Educational Administration: Theory and Practice
2023, 29(4), 1408 - 1414
ISSN: 2148-2403
https://kuey.net/

Research Article

An Improved Intrusion Detection System Utilizing Generative Adversarial Networks

Mr. B Pandu Ranga Raju[1*], K. Rohitha[2], K.V. Bhavana[3], M. Mahitha[4], M. Sweety[5]

[1*,2,3,4,5]Assistant Professor, Department of Artificial Intelligence and Data Science, Annamacharya Institute of Technology and Sciences (Autonomous), Rajampet, Andhra Pradesh, India-516126, *Email: balaraju.pandu@gmail.com, [2]Email: rohitha1603@gmail.com,[3]Email:kbhavana765@gmail.com,[4]Email:mahithareddy174@gmail.com,[5]Email: sweetymangala123@gmail.com

Citation: Mr. B Pandu Ranga Raju, et al (2023), An Improved Intrusion Detection System Utilizing Generative Adversarial Networks, *Educational Administration: Theory and Practice,* 29(4), 1408 – 1414,
Doi: 10.53555/kuey.v29i4.6399

ARTICLE INFO

ABSTRACT

In the present study an attempt has been made to investigate whether awareness towards Information and Communication Technology (ICT) is imparted among Higher Secondary School teachers by conducting research on data collected from different higher secondary schools in Tamil Nadu. During Covid pandemic, every school teachers working in Private, Government, management schools in one way or other way are forced to use the ICTs and practice online mode of delivery for teaching learning process in spite of their locality, availability of interrupted Net facilities etc. That is the motivational factor for conducting this investigation. The sample included 300 teachers (inclusive of 181 male and 119 female) randomly selected from different higher secondary schools in Tamil Nadu. The investigator himself developed a customized scale to measure the awareness on ICTs such as ETV, CD-ROM, Multimedia, Interne, EDUSAT in Arts and Science Education. The results of the presents study cleared indicate that both male and female teachers in higher secondary schools have the same level of awareness in ICTs. This study, aims to provide various possibilities to know the extent of the ICT facilities available in various educational institutions and to what extent they permit faculty members to utilize ICT for classroom Learning.

Keywords: Teaching learning process, ICT, Education, Higher secondary school, Teachers.

I INTRODUCTION

Big data is being produced at a rapid pace due to recent developments in information technology (IT) [1], as the amount of data with high dimensional characteristics grows exponentially across several areas. Consequently, handling high-dimensional data poses additional difficulties for the efficacy and efficiency of data processing. One of the most popular dimensionality reduction techniques for addressing these issues is feature selection (FS), which helps reduce the high dimensionality of large-scale data by selecting a small subset of relevant and significant features and removing irrelevant and redundant features in order to build efficient prediction models. The large and high-dimensional data [2] that we deal with nowadays has increased the amount of features in datasets, which has raised the computing cost. Feature selection is an efficient and an appropriate approach in preprocessing. "An Improved Intrusion Detection System Utilizing Generative Adversarial Networks[3] to Balance Network Intrusion Benchmark Datasets" provides a thorough overview of the crucial function intrusion detection systems (IDS) play in contemporary network security settings. With the increasing sophistication of cyberattacks and the expansion of digital systems, robust and trustworthy intrusion detection systems are becoming indispensable. Preset criteria or signatures are commonly used by conventional security systems that detect intrusions to identify malicious behavior; however, these techniques are not up to date with the constantly evolving computer risk scenario.

A notable obstacle to the advancement and assessment of intrusion detection systems is the scarcity of superior benchmark datasets. By providing the foundation for training and testing surveillance algorithms, these datasets enable researchers and industry professionals to assess the efficacy and viability of various detection methodologies. Unfortunately, a lot of the benchmark datasets that are currently available include flaws such class imbalances, which cause some forms of network intrusions to be underrepresented. This results in biased assessments and subpar performance from IDS models [4]. The paper suggests a unique

Copyright © 2023 by Author/s and Licensed by Kuey. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

strategy utilizing Generative Adversarial Networks (GANs) to overcome these drawbacks and improve the usefulness of benchmark datasets for IDS research. Synthetic data distributions that closely mirror real-world data distributions have been produced with remarkable efficacy using computational adversarial networks, or GANs.

Our objective is to use GANs to generate synthetic instances of network traffic data in order to rebalance metrics. This will improve the generality and durability of IDS models and lessen the effects of class imbalances. IDS research may benefit from using GANs for data augmentation and balancing in a number of ways. First off, it makes it possible for researchers to generate a wider variety of actual network traffic instances— including invasions and scenarios—than what may be seen in already published datasets. This diversity is essential for teaching intrusion detection systems (IDS) models to distinguish and identify different kinds of malicious activity [5], including both well-known and undiscovered threats. Our method enables more fair and representative assessments of IDS models by creating artificial data to rectify class disparities. This helps avoid models being overfit to certain classes or instances in the dataset, which is especially crucial for maintaining the validity and fairness of comparison research. Researchers may choose and optimize IDS strategies more intelligently when a more full and balanced picture of model performance is presented. The IDS development pipeline now has the ability to continuously learn from and react to changing cyber threats thanks to the incorporation of GAN-based data synthesis [6].

II LITERATURE SURVEY

The context of this work investigates the body of knowledge currently accessible on intrusion detection systems (IDS) and the challenges presented by benchmark datasets used in IDS research. Plenty of research studies have looked at various tactics and ways to increase alerting systems effectiveness and efficiency in locating and resolving network intrusions. These include conventional signature based approaches, anomaly detection techniques, and, more recently, neural networks and deep knowledge-based approaches [7]. A comprehensive analysis of the literature has led researchers to identify common shortcomings and limitations in the frameworks of current surveillance systems. These include their vulnerability to false positives, their incapacity to identify new threats, and their reliance on manually curated datasets that might not accurately represent network traffic in the real world. The function of benchmark datasets in IDS research and assessment is one of the literature survey's main areas of emphasis. Benchmark datasets are vital resources for IDS model training and testing because they offer standardized datasets that researchers can use to compare the effectiveness of various detection methods and algorithms. Unfortunately, many of the benchmark datasets that are now in use have a number of drawbacks, such as class imbalances, a lack of diversity in the sorts of intrusions [8] that are represented, and the incapacity to capture threats that are emerging. These flaws have the potential to seriously impair the generality and dependability of IDS models, resulting in skewed assessments and less-than-ideal results in practical situations. A shared platform for hybrid systems is being created by the convergence of IoT and virtual physical systems, as suggested by Shahriar et al. AI and CPS are enabling cyberattacks, which makes a computerized intrusion detection system training difficult.

This study proposes a GAN-based infiltration detection systems [9], which leverages fake samples generated during training. The model outperforms standalone IDS in attack detection and model stability during training, addressing issues with missing or imbalanced data. Huang et al.'s research presents a unique Imbalanced adversarial network as a means of addressing class imbalance in security detection. Lin et al. in order to create malicious traffic records for adversarial assaults, this study suggests using the IDSGAN framework [11] for generative adversarial networks. The model exhibits efficacy and resilience by preserving original attack features through the use of a generator, discriminator, and restricted modification mechanism. Shu et al. suggests a technique for assessing adversarial assaults on ML-based intrusion detection systems (IDS) that makes use of generative adversarial networks [12] and active learning. Bypassing the IDS model with a success rate of 98.86%, the approach becomes more resilient to similar attacks. Usama et al. propose an adversarial machine learning (ML) technique that uses generative adversarial networks to successfully elude adversarial perturbations, hence increasing theresilience of an ML-based [13] IDS that detects intrusions against them.

Using Generative Adversarial Networks to benchmark dataset-related IDS research problems. Because of its ability to generate artificial data that closely resembles real-world distributions, GANs have garnered a lot of interest recently. In order to improve the representativeness and usefulness of these datasets for training and assessing IDS models, researchers are utilizing GANs to supplement current benchmark datasets [14] and rectify class imbalances. Numerous research have shown how well GAN-based data synthesis works to improve IDS model performance, including lowering false positive rates, raising detection accuracy, and strengthening the models' resistance to new and unidentified threats. The future paths and the advantages of including GAN-based data synthesis into the pipeline for developing IDS. In addition to correcting class imbalances in benchmark datasets, GANs may be used to improve the diversity and realism of synthetic data, which can lead to more thorough training and assessment of IDS models. Furthermore, continuing studies are looking at more sophisticated GAN structures and methods for creating dynamic, adaptive synthetic data that may more accurately depict the ever- changing nature of network incursions. Researchers want to create more robust and efficient detection systems that can protect network infrastructures from a variety of cyberattacks by integrating these developments into IDS frameworks.

III DATA COLLECTION&PREPROCESSING

An essential part of setting up benchmark datasets for intrusion detection research is data gathering and preprocessing. The technique of gathering data for the NSLKDD dataset, a popular benchmark dataset in this field, entailed recording network traffic from a simulated environment that included both typical activities and other kinds of assaults. The dataset consists of several network connections, each of which is categorized according to one of many predefined kinds, including normal, user-to-root, denial disruption of service , and remote-to-local attacks. Notwithstanding its widespread use, the NSL-KDD dataset has several drawbacks, such as duplicate instances and class imbalances, which might impair the efficacy and capacity for generalization of intrusion detection models. Researchers have used a variety of preprocessing methods to solve these issues and raise the NSL-KDD dataset's quality.

To maintain consistency and comparability across several studies, these procedures usually entail filtering out duplicate or unnecessary information, balancing class distributions, and normalizing the data [15]. For example, feature selection techniques such as Principal Component Analysis or the analysis of correlation can be used to identify and eliminate duplicate characteristics that do not significantly improve the prediction ability of intrusion detection models. Resampling techniques such as oversampling or under sampling can also be used to balance the class distributions within the dataset, hence reducing the impact of class imbalances on model performance. Similarly, the UNSW-NB15 dataset, another well-liked benchmark dataset for intrusion detection research, underwent a comprehensive data collection and preparation process. The dataset was acquired by the capturing of network traffic in a regulated setting, encompassing both benign and malicious operations such as denial-of-service attacks, reconnaissance, and exploitation efforts. However, the UNSW-NB15 dataset has imbalances in classes and other irregularities similar to the NSL-KDD dataset that might affect the effectiveness of intrusion detection systems. Researchers have preprocessed the UNSW-NB15 dataset[16] using a variety of methods in an effort to address these problems.

These methods consist of class rebalancing, feature engineering, and data cleansing. Removing noise and superfluous characteristics from the dataset is known as data cleaning, and it guarantees that only pertinent information is kept for training and assessment. Raw network traffic data may be transformed or aggregated using feature engineering techniques to provide more interpretable representations, including statistical features or frequencybased metrics. Additionally, class rebalancing techniques like under sampling or oversampling may be used to correct class imbalances within the dataset, improving the performance of intrusion detection models on minority classes. The data collection and preparation phases are crucial to the creation of benchmark datasets for intrusion detection research, such as NSL-KDD and UNSW-NB15. Using a range of techniques to clean, transform, and balance the data, researchers may enhance the quality and use of these datasets. This makes evaluations of intrusion detection methods more accurate and reliable. Nonetheless, it is crucial to carefully assess how preprocessing choices may affect the features and representativeness of the dataset, as improper preprocessing techniques may add bias or distortions that negatively affect the validity of study findings.

IV PRINCIPLES AND METHODS

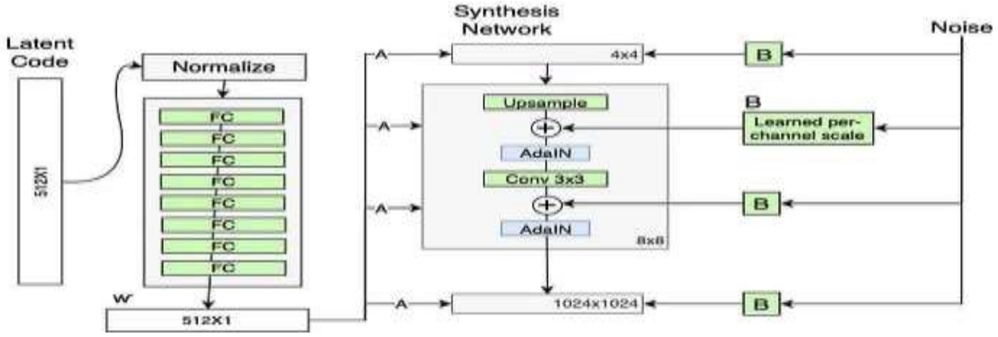

Fig.1 GAN Architecture

The paper offers a comprehensive approach to address class imbalances and dataset quality problems in intrusion detection benchmark datasets. The fundamental component of this methodology is the generation of synthetic data that closely mimics the distribution of real network traffic through the use of Generative Adversarial Networks
a well-liked deep learning technique. The project's objective is to use GANs to increase the representativeness and diversity of existing benchmark datasets, such as UNSW-NB15 and NSL-KDD. The GAN architecture (Fig.1) is composed of a generator network that generates synthetic data samples and a discriminator network that is trained to distinguish between real and synthetic data [17]. It is composed of many layers of neurons organized in a neural network architecture suitable for distinguishing between real and fake input,

just as the discriminator network. Backpropagation and gradient descent optimization are used to update the weights and biases of both the generator and discriminator networks during training in order to lower the generator's loss and raise the discriminator's accuracy. In addition, the study uses class rebalancing and feature engineering as preprocessing techniques to improve the quality of the benchmark datasets. By merging GAN-based data synthesis with traditional preprocessing approaches, the research intends to generate more realistic, balanced, and diverse datasets for the purpose of training and evaluating intrusion detection models. Through actual testing and assessment, the efficacy of the proposed approach is assessed, demonstrating its potential to enhance the robustness and performance of intrusion detection systems in detecting and mitigating network threats

A. GENERATIVE ADVERSARIAL NETWORKS ON NSL- KDD

Generative Adversarial Networks (GANs) are a class of deep learning architectures where two neural networks, the discriminator and the generator, compete against each other to produce realistic synthetic data in a fashion similar to a game. The generator network is in charge of producing data samples, while the discriminator network distinguishes real samples from artificial ones. During training, both networks are repeatedly optimized. The discriminator's capacity to distinguish between true and false data will improve as a result of the generator's creation of data that fools it into believing it to be true. As training progresses, the generator gets more adept at generating data that closely resembles real samples from the training dataset. Usually, the generator is made up of several layers of neurons arranged in a deep neural network design. Depending on the type of data being created, these layers might comprise convolutional layers, dense (completely connected) layers, and activation functions like sigmoid
[18] or ReLU (Rectified Linear Unit). Usually, a random noise vector taken from a latent space is fed into the generator, where it undergoes a number of nonlinear modifications to produce synthetic data samples.

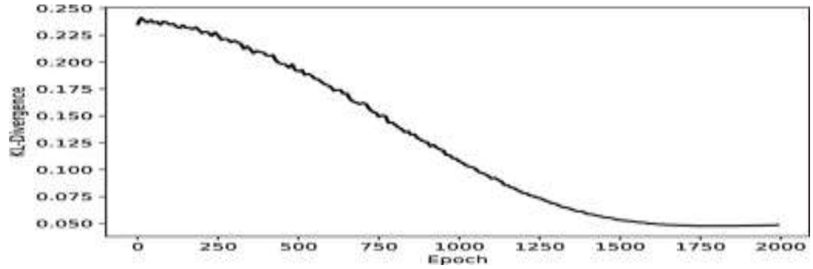

Fig.2 Divergence vs Epochs plots for NSL-KDD

The discriminator network has many layers of neurons, just as other neural network topologies. The discriminator receives samples of genuine or artificial input data, and it outputs a probability score (Fig. 2) that indicates how likely it is that the input sample is real. The discriminator's layers may include activation functions, convolutional layers, and dense layers, much like the generator's layers do. During training, the discriminator learns to distinguish between genuine and false data by adjusting its weights and biases via gradient descent optimization. Before training GANs on benchmark datasets such as NSL-KDD, researchers often preprocess the data to remove noise, standardize features, and balance class distributions. After the data preparation is complete, the GAN architecture is trained using the preprocessed dataset [19]. Real data samples from the training dataset are sent into the discriminator together with synthetic data samples generated by the generator network during training. The discriminator provides the generator with feedback on how to improve the generation process by learning to discriminate between real and synthetic samples. This adversarial training process is done iteratively until the discriminator and generator achieve a state of equilibrium where the generator produces realistic synthetic data that closely reflects the distribution of real data. Using a variety of assessment criteria, including the generator's loss function and the discriminator's accuracy, this monitors the GAN's performance throughout training. Plotting parameters like the discriminator's loss, generator's loss, and the distribution of actual and synthetic data samples over time is another way that researchers may look at how the GAN is learning. These graphs assist researchers in evaluating the caliber of the data produced and offer insights into the convergence behavior of the GAN. Through the use of GANs for training on benchmark datasets such as NSL-KDD and data synthesis, researchers hope to increase the diversity and resilience of intrusion detection systems. More realistic and diverse training data will be produced in order to do this.

B. GENERATIVE ADVERSARIAL NETWORKS ON UNSW-NB15

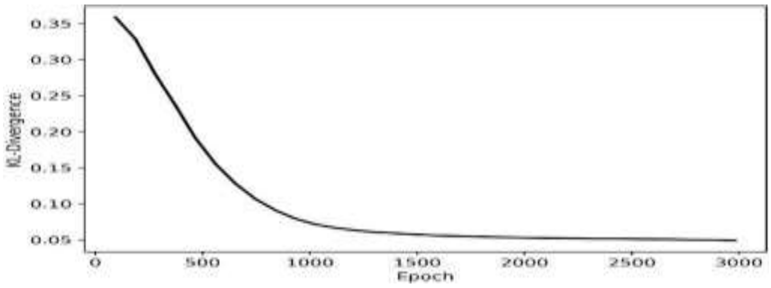

Fig.3 Divergence vs Epochs plots for UNSW-NB15

Within the Generative Adversarial Networks (GANs) family of deep learning architectures, there is rivalry between thediscriminator and generator neural networks for learning. Whereas the discriminator network discerns between actual and fake samples, the generator network creates synthetic data samples. The generator is usually a deep neural network structure consisting of several layers of neurons. Convolutional layers, thick (completely linked) layers, and activation functions like sigmoid or ReLU are examples of these layers [20]. Typically, the generator receives as input a random noise vector that is taken from a latent space and converted into synthetic data samples by nonlinear transformations. As with other neural network designs, the discriminator network consists of many layers. When using benchmark datasets like UNSW-NB15 for GAN training, researchers usually preprocess the data to balance class distributions, eliminate noise, and normalize features. The UNSW-NB15 dataset includes network traffic data that was collected in a controlled setting and includes malicious as well as legitimate activity.

The discriminator and generator neural networks in deep learning are in competition with one another within the Generative Adversarial Networks (GANs) family of architectures. The generator network generates synthetic data samples, whereas the discriminator network distinguishes between real and phony ones. Typically, the generator is a deep neural network structure made up of several neuronal layers. These layers include convolutional layers, thick (fully connected) layers, and activation functions such as sigmoid or ReLU [20]. Usually, the generator takes as input a random noise vector extracted from a latent space and applies nonlinear modifications to turn it into synthetic data samples. These graphs assist researchers in evaluating the caliber of the data produced and offer insights into the convergence behavior of the GAN. Through the use of GANs for training on benchmark datasets such as UNSW-NB15 and data synthesis, researchers hope to increase the diversity and resilience of intrusion detection systems. More realistic and diverse training data will be produced in order to do this.

V RESULTS

The results of training Generative Adversarial Networks (GANs) with benchmark datasets such as NSL-KDD and UNSW-NB15 are used to assess how effectively the proposed technique produces synthetic data that closely reflects the distribution of real-world network traffic. One of the main measures for assessing GAN efficacy is the discriminator network's accuracy in distinguishing between real and artificial data samples. The accuracy plot, which pertains to the NSL-KDD dataset, shows the discriminator's learning curve over time and demonstrates its capacity to discriminate between real network traffic and fake data generated by the GAN.

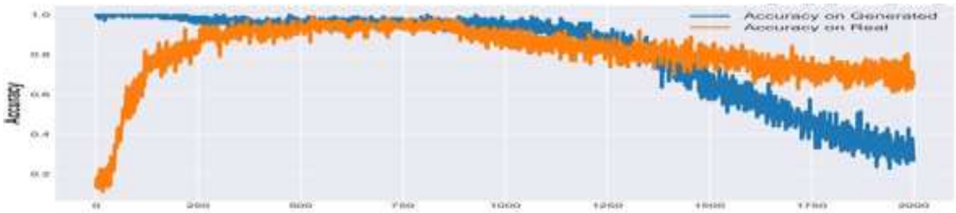

Fig.4 Accuracy plot for GAN model

Similarly, the UNSW-NB15 dataset's accuracy plot illuminates the discriminator's ability to discern between legitimate and fraudulent network traffic. In addition to discriminator accuracy, researchers may also examine performance metrics like as precision, recall, and F1-score to obtain a more comprehensive understanding of the GAN's capabilities (Fig. 4). These metrics help evaluate the discriminator's effectiveness in distinguishing between malicious and authentic network traffic. Precision-recall curves and confusion matrices can be used by researchers to assess the discriminator's effectiveness in accurately categorizing data samples across several classes and identify areas that require further development.

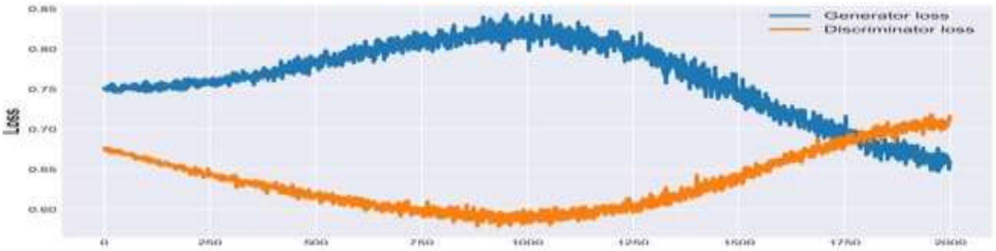

Fig.5 Loss plot for GAN model

The convergence of the GAN may be observed by plotting the loss functions of the generator and discriminator networks over time. The loss functions provide insight into how well the GAN is learning to trick the discriminator and generate synthetic data that seems realistic. They are frequently stated as a function of the quantity of training epochs, or iterations. By monitoring the discriminator's and generator's losses, researchers may follow the development of the adversarial training process and identify any issues like mode collapse or instability that may obstruct convergence (Fig.5). Along with accuracy and loss charts, it may analyze the distribution of real and synthetic data samples using techniques like kernel density estimation (KDE) or histograms. By contrasting the feature or attribute distributions of the generated data with those of the original dataset, researchers may assess the veracity and realism of the synthetic data created by the GAN. Discrepancies or outliers in the distributions may suggest that the GAN architecture has to be further tweaked or modified in particular places in order to improve the quality of the generated data.

The simulated data generated by the GAN may be evaluated statistically through the use of measures such as domain adaptation measurements and similarity scores. These metrics provide objective evaluations of the extent to which the GAN accurately represents the underlying data distribution by calculating the degree of similarity between the distributions of synthetic and real data samples. By comparing similarity scores between real and synthetic data samples across a variety of attributes or qualities, researchers may identify areas where the GAN could struggle to provide realistic data and devise solutions. An important factor in determining the efficacy and caliber of the synthetic data produced is the output of GAN training on benchmark datasets like NSL-KDD and UNSW- NB15. Through the examination of accuracy plots, loss functions, distribution visualizations, and quantitative metrics, scientists can acquire a deeper understanding of the effectiveness of GANs and pinpoint areas where the synthetic data can be made more realistic and authentic. This will ultimately boost the effectiveness of intrusion detection systems that have been trained on these datasets.

VI CONCLUSION

Improving the robustness and effectiveness of intrusion detection systems (IDS) through the use of Generative Adversarial Networks (GANs) on benchmark datasets such as NSL-KDD and UNSW-NB15 presents a feasible approach. GANs can resolve common problems with dataset quality and class imbalances by creating synthetic data that closely mimics the distribution of actual network traffic. This will improve the IDS models' functionality and ability to generalize. By merging GANs with traditional preprocessing techniques, researchers may offer more realistic, diverse, and well-balanced datasets for intrusion detection system training and assessment. The outcomes of training GANs on these benchmark datasets offer insightful information on the integrity and caliber of the GAN architecture, as well as its performance and convergence behavior. Additionally, through the examination of distribution visualizations, accuracy plots, loss functions, and quantitative indicators, researchers may evaluate how well the GAN technique generates synthetic data and pinpoint areas in need of additional improvement and optimization. In general, there is a lot of potential for enhancing the state-of-the-art in intrusion detection research and strengthening the resilience of network security infrastructures against a variety of cyber threats through the incorporation of GAN-based data synthesis into the IDS development pipeline.

REFERENCES

1. Hashem, Ibrahim Abaker Targio, et al. "The rise of “big data” on cloud computing: Review and open research issues." Information systems 47 (2015): 98-115.
2. Kogan, Jacob. Introduction to clustering large and high-dimensional data. Cambridge University Press, 2007.
3. Park, Cheolhee, et al. "An enhanced ai-based network intrusion detection system using generative adversarial networks." IEEE Internet of Things Journal 10.3 (2022): 2330-2345.
4. Lee, Wenke, and Salvatore J. Stolfo. "A framework for constructing features and models for intrusion detection systems." ACM transactions on Information and system security (TiSSEC) 3.4 (2000): 227-261.
5. Shrivastava, Gulshan, and Prabhat Kumar. "SensDroid: analysis for malicious activity risk of Android application." Multimedia Tools and Applications 78.24 (2019): 35713-35731.

6. Zhang, Hongbin, et al. "A novel MAS-GAN-based data synthesis method for object surface defect detection." Neurocomputing 499 (2022): 106-114.
7. Shinde, Pramila P., and Seema Shah. "A review of machine learning and deep learning applications." 2018 Fourth international conference on computing communication control and automation (ICCUBEA). IEEE, 2018.
8. Galar, Mikel, et al. "A review on ensembles for the class imbalance problem: bagging-, boosting-, and hybrid- based approaches." IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)42.4 (2011): 463-484.
9. Shahriar, Md Hasan, et al. "G-ids: Generative adversarial networks assisted intrusion detection system." *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 2020.
10. Huang, Shuokang, and Kai Lei. "IGAN-IDS: An imbalanced generative adversarial network towards intrusion detection system in ad-hoc networks." *Ad Hoc Networks* 105 (2020): 102177.
11. Lin, Zilong, Yong Shi, and Zhi Xue. "Idsgan: Generative adversarial networks for attack generation against intrusion detection." *Pacific-asia conference on knowledge discovery and data mining*. Cham: Springer International Publishing, 2022.
12. Shu, Dule, et al. "Generative adversarial attacks against intrusion detection systems using active learning."*Proceedings of the 2nd ACM workshop on wireless security and machine learning*. 2020.
13. Usama, Muhammad, et al. "Generative adversarial networks for launching and thwarting adversarial attacks on network intrusion detection systems." *2019 15th international wireless communications & mobile computing conference (IWCMC)*. IEEE, 2019.