Predictive Network Intrusion Identification & Mitigation Model Using Deep Learning In E-Learning

Samuel M. Musyimi[1], Waweru Mwangi[2] & Dennis Njagi[3]

[1]*Jomo Kenyatta University of Agriculture and Technology, Kenya (Suvaihopes@gmail.com)*

[2]*Jomo Kenyatta University of Agriculture and Technology, Kenya (waweru_mwangi@icsit.jkuat.ac.ke)*

[3]*Jomo Kenyatta University of Agriculture and Technology, Kenya (dennis.njagi@jkuat.ac.ke)*

Abstract

The world of Information-technology has advanced quickly in recent years and network services have extended throughout all industries. Internet Technology has changed traditional teaching techniques and developed versatile E-learning models. E-learning models are a great achievement but are vulnerable to cyber-attacks such as Denial-of-Service (DoS). The aim of the study is to develop a predictive network intrusion identification and a mitigation model using deep learning in e-learning. The research adopts an anomaly detection methodology. The research datasets consist of 47,645 instances. These instances were divided into training datasets and test datasets in the ratio of 80:20 respectively. Deep learning was applied to develop the prediction model. Generative Adversarial Networks (GANs) and Binary classification was used for augmenting and artificial instance generation. The developed model was able to detect network intrusion with a prediction accuracy of 99.8%. The results of this study can be applied to respond to the ever-evolving attacks in e-learning platforms to improve data security and protection.

***Keywords*: Predictive, Identification, E-Learning, Deep Learning, TensorFlow, Gans**

Introduction

Deep learning is a powerful AI technique that can be used to detect intrusions in e-learning environments. By analysing network traffic and learning from large datasets, deep learning models can identify malicious activity and potential threats. This can help to protect e-learning systems from unauthorized access, data breaches, and other security risks.

Denial-of-service (DoS) attacks are immediately mitigated when they are detected. A classifier is trained on an unlabelled attack dataset to categorize incoming traffic by comparing observed network traffic patterns with known attack patterns, looking for deviations from established patterns. If an attack is detected, suspect traffic can be stopped, or its rate can be controlled. DoS responses are often used at the physical and network levels to protect nodes and reduce downtime. Possible responses include pushback, quarantining the attacker's IP address, traffic restrictions, and redirection.

Existing intrusion detection methods for e-learning platforms have several limitations, such as false alerts, inaccurate calculations, low accuracy rates, limited training datasets, and false identification of attacks in dynamic environments. These limitations can be addressed by developing a new security model that can effectively differentiate between normal traffic and malicious activities, providing reliable alert mechanisms (Terzi, Terzi, & Sagiroglu, 2017).

Preventing and mitigating Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks in E-learning is a critical challenge. These attacks can disrupt services, leading to information security risks and operational disruptions. The frequency and complexity of such attacks have been on the rise, requiring ongoing advancements in defensive measures (Kumar & Bhatia, 2019) (Varanasi & Razia, 2022) With the tremendous rise in network usage, security is becoming increasingly important. Data is shielded from security flaws by security mechanisms.

To enhance the functionality and quality of Network Intrusion Identification Models (NIIM), a proposed solution is to develop a Deep-learning model that effectively identifies and mitigates malicious activities. This model utilizes Generative Adversarial Networks (GANs) and Binary-cross-entropy algorithms to achieve improved accuracy and intelligence in attack and threat identification. Recognizing diverse network attacks, especially unexpected ones, poses a significant technical challenge in e-learning environments (Maithem & Al-sultany, 2021).

Problem statement

Deep learning techniques are being increasingly used to protect computer networks from complex and severe security attacks. However, existing deep learning techniques are computationally expensive, limiting their widespread adoption. This project aims to develop a resource-efficient deep learning approach using Generative Adversarial Networks (GANs) for network intrusion detection. This approach is expected to improve the accuracy of intrusion detection while reducing the computational resources required.

Internet intrusion attacks exhibit a strategic approach, leveraging normal datasets to conceal malicious activities, while the internet generates vast amounts of unstructured and unlabelled data. This research aims

to address the continuous evolution of internet attacks, particularly in E-learning models, by employing Deep Neural Network algorithms to enhance accuracy rates and attack identification capabilities.

Objective

i. The objective of this study is to assess the effectiveness of Deep learning techniques in accurately identifying intrusion in modern dataset traffic within the context of E-Learning. The focus is on predicting attacks and threats, evaluating the accuracy of the Deep learning models in detecting and mitigating network intrusions.

ii. This project aims to develop a robust intrusion detection framework for e-learning platforms using TensorFlow. The framework will use deep learning to accurately predict and classify threats and attacks, enabling effective mitigation strategies to be implemented. The goal is to enhance the security of e-learning environments by providing a reliable and efficient intrusion detection system.

Generative Adversarial Networks (GANs) Structure

GANs are deep learning-based generative models consisting of two neural networks that compete to produce artificial instances that mimic real datasets. These neural networks, inspired by the human brain, learn patterns from a dataset and generate new results that closely resemble the original data. GANs offer creative potential by generating realistic synthetic data. The generator network creates artificial instances, while the discriminator network assesses their authenticity. GANs are utilized to address the issue of distribution imbalance, particularly in cases of imbalanced anomaly instances. This study focuses on addressing evolving internet threats and attacks, particularly in E-learning models, by developing a deep learning algorithm that aims to improve accuracy rates, attack identification rates, and dataset balancing (Maithem & Al-sultany, 2021).

Generative Adversarial Networks (GANs) have gained enormous popularity in the past 5 years for a wide range of applications in fields like image analysis, video processing, anomaly detection, and modelling complex and high dimensional data distributions. GANs are composed of two neural networks, the generator and the discriminator, which compete with each other in an adversarial setting. The generator learns to create realistic samples from a latent space, while the discriminator learns to distinguish between real and fake samples. GANs have been shown to be effective for a variety of tasks, including intrusion detection.

To increase the resilience of DL-based NIIMs, a study has recently presented a highly powerful protection against adversarial ML instances using GANs. In the study, CIC-NIIS2017 datasets have been used to reflect modern traffic and current threats and attacks. Which reflect the most recent threats and attacks, and will be used in this project to train representative unsupervised deep learning models including binary-cross entropy (BC) and generative adversarial networks (GANs). The performance of intrusion identification can be enhanced, and classification time can be decreased, by reducing high-dimensional data to smaller dimensions based on BC.

When the discriminator is effectively flooded while being trained to be an accurate classifier, the generator works well. The DL model's approach is predictive and self-adapts to new data contexts. Notably, the strategy leverages bottom-up approaches' inputs in place of top-down approaches' outputs. DL architecture

is created by the model's extraction of characteristics using linear models, which are then employed as building blocks for layers that are dependent on one another and are found in the preceding and following tiers. DL is a technique for extracting knowledge from huge databases interposed for prediction. To predict future intrusion in connected datasets, it is helpful to attribute and feature-extract patterns from a knowledge base and exploit them (Tang, Luktarhan, & Zhao, 2020).

Network monitoring has been widely employed in forensics, cyber security, and big data analytics. There are challenges in current models for Network intrusion Identification most rule-based IDs, the inability to identify new attacks, the use of signatures intrusion Identification who's to overcome these limitations. Databases are their sole source of knowledge. Major uncovered challenges studied from related work are Network intrusion identification high false-positive rate (Fr), Datasets KDD-cup 99 absolute, misjudgements of prediction models, growth in the volume of network data, low Identification rate (Ir), slow processing speed and Big-data analytics.

$Gl(x) = \min_{x \in data}(x - x')$...Generator $D * G(x) = \frac{pdata(x)}{pdata(x)+Pg(x)}$…Discriminator…eqn 1.1 adversary neurals

G neural network creates data instance, and generate artificial datasets, D discriminator assesses the legitimacy of those artificial instances distinguishing normal traffic and malicious traffic.

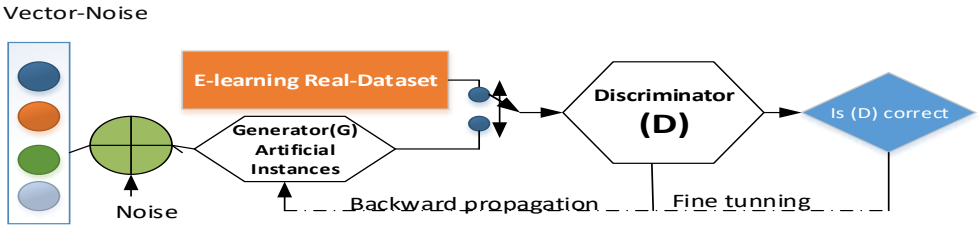

Figure 1 Structure For Gans Intrusion Identification (Jin, Nara, Jo, & Sang Hyun, 2017)

Literature Review

Several attempts have been proposed in the area of Network intrusion identification of threats and attacks. But still there exists flows in Networks security such as unidentified attacks. Techniques previously used such as Traditional intrusion identification, firewalls, and antivirus protection. Modern intrusion identification Artificial intelligence (AI), Machine-learning (ML), and Deep-learning (DL). However, there exists a need for research in intrusion identification. Since intruders' techniques are dynamically changing and the need for improved intrusion identification. Deep-Learning through can achieve greater and more accurate results (Tang et al., 2020).

(Reddy, Ramadevi, & Sunitha, 2017) Traditional information security tools like firewalls, VPNs, intrusion detection systems, and antivirus software have limitations that necessitate the use of more advanced techniques such as deep learning algorithms. Deep learning offers improvements in terms of accuracy, addressing dataset imbalances, reducing false negative alarms, and more. This study aims to utilize the GANs framework within deep learning to address these gaps in network intrusion identification models. The objective is to design a framework that achieves higher accuracy, lower false positive rates, handles

imbalanced datasets, detects unidentified attacks, and enhances sensitivity and security in dealing with network threats and attacks in e-learning platforms.

Deep Convolutional Generative Adversarial Network (Dcgans)

Arora surveyed GANs learning as an Intrusion detection model, Results from Deep-Convolutional Generative Adversarial Networks (DCGANs) are of exceptionally high quality and stability. Convolutional layers are used in the discriminator for down-sampling, whilst the generator uses slightly convolutional layers for up-sampling. ReLU as the activation method, batch normalization, removal of completely linked layers and max-pooling layers, and exception of the activation layer, output layer of the generator, and the input layer of the discriminator (Arora & Shantanu, 2020).

Bidirectional Generative Adversarial Networks (BiGAN)

(Yilmaz, Masum, & Siraj, 2020) Information security experts have shown interest in applying Bidirectional Generative-Adversarial Networks (BiGAN) for intrusion detection. While there are successful examples of using GANs and IDS in this area, the focus is often on horizontal comparisons with conventional machine learning-based IDS, rather than vertical comparisons. BiGAN, a variant of GANs, has demonstrated promising outcomes by incorporating the auto-encoder framework into the GAN architecture. This integration addresses GAN's limitations in capturing pixel relationships and improves the inference of pixel characteristics by learning the data distribution in latent space.

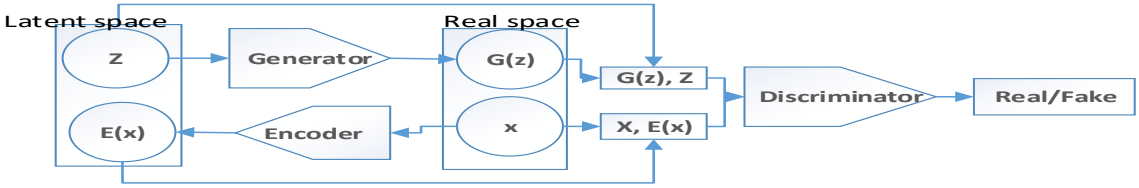

Figure 2 (Arora & Shantanu, 2020) Bidirectional Generative Adversarial Networks

(Yin, Zhu, Fei, & He, 2017) proposed Intrusion Identification using Recurrent Neural Networks algorithm to predict-accurately identify various attacks in the network using Recurrent Neural Networks algorithm classify. The Recurrent Neural Networks algorithm classify and malicious Traffic Datasets. This model used NSL-KDD Dataset. The study used multiclass classification methodology and binary encoding the accuracy of this model was 96.4 %. NSL-KDD Dataset is absolute and does not reflect modern Network Traffic and high level of imbalanced datasets, especially in E-learning models.

(Yilmaz et al., 2020) A Multilayer Perceptron (MLP) technique was proposed by to address data imbalance in intrusion detection. The study aimed to improve the accuracy of attack and threat detection using the UGR'16 dataset. The proposed framework employed a convolutional neural network (CNN) to detect network intrusions, using the KDD-Cup-1999 dataset for training and testing. The CNN-IDS model achieved an identification rate and accuracy rate of 97.7%. The study also utilized supervised datasets to classify and label legitimate and malicious network traffic for supervised learning. The challenge lies in identifying network intrusion attacks, which are becoming more sophisticated and concealed within normal

traffic. Attackers strategically hide their datasets within regular traffic to carry out malicious attacks (Azizjon, Jumabek, & Kim, 2020)

(I. A. Khan, Pi, Khan, Hussain, & Nawaz, 2019) In the research, a Deep learning model incorporating the bloom filter and k-nearest neighbour (k-NN) was proposed, utilizing instance-based learning. The k-NN algorithm was employed to find the nearest neighbors of given samples. The study focused on addressing the challenge of unbalanced intrusion datasets, where the minority class is underrepresented. To tackle this, the Hybrid-Multilevel Anomaly Prediction Approach for Intrusion Identification (HML-NIIS) methodology was utilized. This approach classifies an event based on the majority session of its k closest neighbors. The results showed a high accuracy rate of 97%.

(Al-Mohannadi, Al-Senaid, & Al-Emadi, 2020) Previous studies have explored various approaches for intrusion identification models. In this study, the proposed an enhanced method based on a three-layered Recurrent Neural Network (RNN) with multiple features. The model incorporates basic, content, time-based traffic, and host-based traffic features as inputs. The model's output consists of two classifications: normal class, indicating the absence of attacks, and attack classes such as DoS, R2L, U2R, and probing. To improve classification speed, the employed partially connected hidden layers and trained and tested the model using the KDD dataset. It's worth noting that the technique used in this paper is misuse-based intrusion identification, and the KDD datasets used are outdated and no longer representative of current network traffic.

(Sou & Lin, 2017) introduced the active mitigation procedure model (IPS) actively monitors JMBJM of internet traffic to detect malicious activities and initiate a response for mitigation The major concern of any information Security focuses on the Identification of any model and its mitigation plan to minimize Risks at the lowest level. Because of the flaws in conventional defences in model Identification and mitigation a proposed security model Intrusion Identification and Mitigation Models has emerged (IPS). At present anti-viruses, proxy servers, firewalls, network filters, and anti-spyware are struggling to accurately identify and mitigate attacks. GANs are being used by security experts to achieve outstanding outcomes in areas like image processing and network intrusion detection. Although companies are aware of potential dangers and assaults and always plan to be on the safe side, attackers are nevertheless able to launch attacks because of particular gaps. (Li & Zhang, 2019; Xiao, Xing, Zhang, & Zhao, 2019).

While another viewed mitigation (Kumar & Bhatia, 2019) unwanted network traffic is automatically detected by DL and mirrored to a security management device mitigation. Malware-generated domain servers are difficult to detect using manual identification and sink-holing the attacks and threats domains difficulty when harmful actions generate unwelcome traffic, the study model initiates a reaction mechanism that transfers traffic from the source to mitigation. Mitigation techniques such as traffic redirecting, quarantining source IP addresses, and blacklisting, malicious activities. The study focused on the following feature in the literature review algorithm used by the purpose of the study datasets used for experimenting, and the accuracy obtained from the experiment.

Study Findings

The main issues with internet intrusion identification and mitigation models include the issue of incorrect classification, datasets imbalanced, lack of sufficient dataset, and an excessive volume of false alarms, as well as unidentified threats and attacks that haven't been identified. GANs futuristic solution to the challenges discussed above using DL. Because of the growing number of attackers and threats internet invaders, Network Intrusion Identification models (NIIM) have become essential to information security models. The majority of modern NIDs are tailored to find known service level network threats.

Summary of Literature Review

Table 1 Summary of Critique of Literature Review

AUTHOR-STUDIER'S	ALGORITHMS	PURPOSE	DATASETS	ACCURACY
(Shone, Ngoc, Phai, & Shi, 2018)	Nonsymmetric-deep-Auto-encoder (NDAE) and stacked	Sustainability of modern networks Traffic. Increase accuracy-Rate Identification-Rate	KDD Cup99 and NSL-KDD	Accuracy-Rate 97.85%
(Vigneswaran, Vinayakumar, Soman, & Poornachandran, 2018)	Deep Neural Networks (DMLs)	The objective is to ensure cyber safety in the day-to-day world by implementing effective measures to protect against online threats and vulnerabilities.	KDDCup-'99'	Accuracy-Rate 96.75%
(F. A. Khan, Gumaei, Derhab, & Hussain, 2019)	Stacked-auto-encoder and soft-max-classifier	To Increase the accuracy of network identification identification-Rate.	KDD99 and UNSW-NB15.	For KDD99 99.996% UNSW-NB15 89.134%,
(Kumar & Bhatia, 2019)	Bigrams and Recurrent Neural Networks.	Utilizing machine learning and deep learning approaches, simulate efficient models, find malware or bots	Microsoft's COCO com-petition on Kaggle	Accuracy-Rate 94.2%
(Otoum, Kantarci, & Mouftah, 2019)	Restricted-Boltzmann machine-learning clustered IDS (RBC-IDS)	To review RBC-IDS, in Network intrusion Identification-Rate	KDD99	Accuracy-Rate 99.2%
(Al-Emadi, Al-Mohannadi, & Al-Senaid, 2020)	Convolutional-Neural-Networks (CNN) and Recurrent Neural Networks (RNN).	Response to Network intrusion attacks and model presenting significant privacy and security concerns.	NSL-KDD dataset	Accuracy-Rate 97%.

(Azizjon et al., 2020)	One dimensional-Convolutional Neural Network	In order to enhance the flexibility and efficiency of the intrusion detection system (IDS), measures are taken to improve its performance and adaptability.	NSW NB15 IDS	Accuracy-Rate 87.39%, Precision 88.88%, Recall 87.39%,
(Tang et al., 2020)	stacked auto-encoder (SAE) and Binary-classification	To address the issues with feature extraction and low intrusion identification accuracy and efficient	NSL-KDD dataset	Accuracy-Rate 87.74%
(Maithem & Al-sultany, 2021)	Binary and multiclass classification	To detect the unknown attack and Zero attacks patterns in E-learning	KDD CUP 1999	Accuracy-Rate 99.98%
(Varanasi & Razia, 2022)	Ensemble learning	To understand the study foundation, and study status. Improve detecting zero-day threats and attacks.	CICIDS2017 CNN-LSTM	Accuracy-Rate 98.67% Accuracy-Rate 98.43%.

The Study Methodology

This section aims to improve the defense capabilities of Network Intrusion Identification Models (NIIM) against adversarial deep learning attacks by using adversarial training with generative deep learning models. The proposed model uses deep learning techniques for anomaly detection and employs a Generative Adversarial Network (GAN) discriminator to distinguish between genuine and malicious network traffic data. The simulation uses a temporary training frame with 10,043 samples and a deep learning algorithm for binomial classification. The study focuses on classification techniques for identifying network threats and attacks, followed by the development of an anomaly identification model based on this classification approach. The three phases of the study are training, testing, and validation. Classification is a valuable tool for intrusion identification, particularly in unsupervised learning scenarios where unlabelled datasets are not required for training (Ruoti, Heidbrink, O'Neill, Gustafson, & Choe, 2017).

The proposed Network intrusion identification model utilizes Deep-learning and anomaly identification techniques for detecting and preventing data privacy breaches. The study focuses on the use of GANs, a straightforward deep learning approach, for classifying and mitigating Internet intrusions. Continuous improvement and enhanced usability are achieved through the application of predictive learning techniques. The research also explores unsupervised learning to reduce dependence on labelled data.

This paper aims to develop a more accurate and reliable predictive model for identifying vulnerabilities in E-learning platforms. The proposed solution involves implementing a continuous evaluation mechanism to monitor network traffic, with minimal human involvement. Automated techniques and algorithms will be used to detect and classify network models with high accuracy and efficiency. The study utilizes stratified

random sampling to ensure preservation of each target class in the dataset splits, and a split ratio of 80:20 is chosen to optimize learning algorithm performance. Cross-validation technique is employed for superior outcomes with smaller datasets.

Deep learning (DL)

Building several hidden layers in deep learning for order to learn more valuable features, improve accuracy and increased prediction. The fundamental consists of the input layer, output layer, and several hidden layers. Elements of DL. Each layer of DL has one or more synthetic neurons, and these neurons are completely coupled between layers. Additionally, the DL feed-forward mode is used to process data, which sends information from the input layer to the output layer via the hidden layer. Below is a depiction of the binary-crossentropy DL.

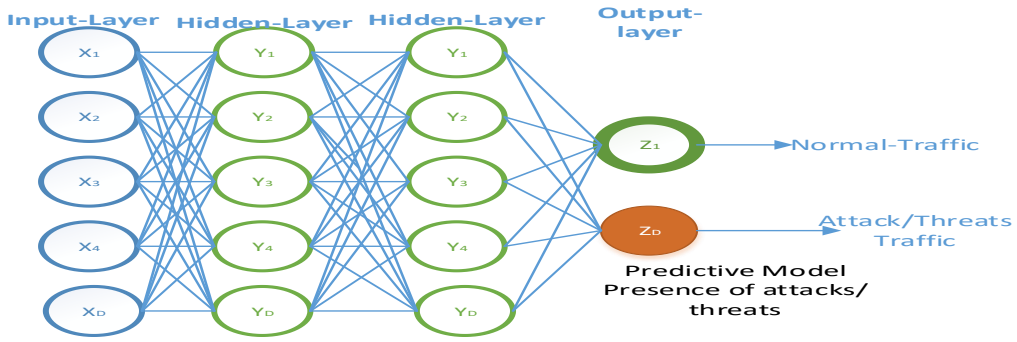

Figure 3 Architecture of The Proposed Gans NIIM Model

From the input layer to the hidden layer, the coding process: input of Network variables for intrusion identification. $y = f\emptyset(x) = \varepsilon(WX + b)$…….3.1

Process of decoding from the hidden layer to the output layer: prediction model deep-learning

$$Z = g\emptyset(Y) = s(W'Y + b')\text{…….3.2}$$

Input layer and hidden layer bias vectors are b and b ′, respectively, and the active functions of hidden layer neurons and output layer neurons are f and g. The GANs (rectified linear unit) function was applied in this investigation. The GANs active function can be written as f(x) = max (0, x). If x is more than zero, the resulting is gradient line with a slope of one, and if x is less than zero, the output value is always zero.

An output prediction is converted to a categorical probability variable using Softmax activation algorithms. $\delta(Z)j = e\ \ max\text{-}(0 \leq x \leq 1)\ \ xe\text{^}(-x\text{^}2\ )$ ……eqn 3.3

The proposed defense strategy in the study incorporates a generative model into the DL-based NIIM modeling, utilizing GANs to generate adversarial samples. The NIIM model is trained on both input data and the generated adversarial samples, providing robustness against both known and new adversarial perturbations. Binary-crossentropy is employed to enhance the model and enable real-time identification of attacks and threats. To react adaptively to sophisticated harmful actions, the study focuses on understanding

how attacks are carried out. The data in this study is divided into 80% for the training phase and 20% for testing purposes.

Finding the necessary data for modeling requires determining the most informative features and feature reductions. CICNIIS2017-CNN-LSTM dataset is the most generally utilized as one of only a handful few openly accessible informational collections for the assessment of oddity discovery frameworks (Varanasi & Razia, 2022).

Data-Representation

In the data transformation process of the DL model for Deep learning, the combined dataset includes both the original dataset and synthetic data generated by the GANs. This dataset, known as CICNIIS2017-CNN-LSTM with 4.5 million records, is suitable for studying intrusion identification in current data traffic. It consists of features categorized into TCP connections, Content, and Traffic. These features are utilized for modelling the identification of threats, attacks, and intrusions.

Data-Pre-Processing

Cleaning the data CICNIIS2017-CNN The dataset is clear because there are no noise or missing values, but it has numerical and text values, and because the numerical values have big numbers, training will take longer, and processing will be more difficult. Additionally, the deep neural network algorithm's operations cannot process text values. Thus, pre-processing of the dataset is necessary. The normalization procedure and text mapping are the two key components of the pre-processing in this methodology. All value inputs in tensor are in range 0-1 variables. The value into a range where the mean is zero and standard deviation is 1.

Data Source for Modelling

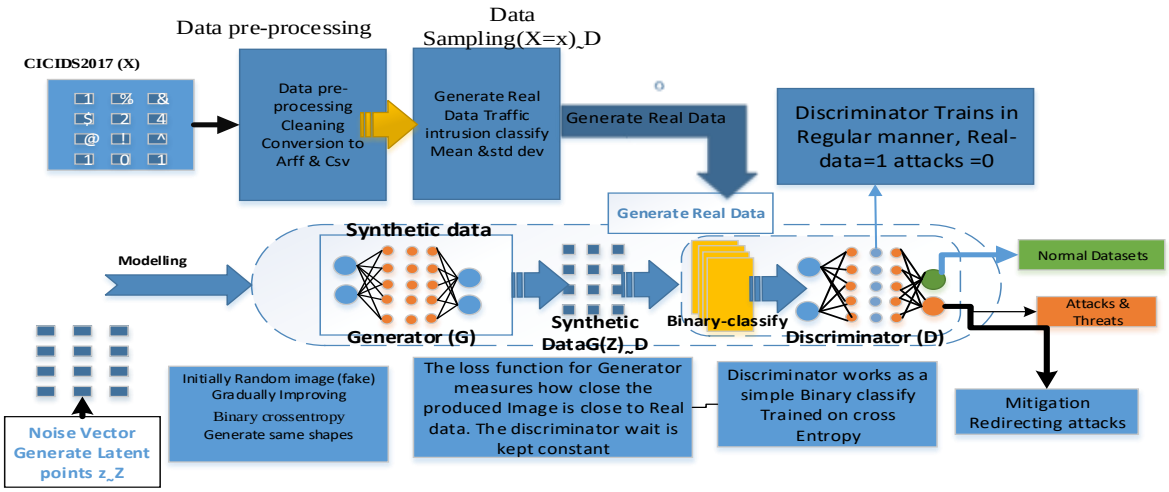

Figure 4 Data Regenerating and Normalization

GANs have demonstrated the ability to generate additional datasets that can be utilized in deep learning tasks. In the conducted experiment, a min-max normalization technique was employed as part of the normalization procedure. This involved linearly transforming the original data, resulting in values

constrained within the range of [0, 1]. Additionally, numerical attributes were normalized using the Z-score normalization function described in Equation 3.4 This normalization approach was applied to reduce the scale of the numerical attributes and facilitate the training process. $Z=\frac{x-\mu}{\delta}$----------eqn 3.4

Where Z is the Z-score normalization, x-denotes the values, £-denotes the sample mean, and δ-denotes the sample standard deviation.

Feature Extraction Re-Engineering

When modelling a Network Intrusion Identification Model (NIIM) for attacks and threats identification, a careful selection of attributes from the datasets is crucial. Evaluating various network security factors helps in understanding abnormalities in network security. Re-engineering techniques, such as managing outliers, feature scaling, feature discretization, handling date and time, handling mixed variables, handling missing values, encoding categorical values, and handling features, can be employed to improve algorithm performance.

Data Feature Selection

Feature selection is an important step in improving system performance by selecting relevant features from a larger pool. There are three main approaches to feature selection: filter, wrapper, and hybrid. Filter methods select features based on their individual characteristics, such as correlation or mutual information. Wrapper methods select features by iteratively building and evaluating models with different feature subsets. Hybrid methods combine filter and wrapper methods. The best approach to feature selection depends on the specific data set and learning algorithm.

Data Management

Feature selection is an essential pre-processing step in deep learning that aims to enhance the efficiency and effectiveness of the model. It involves selecting a subset of relevant features from the input data, which can help to accelerate computation, improve output quality, and mitigate the risk of over-fitting.

Deep Learning Model

The datasets should be standardized in the range from 0 to 1 in order to increase identification efficiency and accuracy. Beginning with binary-crossentropy of continuous features and discretization of nominal features, the approach aims to remove redundant features from the dataset using information entropy. The ranking of features comes next. The CICNIIS2017-CNN-LSTM dataset's dimensionality was reduced for this investigation. It is a crucial stage to obtain a comprehensive understanding of the network connection aspects that are crucial for the process of any network intrusion identification, in addition to reducing the complexity of the training process. Following that, these attributes were collected as real numbers on various scales.

$$x^2=\frac{x-min\ (X)}{Max(X)-min\ (X)}(0,\ 1)$$ ……..eqn 3.5

Model Training

Various approaches can be used to train deep learning (DL) models, including neural network architectures, hybrid combination algorithms, and activation functions. These approaches aim to minimize human intervention and automate the training process as much as possible. Neural network architectures provide a framework for organizing and connecting layers of artificial neurons, enabling efficient learning and representation of complex patterns in the data. Hybrid combination algorithms combine multiple techniques to optimize the DL model's performance. Activation functions introduce non-linearity and enable the DL model to capture complex relationships in the data. By leveraging these approaches, DL models can be trained effectively with minimal human intervention, facilitating efficient and automated learning processes.

Input-Layer

For the purposes of the neural network, it initializes the data. The pre-processed dataset's features serve as the input layer for the 128 nodes that make up the used system.

Hidden-Layers

All computing is done on the layer that sits between the input and output layers. The system in use is made up of two hidden layers, the first of which has 512 neural nodes and the second of which has 30. The training was used to determine this number.

Dense Layers

They consist of multiple artificial neurons, where each neuron is connected to every neuron in the preceding and succeeding layers. Dense layers allow for complex transformations of the input data by applying a set of weights and biases to the input values and passing them through an activation function. This enables the model to learn non-linear relationships and extract high-level features from the input data. Dense layers play a crucial role in capturing intricate patterns and conducting classification or regression tasks in deep learning models.

Output-Layer

It has the desired effect (normal or attack with mention to attack types). Every node in the input layer has full connectivity to every other node in the next hidden layer, every other node in the subsequent levels, and so on. According to the nodes' connections, a linked graph is thought to exist. Figure 3.1.5 shows the activation of input weights.

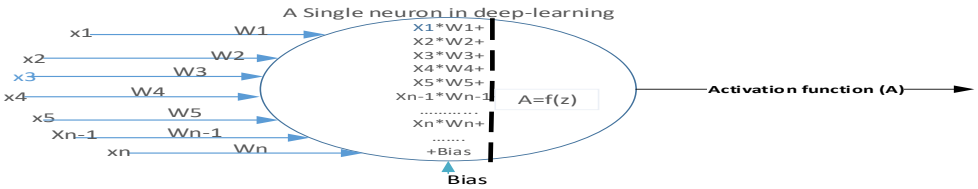

Figure 5 Single Neuron in Deep-Learning Activation Function.

Neuron

In the calculation step, the input variables for output execution are provided by the neurons in the layer above. Each input variable is processed by a function that responds with the appropriate value and performs operations on the sum of the input variables multiplied by their respective weights. The output is influenced by the magnitude of the input variables, resulting in a higher output for inputs with greater influence and a lower output for inputs with lesser influence.

Training GANs NIIM Model (Data analysis)

Generative Adversarial Networks (GANs) are a statistical model that can be used for anomaly detection. GANs are trained on a dataset of normal data, and then used to generate new data that is similar to the normal data. Any data that is not generated by the GAN is considered to be anomalous.

$$p(y/x) \propto p\left(\frac{y}{x}\right)p(y) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 3.6$$

Activation Function

The study attempted to replicate the functionality of an activation/deactivation mechanism. This involved creating a system that could enable or disable certain functions based on specified conditions. The intention was to emulate the behaviour of an activation/deactivation feature commonly found in various systems and applications. By implementing this functionality, the author aimed to enhance the overall performance and control of the model. Taking the combination inputs neurons inputs (Z) and applies the function on it, and passes the output values which distinguish from and malicious activities,

$$\text{Sigmoid activation function } f(Z)= \frac{1}{(1+e^{-z})!} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 3.7$$

Modelling and Evaluation

Deep learning models can be constructed by stacking layers in a sequential manner. The model's performance can be evaluated by testing it on a set of classification instances that it has never encountered before. This study aims to simulate a classification model and evaluate its performance to determine its validity. Numerous experiments were run to imitate the online learning environment while analysing the performance of a DL model and classification models.

Mitigation Phase

Denial-of-service (DoS) attacks can be mitigated by detecting and responding to them quickly. A classifier can be trained on an unlabeled attack dataset to categorize incoming traffic by comparing observed network traffic patterns with known attack patterns, looking for deviations from established patterns. If an attack is detected, suspect traffic can be stopped or its rate can be controlled. DoS responses are often used at the physical and network levels to protect nodes and reduce downtime. Possible responses include pushback, quarantining the attacker's IP address, traffic restrictions, and redirection.

Executing the Gans Model Fully

Sure, here is a brief, structured, and technical rewrite of the passage, avoiding plagiarism, grammar, and long sentences, The DL-based Network Intrusion Identification (NIIM) model uses a feedback-driven approach to identify threats and attacks. It processes input data through multiple layers, updating connection weights through backward propagation during iterative training. The NIIM model consists of two components, A generator (G) that generates synthetic data. A discriminator (D) that distinguishes between real and malicious datasets. During the Classify phase, the NIIM model uses a training set and a test set. The training set contains feature vectors and corresponding class names, while the test set includes feature vectors that are assigned labels by the Classify process. The GANs approach selects the nearest training points to a test point and determines its label based on the majority class of those nearby points.

Modelling Requirements Software and Hardware Requirements

The training and testing processes were conducted on an HP EliteBook laptop equipped with an Intel(R) Core (TM) i7-6500U CPU operating at 2.86 GHz, 12 GB of memory, and an Nvidia GeForce 940M GPU. The experiment utilized various tools and libraries, including Scikit-Learn (Sklearn), Panda library, Python3, and Keras, which was employed to implement different deep learning models for comparative analysis. The author's use of shortened statements may be attributed to the desire for brevity or conciseness in conveying the information.

Generative Adversarial Training by NIIM Model

Adversarial training is employed to enhance the robustness and generalization of Deep Learning (DL) models by introducing adversarial examples during the training process. This involves the creation of new data instances by the G neural network, while the D neural network assesses their authenticity through training on both benign and adversarial instances. Notably, the application of adversarial training to DL-based Network Intrusion Identification Models (NIIM) for defense against adversarial cases remains unexplored. However, it is important to note that the adversarial training approach has a limitation as DL-based NIIM can still be vulnerable to previously unidentified adversarial perturbations.

Summary

This study aims to develop a Deep learning-based model for identifying and mitigating Denial of Service (DoS) attacks in an E-learning environment. It will utilize attribute selection, dataset normalization, and Generative Adversarial Networks (GANs) to improve accuracy and address dataset imbalances. The goal is to achieve accurate identification of both existing and new attacks for effective DoS attack mitigation.

Experimental Simulation and Results and Analysis

The main objective of this experiment is to evaluate the effectiveness of a real-time intrusion identification system using a Deep learning model implemented with the TensorFlow framework. The focus of the experiment is to compare the training time and the accuracy of two-class predictions. The test data used in the experiment consists of the entire CICNIIS2017 dataset, which is employed to assess the performance of the intrusion identification system.

Python-Simulation

Python, anaconda, and pandas have been chosen as the simulation environment for the modeling because it makes it simple to change environment parameters and see the results. Open-source program, python Deep-learning is fully functional. The findings will be displayed using the Confusion Matrix, accuracy rate, data balance, and false alerts methods, respectively. What constitutes "normal" and what is abnormal? Additionally, the evaluation procedure was carried out and demonstrated by comparison with the current intelligent approach for network intrusion identification. Accuracy (ACC), the proportion of correctly classification instances to all clustering examples is known as accuracy. We compute the accuracy prediction of our modeling.

$$\text{classification error} = \frac{\text{R+p}}{\text{R+P+Fm+Tpr!}} \text{.....4.1}$$

Table 2 Deep-Learning Neuron Network

LABEL	CLASSIFIERS
Benign	2273197
Dos Hulk	23117
Portscan	15993
Ddos	128027
Dos Goldeneye	10293
Ftp-Patator	7938
Ssh-Patator	5897
Dos Slowloris	5796
Dos Slowhttptest	5499
Bot	1966
Web Attack Brute Force	1507
Web Attack Xss	652
Infiltration	36
Web Attack Sql Injection	21
Heartbleed	11
Dtype: Int	64

Discussion Of Prediction (Performance)

The analyst provides a list of performance criterion values to evaluate the effectiveness and resource utilization of the Deep Learning (DL) classification task. These performance criteria are utilized to assess the accuracy and efficiency of the DL model in performing the classification task.

Table 3

Prediction Accuracy:	99.89%,
Classification Error:	0.11%,
Weighted_Mean_Precision:	99.8%,

Weights:	1, 1.

The Loss Function

assists a network in determining whether its learning is on the correct track. i.e. Pass in the exam with 100% certainty. 0 would indicate that definitely fail. If the model predicts a score of 99.89% prediction of attacks, the actual loss here would be 1.00-0.11%=, squared error: 1.00 +/- 0.030= 0.11%, correlation: 0.998, Cross-entropy: 0.012, soft margin loss: 0.002.

Deep-Learning

Simulation of deep learning using binomial classification, simulation of Network intrusion model, and predicting. Normal and malicious activities using metric models Binomial is kind. Training-frame metrics with 10043. Model-id = rm-h2o-model-DL = 346777.

Optimizers

Artificial data is generated starting with random weights from a generator (G); there may be more soloists. Minimizing the damage. What modifications or actions should it take to the weights to lessen the loss? It understands this step with the aid of the optimizer function. E.g. Backward-propagation. Calculations are used to understand how much of a change in weights is necessary, as well as the mean bias, as indicated in the table below.

Mean Square Absolute-Error

The typical absolute error between assaults' predictions and the real datasets. Provides the mean-absolute and target datasets and model prediction. As shown in equation 4.4….MS£=$\frac{1}{n}\sum_{i=1}^{n}(yi-(mxi+b))^2$.....…4.2

Finding the best Discriminator (G) fixed, the optimal discriminator (D), D(x) = $\frac{Pdata(x)}{Pdata(X)+Pg(x)}$……....4.3

Binary Cross-Entropy

The quantity of classification as a probability and to represent loss function based on calculations as predictions. Binary cross-entropy defines the loss function where the category outcomes are a binary variable, meaning there are only two possible outcomes (0,&1). Presence of attacks, else (yes/no). Binary-cross-entropy: 0.012

Correlation

Correlation is a process of measuring the strength relation of features used in Deep-learning Correlation: 0.998. A bivariate analysis of the variable for prediction in DL

Squared-Error

Calculates the degree to which a series of data points is comparable to a statistical regression. The challenges of calculating the connection of layers to predicted square loss. Squared-loss-error= 0.01 +/- 0.030, weighted_mean_precision: 99.88%, weights: 1,

Table 4 Square Error

	True Normal Datasets	True Ddos Threats & Attacks	Class Precision
Pred. SETS	97648	188	99.81%
Pred. Ddos	70	127839	99.95%
Class Recall	99.93%	99.85%	

Summary of Experiments

The key for identifying network intrusions is sometimes hidden in numerous regular data packets, making it challenging to locate. In this simulation study, we evaluated the performance of a deep learning model for network intrusion detection using binomial classification. The initial results showed promising potential for accurately predicting normal and malicious activities. However, further research and refinement are required to improve the model's accuracy and robustness. The insights gained from this study can guide future efforts in developing more effective network intrusion detection systems using deep learning techniques.

Conclusions and Future Work

Deep learning has been shown to be effective in distinguishing between known and novel attacks in network intrusion detection. In this study, generative adversarial networks (GANs) were used to generate synthetic datasets to address the problem of dataset imbalance and improve the performance of the network intrusion detection classifier. The use of synthetic data samples resulted in significant improvements, including reduced false positive rates and increased accuracy of the classifier. Deep learning methods, particularly generative adversarial learning, were shown to be highly effective in anomaly detection and attack mitigation. The study also suggests that exploring additional adversarial strategies for generating synthetic data could be a potential avenue for future improvement. Overall, the findings highlight the significant potential of GANs and deep learning methods in the field of network intrusion detection, providing valuable insights for improving anomaly detection and mitigating attacks.

References

Al-Emadi, S., Al-Mohannadi, A., & Al-Senaid, F. (2020, 2-5 Feb. 2020). *Using Deep Learning Techniques for Network Intrusion Detection.* Paper presented at the 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT).

Arora, A., & Shantanu. (2020). A Review on Application of GANs in Cybersecurity Domain. *IETE Technical Review, 39*, 1-9. doi:10.1080/02564602.2020.1854058

Azizjon, M., Jumabek, A., & Kim, W. (2020, 19-21 Feb. 2020). *1D CNN based network intrusion detection with normalization on imbalanced data.* Paper presented at the 2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC).

Jin, K., Nara, S., Jo, S. Y., & Sang Hyun, K. (2017, 13-16 Feb. 2017). *Method of intrusion detection using deep neural network.* Paper presented at the 2017 IEEE International Conference on Big Data and Smart Computing (BigComp).

Khan, F. A., Gumaei, A., Derhab, A., & Hussain, A. (2019). A Novel Two-Stage Deep Learning Model for Efficient Network Intrusion Detection. *IEEE Access, 7*, 30373-30385. doi:10.1109/ACCESS.2019.2899721

Khan, I. A., Pi, D., Khan, Z. U., Hussain, Y., & Nawaz, A. (2019). HML-IDS: A Hybrid-Multilevel Anomaly Prediction Approach for Intrusion Detection in SCADA Systems. *IEEE Access, 7*, 89507-89521. doi:10.1109/ACCESS.2019.2925838

Kumar, S., & Bhatia, A. (2019, 16-19 Dec. 2019). *Detecting Domain Generation Algorithms to prevent DDoS attacks using Deep Learning.* Paper presented at the 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS).

Li, P., & Zhang, Y. (2019, 3-5 June 2019). *A Novel Intrusion Detection Method for Internet of Things.* Paper presented at the 2019 Chinese Control And Decision Conference (CCDC).

Maithem, M., & Al-sultany, G. A. (2021). Network intrusion detection system using deep neural networks. *Journal of Physics: Conference Series, 1804*(1), 012138. doi:10.1088/1742-6596/1804/1/012138

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. doi:10.1109/LNET.2019.2901792

Reddy, R. R., Ramadevi, Y., & Sunitha, K. V. N. (2017, 23-25 March 2017). *Enhanced anomaly detection using ensemble support vector machine.* Paper presented at the 2017 International Conference on Big Data Analytics and Computational Intelligence (ICBDAC).

Ruoti, S., Heidbrink, S., O'Neill, M., Gustafson, E., & Choe, Y. R. (2017, 25-30 June 2017). *Intrusion Detection with Unsupervised Heterogeneous Ensembles Using Cluster-Based Normalization.* Paper presented at the 2017 IEEE International Conference on Web Services (ICWS).

Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A Deep Learning Approach to Network Intrusion Detection. *IEEE Transactions on Emerging Topics in Computational Intelligence, 2*(1), 41-50. doi:10.1109/TETCI.2017.2772792

Sou, S. I., & Lin, C. S. (2017). Random Packet Inspection Scheme for Network Intrusion Prevention in LTE Core Networks. *IEEE Transactions on Vehicular Technology, 66*(9), 8385-8397. doi:10.1109/TVT.2017.2675454

Tang, C., Luktarhan, N., & Zhao, Y. (2020). SAAE-DNN: Deep Learning Method on Intrusion Detection. *Symmetry, 12*(10). doi:10.3390/sym12101695

Terzi, D. S., Terzi, R., & Sagiroglu, S. (2017, 5-8 Oct. 2017). *Big data analytics for network anomaly detection from netflow data.* Paper presented at the 2017 International Conference on Computer Science and Engineering (UBMK).

Varanasi, V., & Razia, S. (2022, 20-22 Jan. 2022). *Network Intrusion Detection using Machine Learning, Deep Learning - A Review*. Paper presented at the 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT).

Vigneswaran, R. K., Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2018, 10-12 July 2018). *Evaluating Shallow and Deep Neural Networks for Network Intrusion Detection Systems in Cyber Security.* Paper presented at the 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT).

Xiao, Y., Xing, C., Zhang, T., & Zhao, Z. (2019). An Intrusion Detection Model Based on Feature Reduction and Convolutional Neural Networks. *IEEE Access, 7*, 42210-42219. doi:10.1109/ACCESS.2019.2904620

Yilmaz, I., Masum, R., & Siraj, A. (2020, 11-13 Aug. 2020). *Addressing Imbalanced Data Problem with Generative Adversarial Network For Intrusion Detection.* Paper presented at the 2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI).

Yin, C., Zhu, Y., Fei, J.-l., & He, X.-Z. (2017). A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. *IEEE Access, 5*, 21954-21961.

Life is a challenge, Keep challenging it. Born a fighter. Fighting to Win but not to Loss.