International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN: 2147-6799 www.ijisae.org Original Research Paper

Intelligent Model Using CGAN and RL for Efficient Contextual Dataset Generation

Dr. Mouneshachari S.[1*], Latharani T. R.[2]

Submitted: 13/05/2024 **Revised:** 25/06/2024 **Accepted:** 08/07/2024

Abstract – Recent advances in machine learning have demonstrated the effectiveness of Conditional Generative Adversarial Network (CGAN) and Reinforcement Learning (RL) techniques in a variety of domains, from image synthesis to decision-making tasks. However, their integration and application to the generation of contextual datasets remains under explored. This paper proposes a novel approach to combine CGAN and RL to increase dataset accuracy in specific context domains. The proposed methodology focuses on using CGANs to generate synthetic data that closely mimic real-world contextual variations corresponding to Advanced Persistent Threat (APT) attacks. By adapting the generator to contextual variables such as environmental conditions or attacker behavior, the generated data are more closely aligned to the target distribution, improving model robustness and generalization. In addition, RL techniques are used to iteratively refine the generated data samples, leading the generator to produce samples that not only adhere to the desired context, but also match the specific objectives of the proposed work. The main contributions of this work include the development of a unified framework that seamlessly integrates CGAN and RL for generating contextual datasets to strengthen Deep Learning Models. The proposed algorithms have been implemented using python programming language along with APIs. Experimental results demonstrate significant improvements in accuracy and reliability compared to traditional dataset augmentation methods.

Index Terms – CGAN, Reinforcement Learning, APT attacks, Dataset generation.

1. Introduction

In recent years, the fields of Generative Adversarial Networks (GAN) and Reinforcement Learning (RL) have seen significant progress in generating synthetic data and improving model accuracy [1]. However, both approaches have their strengths and limitations. GANs excel at generating realistic data distributions by training a generator network against a discriminator network in an adversarial setting [2]. On the other hand, RL focuses on learning optimal policies through trial-and-error interactions with the environment, which often leads to improved decision-making capabilities. APT attacks are predominantly hazardous in cyberspace and occur in six different phases[3].

The change in phases depends on the behavioral changes of the attacker. Mitigation of these attacks needs the context based dataset and it can be achieved through the continuous updation of the dataset as and when new behavior identified. The proposed paper is trying to integrate RL approach with CGAN model to generate data samples based on exceptional behavior of the attacker by supporting conventional computing environment. The CGAN model adopts RNN classifier at the discriminator modules for labeling the generated samples.

The integration of these two techniques, especially in the context of dataset generation, represents a promising avenue for increasing the accuracy and generalization of machine learning models. This integration aims to leverage the strengths of CGANs in generating diverse and realistic data samples and reinforcement learning techniques in directing the generation process to more relevant and contextually appropriate data points.

2. Related Work

The related work emphasizes and deals with the following topics to study the developments taken place in each section.

- APT Attacks
- CGAN
- Reinforcement Learning

2.1. APT Attacks

APT attacks are low-slow attacks characterized by their stealth, persistence and multi-stage nature, aiming to achieve long-term access and achieve strategic objectives such as espionage, sabotage or intellectual property theft. Detecting and mitigating APT attacks requires a

*1*Professor and Head, Department of Computer Science and Engineering, Jain Institute of Technology, Davangere*
Affiliated to Visvesvaraya Technological University, Belagavi, India
2Ph.D. Scholar, Department of Computer Science and Engineering, Jain Institute of Technology, Davangere
Affiliated to Visvesvaraya Technological University, Belagavi, India

comprehensive approach that includes robust cybersecurity defences, continuous monitoring, threat intelligence, and incident response preparedness [4]. The review [3] has examined findings from 49 contemporary studies on threat modelling in cybersecurity, offering a comprehensive analysis of current methodologies and their respective strengths and limitations. The review reveals a consensus across the papers that, while automation plays a role in various stages of the threat modelling process, the overall approach remains predominantly manual. Finally concluded the need of a strong approach to model threats on strategic, tactical, operational and technical intelligence, specific to an organisation's environment.

2.2. CGAN

As dual-network architectures make GANs computationally demanding, the paper [5] explores various hardware solutions intended to accelerate GANs. Because training both the generator and discriminator networks simultaneously requires a large amount of computing power, accelerating GANs entails increasing the speed and efficiency of both training and execution. This is particularly crucial for intricate or large-scale models. It looks at GPU, FPGA, and ASIC performance, emphasizing the benefits of specialized technologies for GAN training and inference such as FPGAs and ASICs. In addition, the survey looks at cutting-edge technologies like neuromorphic and quantum computing, highlighting the necessity for constant innovation in hardware design to keep up with GANs' growing complexity and maximize speed, energy efficiency, and scalability. CGANs have revolutionized generative modeling since their debut, finding applications in text-to-image synthesis and data augmentation. Future studies could concentrate on enhancing CGAN stability, GAN architectures [6], investigating new conditioning methods, and integrating them with other deep learning techniques [7]. Author [8] has tried 3LIDS-CGAN, a three-layered approach for IoT threat detection integrates Conditional Generative Adversarial Networks (CGAN). Support Vector Machines and Golden Eagle Optimization for traffic classification, signature and anomaly-based methods for threat identification, and CGAN for adversarial attack detection are employed. Using long short-term memory networks (LSTM networks) and historical seismic data, the study [9] models earthquake trends. LSTM surpasses Feed Forward Neural Networks (FFNN) by 59\% in prediction accuracy, effectively capturing temporal dependencies.

2.3. Reinforcement Learning

Reinforcement Learning techniques are used to create synthetic datasets that emulate real-world cybersecurity scenarios. These datasets are crucial for training and evaluating security models, especially when real data is scarce or involves privacy concerns [10]. RL can be used to generate datasets that help in developing adaptive security policies by continuously learning and updating security measures based on evolving threats [11]. The study [12] shows that Deep Reinforcement Learning (DRL) can enhance real-time decision making in Security Information and Event Management (SIEM) systems. Unlike traditional machine learning, DRL adapts to evolving threats without prior training, significantly boosting responses to security alerts.

3. Porposed Methodology

Figure 1 depicts the approach followed for the contextual based dataset generation using the fusion of CGAN and Reinforcement Techniques.

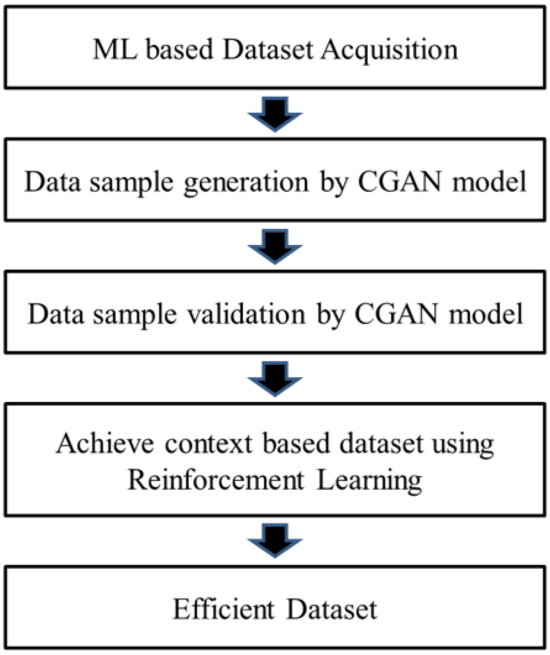

ML based Dataset Acquisition
Data sample generation by CGAN model
Data sample validation by CGAN model
Achieve context based dataset using Reinforcement Learning
Efficient Dataset

Figure 1 Methodology for contextual based dataset generation through the fusion of CGAN and RL models

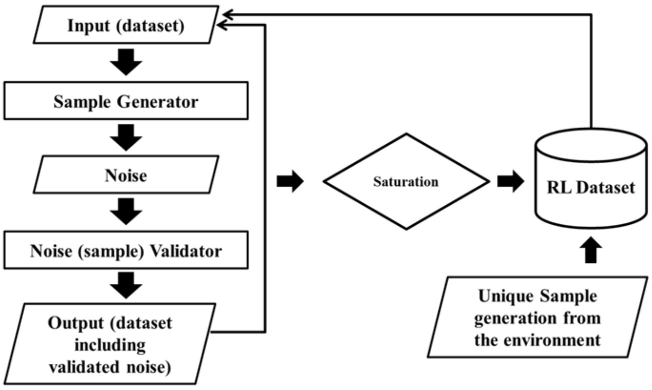

Input (dataset)
Sample Generator
Noise
Noise (sample) Validator
Output (dataset including validated noise)
Saturation
RL Dataset
Unique Sample generation from the environment

Figure 2 Reinforcement Learning integrated to CGAN model

3.1. ML based dataset acquisition

Many datasets are made available by various national and international agencies namely IEEE, UVC and so on. The notable dataset which is considered in this paper is SCVIC-APT-2021 [13]. SCVIC-APT-2021 is a machine learning based dataset on APT attacks through KALI Linux. Two domains were created in the environment by considering one of the machines from the domain as a target to attack for credentials. VPN is used to interconnect two domains. APT has six stages of attacking process namely reconnaissance, initial compromise, lateral movement, pivoting, data exfiltration, and post-attack stage. SCVIC-APT-2021 dataset has been made available with labels for each sample.

The dataset consisting of 84 attributes including the labels of the transaction samples. Also 56487 and 259120 samples are present in testing and training files respectively.

3.2. Data sample generation by CGAN

CGAN demonstrates the generation of the samples based on labels. The labeled dataset (trained) has been utilized to generate additional samples (noise generation) to increase the efficiency of the classification model. The architecture of the generator module is designed using Algorithm 1.

Algorithm 1: *Generation of noise using minimum and maximum distance approach*

```
• Consider D as dataset, m number of attributes and n number similar labeled samples
• For i from 1 to m (number of attributes)
    ▪ For j from 1 to n-1
        o mindistance[i]=min(distance(D[i][j], D[i][j+1]))
        o maxdistance[i]=max(distance(D[i][j], D[i][j+1]))
• For k from 1 to m
    ▪ For r from 1 to n
        o Addnewsample(D[r] + mindistance[r])
        o Addnewsample(D[r] - mindistance[r])
        o Addnewsample(D[r] + maxdistance[r])
        o Addnewsample(D[r] - maxdistance[r])
• Noise dataset D increased to n*4 samples
```

GAN acceleration among conventional architectures is bit challenging [14]. To overcome such issues and to support the conventional architectures Algorithm 1 has been designed. Algorithm 1 demonstrates the Generation of noise using minimum and maximum distances between the values of the attributes among all the samples present in the initial dataset. Algorithm 1 can ensure in increasing four times higher than the existing samples. Furthermore, it has a potential to enhance CGAN models efficiency.

3.3. Data sample validation by CGAN

The data samples generated through Algorithm 1 and the original data samples are fed to discriminator for sample validation. Recurrent Neural Networks (RNNs) are well suitable for textual dataset for classifications [15][16]. The proposed model has adopted ReLU activation function to figure out the proper labels during classification process. Each generated sample from the generated module is fed to discriminator for labelling.

The labelled sample is fed back to generator input to generate new sample. The process continues till it reaches saturation point. The saturation point indicates the maximum samples generation corresponding to the current context.

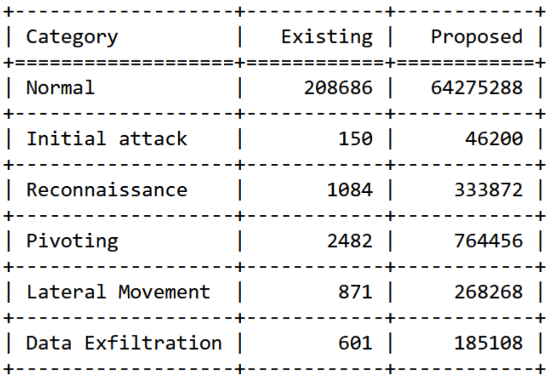
3.4. Context based dataset using RL

```
***Algorithm 2:*** *Identify new sample*
Reg_coef1 = RegressionCoefficient (Prev_Avg_dist_vect[])
Let n = new sample as per CICFlowmeter-V4.0 attributes
Let m = total number of samples from dataset
For i=1 to m
    di = $\sum_{j=1}^{r}$(sij – nj)    where s  is sample
    distvector[i ] = di
avg_dist = $\sum$ distvector[i] / size(n)
Prev_Avg_dist_vect[] = update(Prev_Avg_dist_vect[], avg_dist)
Reg_coef2 = RegCoefficient(Prev_Avg_dist_vect[])
Dev_coeff = | (Reg_coef2 - Reg_coef1) |
If (Dev_coeff != 0)
    n is new sample should be updated to RL dataset and proceed to Algorithm 1.
```

Reinforcement Learning is able to identify the unique sample from the practical scenario and update the same into input dataset for the CGAN model. This can further supports the CGAN model to generate new samples corresponding to the new context. The concept drifts during APT attacks can be handled using the proposed system. Figure 2 depicts the integration of RL model with CGAN to handle concept drift conditions in the APT environments. The new sample detection is based on the Euclidean distance estimation. The features of the dataset are as per CICFlowmeter-V4.0. These features are used to estimate the distance between samples. The average of these distances is estimated and verified with the distances of all the samples with newly arrived sample. Algorithm 2 declares the type of sample as either new or similar to existing samples. The new sample indicates the new behavior detected in the APT environment.

4. Results And Discussions

The proposed research is implemented using python programming language and related APIs. The proposed algorithms are implemented and following results were observed.



```
+------------------+-----------+-----------+
| Category         |  Existing |  Proposed |
+==================+===========+===========+
| Normal           |    208686 |  64275288 |
+------------------+-----------+-----------+
| Initial attack   |       150 |     46200 |
+------------------+-----------+-----------+
| Reconnaissance   |      1084 |    333872 |
+------------------+-----------+-----------+
| Pivoting         |      2482 |    764456 |
+------------------+-----------+-----------+
| Lateral Movement |       871 |    268268 |
+------------------+-----------+-----------+
| Data Exfiltration |      601 |    185108 |
+------------------+-----------+-----------+
```

Figure 3 The count of samples corresponding to the ML dataset and generated through proposed method

The Figure 4 is depict comparative analysis of samples density corresponding to existing and proposed research. The observation found that the proposed method has generated the sufficient samples corresponding to each class.

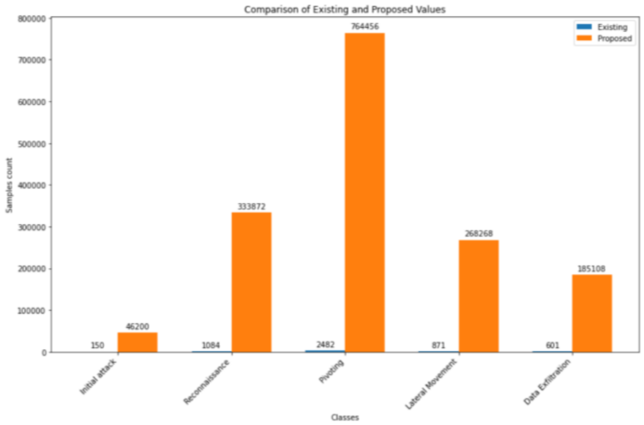


Figure 4 Bar graph depicting the existing and proposed count of samples

Figure 5 show the bar graph depicting the samples count of class Initial attack corresponding to the existing count from the original dataset, proposed algorithm and generic approach followed in GAN model.

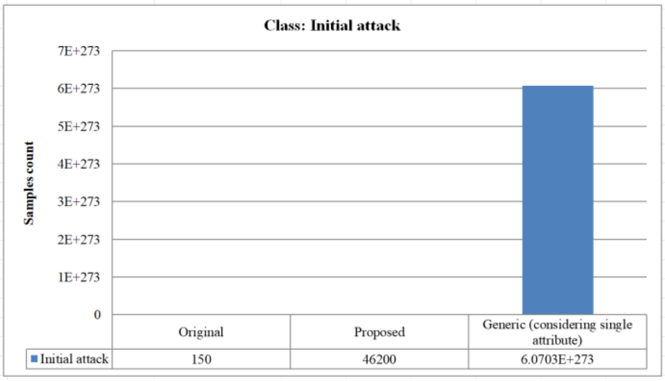


Figure 5 Bar graph depicting the Initial attack class sample count corresponding to Existing, Proposed and Generic models

Results clearly depicting the need of higher end computers or super computers to process generic versions of deep learning based GAN models. Hence the proposed version is able to generate the samples which can be processed using the conventional computers.

Figure 6 depicts the results obtained through the implementation of proposed Algorithm 2. The new behaviour of the attacker can be detected through the diversions which can be observed in the graph. The fourth sample is diverted from the regular behaviour.

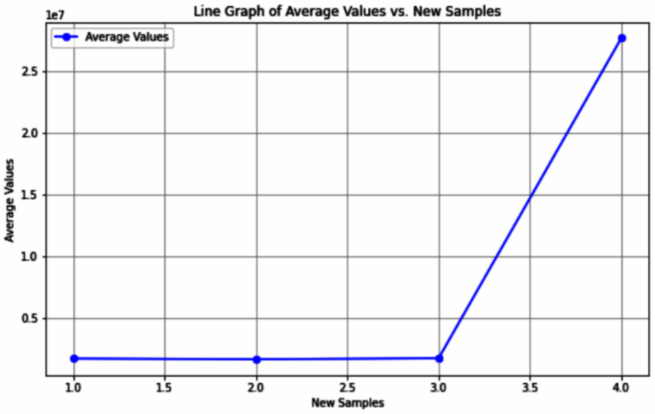


Figure 6 Graph indicating new samples and their behaviors

As per the proposed discussion, these new samples are utilized further to enhance and improve the dataset for contextual based behavioral analysis.

5. Conclusion

This paper has tried to combine two cutting edge models namely CGAN and RL to achieve a strong dataset which can adapt to the environment or behavior of the attacker. Algorithm has been designed to generate data samples based on dataset SCVIC-APT-2021 using CGAN model. Here, RNN is adopted for textual classification and ReLU for activation. Another algorithm has been proposed to identify the new samples in the environment. These new samples have been considered to generate further samples to achieve contextual based dataset. Implementation and utilization of Deep Learning models involving GAN in conventional computing environment is highly challenging. The results indicate that high computing facilities are essential for executing complex tasks effectively. However, the findings also suggest that optimizing the dataset size can reduce the need for such advanced computing resources. Currently it is applied for textual dataset and the same can be applied to various other data modes of dataset namely image, video and audio.

References

[1] Ramzan, Faisal, et al. "Generative Adversarial Networks for Synthetic Data Generation in Finance: Evaluating Statistical Similarities and Quality Assessment." AI 5.2 (2024): 667-685.

[2] Goodfellow, Ian, et al. "Generative adversarial networks." Communications of the ACM 63.11 (2020): 139-144.

[3] Tatam, Matt, et al. "A review of threat modelling approaches for APT-style attacks." Heliyon 7.1 (2021).

[4] Yue, Hao, et al. "Detecting APT attacks using an attack intent-driven and sequence-based learning approach." Computers & Security 140 (2024): 103748.

[5] Habibi Lashkari, Arash. (2018). CICFlowmeter-V4.0 (formerly known as ISCXFlowMeter) is a network traffic Bi-flow generator and analyser for anomaly detection. https://github.com/ISCX/CICFlowMeter. 10.13140/RG.2.2.13827.20003.

[6] Shrivastava, Nivedita & Hanif, Muhammad & Mittal, Sparsh & Sarangi, Smruti & Shafique, Muhammad. A Survey of Hardware Architectures for Generative Adversarial Networks. Journal of Systems Architecture. 118. 10.1016/j.sysarc.2021.102227.

[7] Mirza, Mehdi, and Simon Osindero. "Conditional generative adversarial nets." arXiv preprint arXiv:1411.1784 (2014).

[8] Abdulameer, Hasan, Inam Musa, and Noora Salim Al-Sultani. "Three level intrusion detection system based on conditional generative adversarial network.", International Journal of Electrical & Computer Engineering (2088-8708) 13.2 (2023).

[9] Vardaan, K., et al. "Earthquake trend prediction using long short-term memory RNN." International Journal of Electrical and Computer Engineering 9.2 (2019): 1304-1312.

[10] Caminero, Guillermo, Manuel Lopez-Martin, and Belen Carro. "Adversarial environment reinforcement learning algorithm for intrusion detection." Computer Networks 159 (2019): 96-109.

[11] Otoum, Safa, Burak Kantarci, and Hussein Mouftah. "Empowering reinforcement learning on big sensed data for intrusion detection." Icc 2019-2019 IEEE international conference on communications (ICC). IEEE, 2019.

[12] Jinxin Liu, Yu Shen, Murat Simsek, Burak Kantarci, Hussein Mouftah, Mehran Bagheri, Petar Djukic, "A New Realistic Benchmark for Advanced Persistent Threats in Network Traffic", IEEE Networking Letters, 2022.

[13] Shrivastava, Nivedita, et al. "A survey of hardware architectures for generative adversarial networks." Journal of Systems Architecture 118 (2021): 102227.

[14] Alturkistani, Hilala, and Mohammed A. El-Affendi. "Optimizing cybersecurity incident response decisions using deep reinforcement learning." International Journal of Electrical and Computer Engineering 12.6 (2022): 6768.

[15] Venubabu, Rachapudi. (2023). An Efficient Text based Classification using Neural Networks and Long Short-Term Memory. 251-258. doi: 10.1109/ICAIS56108.2023.10073886

[16] Conneau, Alexis, et al. "Very deep convolutional networks for text classification." arXiv preprint arXiv:1606.01781 (2016).

Authors

Dr. Mouneshachari S received the B.Eng. degree in Computer Science and Engineering from Kuvempu University, India, in 2000 and the M.Tech in Computer Science and Engineering from VTU, Belagavi, India and Ph.D. degree in Computer Science and Engineering from Jain University, Bengaluru, India in 2017. Currently, he is working as Professor at the Department of Computer Science and Engineering under VTU, Belagavi, India. His research interests include Cybersecurity, Internet of Things, EEG Analysis and Cloud computing. Also he has developed software solutions to societal and organization challenges. He is a reviewer for many reputed national and international journals and conferences. He can be contacted at email: drmounesh.cs@gmail.com.

Latharani T R is a Ph.D. scholar from Department of Computer Science and Engineering, Jain Institute of Technology, Davangere. Received B.E. degree in Computer Science and Engineering from Visveswaraya Technological University, Belagavi, in 2007 and M.Tech. from Visveswaraya Technological University, Belagavi, in 2011. Currently she is working as Assistant Professor, in the department of Computer Science and Engineering under VTU, Belagavi, India. Her research interests include Cybersecurity and Internet of Things. email: lathaquick@gmail.com