AI Driven Synthetic Data Generation for Cybersecurity Applications

Yigit SARIOGLU

Advisors : Dr. Beytullah YIGIT , Prof.Dr Fatih ALAGÖZ

Introduction

Generative Adversarial Networks (GANs), introduced by Ian Goodfellow and his team in 2014, have revolutionized the field of data generation. GANs generate data samples from the statistical distribution of the data. GANs consist of two neural networks – a generator and a discriminator – that compete against each other in a game-like training process. The generator aims to create synthetic data that resembles real data, while the discriminator strives to distinguish between real and fake data. This adversarial process leads to the production of highly realistic synthetic data.

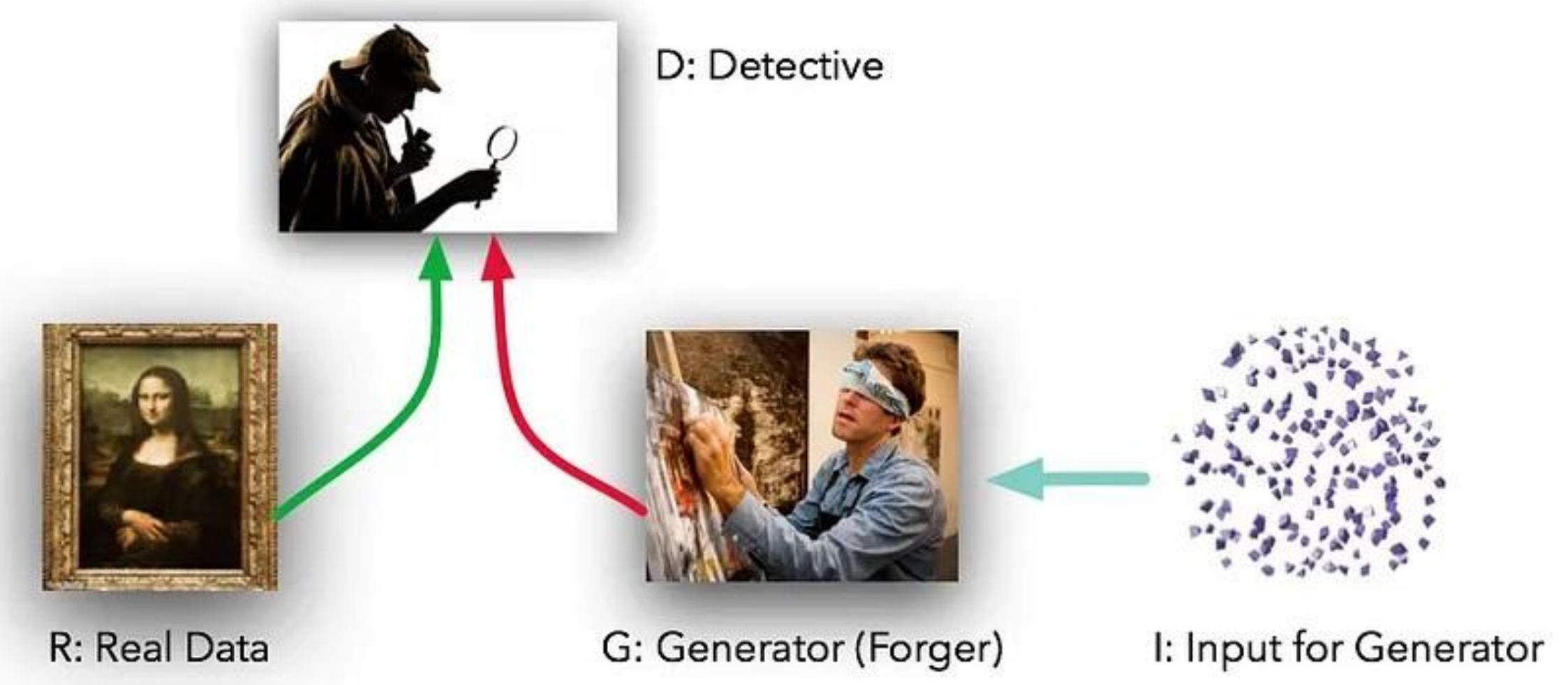


Figure 1. Illustration of a Generative Adversarial Network (GAN).

In the field of cybersecurity, GANs have found increasing applications. They are particularly useful in scenarios with limited data availability, as they can generate synthetic datasets to augment training data. This capability is essential for tasks like detecting DDoS attacks, creating simulations of cyber threats, and enhancing the accuracy of security systems.

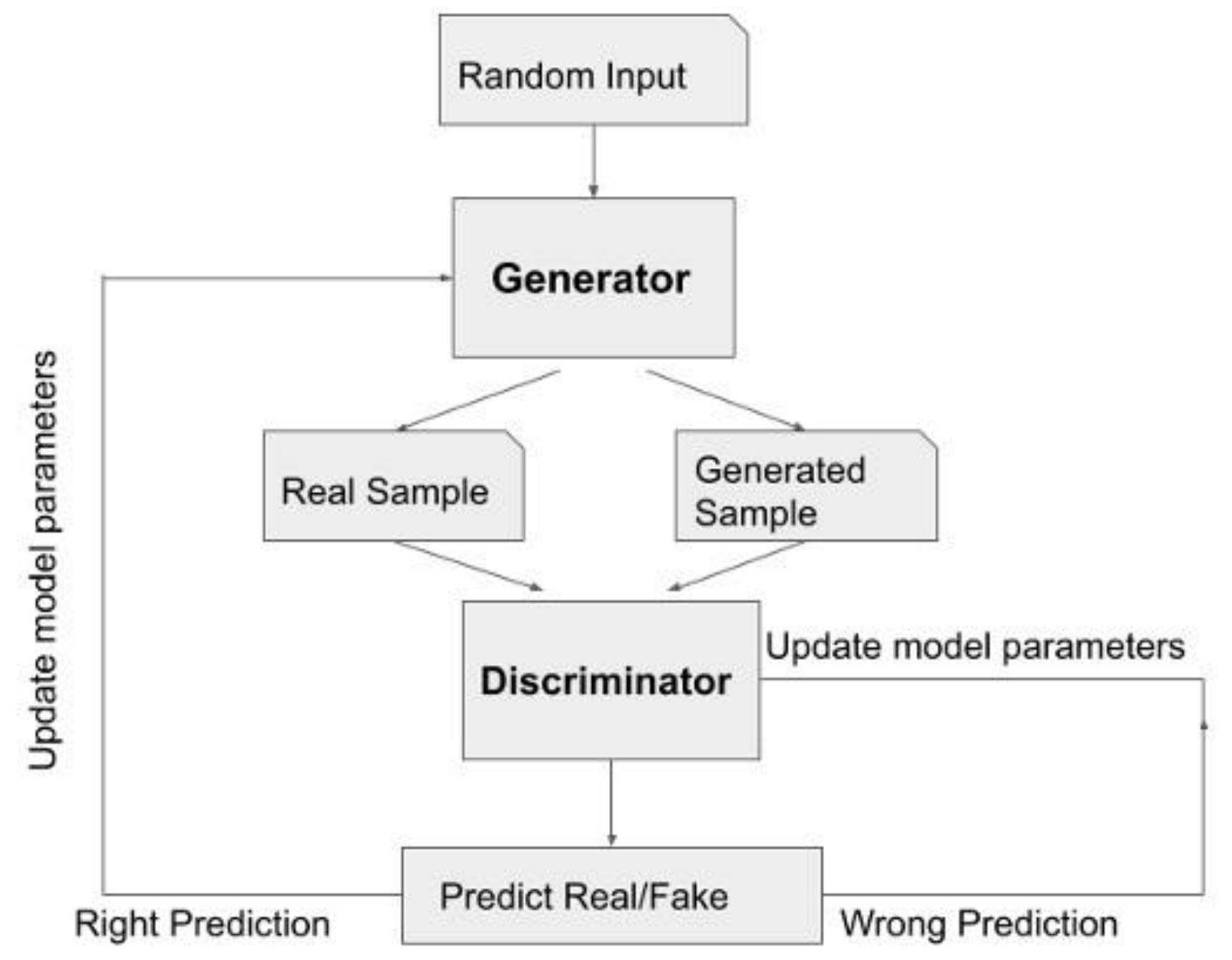


Figure 2. Working mechanism of GANs, where the generator produces synthetic samples to mimic real data, while the discriminator evaluates their authenticity in an adversarial training loop.

Methods and Materials

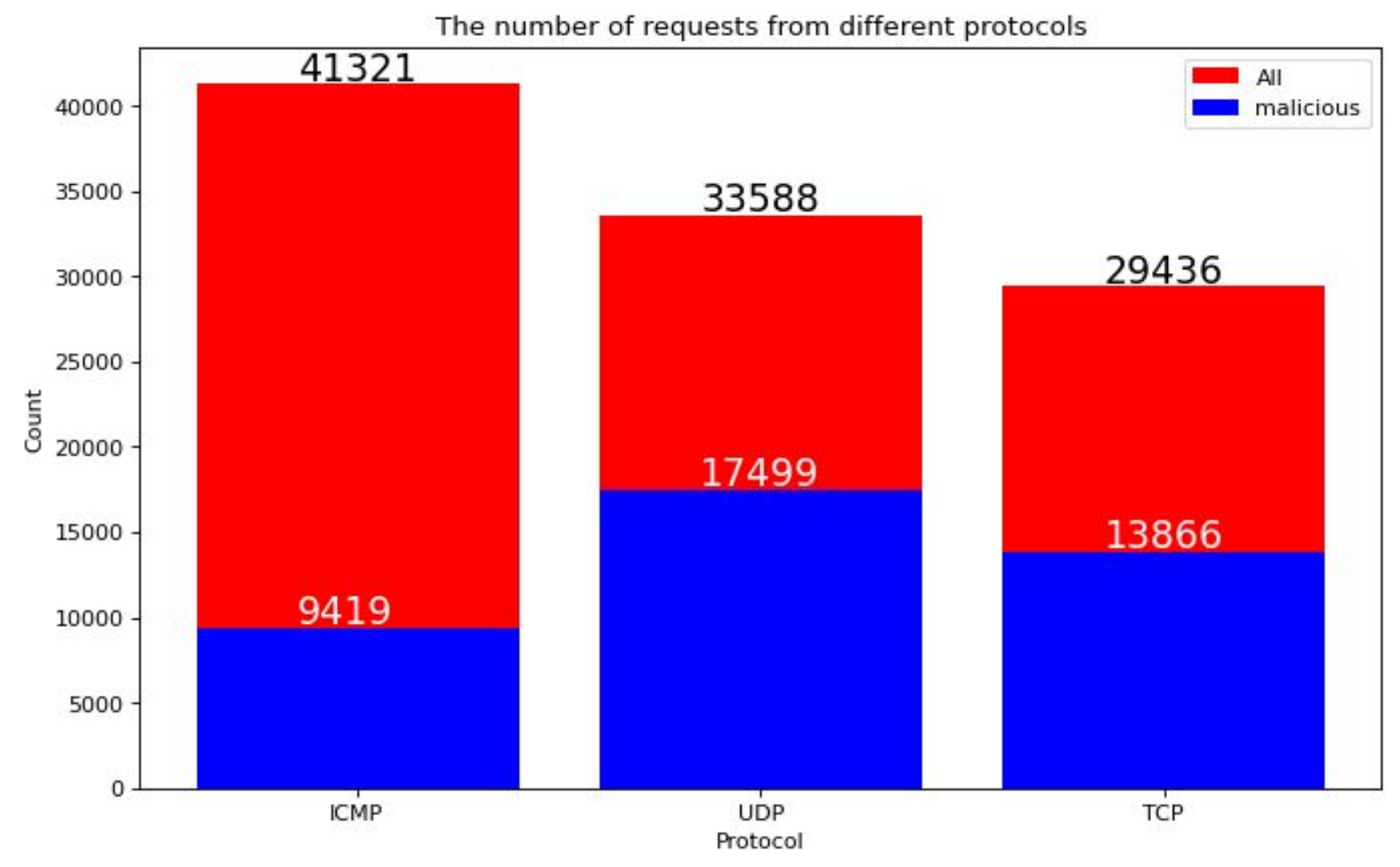
The training process was conducted on a personal computer equipped with an NVIDIA GTX 1050 Ti GPU and CUDA support. The GAN model was implemented using the PyTorch library, with additional libraries such as NumPy, Matplotlib, and Seaborn employed for data preprocessing and visualization.

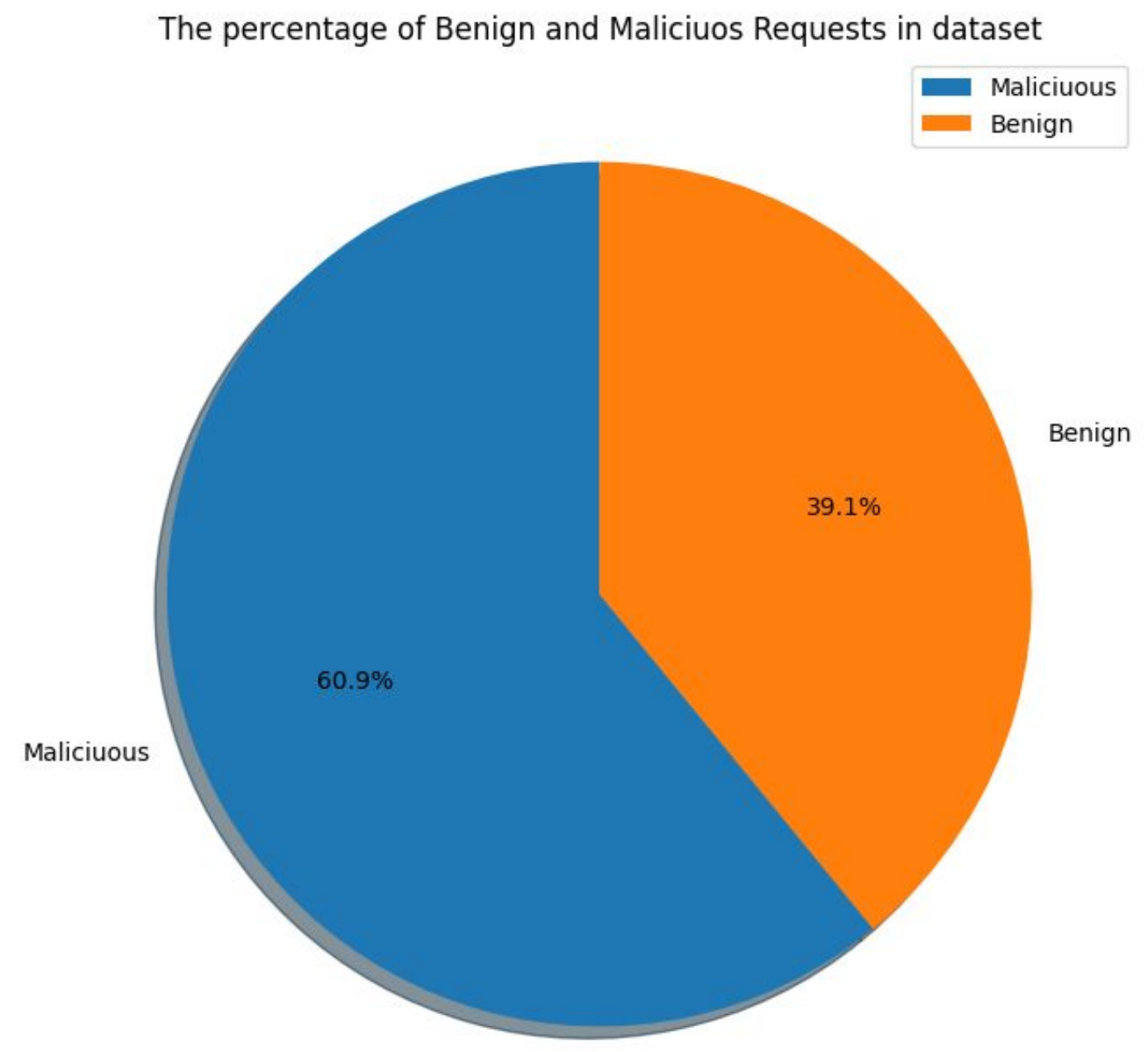
The dataset used was the DDoS-SDN Dataset , consisting of 23 features, including 3 categorical and 20 numerical attributes. The dataset was preprocessed to normalize features to the range [-1, 1].

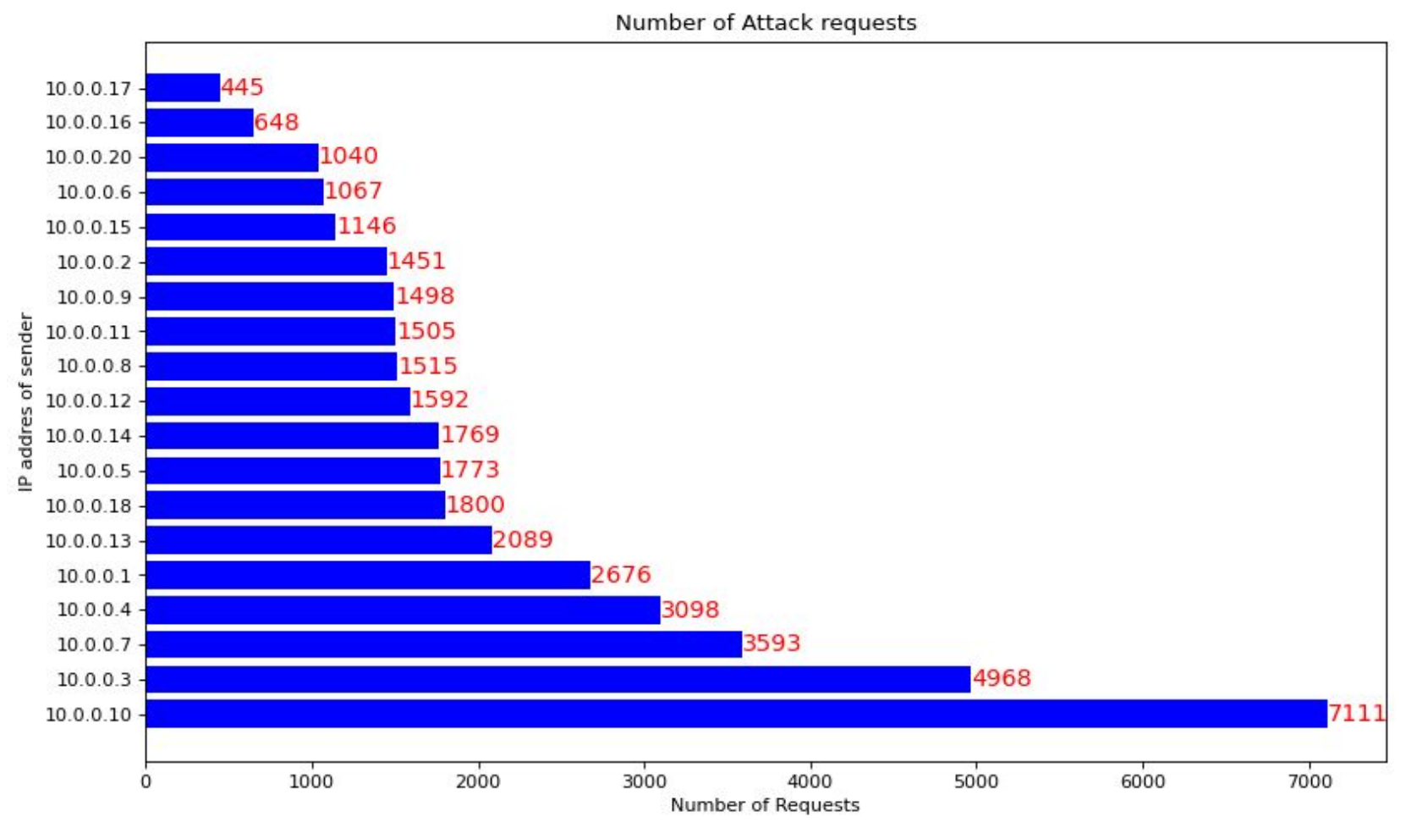
The generator and discriminator networks were trained using the Adam optimizer with learning rates of 0.0002. Jensen-Shannon Divergence (JSD) was computed to evaluate the similarity between real and synthetic data distributions. Dimensionality reduction and visualizations were performed. using PCA, enabling comparison between real and generated datasets.

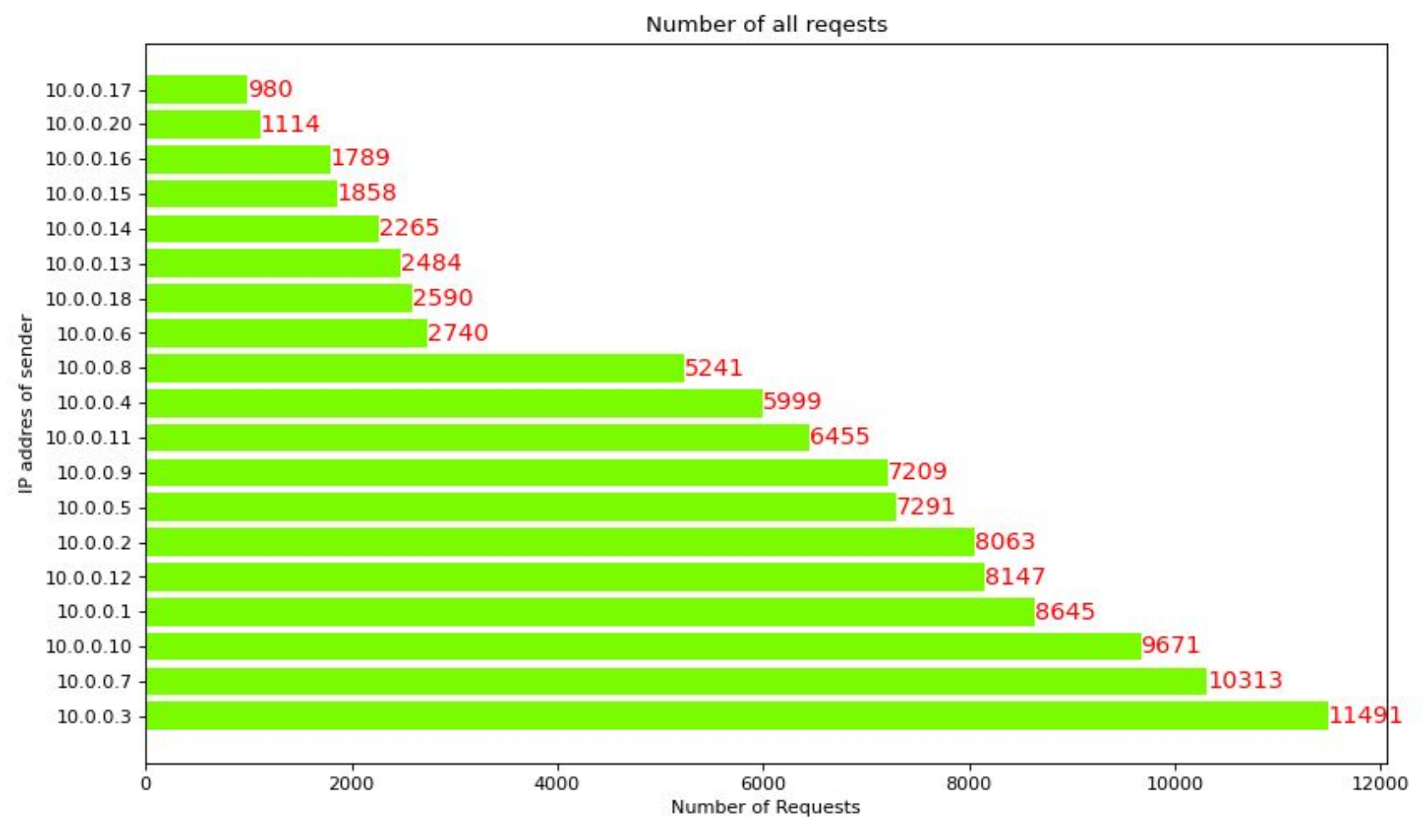
Data Visualizations

The visualizations illustrate the dataset's key characteristics, including the distribution of requests from various IP addresses, different protocols and the proportion of benign versus malicious requests.



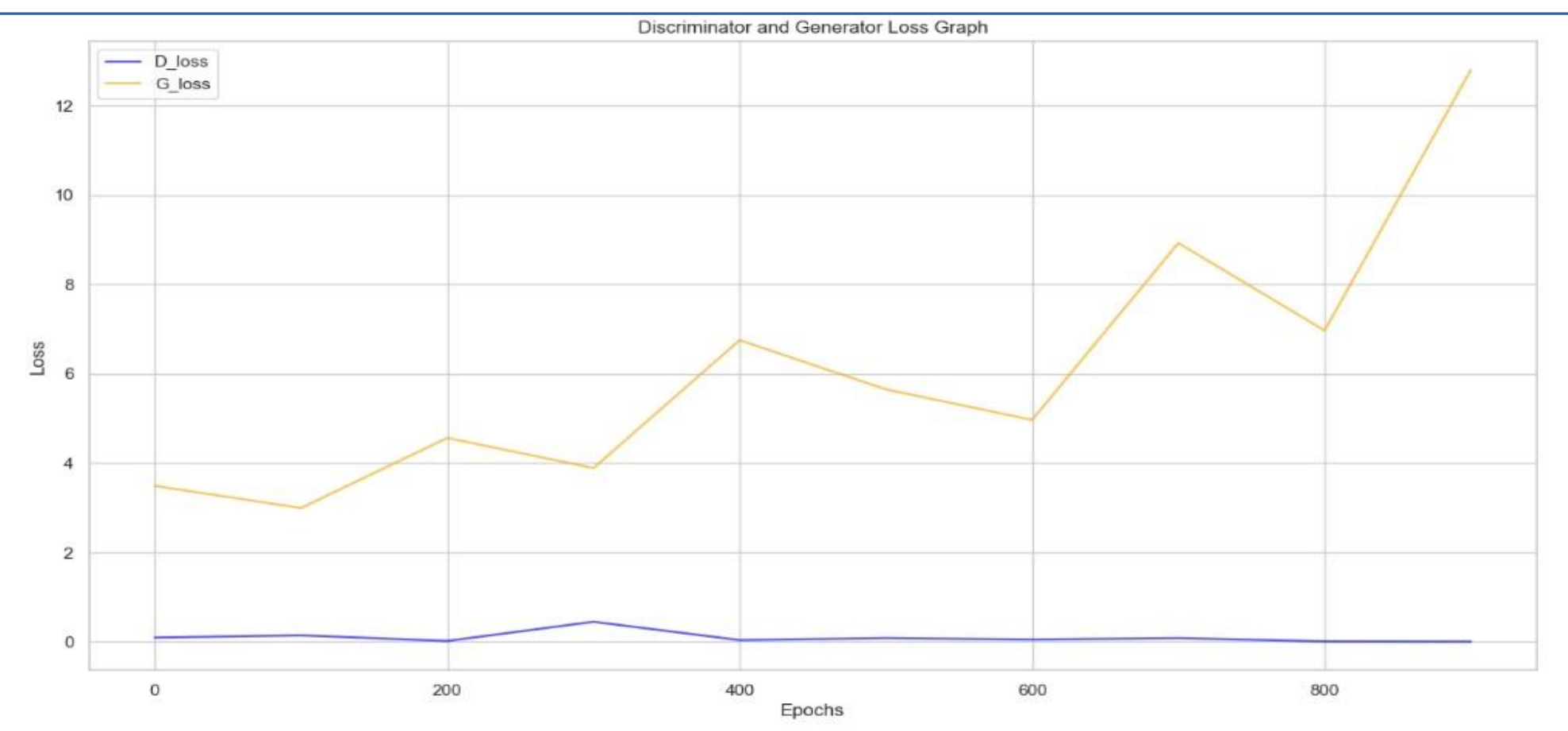




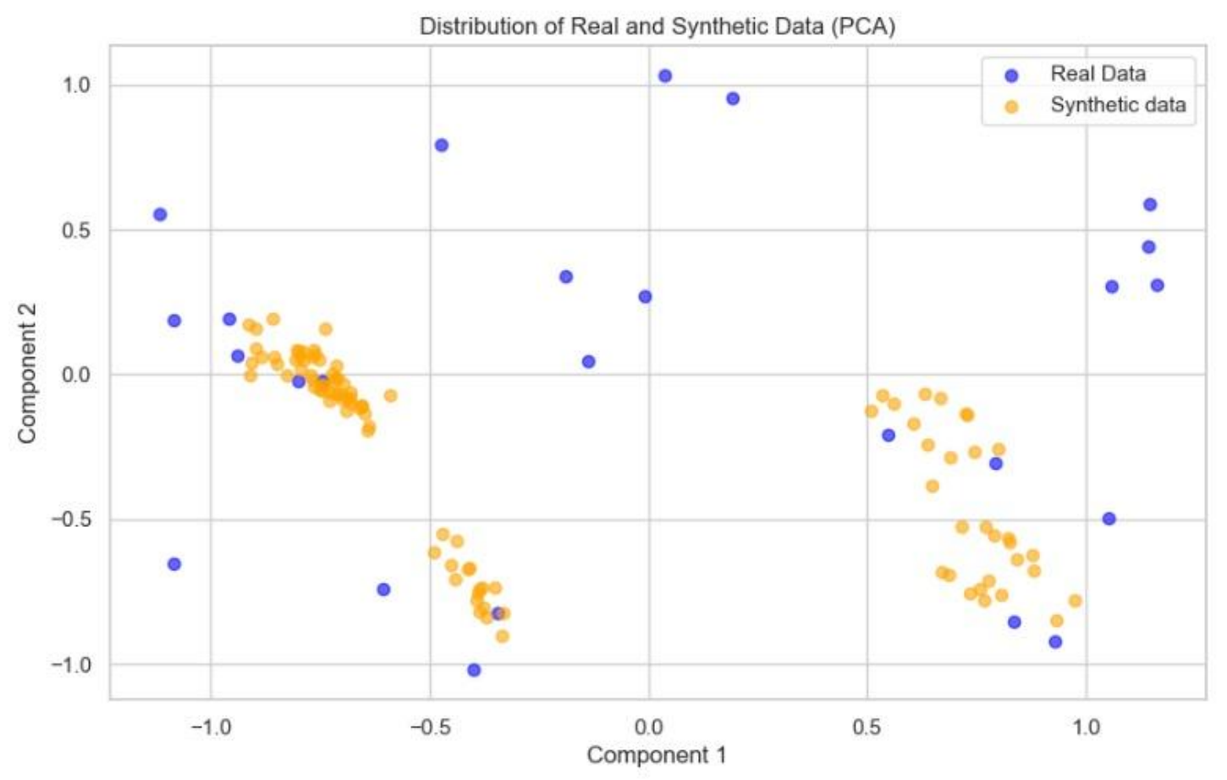


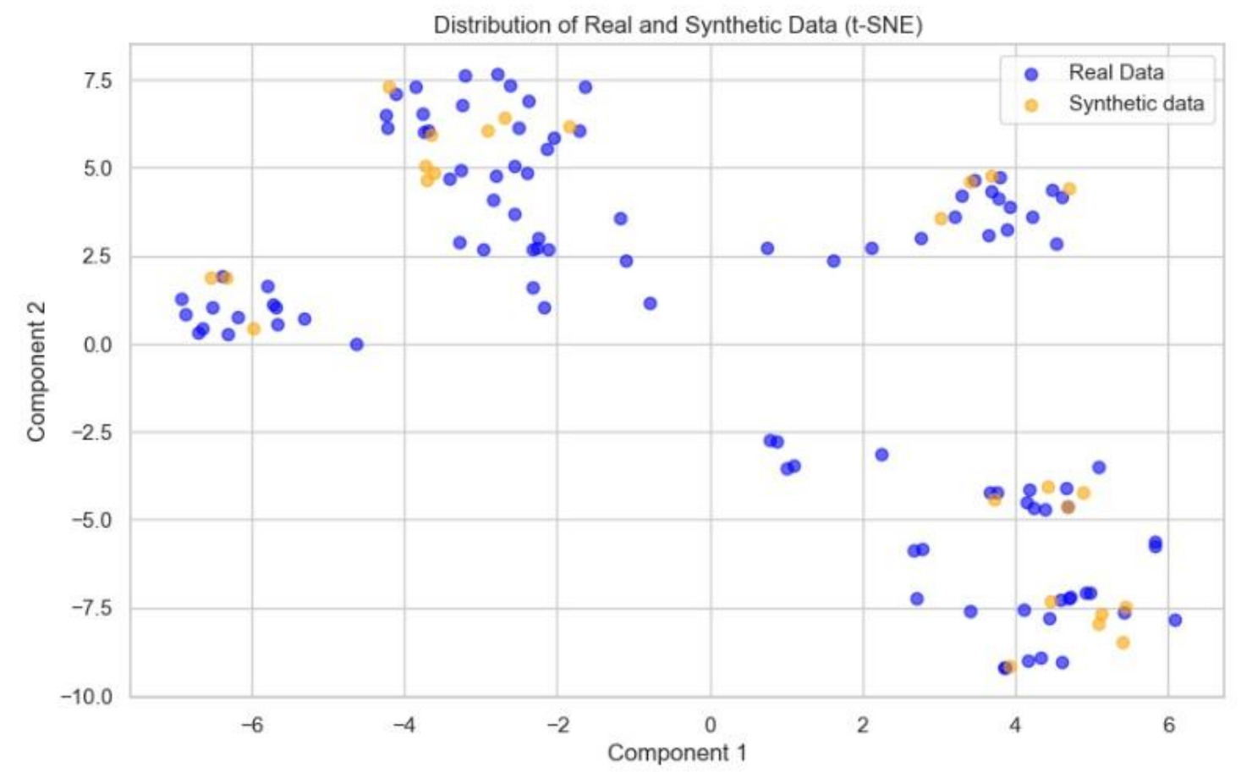
Results

The performance of the discriminator and generator was analyzed throughout the training process. The discriminator's loss (Loss_D) remained low (~0.01-0.08), indicating its effectiveness in distinguishing real data from synthetic data. By epoch 700, Loss_D reached ~0.0025, suggesting the discriminator became highly proficient, making almost no errors in classification. Conversely, the generator's loss (Loss_G) gradually increased, peaking at ~12.8 by epoch 900. This increase suggests that the generator struggled to produce realistic data due to the discriminator's strength, although some of this may be attributed to the natural oscillations in GAN training..



Statistical tests further validated the quality of the generated data. The Jensen-Shannon Divergence (JSD) was calculated as 0.0331, a low value indicating a high similarity between the real and generated data distributions. A JSD value below 0.1 is generally considered good, demonstrating that the generated data closely resembles the real data statistically.





Conclusions and Future Work

This study demonstrates the effectiveness of GANs in generating synthetic cyber security datasets that closely resemble real-world data, as evidenced by statistical evaluations such as Jensen-Shannon Divergence. The generated dataset can be utilized for further testing and training of intrusion detection systems (IDS) like Snort, enabling robust evaluation in cybersecurity scenarios. Future work includes experimenting with advanced GAN architectures, to further enhance data quality. Beyond DDos attack scenarios, we aim to extend this approach to other cybersecurity domains, such as malware detection and UAV security, to address a broader range of challenges in the field.

Contact

Yiğit SARIOĞLU
Bogazici University CMPE
Email:yigit.sarioglu@std.bogazici.edu.tr
Website: https://yigitsarioglu.github.io/
Phone: +905553360825

Cmpe 491 Repo

References

1. Sarıkaya, B. S., Bahtiyar, S. Generative Adversarial Networks for Synthetic Jamming Attacks on UAVs.
2. Razghandi, M., Zhou, H., Erol-Kantarci, M., Turgut, D. (2022). Variational Autoencoder Generative Adversarial Network for Synthetic Data Generation in Smart Home.
3. Saif, S., Widyawan, W., & Ferdiana, R. (2024). IoT-DH dataset for classification, identification, and detection DDoS attack in IoT. Data in Brief, 54. https://doi.org/10.1016/j.dib.2024.110496
4. Huraj, L., Šimon, M., & Lietava, J. (2024). Dataset of DDoS attacks on Fibaro home center 3 for smart home security. Data in Brief, 57. https://doi.org/10.1016/j.dib.2024.110991
5. Highnam, K., Arulkumaran, K., Hanif, Z., & Jennings, N. R. (2021). BETH Dataset: Real Cybersecurity Data for Anomaly Detection Research.
6. Dunmore, A., Jang-Jaccard, J., Sabrina, F., & Kwak, J. (2023). A Comprehensive Survey of Generative Adversarial Networks (GANs) in Cybersecurity Intrusion Detection. IEEE Access, 11, 76071–76094.
7. Changala, R., Kayalvili, S., Farooq, M., Rao, L. M., Rao, V. S., & Muthuperumal, S. (2024). Using Generative Adversarial Networks for Anomaly Detection in Network Traffic: Advancements in AI Cybersecurity. 2nd IEEE International Conference on Data Science and Network Security, ICDSNS 2024.
8. Hitaj, B., Gasti, P., Ateniese, G., & Perez-Cruz, F. (2017). PassGAN: A Deep Learning Approach for Password Guessing.
9. https://www.snort.org/