of commonly utilized datasets for NIDS, such as NSL-KDD, KDD CUP-99, and CICIDS 2017. These datasets are highly important for researchers, organizations, and institutions for further evaluation of NIDS models. Future research efforts could concentrate on addressing existing limitations within NIDS, utilizing advancements in ML, DL, and ensemble techniques to enhance detection capabilities and strengthen network defenses against evolving cyber threats.

Keywords: Intrusion, detection, NIDS, datasets, cyber, threats

INTRODUCTION

Rapid expansion of information and communication technology has led to an increase in global internet access and network-based services. The COVID-19 pandemic has compelled almost all organizations and individuals to turn to online platforms for their operations. The growing reliance on internet-based activities has heightened the susceptibility of users and networks to potential attacks, prompting numerous researchers to focus on creating models to detect and mitigate these threats (Kumar et al., 2021).

Network Intrusion Detection Systems (NIDS) are security systems designed to continuously monitor, detect, and mitigate unauthorized user intrusions (Cao et al., 2022). This is done by collecting data from several computer nodes and analyzing it to determine the network's threat level. Several strategies have been developed to detect intrusions. This includes rule-based systems, whose performance is heavily dependent on security professionals' rules. Because of the massive volume of network traffic, encoding rules is both costly and time-consuming. Data mining technology is used in intrusion detection systems for wireless sensor networks to overcome the limitations of rule-based systems (Ieracitano et al., 2018; Tan et al., 2019). Some of the latest and most efficient strategies for detecting intrusions includes the utilization of Machine Learning (ML) techniques.

DOI: 10.56892/bima.v8i3.772

(Kilincer et al., 2021; Othman et al., 2018), Deep Learning (DL) methods (Wu et al., 2020; Thapa et al., 2020; Mulyanto et al., 2021; Muhuri et al., 2020), hybrid and ensemble methods (Cao et al., 2022; Muhuri et al., 2020; Liu et al., 2021; Khare et al., 2020; Devan et al., 2020).

Traditional machine learning techniques, such as Support Vector Machine (SVM), Decision Trees (DT), Bayesian Networks (BN), and Logistic Regression (LR), have been extensively utilized in the field of Network Intrusion Detection Systems (NIDS) and have demonstrated satisfactory performance outcomes. However, They are not suitable for Network Intrusion Detection Systems (NIDS) that deal with large and multidimensional datasets. (Cao et al., 2022). The performance of ML techniques is heavily influenced by noise and evolving cyber threats. DL techniques has proven to be very effective for NIDS with huge and high-dimensional data. DL techniques such as Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and Recurrent Neural Networks (RNN) has produced good results when applied to NIDS (Coa et al., 2022), (Wu et al., 2020), (Li et al., 2020). However, their performance relies on appropriate settings of their parameters. The data size and dimension also increase their complexity and performance. Other techniques such as hybrid and ensemble methods have offered better performances compared to the DL and ML methods (Muhuri et al., 2020; Liu et al., 2021; Khare et al., 2020) (Devan et al., 2020), (Gao et al., 2020). Their performances are however still affected by the nature of the dataset and parameter settings.

Most of the existing NIDS were tested using some publicly available data sets. These datasets contain varying numbers of classes, and data counts and are collected differently. Some of the most used data sets include; NSL-KDD, KDD-CUP99, CIDDS-01, UNSW-NB15, and so on (Kilincer et al., 2021). Figure 1 shows some public NIDS datasets from seven different categories. The NSL-KDD dataset is recognized as a prominent data repository utilized for Network Intrusion Detection (NID). Its creation was motivated by the necessity to address deficiencies in the KDD-CUP99 dataset, achieved through the elimination of superfluous and inconsequential entries from the primary KDD-CUP99 dataset. The dataset comprises of 43 features and 150000 records. The dataset comprises five distinct classes, namely Normal, Probe, Remote-To-Local (R2L), Dos, and User-to-Root (U2R) attacks.

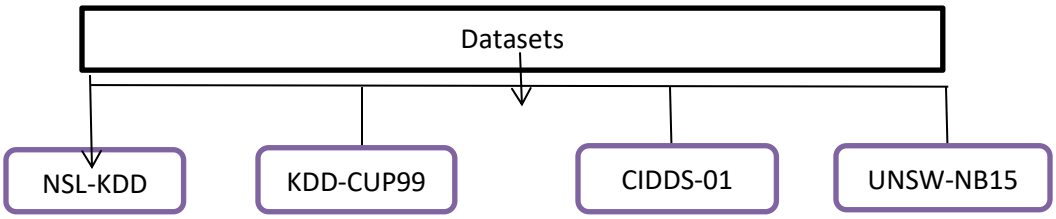

Figure 1: Most used Datasets.

The Contribution of the paper is summarized as follows:

I. Overview of Network Intrusion Detection System (IDS) techniques
II. Review the dataset for NIDS for performance evaluation
III. Recent Datasets used for NIDS

DOI: 10.56892/bima.v8i3.772

The paper is organized as follows: section 2 discusses the techniques of IDS. Section 3 reviews the dataset used for IDS for performance evaluation. Section 4 discusses the characteristics of the datasets and their limitations. The paper concluded with a conclusion and recommendation for future work in section 5.

Techniques for Network Intrusion Detection System

Network Intrusion Detection Systems (NIDS) refer to technological solutions with the ability to identify unauthorized intrusions within a network. Various methodologies are documented in the existing body of literature for the advancement of NIDS. Numerous scholars have utilized superficial Machine Learning (ML) techniques for the identification of intrusion within a network. Approaches like Support Vector Machine (SVM), Decision Trees (DT) algorithms, and Neural Networks, among others, have demonstrated their ability to offer viable solutions. (Tan et al., 2019), (Othman et al., 2018), (Taher, 2019). Despite achieving notable accomplishments, superficial Machine Learning (ML) encounters limitations when dealing with extensive datasets. Consequently, this prompted scholars to shift their attention towards Deep Learning (DL), amalgamated DL, and ensemble approaches for identifying intrusions within a networking system. (Wu et al., 2020), (Mulyanto et al., 2021), (Muhuri et al., 2020), (Tang et al., 2020), (Chen et al., 2021). Among the available research works, various datasets were utilized; certain researchers examined multi-class scenarios, whereas others focused on binary classification instances. Additionally, certain researchers investigated class imbalance and suggested methods to mitigate them, while others did not. The subsequent review examined several handpicked research works on intrusion detection.

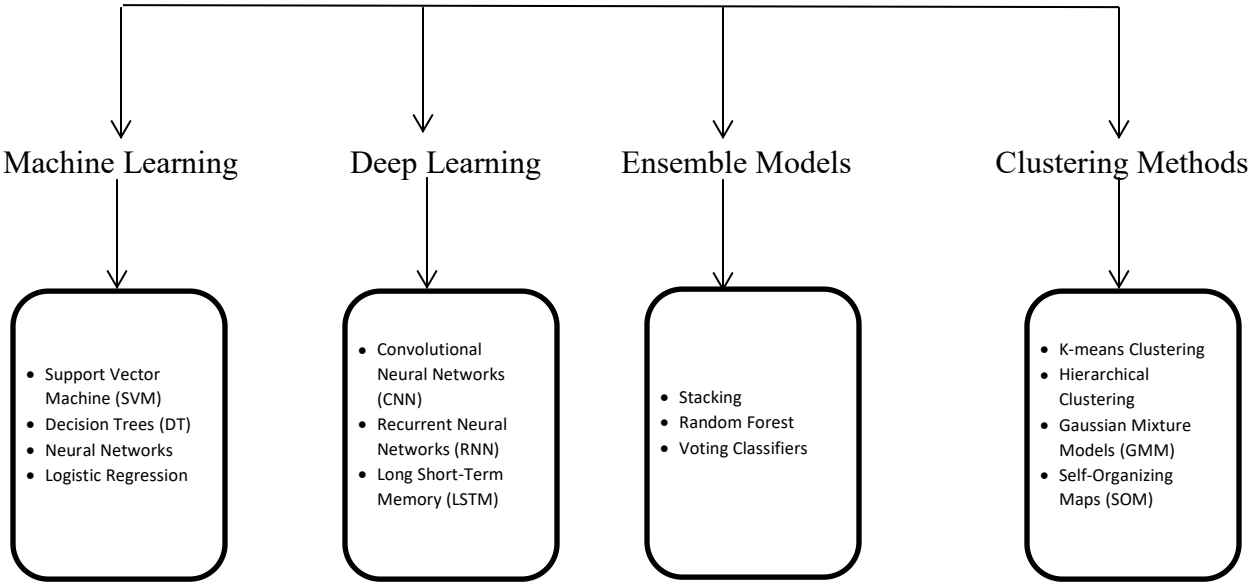

Figure 2: Taxonomy of NIDS Techniques

DOI: 10.56892/bima.v8i3.772

REVIEW ON THE DATASETS FOR NIDS FOR PERFORMANCE EVALUATION

Table 1: Examined an overview of network intrusion detection methods and the datasets they used

Refs	Data	Methods	Results	Strengths	Weaknesses
(Othman et al., 2018)	KDD-99	Applied the Chi-Square test for independence for feature selection and then trained an SVM classifier optimized with SGD classifier.	accuracy of 99.55% while taking 10.79s.	Achieved a very high performance with speed	Cannot classify multi-class intrusion
(Ieracitano et al., 2018)	NSL-KDD	Deep Auto Encoder (DAE) with statistical greedy step-wise feature extraction	Accuracy of 87% for DAE and 81.43% for MLP	Result show improvement over other methods	Performance is low
(Gao et al., 2019)	KDD-19, NSL-KDD, CICIDS 2017	Pearson correlation and hyper parameter tuned Random Forest Model.	High accuracies of across the three datasets.	The proposed approach yielded very high accuracy.	The model is only applicable for binary classification
(Tan et al., 2019)	NSL-KDD	Random Forest (RF) for classification, SMOTE for data balancing	92.39% for RF and 92.57% for SMOTE-RF	The class imbalance was balanced	Performance can still be improved in a multiclass scenario
(Abdulhammed et al., 2019)	CICIDS2017	Auto-encode (AE) and PCA for dimensionality reduction and RF, LDA, QDA and BN	Average 99.6% combined accuracy from all classifiers	Significant reduction in the dimension of the dataset (81 to 10)	Increased complexity
(Alkahtani et al., 2020)	KDD-99, NSL-KDD, ISCX and ICI-Id2017	LSTM-RNN	99.81%, 93.55%, 99.87%, 98.92%	outperformed SVM and kNN	the model as not compared with other DL based approaches.
(Wu et al., 2020)	NSL-KDD and the dataset collected from web attack.	Semantic re-encoding and deep learning SRDLM	It shows that all data is processed by SRDLM which the accuracy is over 99% and NSL-KDD is improve by 8%	ResNet network architecture and combine ResNet with semantic re-encoding to improve the generalisation ability of the network anomaly detection model	It do not study the prediction of network abnormal traffic to enhance the robustness of the network detection model
(Thapa et al., 2020)	CIDDS-001, CIDDS-002, CIC-IDS2017, KDD 99 and NSL-KDD	Using different machine learning and deep learning model	High performance metric with a relatively low training time was achieve for both ML and DL model in network intrusion detection	It helps to select the best relevant feature of data with mutual information criterion and reduce the feature set for better accuracy and faster computation in performance	Ensemble model was not used for internal server datasets and combine dataset, because they are large in size than the external server dataset

DOI: 10.56892/bima.v8i3.772

(Kushwah & Ranga, 2020)	NSL-KDD and the ICSX datasets	Extreme learning classifier	On the NSL-KDD dataset, an accuracy of 99.18%, sensitivity of 99.55% and specificity of 98.86% while taking 141.57s to train. While on the ICSX dataset, an accuracy of 92.11%, sensitivity of 84.34% and specificity of 99.77%	Has the advantage of having a simple computational complexity	Inference is done only on batches of samples over a predefined time intervals.
(Chkirbene et al., 2020)	NSL-KDD, and UNSW	Trust-based Intrusion Detection and Classification System (TIDCS)	91% accuracy for TICDS and	The two models recorded higher accuracies	False alarm rate can be improved
(Khare et al., 2020)	NSL-KDD and KDD-99	DNN with Spider monkey algorithm	Accuracy of 99.4% and 92% on the datasets respectively	It reduces the dimensionality of the features.	This method was only applied however for binary classification not for specifying a particular type of attack in a multi-class scenario
(Devan & Khare, 2020)	NSL-KDD	XGBoost algorithm was used for feature selection to train a DNN.	accuracy of 97.6% was achieved with 7000 samples	Achieved a high accuracy.	no experiments were tested on a multi-class scenario and the computational time of the XGBoost was not experimented.
(Li et al., 2020)	NSL-KDD	multi-fusion CNN	Accuracy of 81.33% in the multi class and 86.69% in the binary class.	It can effectively detect the classes of attacks with limited training samples.	The accuracy falls short of other DL based methods
(Muhuri et al., 2020)	NSL-KDD dataset	GA- LSTM-RNN	Experiments were carried out in the multi-class and binary class scenario with accuracies of 82.68% and 96.51% without the GA and 93.88% and 99.91% with the GA	Showed that the feature selection effectively increased the performance of the IDS	The computational times are not recorded
(Nagaraja et al., 2020)	KDD-19 dataset.	presented a gaussian distanced feature transformation technique.	The feature transformation improves the performance of the J48 Decision Tree, kNN, Naïve Bayes, BayesNet and SMO classifiers on the KDD-19 dataset	The feature transformation reduces the dimensions of the features while showing improvements with several classifiers	The effects of the feature transformation on the computational complexity was not stated.
(Wang et al., 2022)	NSL-KDD and KDD-99.	Stacked Contractive Autoencoder (SCAE) for feature extraction to train an SVM classifier.	on the NSL-KDD dataset results to an accuracy of 87.33%, while 97.87% is achieved on the KDD-	The model showed significant performance in the multi-class	a careful analysis of the results show that that it finds it difficult to classify some new attacks in the dataset

DOI: 10.56892/bima.v8i3.772

			99 data.	scenario.	
(Dey & Rahman, 2019)		Two methods are proposed, first is a gain ratio feature selection for a random forest model. Secondly is the Analysis of Variance (ANOVA) F-test and recursive feature elimination for the Gated LSTM model.	Experiments show an accuracy of 82% for the first method and 88% for the second method	Tests were carried out in the multiclass scenario	the computational times of the two methods were not discussed.
(Sarker et al., 2020)	NSL-KDD	proposed a decision tree model called "IntruDTree" for IDS	An accuracy of 98% was achieved		experiments were tested on a multi-class scenario
(Sarumi et al., 2020)	UNSW-NB15	compared the performance of SVM and an association rule method for IDS	Experiments results in accuracies of 90.41% and 64.09% for the SVM and (77.17%, 67%) for the NSL-KDD	Showed that SVM performs better than the apriori approach.	.
(Zhou et al., 2020)	NSL-KDD & CIC-IDS2017	used an ensemble classifier comprising of an RF, C.45 Decision tree and Forest by Penalizing classifiers for IDS	an accuracy of 99.81% for the NSL-KDD, 99.89% for the CIC-IDS2017 and 99.52% for the AWID	Achieved high accuracy across different datasets.	The model was not experimented in the multi-class scenario.
(Khare et al., 2020b)	NSL-KDD and KDD Cup 99	Spider Monkey Optimization (SMO) and DNN	99.4% and 92% accuracy respectively	High accuracy and reduced features	Model cannot be used for a multi-class problem
(Maniriho et al., 2020)	NSL_KDD, UNSW-NB15	Gain Ratio Feature Evaluator (GRFE), and Correlation Ranking Filter (CRF) feature selection methods coupled with various machine-learning techniques	misclassification gap of 0.969% and 1.19% (obtained using NSL-KDD dataset) and 1.62% and 1.576% (obtained using UNSW-NB15	Ensemble technique performs better	Filter based feature selection are prone to errors
(Isa, 2020)	NSL-KDD, KDD 99 and CICIDS 2017 dataset	Pearson Correlation and Tune Model Hyper Parameter on Microsoft Azure Platform	accuracy, detection rate and false positive rate improved when compared to existing models	Improvement in the detection accuracy	Have not been tested in real network environment
(Dey & Rahman, 2019b)	NSL-KDD	RF, and (GRU-LSTM) using suitable ANOVA F-Test and recursive feature elimination selection	82%, 88% accuracies respectively	DNN IDS performs better	Have not been tested on other controllers
(Alzahrani & Alenazi, 2021)	NSL-KDD	Decision Tree, Random Forest and XGBoost	Average accuracy 95.95%.	Good average performance	The performance of the minority class needs to be improved
(Kumar et al., 2019)	UNSW-NB15	UIDS, ENADS and DENDRON	an accuracy of 88.92%, 85.56% and 84.33% for UIDS, ENADS and	Tested on new attacks	Performance requires improvement

DOI: 10.56892/bima.v8i3.772

			DENDRON respectively		
(Venkatesh, 2021)	NSL-KDD	DL-UAI and DL models	A maximum of 81.29% and 64.67% respectively for RNN	RNN proves better than other DL models	Performance of the system can still be improved
(Pu et al., 2021)	NSL-KDD dataset	combines Sub-Space Clustering (SSC) and One Class Support Vector Machine (OCSVM) to detect attacks without any prior knowledge	0.99, 0.85, 0.52 and 0.90 Detection rates for Probe, Dos, R2L and U2R respectively	Can detect anomaly without prior knowledge	Lack of class balancing affects the performance of minority class
(Chiche & Meshesha, 2021)	NSL-KDD	integrated approach of machine learning with knowledge-based system is proposed for intrusion detection	99.91%	High detection rate	Tested on binary classification only
(Chen et al., 2021)	NSL-KDD, UNSW-NB15 and CICIDS2017	Attempted to intrude networks using a Generative Adversarial Networks (GAN).	For UNSW-NB15, CNN-LSTM model the detection rate reduced from 98.71% to 1.44%, Logistic Regression from 87.51% to 5.53%, KNN from 97.14 % to 7.11%.	A good detection accuracy	The model was not experimented on models hardened for adversarial attack detection
(Mulyanto et al., 2020)	NSL-KDD, UNSW-NB15	Cost-sensitive neural network based on focal loss	An accuracy of 89% for binary and 78% for multiclass classification was obtained	Increase in detection of intrusion in imbalance dataset	The proposed technique has not been applied to sequential tasks problems, and the performance is low
(Cao et al., 2022)	UNSW_NB15, NSL-KDD, and CIC-IDS2017	CNN and Gated Recurrent Unit (GRU), Adaptive Synthetic Sampling (ADASYN) and Repeated Edited nearest neighbors (RENN)	Accuracy of 86.25%, 99.69%, 99.65% were achieved and can solve the problems of low classification accuracy	Improved classification performance	Higher running time, model parameters is high, Detection accuracy for class with lower samples are significantly low
(Amru et al., 2024)	IOT-Network Intrusion database 2024	Ensemble model with Different Machine Learning and XGBoosting Algorithms were used to predict different types of network attacks	It was found that XGBoosting algorithm was used to predict different classes of attack with an accuracy of 94%.	Ensemble model outperformed the traditional machine learning algorithms with an accuracy of 94%.	The esmeble model cannot detects clone attack in the network.
(Qazi et al., 2023)	CICIDS-2018 2023	A Convolutional recurrent Neural Network was employed that construct a hybrid deep learning intrusion detection sytem for detecting different types of attack within network.	The proposed Hybrid deep learning intrusion detecting model outperforms the current intrusion detection models in detecting malicious attack with an average accuracy of 98.90%.	THE mdoel achieved and optimal accuracy of 98.8%.	More network traffic attack should be considered in the future. Employing Backbone network traffic to demonstrates the effectiveness of the model.
(Sivamohan &	Honeypot and	Biderectional Long Short	The developed	The developed	Other advarserial

DOI: 10.56892/bima.v8i3.772

Sridhar, 2023)	NSL-KDD 2023	Term Memory based Explainable Artificial Intellegence framework was developed for	framework achieved a higher accuracy of 97.2% and 95.3% for Honeypot and BSL-KDD dataset in detecting intrusion attack within a network.	framework provides better security and privacy in the industry.	attacks in the network are still not detected

I. A DOS attack involves overloading or disrupting a network or system's resources to prevent its intended users from using it. Attackers overwhelm the target with a large amount of traffic or requests, which makes the system sluggish or unresponsive (Goyal et al., 2022).

II. A probe attack involves an unauthorized attempt to access or gather information about a network or system to identify vulnerabilities (Grover et al., 2016). It is often a precursor to a more sophisticated attack and is used to gather information about the target.

III. User-to-root attacks involve an attacker who has gained regular user access to a system and attempts to escalate their privileges to gain super user or root access (Goyal et al., 2022). These attacks exploit vulnerabilities in the system to gain unauthorized privileges.

IV. An attacker attempting to obtain unauthorized access to a local system from a remote location is known as a remote-to-local attacker. (Grover et al., 2016). These attacks typically target vulnerabilities in the login mechanisms or other services running on the system.

Table 1 above shows that, most of the papers reviewed developed models for binary or multi-class intrusion detection. The related papers that were reviewed revealed that several machine learning and deep learning models has been developed, with the NSL-KDD and KDD datasets being the most widely utilized datasets. Some works used the complete feature set, while few reported feature selection strategies utilizing metaheuristics like GA and bat algorithms. Furthermore, most of the works that tried the multi-class classification of attacks, did not consider class imbalance between the various intrusion attacks such as U2R, R2L, probe, and DoS attacks. This causes a reduction in the performance of the attacks with fewer samples such as U2R and R2L. In examining the datasets presented in Table 2 below, it becomes evident that while NSL-KDD and KDD datasets are widely utilized, a thorough investigation of alternative datasets such as CIDDS-01 is warranted. The Cyber Intrusion Detection Data Sets, or CIDDS-01, are an essential tool for assessing intrusion detection systems in actual operating settings. Its versatility spans various research domains, enabling scholars to meticulously evaluate and refine intrusion detection models across a diverse range of cyber threats. Notably, CIDDS-01 offers the advantage of providing authentic network traffic data, thereby offering a realistic representation of contemporary cyber threats and associated attack scenarios. However, it is essential to acknowledge the dataset's inherent limitations. Chief among these is the potential challenge of class imbalance, which may impact the accuracy of model performance assessments. Additionally, the documentation accompanying CIDDS-01 may contain gaps, potentially hindering comprehensive understanding and utilization. Notwithstanding these drawbacks, CIDDS-01 is still a useful tool for intrusion detection research since it was crucial in creating and refining strong intrusion detection

DOI: 10.56892/bima.v8i3.772

techniques that could successfully navigate the ever-changing world of cyber threats.

DISCUSSION ON RECENT DATASETS USED FOR NIDS

Based on the above-reviewed literatures where several datasets were used for NIDS and shows that there are 41 features for identifying Dos, Probe, U2R, and R2L attacks, with the NSL KDD dataset being the most commonly used for NIDS. The following dataset, KDD CUP-99, CICIDS-2017, contains 41 and 81 features, respectively. Table 2 below displays the different sorts of attacks along with their dataset descrptions.

Table 2: Summary of the recently used Dataset for NIDS

Name of Dataset	Developed by	Features	Types of Attack	Description
NSL KDD	University of California	41	Dos, Probe U2R, R2L	The NSL KDD dataset, an enhanced version of KDD CUP 99, features a curated selection of attack types like Denial of Service, Probe, U2R, and R2L, offering a focused framework for intrusion detection system development. Renowned for its refined curation and credibility from the University of California, it serves as a valuable resource for confronting modern cybersecurity challenges.
KDD CUP-99	University of California	41	Dos, Probe U2R, R2L	The KDD CUP-99 dataset is characterized by redundant and duplicate data samples, posing challenges for accurate intrusion detection system development.
CICIDS 2017	Canadian Institute of Cybersecurity	80	Brute force, Portscan, Botnet, Dos, DDoS, Web, Infiltration	The CICIDS 2017 dataset is meticulously crafted using network profiles, ensuring a specific and deliberate construction approach for comprehensive intrusion detection system evaluation.
UNSW-NB15	The UNSW-NB15 dataset was created in response to the shortcomings of earlier benchmark datasets, such as KDD99 and NSLKDD, which failed to accurately represent contemporary network traffic and attack scenarios. A group of scholars established the dataset sto offer a more realistic and comprehensive dataset for assessing Network Intrusion Detection Systems (NIDSs)		The dataset includes nine types of modern attack patterns, which are more representative of current network threats compared to older datasets. These attack types cover a wide range of intrusion methods, making the dataset more comprehensive for evaluating the effectiveness of NIDSs	The UNSW-NB15 dataset features a comprehensive selection of attack types like Shellcode, Worms, Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, and Reconnaissance. This well-curated dataset includes both legitimate and harmful activity to give a realistic and balanced depiction of network traffic. Renowned for its detailed features and credibility, it serves as an essential resource for advancing the development and evaluation of intrusion detection systems in contemporary cybersecurity environments.

DOI: 10.56892/bima.v8i3.772

Characteristics of the Datasets

(NSL KDD, KDD CUP-99, CICIDS 2017)

The NSL KDD dataset, which evolved from the KDD CUP-99 dataset, includes a refined selection of attack types such as Denial of Service, Probe, U2R, and R2L, providing researchers with a targeted framework for developing intrusion detection systems. NSL KDD is renowned for its curated composition and credibility stemming from the University of California. It empowers scholars to address contemporary cybersecurity challenges with precision. The KDD CUP-99 dataset, on the other hand, is notable for the presence of redundant and duplicate data samples, which presents difficulties in developing an accurate intrusion detection system. Despite its complexities, this dataset remains a pillar of the field, providing valuable insights into network intrusion patterns.

Meanwhile, the CICIDS 2017 dataset is notable for its meticulous construction with network profiles, which ensures a deliberate approach to comprehensive intrusion detection system evaluation. The dataset's unique methodology allows researchers to precisely investigate various network intrusion scenarios, fostering advancements in cyber security research and development.

Limitation of the Datasets (NSL KDD, KDD CUP-99, CICIDS 2017)

The datasets NSL KDD, KDD CUP-99, and CICIDS 2017, while valuable, present certain limitations. NSL KDD, despite its curated attack types, may suffer from class imbalance issues, potentially skewing model evaluations. Additionally, the KDD CUP-99 dataset's inclusion of redundant and duplicate data samples poses challenges for accurate intrusion detection system development. Similarly, while CICIDS 2017's construction using network profiles ensures a specific approach, it may lack diversity in representing real-world network intrusion scenarios, limiting its applicability in certain contexts. These limitations underscore the importance of careful consideration and validation when utilizing these datasets for intrusion detection research.

Specification of the dataset (NSL KDD, KDD CUP-99, CICIDS 2017).

Table 3 below shows the specification of the three datasets along with their related information such as attack infrastructure, victims' infrastructure, number of features and classes.

Table 3: Dataset Specification

Dataset Name	NSL KDD	KDD CUP-99	CICIDS 2017
Dataset Type	Network intrusion datasets	Network intrusion datasets	Network intrusion datasets
Year of Information	2009	1998	2017
Duration of Capture	Collected over varying periods, including days and weeks	Approximately one week of network traffic	Collected over 5 days
Attack Infrastructure	Utilizes ML/DL models for cyber threat detection: preprocesses data, selects features, trains models, and deploys them for monitoring and updating, ensuring	Employs ML/DL techniques for cybersecurity: preprocesses data, selects relevant features, trains models with cross-validation, and deploys them for	Leverages ML/DL models for cyber defence: preprocesses data, selects features, trains models with cross-validation, and deploys for monitoring and updating while implementing

DOI: 10.56892/bima.v8i3.772

	security measures.	monitoring, updating, and securing.	security.
Victim Infrastructure	Consists of network systems, servers, and applications prone to cyber threats such as intrusion attempts, malware infections, and denial-of-service attacks.	Includes network environments and systems vulnerable to various types of cyber attacks, aiming to detect and mitigate intrusion attempts and malicious activities.	Comprises network infrastructure, hosts, and services susceptible to cyber threats, including malware infections, botnet activity, and other malicious behaviors.
Features	41	41	80
Number of Classes	23	2	15

CONCLUSION

In conclusion, the rapid advancement of information and communication technology has led to a significant increase in global reliance on Internet-based services. The COVID-19 pandemic has accelerated this trend, prompting organizations and individuals to shift to online platforms for daily activities. However, the increase in online activity has made users and networks more vulnerable to various types of cyber threats. A diverse array of techniques and methodologies employed in NIDS development were explored, spanning from complex machine learning (ML) and deep learning (DL) models to hybrid and ensemble approaches, as well as conventional rule-based systems. Although classical machine learning methods such as Support Vector Machine (SVM) and Decision Trees (DT) have proven to be effective, their applicability diminishes when faced with massive and high-dimensional data.

In contrast, DL techniques, such as Long Short-Term Memory (LSTM) and Convolutional Neural Networks (CNN), have shown remarkable prowess in handling extensive and complex datasets, However, with the caveat that their performance relies on meticulous parameter tuning and appropriate dataset scaling. Additionally, hybrid and ensemble methods have emerged as promising avenues, offering enhanced performance compared to standalone ML and DL techniques.

The exploration further delved into commonly used datasets for NIDS evaluation, such as NSL-KDD, KDD CUP-99, and CICIDS 2017. These datasets serve as indispensable resources for researchers, enabling comprehensive evaluations of the proposed NIDS models. However, limitations such as class imbalance and dataset specificity underscore the necessity for meticulous validation and consideration when employing these datasets.

As we navigate the ever-evolving landscape of cyber threats, continuous innovation and refinement of NIDS methodologies are imperative to effectively combat emerging challenges.

Future Work

Future research endeavours may focus on addressing existing limitations within NIDS, leveraging advancements in ML, DL, and ensemble techniques to bolster detection capabilities and fortify network defences against evolving cyber threats. Collaboration between academia, industry, and cybersecurity practitioners will be instrumental in paving the way towards more robust and resilient NIDS frameworks, safeguarding the integrity and security of network infrastructures worldwide.

DOI: 10.56892/bima.v8i3.772

REFERENCES

Abdulhammed, R., Musafer, H., Alessa, A., Faezipour, M., & Abuzneid, A. (2019). Features dimensionality reduction approaches for machine learning based network intrusion detection. Electronics, 8(3). https://doi.org/10.3390/electronics8030322

Alkahtani, H., Aldhyani, T. H. H., & Al-Yaari, M. (2020). Adaptive anomaly detection framework model objects in cyberspace. Applied Bionics and Biomechanics, 2020. https://doi.org/10.1155/2020/6660489

Alzahrani, A. O., & Alenazi, M. J. F. (2021). Designing a network intrusion detection system based on machine learning for software-defined networks. Future Internet, 13(5). https://doi.org/10.3390/fi13050111

Bhati, B. S., & Rai, C. S. (2020). Analysis of support vector machine-based intrusion detection techniques. Arabian Journal for Science and Engineering, 45(4), 2371–2383. https://doi.org/10.1007/s13369-019-03970-z

Cao, B., Li, C., Song, Y., Qin, Y., & Sciences, C. C.-A. (2022). Network intrusion detection model based on CNN and GRU. Applied Sciences, 12, Article 4184. https://doi.org/10.3390/app12094184

Chen, J., Wu, D., Zhao, Y., Sharma, N., Blumenstein, M., & Yu, S. (2021). Fooling intrusion detection systems using adversarially autoencoder. Digital Communications and Networks, 7(3), 453–460. https://doi.org/10.1016/j.dcan.2020.11.001

Chiche, A., & Meshesha, M. (2021). Towards a scalable and adaptive learning approach for network intrusion detection. Journal of Computer Networks and Communications, 2021. https://doi.org/10.1155/2021/8845540

Chkirbene, Z., Erbad, A., Hamila, R., Mohamed, A., Guizani, M., & Hamdi, M. (2020). TIDCS: A dynamic intrusion detection and classification system based feature selection. IEEE Access, 8, 95864–95877. https://doi.org/10.1109/ACCESS.2020.2994931

Dey, S. K., & Rahman, M. M. (2020). Effects of machine learning approach in flow-based anomaly detection on software-defined networking. Symmetry, 12(1). https://doi.org/10.3390/SYM12010007

Devan, P., & Khare, N. (2020). An efficient XGBoost–DNN-based classification model for network intrusion detection system. Neural Computing and Applications, 32(16), 12499–12514. https://doi.org/10.1007/s00521-020-04708-x

Gao, X., Shan, C., Hu, C., Niu, Z., & Liu, Z. (2019). An adaptive ensemble machine learning model for intrusion detection. IEEE Access, 7, 82512–82521. https://doi.org/10.1109/ACCESS.2019.2923640

Goyal, G., Singh, Y., Dhwaj, D., & Malik, D. (2022). Wireless sensor network: Attacks and countermeasures. Manuscript submitted for publication.

Grover, J., & Sharma, S. (2016). Security issues in wireless sensor network — A review. In 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) (pp. 397–404). IEEE. https://doi.org/10.1109/ICRITO.2016.7784988

DOI: 10.56892/bima.v8i3.772

Gu, J., & Lu, S. (2021). An effective intrusion detection approach using SVM with naïve Bayes feature embedding. Computers & Security, 103. https://doi.org/10.1016/j.cose.2020.102158

Ieracitano, C., et al. (2018). Statistical analysis driven optimized deep learning system for intrusion detection. In Lecture Notes in Computer Science (including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Vol. 10989 LNAI, pp. 759–769). Springer. https://doi.org/10.1007/978-3-030-00563-4_74

Isa, F. M. (2020). Optimizing the effectiveness of intrusion detection system by using Pearson correlation and tune model hyper parameter on Microsoft Azure platform. International Journal of Advanced Trends in Computer Science and Engineering, 9(1.3), 132–138. https://doi.org/10.30534/ijatcse/2020/1991.32020

Kilincer, I. F., Ertam, F., & Sengur, A. (2021). Machine learning methods for cyber security intrusion detection: Datasets and comparative study. Computer Networks, 188. https://doi.org/10.1016/j.comnet.2021.107840

Khare, N., et al. (2020). SMO-DNN: Spider monkey optimization and deep neural network hybrid classifier model for intrusion detection. Electronics, 9(4). https://doi.org/10.3390/electronics9040692

Kumar, V., Das, A. K., & Sinha, D. (2021). UIDS: A unified intrusion detection system for IoT environment. Evolutionary Intelligence, 14(1), 47–59. https://doi.org/10.1007/s12065-019-00291-w

Kushwah, G. S., & Ranga, V. (2020). Voting extreme learning machine based distributed denial of service attack detection in cloud computing. Journal of Information Security and Applications, 53. https://doi.org/10.1016/j.jisa.2020.102532

Li, Y., et al. (2020). Robust detection for network intrusion of industrial IoT based on multi-CNN fusion. Measurement, 154. https://doi.org/10.1016/j.measurement.2019.107450

Liu, C., Gu, Z., & Wang, J. (2021). A hybrid intrusion detection system based on scalable K-means+ random forest and deep learning. IEEE Access, 9, 75729–75740. https://doi.org/10.1109/ACCESS.2021.3082147

Liu, Z., Guo, X., & Tang, H. (2020). Unsupervised learning-based network intrusion detection algorithm. Journal of Ambient Intelligence and Humanized Computing, 11(2), 595–603. https://doi.org/10.1007/s12652-019-01336-9

Lopez-Martin, M., Carro, B., & Sanchez-Esguevillas, A. (2020). Application of deep reinforcement learning to intrusion detection for supervised problems. Expert Systems with Applications, 141. https://doi.org/10.1016/j.eswa.2019.112963

Maniriho, P., Mahoro, L. J., Niyigaba, E., Bizimana, Z., & Ahmad, T. (2020). Detecting intrusions in computer network traffic with machine learning approaches. International Journal of Intelligent Engineering Systems, 13(3), 433–445. https://doi.org/10.22266/IJIES2020.0630.39

DOI: 10.56892/bima.v8i3.772

Muhuri, P. S., Chatterjee, P., Yuan, X., Roy, K., & Esterline, A. (2020). Using a long short-term memory recurrent neural network (LSTM-RNN) to classify network attacks. Information, 11(5). https://doi.org/10.3390/INFO11050243

Mulyanto, M., Faisal, M., Prakosa, S. W., & Leu, J. S. (2021). Effectiveness of focal loss for minority classification in network intrusion detection systems. Symmetry, 13(1), 1–16. https://doi.org/10.3390/sym13010004

Nagaraja, A., Boregowda, U., Khatatneh, K., Vangipuram, R., Nuvvusetty, R., & Kiran, V. S. (2020). Similarity-based feature transformation for network anomaly detection. IEEE Access, 8, 39184–39196. https://doi.org/10.1109/ACCESS.2020.2975716

Naganhalli, N. S., & Terdal, S. (2019). Network intrusion detection using supervised machine learning technique. International Journal of Science and Technology Research, 8(9), 345–350. https://ieeexplore.ieee.org/document/8644161

Othman, S. M., Ba-Alwi, F. M., Alsohybe, N. T., & Al-Hashida, A. Y. (2018). Intrusion detection model using machine learning algorithm on big data environment. Journal of Big Data, 5(1). https://doi.org/10.1186/s40537-018-0145-4

Pu, G., Wang, L., Shen, J., & Dong, F. (2021). A hybrid unsupervised clustering-based anomaly detection method. Tsinghua Science and Technology, 26(2), 146–153. https://doi.org/10.26599/TST.2019.9010051

Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). IntruDTree: A machine learning based cyber security intrusion detection model. Symmetry, 12(5). https://doi.org/10.3390/SYM12050754

Sarumi, O. A., Adetunmbi, A. O., & Adetoye, F. A. (2020). Discovering computer networks intrusion using data analytics and machine intelligence. Scientific African, 9. https://doi.org/10.1016/j.sciaf.2020.e00500

Tang, C., Luktarhan, N., & Zhao, Y. (2020). An efficient intrusion detection method based on LightGBM and autoencoder. Symmetry, 12(9). https://doi.org/10.3390/sym12091458

Tan, X., et al. (2019). Wireless sensor networks intrusion detection based on SMOTE and the random forest algorithm. Sensors (Switzerland), 19(1). https://doi.org/10.3390/s19010203

Taher, K. A. (2019). Network intrusion detection using supervised machine learning technique with feature selection. In 2019 International Conference on Robotics and Signal Processing Techniques (pp. 643–646). IEEE. https://doi.org/10.1109/ICRSPT.2019.8644161

Thapa, N., Liu, Z., Kc, D. B., Gokaraju, B., & Roy, K. (2020). Comparison of machine learning and deep learning models for network intrusion detection systems. Future Internet, 12(10), Article 167. https://doi.org/10.3390/fi12100167

Ullah, I., Mahmoud, Q. H., & Member, S. (2021). Design and development of a deep learning-based model for anomaly detection in IoT networks. IEEE Access, 9. https://doi.org/10.1109/ACCESS.2021.3082147

Venkatesh, R., Kavitha, S., & Uma Maheswari, N. (2021). Network

DOI: 10.56892/bima.v8i3.772

anomaly detection for NSL-KDD dataset using deep learning. Information Technology in Industry, 9(2), 821–827. https://doi.org/10.17762/itii.v9i2.419

Wang, W., Du, X., Shan, D., Qin, R., & Wang, N. (2020). Cloud intrusion detection method based on stacked contractive auto-encoder and support vector machine. IEEE Transactions on Cloud Computing, 1–1. https://doi.org/10.1109/TCC.2020.3001017

Wu, Z., Wang, J., Hu, L., Zhang, Z., & Wu, H. (2020). A network intrusion detection method based on semantic re-encoding and deep learning. Journal of Network and Computer Applications, 164. https://doi.org/10.1016/j.jnca.2020.102688

Zhou, Y., Cheng, G., Jiang, S., & Dai, M. (2020). Building an efficient intrusion detection system based on feature selection and ensemble classifier. Computer Networks, 174. https://doi.org/10.1016/j.comnet.2020.107247

Amru, M., Kannan, R. J., Ganesh, E. N., Muthumarilakshmi, S., Padmanaban, K., Jeyapriya, J., & Murugan, S. (2024). Network intrusion detection system by applying ensemble model for smart home. International Journal of Power Electronics and Drive Systems/International Journal of Electrical and Computer Engineering, 14(3), 3485. https://doi.org/10.11591/ijece.v14i3.pp3485-3494

Qazi, E. U. H., Faheem, M. H., & Zia, T. (2023). HDLNIDS: Hybrid Deep-Learning-Based Network Intrusion Detection System. Applied Sciences, 13(8), 4921. https://doi.org/10.3390/app13084921

Sivamohan, S., & Sridhar, S. S. (2023). An optimized model for network intrusion detection systems in industry 4.0 using XAI based Bi-LSTM framework. Neural Computing and Applications, 35(15), 11459–11475. https://doi.org/10.1007/s00521-023-08319-0