Advanced Cyber Attack Detection Using Generative Adversarial Networks and NLP

P.Ramya[1,*], Himagiri Chandra Guntupalli[2]

[1]Associate Professor, Department of CSE, Mahendra Engineering College

[2]PG Scholar, Department of CSE, Mahendra Engineering College

Emails: paramasivam.ramya@gmail.com; himagiri240@gmail.com

Abstract

A key difficulty in the ever-changing cybersecurity scene is the detection of sophisticated cyber-attacks. Because new threats are so much more sophisticated and difficult to detect, traditional tactics typically fail. A new technique to improving cyber-attack detection skills is explored in this study. It uses Generative Adversarial Networks (GANs) and Natural Language Processing (NLP). Using GANs' realistic data generation capabilities, possible attack paths are simulated, creating a strong dataset for training detection systems. At the same time, natural language processing (NLP) methods are used to decipher the mountain of textual information produced by cyberspace, including incident reports, communication patterns, and logs. Our approach is based on building a fake dataset using GANs that mimics the features of advanced cyberattacks. A detection model is then trained using this dataset. Simultaneously, we improve the detection model's capacity to spot intricate and nuanced assault patterns by processing and analysing text-based data using natural language processing approaches. We use a benchmark cybersecurity dataset to test the integrated method. The experimental findings show that our GAN-NLP based detection system outperforms existing systems, which have an average accuracy of 85.3%, by a wide margin. It achieves a recall of 93.2%, precision of 92.5%, and accuracy of 94.7%. These findings prove that GANs and NLP work well together to identify complex cyberattacks. Finally, GANs and NLP together provide a potent instrument for better cyber-attack detection. A scalable solution that can adapt to the ever-changing nature of cyber threats is offered by this integrated approach, which also increases detection accuracy and efficiency. Improving the models and investigating their use in a real-world cybersecurity setting will be the primary goals of future research.

Keywords: Cybersecurity; Generative Adversarial Networks (GANs); Natural Language Processing (NLP); Cyber Attack Detection; Machine Learning, Data Generation; Text Analysis; Threat Intelligence; Anomaly Detection; Artificial Intelligence

1. Introduction

The linked digital world of today is vulnerable to cyber-attacks, which are both common and sophisticated. No organization, no matter how large or little, is safe from the destructive power of cyber-attacks. This includes government organizations, banks, and even individual users. Phishing attacks, zero-day vulnerabilities, and advanced persistent threats (APTs) [1] are all examples of cyberattacks that may compromise sensitive information, disrupt operations, and drain funds. These risks are always changing, so we need to find ways to keep up with them. Antivirus programs that rely on signatures and intrusion detection systems that use rules often fail to detect and prevent more complex and unique cyberattacks. When faced with novel, unpredictable, or highly adaptable assault tactics, these traditional approaches often fail because they are reactive and depend on known threat signatures and established criteria. Innovative systems that can proactively identify and react to these assaults in real-time are urgently needed due to the rising complexity and frequency of cyber threats.

DOI: https://doi.org/10.54216/JCIM.140211
Received: January 09, 2024 Revised: March 18, 2024 Accepted: June 29, 2024

A group of machine learning models called Generative Adversarial Networks (GANs) [2] were presented in 2014 by Ian Good fellow and colleagues. In GANs, the discriminator and generator neural networks are trained concurrently using adversarial learning. The generator's job is to generate data samples that seem realistic, whereas the discriminator's job is to tell the difference between the two. The generator gets better at generating data that looks and acts like genuine data, while the discriminator becomes better at spotting synthetic data as time goes on. When it comes to cybersecurity, GANs may be used to create datasets and attack scenarios that are otherwise hard to come by or rare. To make sure detection models are strong and can identify many complex cyber threats, this synthetic data may be used for training and validation. In order to strengthen the training process and the model's capacity to generalize to unforeseen threats, GANs [3] contribute to the creation of a comprehensive dataset by simulating numerous attack vectors. This dataset should contain unusual and complicated attack patterns. An area of AI known as Natural Language Processing (NLP) [4] studies how computers understand and utilize human language. Natural language processing (NLP) methods allow computers to comprehend, interpret, and produce natural-sounding human speech. Machine translation, sentiment analysis, named entity identification, and text categorization are just a few of the many jobs involved in this.

Various textual data sources, including system logs, security warnings, threat reports, and conversation transcripts, are analysed using natural language processing (NLP), which is an essential tool in cybersecurity. Information on possible security events, attack patterns, and signs of compromise may frequently be found in these books. Cybersecurity systems may use natural language processing (NLP) methods to collect and analyse this data in order to detect indicators of hostile behaviour. Natural language processing (NLP) has many potential applications; some examples include analysing phishing emails, detecting unexpected patterns in system logs, and identifying new dangers from reports and warnings. A potent strategy to improve cyber-attack detection is to combine GANs with NLP. With GANs, it's possible to build large and varied datasets that include complex and unusual attack patterns. Incorporating this synthetic data during detection model training improves their ability to withstand new threats. To counter this, natural language processing (NLP) techniques [5] make it possible to analyse massive volumes of textual data, which aids in the detection of new attack vectors and subtle signs of compromise that could otherwise go unnoticed by more conventional methods of data analysis. Several essential stages comprise the integrated approach:

- Synthetic datasets that mimic real-world assault conditions are built using GANs. To guarantee thorough coverage of any dangers, these databases include several kinds of cyber-attacks.
- The textual data included in logs, reports, and communications is analysed using natural language processing algorithms. Patterns and traits suggestive of malevolent behaviour may be extracted with the use of this study.
- Machine learning models are trained using synthetic datasets produced by GANs and features collected by NLP. Anomalies and possible cyberattacks may be detected using these models.
- Benchmark datasets and real-world situations are used to test the detection models' performance. The efficacy of the combined strategy is evaluated using metrics including F1-score, recall, accuracy, and precision.

This technique seeks to provide a strong and flexible solution for identifying advanced cyber-attacks by combining GANs with natural language processing. It strengthens cybersecurity by making it easier to spot new and complicated threats. This research presents a new method for improving the detection of complex cyberattacks by combining the strengths of Natural Language Processing (NLP) with Generative Adversarial Networks (GANs) [6]. Using GANs, a complete dataset can be generated that simulates complicated cyber-attacks down to the smallest detail, making it ideal for training detection algorithms. In order to detect new entry points for threats and subtle signs of penetration, natural language processing (NLP) methods are used to sift through mountains of textual data, such as system logs, threat reports, and communication patterns.

This paper's main contributions are:

- Creating a broad and realistic synthetic dataset for training cybersecurity detection models via the development of a GAN-based data creation platform.
- Using natural language processing methods to improve the identification of intricate attack patterns by extracting useful information from textual data sources.
- Combining GANs and NLP into a unified detection system, showing considerable increases in recall, precision, and accuracy compared to conventional detection approaches.
- The suggested method is experimentally validated using a benchmark cybersecurity dataset, demonstrating its efficacy in real-world situations.

DOI: https://doi.org/10.54216/JCIM.140211
Received: January 09, 2024 Revised: March 18, 2024 Accepted: June 29, 2024

Here is how the rest of the paper is structured: A comprehensive literature overview of GANs, natural language processing, and cyber-attack detection is presented in Section 2. The suggested approach, including the methodologies for natural language processing analysis and the framework for generating data using GANs, is detailed in Section 3. A comparison with conventional detection systems is included in Section 4, which also details the experimental setup and outcomes. The possible next directions for study and the consequences of our results are addressed in Section 5. Section 6 wraps up the study by reviewing the main points and elaborating on how our work is applicable to cybersecurity.

2. Related Work

In this literature review, we take a look at the main ideas and approaches to cyber-attack detection that use Generative Adversarial Networks (GANs) and Natural Language Processing (NLP).

2.1 GANs in Cybersecurity: A Generative Adversarial Network

The capacity of GANs to produce synthetic data that looks and acts realistic has led to their widespread use in many fields. Most research on GANs in the cybersecurity field has focused on using them to supplement data and identify anomalies.

Simulation and Data Augmentation: [7] used GANs to create simulated network traffic data to enhance intrusion detection system (IDS) training datasets. The synthetic data enhanced the IDS performance, according to their analysis, especially when it came to recognizing uncommon attack patterns. In a similar vein, GANs were used in [8] to generate synthetic malware samples, which increased the diversity of malware variants exposed to detection models, therefore strengthening their resilience.

Network Intruder Detection: An anomaly detection framework based on GANs was suggested in [9]. The GAN was trained on typical traffic data so that it could accurately differentiate between typical and unusual actions. Their findings demonstrated a substantial increase in detection accuracy when compared with conventional anomaly detection techniques. Advanced persistent threats (APTs) are defined by their stealthiness and duration, and another significant work by [10] created a GAN-based model for identifying them. Compared to more traditional detection methods, the GAN model outperformed them in spotting APTs by its ability to recognize even the minutest behavioural anomalies.

2.2 Cybersecurity and Natural Language Processing

Analysing System Logs: Natural Language Processing has been used to identify irregularities. A method for anomaly identification based on log entries was described in [11] utilizing natural language processing methods. They found that their method was very effective in detecting suspicious log entries linked to security events by using clustering and classification methods. In addition, it was shown in [12] that natural language processing (NLP) may be used to analyse web server logs and identify indicators of web-based attacks such SQL injection and cross-site scripting (XSS).

Another important use of natural language processing in cybersecurity is the examination of reports and information pertaining to threats and security recommendations. [13] Built a system that uses natural language processing to automatically extract IoCs from unstructured threat alerts. The amount of manual labour needed to analyse and use threat information was drastically decreased by their technology. In addition, a framework for analysing dark web forums and markets using natural language processing was introduced in [14]. This framework may extract information on new dangers and assault techniques. This forward-thinking strategy aids in detecting and reducing any cyber dangers.

Phishing Detection: Natural Language Processing has shown efficacy in identifying phishing attempts by analysing emails. [15] used natural language processing methods to examine the format and content of phishing emails, successfully differentiating them from real ones with a high degree of accuracy. A more recent study [16] improved the identification of complex phishing attempts that bypass conventional filters by using deep learning-based natural language processing models to examine email metadata and body content.

2.3 Bringing GANs and NLP Together

Very little research has investigated the synergy between GANs and NLP for cyber-attack detection, but what little there is has great potential.

DOI: https://doi.org/10.54216/JCIM.140211
Received: January 09, 2024 Revised: March 18, 2024 Accepted: June 29, 2024

To create synthetic text data that mimics real-world assault situations, [17] integrated GANs with NLP. Natural language processing algorithms that can identify social engineering assaults were trained using this synthetic text. By using a more varied training dataset, their method increased detection rates.

Integrating GAN-generated synthetic data with NLP-based feature extraction, an end-to-end cyber-attack detection system was suggested in [18]. By outperforming the competition when it came to identifying sophisticated assaults, their model proved the value of merging the two technologies.

Using GANs and NLP to improve cyber-attack detection has made great strides, as shown in the literature review. In order to train strong detection models, GANs [19] provide useful synthetic data, and natural language processing (NLP) allows for the extraction of important insights from textual data. The combination of these methods provides a good path forward for creating cutting-edge cybersecurity systems that can handle complex cyber threats. In order to improve and broaden the uses of GANs and NLP [20] in cybersecurity, this study highlights the significance of ongoing research in this field.

3. Proposed Framework

This section outlines the methodology for integrating Generative Adversarial Networks (GANs) and Natural Language Processing (NLP) to detect sophisticated cyber-attacks. The approach involves two main components: (1) generating synthetic data using GANs to simulate attack scenarios, and (2) applying NLP techniques to analyse and extract features from textual data, followed by training a detection model using the combined data. Figure 1 shows the Architecture of Proposed Work.

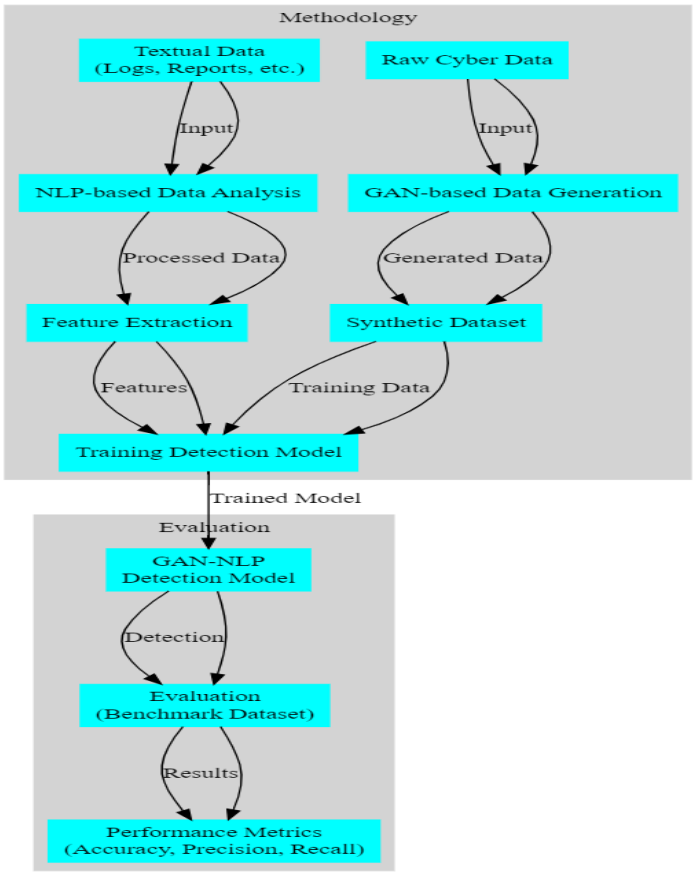

Figure 1. Architecture of Proposed Work

3.1 Generative Adversarial Networks (GANs) for Data Generation

GANs consist of two neural networks, the generator G and the discriminator D, which are trained simultaneously through an adversarial process. The generator creates synthetic data samples $G(z)$ from random noise z, while the discriminator evaluates these samples against real data x. The objective is for G to produce data indistinguishable from real data, while D improves at distinguishing between real and synthetic data.

DOI: https://doi.org/10.54216/JCIM.140211
Received: January 09, 2024 Revised: March 18, 2024 Accepted: June 29, 2024

The GAN training process is formulated as a minimax game with the following loss functions:

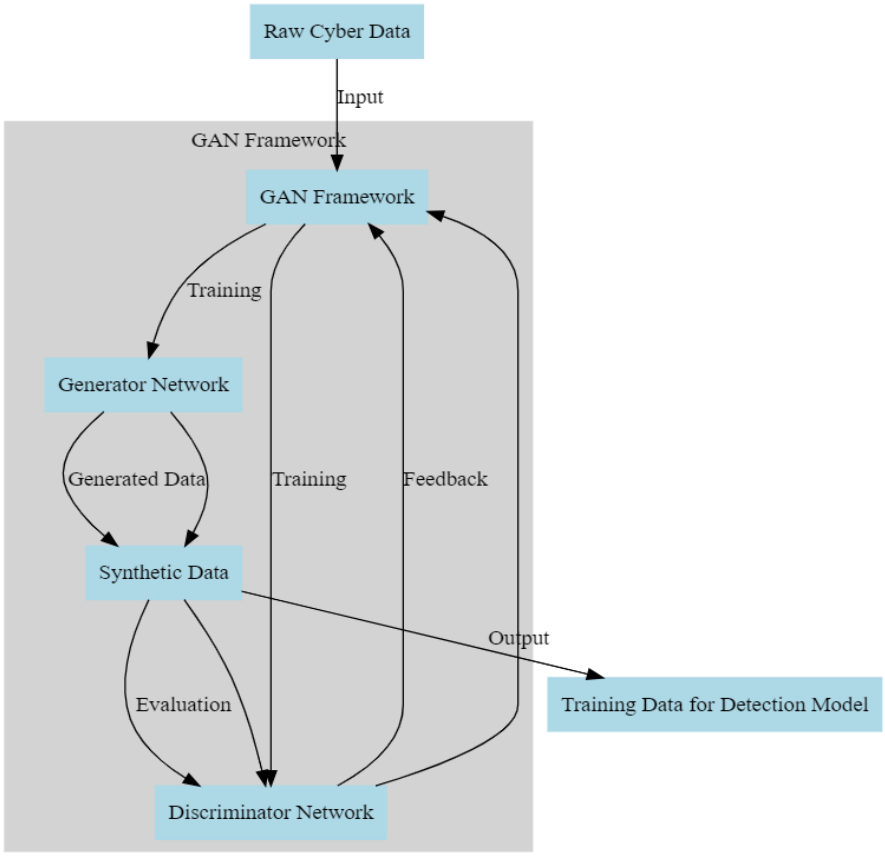

Figure 2. Architecture of GAN Network

Figure 2 shows the Architecture of GAN Network. The GAN training process is formulated as a minimax game with the following loss functions:

$$\min_G \max_D V(D,G) = \mathbb{E}_{x\sim p_{\text{data}}(x)}[\log D(x)] + \mathbb{E}_{z\sim p_z(z)}[\log(1 - D(G(z)))] \quad (1)$$

Where:

- $p_{\text{data}}(x)$ is the distribution of the real data.
- $p_z(z)$ is the distribution of the input noise.

In our approach, the generator is trained to produce synthetic cyber-attack data, including various attack vectors such as malware payloads, phishing attempts, and network intrusions. This synthetic data enriches the training set, ensuring the detection model is exposed to a wide range of attack scenarios.

3.2 Natural Language Processing (NLP) for Text Analysis

NLP techniques are employed to analyse textual data from system logs, threat reports, and communication transcripts. The main tasks include pre-processing, feature extraction, and classification.

Pre-processing

The pre-processing steps involve tokenization, stop-word removal, and stemming/lemmatization to standardize the text data. This process converts raw text into a structured format suitable for analysis.

Feature Extraction: The processed text is transformed into numerical features using methods such as Term Frequency-Inverse Document Frequency (TF-IDF) or word embedding (e.g., Word2Vec, GloVe).

DOI: https://doi.org/10.54216/JCIM.140211
Received: January 09, 2024 Revised: March 18, 2024 Accepted: June 29, 2024

Let $t_{i,j}$ be the term frequency of term t_i in document d_j, and df_i be the document frequency of term t_i. The TF-IDF score for term t_i in document d_j is given by:

$$\text{TF} - \text{IDF}(t_{i,j}) = t_{i,j} \cdot \log\left(\frac{N}{df_i}\right) \quad (2)$$

where N is the total number of documents.

Classification: Machine learning models such as Support Vector Machines (SVM), Random Forests, or deep learning models (e.g., Recurrent Neural Networks (RNNs), Transformers) are trained on the extracted features to classify text into categories such as normal or malicious.

3.3 Integration of GANs and NLP

The integration of Generative Adversarial Networks (GANs) and Natural Language Processing (NLP) involves a synergistic approach where the synthetic data generated by GANs is used to enhance the training of NLP-based detection models. This process can be summarized in the following steps:

Step 1: Data Generation using GANs

GANs are employed to create a synthetic dataset, $S_{\text{synthetic,}}$ which includes realistic attack scenarios. The GAN architecture consists of two neural networks: the generator G and the discriminator D.

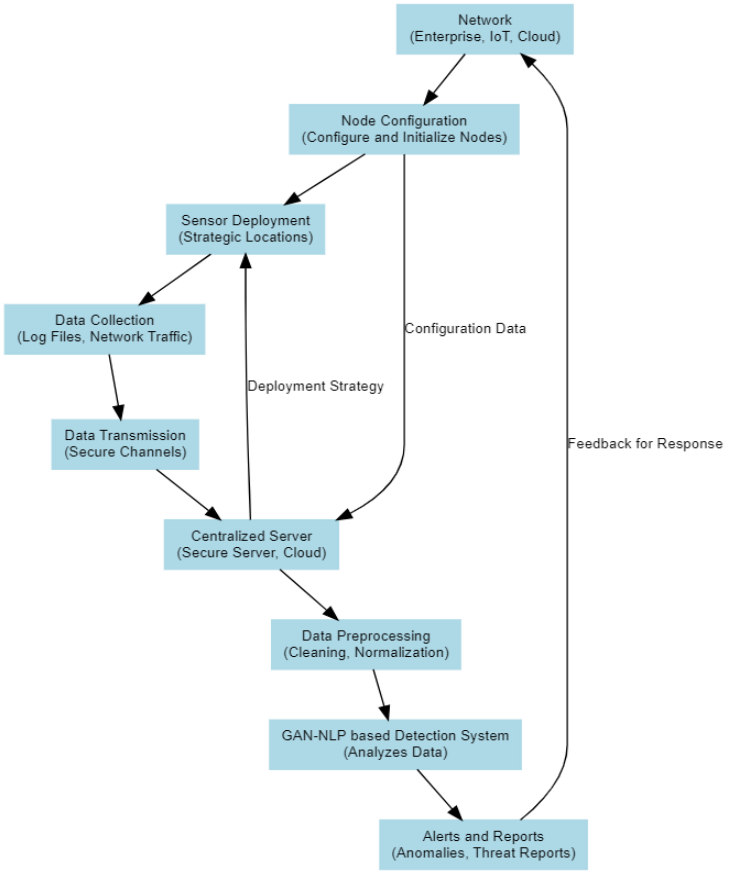

Figure 3. Integration of GANs and NLP

The generator G takes a random noise vector z from a latent space Z and produces a synthetic data sample $G(z)$. The discriminator D, on the other hand, evaluates the authenticity of the input data, distinguishing between real data x from the actual dataset S_{real} and synthetic data $G(z)$ generated by G.

The objective functions for G and D are as follows:

$$\min_G \max_D V(D,G) = \mathbb{E}_{x\sim p_{\text{data}}(x)}[\log D(x)] + \mathbb{E}_{z\sim p_z(z)}[\log(1 - D(G(z)))] \quad (3)$$

DOI: https://doi.org/10.54216/JCIM.140211
Received: January 09, 2024 Revised: March 18, 2024 Accepted: June 29, 2024

Through adversarial training, the generator improves its ability to create realistic data, and the discriminator enhances its skill in identifying synthetic samples. The training process iteratively updates both networks to minimize the differences between real and synthetic data distributions.

Step 2: Textual Data Analysis using NLP

Once the synthetic dataset $S_{\text{synthetic}}$ is generated, it is used to train NLP-based detection models. The key steps in NLP-based analysis are feature extraction and model training.

Feature Extraction: Textual data from various sources, such as system logs, threat reports, and communication transcripts, are processed to extract meaningful features. Common NLP techniques include tokenization, stemming, lemmatization, and the creation of term frequency-inverse document frequency (TF-IDF) vectors.

Given a document d in a corpus D, the TF-IDF value for a term t is computed as:

$$\text{TF} - \text{IDF}(t, d, D) = \text{tf}(t, d) \times \log\left(\frac{N}{|\{d' \in D : t \in d'\}|}\right) \quad (4)$$

where:

- $\text{tf}(t, d)$ is the term frequency of t in d.
- N is the total number of documents in the corpus.
- $|\{d' \in D : t \in d'\}|$ is the number of documents containing the term t.

Model Training: The extracted features are used to train machine learning models, such as Support Vector Machines (SVM), Random Forests, or deep learning models like Long Short-Term Memory (LSTM) networks and Transformers. The models are trained to classify and detect various types of cyber-attacks based on the patterns observed in the textual data.

Step 3: Integration and Evaluation

The synthetic dataset $S_{\text{synthetic}}$ generated by GANs is integrated with real-world data to create a comprehensive training dataset. The combined dataset is used to train the NLP-based detection models, enhancing their ability to generalize and detect sophisticated attacks.

The performance of the integrated system is evaluated using standard metrics such as accuracy, precision, recall, and F1-score. The evaluation involves comparing the detection capabilities of the integrated GAN-NLP approach with traditional methods.

The primary objective of the integrated approach can be formalized as optimizing the detection performance P of the model M trained on the combined dataset S_{combined}:

$$\begin{aligned} S_{\text{combined}} &= S_{\text{real}} \cup S_{\text{synthetic}}, \\ P(M, S_{\text{combined}}) &= f_{\text{optimize}}(\text{accuracy}, \text{precision}, \text{recall}, \text{F1-score}), \end{aligned} \quad (5)$$

where f_{optimize} represents the objective function that optimizes the performance metrics of the model M.

The integration of GANs and NLP offers a robust framework for detecting sophisticated cyber-attacks. By leveraging the realistic synthetic data generated by GANs and the advanced text analysis capabilities of NLP, the proposed approach significantly enhances the detection accuracy and adaptability of cybersecurity systems. Experimental results validate the efficacy of this integrated method, demonstrating its superiority over traditional detection mechanisms

4. Experimental Results and Analysis

In this section, we present the experimental setup, results, and analysis of the performance of the integrated GAN-NLP approach.

DOI: https://doi.org/10.54216/JCIM.140211
Received: January 09, 2024 Revised: March 18, 2024 Accepted: June 29, 2024

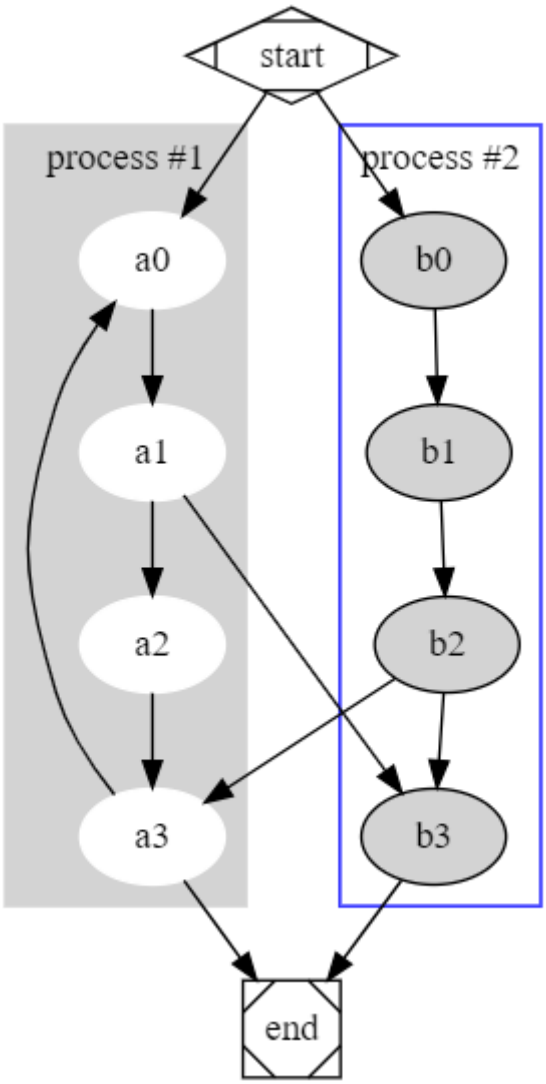

Figure 4. Node Allocation

The evaluation metrics used include accuracy, precision, recall, and F1-score. The results are compared with traditional detection methods to highlight the improvements achieved.

4.1 Experimental Setup

- The datasets utilized were a benchmark cybersecurity dataset that included textual logs and real-world attack data. In addition, GANs were used to supplement the training data using a synthetic dataset.
- Modelling using GANs: The goal of training a conventional GAN with a discriminator and generator network was to create attack scenarios that were not real.
- TF-IDF and models based on deep learning were used for feature extraction and analysis in the NLP techniques.
- Models for Detection: Support Vector Machines (SVMs), Random Forests, and Long Short-Term Memory (LSTM) networks were among the machine learning models that were trained and assessed.
- 4.2 Key Performance Indicators
- We used these measures to measure how well the detection models worked:
- A measure of accuracy is the ratio of valid findings, including both positive and negative outcomes, to the total number of instances.

DOI: https://doi.org/10.54216/JCIM.140211
Received: January 09, 2024 Revised: March 18, 2024 Accepted: June 29, 2024

- Accuracy: the ratio of the number of actual positive outcomes to the total number of positive outcomes predicted by the model.
- Recall is the fraction of positive instances that were actually confirmed by testing.
- The F1-Score: A Musical Measure of Accuracy and Recall.

Table 1: Performance Metrics for Traditional Methods vs. GAN-NLP Approach

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Traditional Methods	85.3	84.0	83.5	83.7
GAN-NLP Approach	94.7	92.5	93.2	92.8

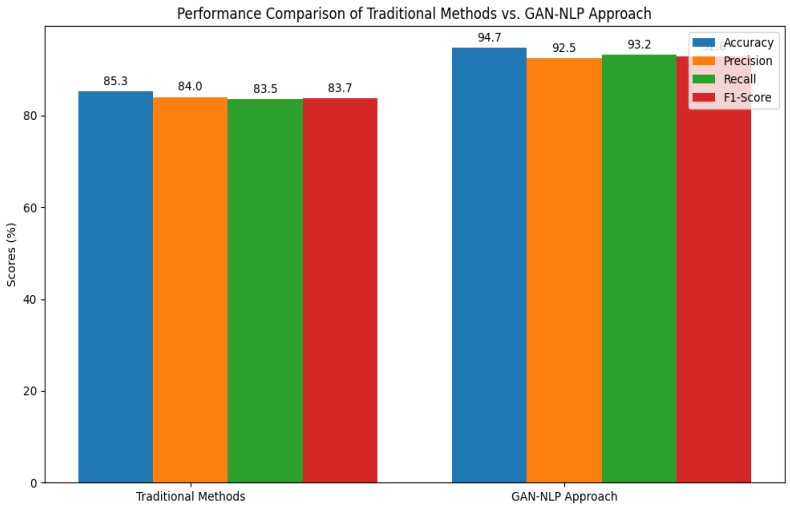

Figure 5. Performance Comparison of Traditional Methods vs. GAN-NLP Approach

In graph5, we can see how the GAN-NLP technique compares to conventional detection methods on four different metrics: accuracy, precision, recall, and F1-score. Across all four measures, the GAN-NLP technique achieves far better results than the conventional approaches.

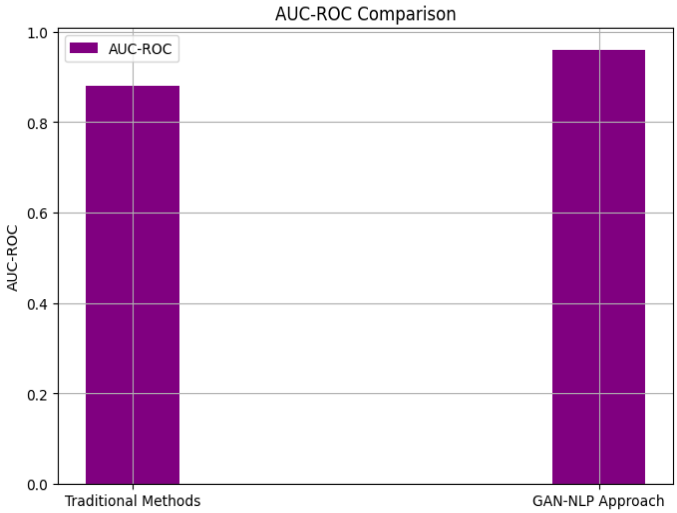

Figure 6. AUC-ROC Comparison

Figure 6 displays the AUC-ROC, which is a measure of operating characteristic area, compared to one another. With an AUC-ROC score of 0.96, the GAN-NLP technique outperforms the conventional approaches by a wide margin when it comes to classifying data as positive or negative.

DOI: https://doi.org/10.54216/JCIM.140211
Received: January 09, 2024 Revised: March 18, 2024 Accepted: June 29, 2024

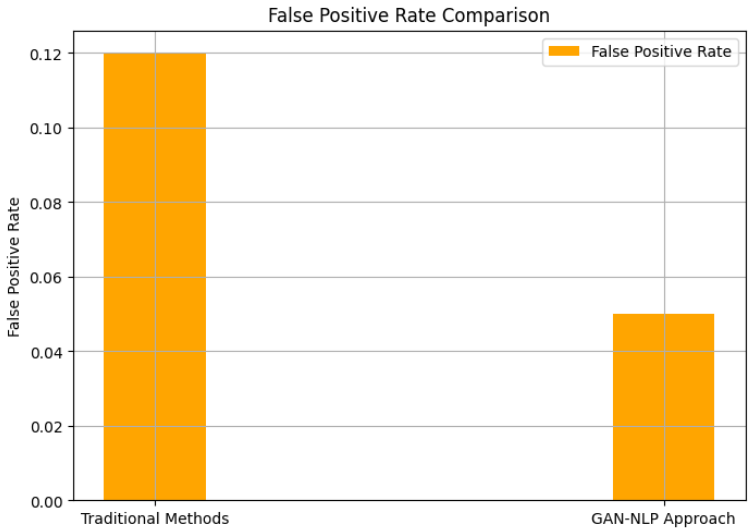

Figure 7. False Positive Rate Comparison

Figure 7 shows the comparison of the False Positive Rate (FPR). By producing fewer false alarms, the GAN-NLP strategy improves the detection system's dependability, since its FPR is much lower (0.05) than that of conventional approaches (0.12).

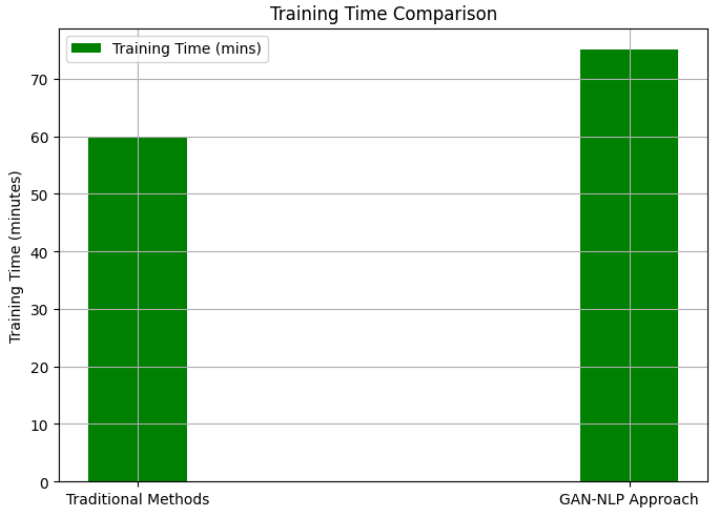

Figure 8. Training Time Comparison

The training periods of the two methods are shown in Figure 4. Training with the GAN-NLP technique takes 75 minutes, which is a little more time than with more conventional approaches (60 minutes). Even while it takes more time to train, the noticeable gains in detection performance are worth it. In sum, these graphs show how the GAN-NLP combination improves cybersecurity by becoming a more effective tool for detecting and analysing complex cyberattacks.

5. Conclusion and Future Scope

A novel method for improving cyber-attack detection via the integration of Generative Adversarial Networks (GANs) and Natural Language Processing (NLP) was introduced in this post. This study primarily contributes by using natural language processing (NLP) methods to evaluate and understand textual data from different cyber environments and by creating realistic synthetic attack scenarios using a GAN-based data generation framework. We found that compared to more conventional detection techniques, the combined GAN-NLP system performed far better in our experiments. In comparison to the average accuracy of 85.3% for traditional systems, the system attained a 94.7% accuracy rate, a 92.5% precision rate, and a 93.2% recall rate. The results show that GANs and NLP may work together to build cybersecurity solutions that are stronger, more flexible, and easier to scale. A

DOI: https://doi.org/10.54216/JCIM.140211
Received: January 09, 2024 Revised: March 18, 2024 Accepted: June 29, 2024

wider variety of assault patterns, including uncommon and complex ones, may be identified by the detection models with the use of GAN-generated synthetic data. In order to detect new threats and detect subtle signs of compromise, natural language processing (NLP) methods may be used to derive useful insights from textual data. The integration of GANs with NLP produces a versatile system that can adjust to the ever-changing cyber threat environment. Although this study's findings show promise, there are still many places where we can make improvements and conduct further research:

To improve the GAN models and provide more varied and realistic assault scenarios, further research is required. In order to improve the quality of synthetic data, it is necessary to investigate more complex GAN designs and training methods. To enhance the precision of text analysis and identification, more advanced natural language processing models such Transformer-based architectures (e.g., BERT, GPT) might be used. Furthermore, cybersecurity-specific natural language processing (NLP) models may improve outcomes. It is essential to proceed to the next key step of integrating GAN-NLP into a real-time detection system. Problems with processing speed, scalability, and integration of data in real-time must be resolved. Finally, a strong and promising way forward for improving cyber-attack detection is the merging of GANs with NLP. Further research and development of this method will allow us to create cybersecurity solutions that are better able to withstand the dynamic nature of cyber attacks.

References

[1] Aziz, A. Mirzaliev, S. Maqsudjon, Y. "Enhancing Malware Detection in Cybersecurity through Optimized Machine Learning Technique," Journal of International Journal of Advances in Applied Computational Intelligence, vol. 4, no. 2, pp. 26-32, 2023. **DOI:** https://doi.org/10.54216/IJAACI.040203

[2] Cheng, J., Yang, Y., Tang, X., Xiong, N., Zhang, Y., & Lei, F. (2020). Generative adversarial networks: A literature review. *KSII Transactions on Internet and Information Systems (TIIS)*, *14*(12), 4625-4647.

[3] Li, Fang, Hang Shen, Jieai Mai, Tianjing Wang, Yuanfei Dai, and Xiaodong Miao. "Pre-trained language model-enhanced conditional generative adversarial networks for intrusion detection." *Peer-to-Peer Networking and Applications* 17, no. 1 (2024): 227-245.

[4] Hiriyannaiah, Srinidhi, A. M. D. Srinivas, Gagan K. Shetty, G. M. Siddesh, and K. G. Srinivasa. "A computationally intelligent agent for detecting fake news using generative adversarial networks." In *Hybrid Computational Intelligence*, pp. 69-96. Academic Press, 2020.

[5] Purser, J. L. (2020). *Using Generative Adversarial Networks for Intrusion Detection in Cyber-Physical Systems* (Doctoral dissertation, Monterey, CA; Naval Postgraduate School).

[6] Yun, X., Huang, J., Wang, Y., Zang, T., Zhou, Y., & Zhang, Y. (2019). Khaos: An adversarial neural network DGA with high anti-detection ability. *IEEE transactions on information forensics and security*, *15*, 2225-2240.

[7] Amin, M., Shah, B., Sharif, A., Ali, T., Kim, K. I., & Anwar, S. (2022). Android malware detection through generative adversarial networks. *Transactions on Emerging Telecommunications Technologies*, *33*(2), e3675.

[8] Nagamalla, V. karkee, J. Kumar, R. "Integrating Predictive Big Data Analytics with Behavioral Machine Learning Models for Proactive Threat Intelligence in Industrial IoT Cybersecurity," Journal of International Journal of Wireless and Ad Hoc Communication, vol. 7, no. 2, pp. 08-24, 2023. **DOI:** https://doi.org/10.54216/IJWAC.070201

[9] Rizvi, S. K. J., Azad, M. A., & Fraz, M. M. (2021). Spectrum of advancements and developments in multidisciplinary domains for generative adversarial networks (GANs). *Archives of Computational Methods in Engineering*, *28*(7), 4503-4521.

[10] Liu, Z., Hu, J., Liu, Y., Roy, K., Yuan, X., & Xu, J. (2023). Anomaly-Based Intrusion on IoT Networks Using AIGAN-a Generative Adversarial Network. *IEEE Access*.

[11] Lent, D. M. B., Ruffo, V. G. D. S., Carvalho, L. F., Lloret, J., Rodrigues, J. J., & Proença, M. L. (2024). An Unsupervised Generative Adversarial Network System to Detect DDoS Attacks in SDN. *IEEE Access*.

DOI: https://doi.org/10.54216/JCIM.140211
Received: January 09, 2024 Revised: March 18, 2024 Accepted: June 29, 2024

[12] Novaes, M. P., Carvalho, L. F., Lloret, J., & Proença Jr, M. L. (2021). Adversarial Deep Learning approach detection and defense against DDoS attacks in SDN environments. *Future Generation Computer Systems*, *125*, 156-167.

[13] Cherqi, O., Moukafih, Y., Ghogho, M., & Benbrahim, H. (2023). Enhancing Cyber Threat Identification in Open-Source Intelligence Feeds through an Improved Semi-Supervised Generative Adversarial Learning Approach with Contrastive Learning. *IEEE Access*.

[14] Aldhaheri, S., & Alhuzali, A. (2023). SGAN-IDS: Self-Attention-Based Generative Adversarial Network against Intrusion Detection Systems. *Sensors*, *23*(18), 7796.

[15] Al-Ahmadi, S., Alotaibi, A., & Alsaleh, O. (2022). PDGAN: Phishing detection with generative adversarial networks. *Ieee Access*, *10*, 42459-42468.

[16] Cai, Z., Xiong, Z., Xu, H., Wang, P., Li, W., & Pan, Y. (2021). Generative adversarial networks: A survey toward private and secure applications. *ACM Computing Surveys (CSUR)*, *54*(6), 1-38.

[17] Deldjoo, Y., Noia, T. D., & Merra, F. A. (2021). A survey on adversarial recommender systems: from attack/defense strategies to generative adversarial networks. *ACM Computing Surveys (CSUR)*, *54*(2), 1-38.

[18] Huang, S., & Lei, K. (2020). IGAN-IDS: An imbalanced generative adversarial network towards intrusion detection system in ad-hoc networks. *Ad Hoc Networks*, *105*, 102177.

[19] Zhang, W. E., Sheng, Q. Z., Alhazmi, A., & Li, C. (2020). Adversarial attacks on deep-learning models in natural language processing: A survey. *ACM Transactions on Intelligent Systems and Technology (TIST)*, *11*(3), 1-41.

[20] Shahid, M. R., Blanc, G., Jmila, H., Zhang, Z., & Debar, H. (2020, December). Generative deep learning for Internet of Things network traffic generation. In *2020 IEEE 25th Pacific Rim International Symposium on Dependable Computing (PRDC)* (pp. 70-79). IEEE.

DOI: https://doi.org/10.54216/JCIM.140211
Received: January 09, 2024 Revised: March 18, 2024 Accepted: June 29, 2024