The modern digital infrastructure is needed to include intrusion detection as an intrinsic constituent towards the entire system. This study explores the application of GANs to enhance NIDS. Traditional NIDS's detection capability was improved by using GANs, including generator and discriminator networks, to produce plausible but anomalous network traffic that the system could pick up, even the most sophisticated or novel patterns of attack. The models are trained on imbalanced datasets simulating network environments that prevail in the real world, hence achieving synthetic data that would help improve the system's performance as far as classes of network intrusion are concerned. Accuracy, precision, recall, and F1 score were some of the core performance metrics in determining the suitability of the model. At times, it significantly increased the detection of rare attacks that usually remain underrepresented in such datasets. Techniques of class weighting and early stopping were applied to the optimization process so that over-fitting did not occur and convergence was guaranteed. Since the model based on GAN has been shown to perform quite robustly, further work into its finer application in highly dynamic and large-scale network environments is expected in the future. The results, indeed, are promising and may look viable to make the effectiveness and resiliency of NIDS better compared with the evolution of cyber threats.

Keywords: GAN, NIDS, Imbalanced data, Deep learning, Anomaly detection, Cybersecurity, Federated Learning, Differential Privacy, Gaussian Noise