Convergence Behaviors and Variabilities of Loss Functions in Quantum GANs and GANs

Md Abdur Rahman
Dept. of Intelligent Systems and Robotics
University of West Florida, USA
mr252@students.uwf.edu

Alfredo Cuzzocrea[§]
iDEA Lab, University of Calabria, Italy
& Dept. of CS, University of Paris City, France
alfredo.cuzzocrea@unical.it

Hossain Shahriar
Center for Cybersecurity
University of West Florida, USA
hshahriar@uwf.edu

***Abstract*—The rapid advancement of Quantum Machine Learning (QML) has introduced new possibilities and challenges in the field of cybersecurity. Generative Adversarial Networks (GANs) have been used as promising tools in Machine Learning (ML) and QML for generating realistic synthetic data from existing (real) dataset which aids in the analysis, detection, and protection against adversarial attacks. In fact, Quantum Generative Adversarial Networks (QGANs) has great ability for numerical data as well as image data generation which have high-dimensional features using the property of quantum superposition. However, effectively loading datasets onto quantum computers encounters significant obstacles due to losses and inherent noise which affects performance. In this work, we study the impact of various losses during training of QGANs as well as GANs for various state-of-the-art cybersecurity datasets. This paper presents a comparative analysis of the stability of loss functions for real datasets as well as GANs generated synthetic dataset. Therefore, we conclude that QGANs demonstrate superior stability and maintain consistently lower generator loss values than traditional machine learning approaches like GANs. Consequently, experimental results indicate that the stability of the loss function is more pronounced for QGANs than GANs.**

***Index Terms*—Generative Adversarial Networks, Quantum Computing, Loss Functions, Entropy**

I. Introduction

QML has gained remarkable interest among researchers and became a prominent field of study. Google recently made a significant breakthrough by proclaiming the attainment of ”quantum supremacy”. While the classical supercomputer would take an estimated 10,000 years to complete the task, Google's quantum computer accomplished it in just 3 minutes and 20 seconds [1]. That is why, quantum computing has caught huge attention in recent years, because it can solve complex problems using special features like superposition and entanglement, which regular computers can not handle [2-3].

Also, researchers are using machine learning for network security in different ways to stop various attacks, which make networks crash. They are also working on making sure important data gets sent quickly and smoothly over industrial wireless networks. They are focusing on making the rules for how devices communicate really well to support important jobs in factories and other industrial places [4-5]. Also, Akter et al., 2023 used different machine learning approaches for the prediction of risk factor for elements of the cryptocurrency market [6]. Moreover, Rahman et al., 2023 used K-means clustering to make the datasamples as clustered input to the Random Forest classifier for big data distributed systems for detecting in a high accuracy using big data processing because it was introduced to use computing capabilities across clusters of machines in the case of huge amount of data [7]. Generative Adversarial Networks (GANs) have gained widespread recognition and applications as powerful generative models in machine learning [8], also related to deep learning for network intrusion detection problems [28]. Moreover, they focused on enhancing this work to address the imbalanced dataset problem using GANs by generating datasamples for specific classes so that the imbalanced dataset issues can be resolved for IDS in distributed computing using PySpark [9]. The related problem of efficiently managing datasets has been also investigated by several research proposals, such as event-based compression [23] and privacy-preserving [25] frameworks, handling large data streams and sensor networks [24], or data visualization [26] and adaptive hypermedia using object-oriented approaches and XML [27].

Researchers in diverse fields have proposed various GANs variants. For instance, conditional generative adversarial nets (cGAN) introduced by Mirza and Osindero in November 2014 greatly improved image generation by incorporating data point labels as conditions [10]. Radford, Metz, and Chintala proposed Deep convolutional generative adversarial networks in November 2015 addressed gradient instability through the integration of convolutional networks [11]. Further advancements include the introduction of least squares generative adversarial networks (LSGAN) by Mao et al. in January 2016, which mitigated issues like vanishing gradients, poor image quality, and mode collapse by adopting the least squares loss function [12]. Additionally, the theoretical insights provided by Arjovsky, Chintala, and Bottou in January 2017 led to the development of the Wasserstein GAN (WGAN) algorithm. WGAN effectively resolved the vanishing gradient problem and training instability by incorporating the Wasserstein distance into its loss function, resulting in a more diverse sample generation [13-14].

In our study, we analyzed the stability of various loss functions when training Large Language Models (LLMs) on cybersecurity datasets—specifically, malicious prompt injec-

[§]This research has been made in the context of the Excellence Chair in Big Data Management and Analytics at University of Paris City, Paris, France.

tion detection [15-16] and HIPAA safeguard compliance classification [17]. Fine-tuned LLMs such as Multilingual BERT and domain-specific embeddings consistently demonstrated smoother and more stable convergence, particularly when regularization techniques and balanced datasets were applied. For the HIPAA rule classification task, loss variability was minimal due to the semantic richness of the input embeddings, leading to faster convergence with fewer fluctuations. Similarly, prompt injection datasets showed steady loss decline with minimal oscillation, especially when LLMs were pre-trained or fine-tuned, confirming previous findings that LLMs reduce training sample dependence [18]. The probabilistic nature of quantum circuits contributed to smoother gradients and less frequent mode collapse during training. While classical GANs exhibited unstable adversarial loss dynamics—often oscillating without convergence—QGANs maintained consistent learning curves, reflecting better equilibrium between generator and discriminator. Thus, both LLMs and QGANs, in their respective domains, contribute significantly to stabilizing training processes and minimizing loss volatility across cybersecurity and compliance tasks.

Researchers are becoming interested in using quantum algorithms to fix many issues like few datasamples [19], and reduce the time complexity of machine learning algorithms [20], etc. QuGAN achieves almost similar performance with reduced parameter set compared with classical GANs [21]. QGANs have great ability for image generation which have high-dimensional features using the property of quantum superposition [22]. This is the first work to explore and compare the stability and convergence behaviors of loss functions across GAN and QGANs. Previous works focused on task performance, but none analyzed loss dynamics in these paradigms.

Our research is structured into several sections: Section II provides a detailed information on state of the art cybersecurity datasets. Section III and Section IV gives an overview of quantum computing and provides loss Functions respectively. The flowchart of this work is described with a diagram in Section V. Also, results and discussion is provided in Section VI. In the final section, we conclude the summary and finding of this work.

II. Loss Functions

Loss functions are fundamental components in the training of Generative Adversarial Networks (GANs) and Quantum Generative Adversarial Networks (QGANs). In GANs, binary cross entropy is employed to optimize the discriminator and generator, while QGANs utilize diverse loss functions, such as Jensen-Shannon divergence, to quantify the disparity between real and generated quantum distributions. The selection of effective loss functions is vital for ensuring stable convergence and generating superior synthetic data in both GANs and QGANs.

A. Loss Function of GANs

Generative Adversarial Networks (GANs) have gained substantial acclaim in diverse fields owing to their versatility and broad applicability. This section presents a comprehensive examination of the underlying principles driving GANs and delves into the complexities of their training process.

The origin of Generative Adversarial Networks (GANs) can be attributed to the groundbreaking research conducted by Goodfellow et al. in 2014 [8]. GANs feature a unique architectural framework, vividly depicted in Fig. 1, comprising two key components: a generative network denoted as G and a discriminative network referred to as D.

The generative network G serves as a creator by taking a random noise vector, z, as input, adhering to either a Gaussian or uniform distribution. Employing a sophisticated mapping mechanism, the generator G transforms z into a novel probability distribution, generating synthetic samples represented as $G(z)$.

In contrast, the discriminative network D functions as a binary classifier, processing two distinct types of inputs. It encounters the counterfeit samples, $G(z)$, produced by the generator G, as well as authentic samples denoted as x, sourced from real datasets. The discriminator D endeavors to estimate the likelihood of an input sample originating from the genuine dataset rather than the artificially generated one.

Inspired by game theory, GANs operate as a competitive interplay between the generator and the discriminator. The primary objective of the generator is to produce synthetic samples that closely resemble real data, effectively deceiving the discriminator D. Conversely, the discriminator strives to discern between fake and authentic samples. This adversarial relationship fosters a dynamic equilibrium, enabling the generator to progressively enhance its capability to generate samples aligning with the distribution of real data, rendering the discriminator unable to differentiate between genuine and synthetic samples.

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

Where x is used to express the real observations from $p_{\text{data}}(x)$. E and z are expectation and the vector respectively. During training, the generator and discriminator iteratively strengthen their networks. The value of the objective function of Generative Adversarial Networks (GANs) is a minimax game (Equation 1) that maximizes the discriminator's accuracy in classifying real and generated samples. The generator maximizes $D(G(z))$ to deceive the discriminator, minimizing $\log(1 - D(G(z)))$. The discriminator uses cross entropy to differentiate real data from generated data, maximizing the overall objective function $V(D,G)$. The generator is optimized with a fixed discriminator. Research indicates that the discriminator achieves optimality when it satisfies the condition $D^*(x) = \frac{pdata(x)}{pdata(x)+pg(x)}$. When both have sufficient capacity, the model reaches a Nash equilibrium where discriminating between real and synthetic data becomes challenging.

B. Loss Function of QGANs

A Survey Quantum Generative Adversarial Networks (QGANs) have emerged as algorithmic frameworks that integrate classical and quantum elements, amalgamating Generative Adversarial Networks (GANs), and Quantum Machine Learning. In 2018, the Quantum Generative Adversarial Learning (QGAL) protocol was proposed by Lloyd, which explored potential scenarios for adversarial learning and speculated on the possibility of QGANs achieving quantum supremacy and unlocking unprecedented computational capacities. To address the limitations of classical GANs in generating discrete data, Situ et al. proposed an innovative solution in October 2018. They integrated quantum Born rules into QGANs, complementing classical GAN theory and enhancing the efficacy of discrete data generation. In January 2019, Hu et al. successfully implemented QGANs within a superconducting quantum circuit which is depicted in (Fig. 2), achieving an impressive fidelity of 98.8% between the generated quantum state and the actual quantum state. This groundbreaking achievement highlighted the exponential advantage QGANs hold over their classical counterparts. A specialized QGAN was proposed which presented heightened learning challenges due to the generation and assimilation of quantum data, alongside the consideration of wave function phases. Finally, Zeng et al. made significant strides in May 2019 by designing a quantum-classical hybrid QGAN model.

Data observations g^l from the quantum generator and we chosen training data observation x^l, where $l = 1, \dots, m$. We can wrire the qGANs' loss functions of the generator by the given equation:

$$L_G(\phi, \theta) = -\frac{1}{m} \sum_{l=1}^{m} \log D_\phi(g^l),$$

and, the discriminator is:

$$L_D(\phi, \theta) = \frac{1}{m} \sum_{l=1}^{m} \left(\log D_\phi(x^l) + \log(1 - D_\phi(g^l)) \right),$$

According to the discriminator's parameters ϕ and the generator's parameters θ, the loss functions are optimized.

C. Entropy for QGANs

In the context of Quantum Generative Adversarial Networks (QGAN), the entropy for the generator and discriminator refers to the level of uncertainty or randomness in the generated data and the discriminator's classification decisions, respectively. Entropy can be computed using the formula for Shannon entropy for the Generator and the Discriminator:

$$Entropy_{\text{Generator}} = -\sum_{i} p_i \log(p_i)$$

$$Entropy_{\text{Discriminator}} = -\sum_{i} q_i \log(q_i)$$

Where p_i represents the probability of each data sample being generated by the generator, and q_i represents the probability of each data sample being classified correctly by the Discriminator.

Moreover, the generator and the discriminator can be trained with binary cross entropy which is known the loss function:

$$L(\theta) = \sum_{j} p_j(\theta) \left[y_j \log(x_j) + (1 - y_j) \log(1 - x_j) \right],$$

where x_j are observations and y_j to the corresponding labelled observation.

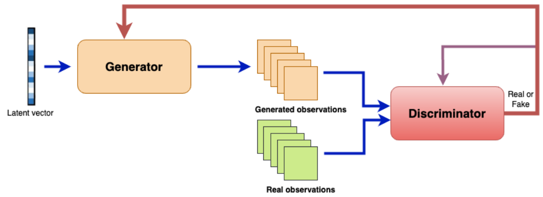

Fig. 1. The architecture of a typical models with generator (G) and discriminator (D) for GANs.

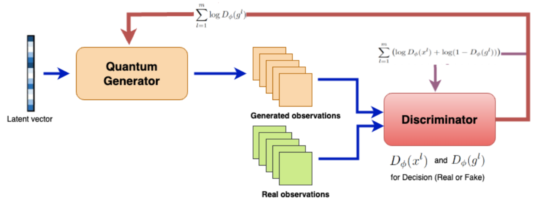
$\sum_{l=1}^{m} \log D_\phi(g^l)$
$\sum_{l=1}^{m} (\log D_\phi(x^l) + \log(1 - D_\phi(g^l)))$
Latent vector
Quantum Generator
Generated observations
Real observations
Discriminator
$D_\phi(x^l)$ and $D_\phi(g^l)$
for Decision (Real or Fake)

Fig. 2. The architecture of a typical models with generator (G) and discriminator (D) for QGANs.

III. Methods

Our research successfully employed two neural networks, specifically a quantum generator and a classical discriminator, to accomplish our goal. The quantum generator utilized a quantum neural network, while the classical discriminator was implemented using PyTorch. To optimize hardware efficiency, we adopted a hardware-efficient ansatz with six repetitions for the quantum generator. This ansatz involved parameterized quantum circuits with R_Y and R_Z rotations, as well as C_X gates, which is built upon the dataset observations as input states.

We were very careful for selection of generator parameters considered circuit depth which enables the incorporation of more intricate structures. This deeper circuit depth plays a pivotal role in accurately capturing and representing the observations, which helps comprehensive analysis. The quantum generator with chosen ansatz and its corresponding parameters collaborated with the classical discriminator implemented in PyTorch. Both models were trained using a manual implementation of the binary cross-entropy loss function to assess gradients.

We proposed the integrated framework (Fig. 3) in which high-quality synthetic data is successfully generated from existing datasets using Generative Adversarial Networks (GANs). The process involved in the strengths of GANs to

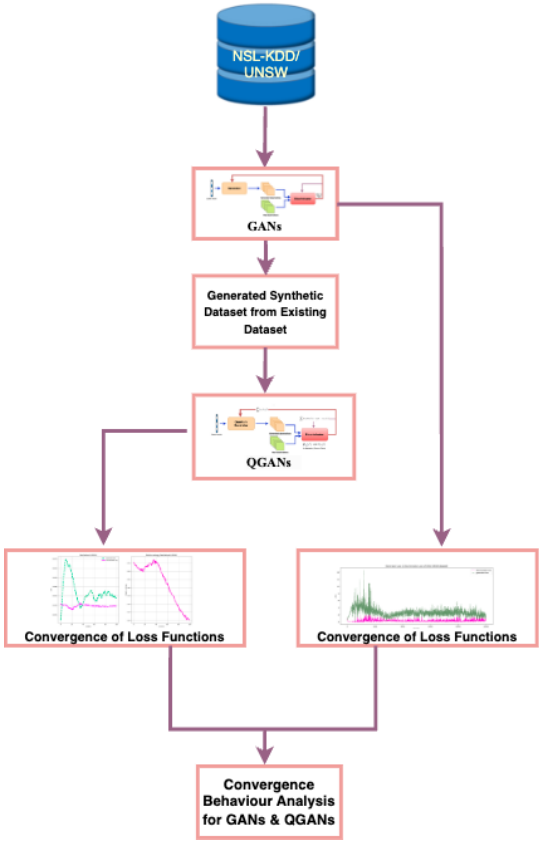
NSL-KDD/ UNSW
GANs
Generated Synthetic Dataset from Existing Dataset
QGANs
Convergence of Loss Functions
Convergence of Loss Functions
Convergence Behaviour Analysis for GANs & QGANs

Fig. 3. The Flowchart to Investigate the Convergence Behaviours of GANs and QGANs

create synthetic data that closely mirrors the characteristics of the original datasets. This synthetic dataset, along with the existing dataset, was then fed separately into typical Quantum Generative Adversarial Networks (QGANs) to examine the convergence behaviors of their respective loss functions with the convergence behaviors by GANs. By comparing the performance of QGANs when trained on both synthetic and original datasets, we aimed to gain deeper insights into their learning dynamics and effectiveness. The results highlighted the potential of synthetic data in enhancing the training process and provided valuable information on how QGANs can adapt to different data sources. This integrated approach underscores the importance of combining classical and quantum machine learning techniques to address complex data challenges in cybersecurity.

However, the classical discriminator is implemented as a PyTorch-based neural network that follows its advanced capabilities with automatic gradient computation. This feature streamlines the training process and can optimize the discriminator's parameters efficiently. By using the strengths of both the quantum generator and the classical discriminator, the system benefits from their complementary nature which leads to enhanced performance and more accurate generation and discrimination of data samples than GANs of classical computing. The integration of these components enables a robust framework for training and analysis tasks in quantum generative adversarial networks.

TABLE I
LOSS BY GANS FOR EPOCH 10000 (REAL DATASET)

Dataset	Network	Min. loss	Max. loss
UNSW	Generator	0.33	14.45
	Discriminator	0.12	2.6
NSL-KDD	Generator	0.32	2.9
	Discriminator	0.1	1.2

IV. Results and Discussion

In our research, we utilized Google Colab as a powerful computing platform to perform quantum computations and implement classical ML as well as Quantum ML. Google Colab provides a cloud-based environment with access to quantum computing resources which enables us to leverage quantum capabilities for our experiments. With the aid of user-friendly interface and integration with QGAN libraries, we efficiently executed the QGAN algorithms and conducted quantum simulations in colab. This enabled us to explore the potential of QGANs and quantum computing in generating synthetic data and advancing research in the field of quantum machine learning. Access to quantum processors is typically provided through the Google Quantum Computing service through the Quantum Computing API which allows users to submit quantum circuits and execute them. We trained classical ML with cyber dataset, and then QML will be trained to observe the stability as well as convergence.

We used two datasets. The UNSW dataset [29] comprises various features critical for cybersecurity tasks like intrusion detection and anomaly classification. Key features include protocol type (indicating the network protocols used, such as TCP, UDP, and ICMP), service (representing network services like HTTP, FTP, and SMTP), source and destination IP addresses (helping identify malicious communication patterns), and source and destination ports (which can reveal uncommon or suspicious activity). The NSL-KDD dataset [30] consists of a training subset with 125,973 records and a test subset containing 22,544 records. For supervised modeling, key features include protocol type, service, bytes transferred (src and dst), and several destination host metrics, including srv count, same srv rate, and different srv rate.

Firstly, classical ML has consistently higher losses for UNSW dataset than the NSL-KDD dataset. While training the generator and the discriminator of GANs, we observed that ML encounters greater challenges and difficulties in generating synthetic data than QML. It is also noted that the higher loss values suggest a higher degree of fluctuations and potentially slower convergence during training, which may be attributed to the complexity and variability of the UNSW dataset. In contrast, the NSL-KDD dataset appears to be more stable to the GANs model.

TABLE I provides a summary of the GANs training results for both the datasets. The table includes information on the dataset, the type of network (generator or discriminator), epochs and the minimum and maximum loss values recorded during training.

For the UNSW dataset, the generator got a minimum loss of 0.33 and a maximum loss is 14.45, while the discriminator has a minimum loss and a maximum loss which are 0.12 and 2.6. On the other hand, for the NSL-KDD dataset, a minimum loss is 0.32 for the generator and a maximum loss is 2.9 for discriminator, while a minimum loss and maximum losses are 0.1 and 1.2 respectively. These outcomes suggest that the GAN model faced higher losses for the UNSW dataset compared to the NSL-KDD dataset, both in terms of generator and discriminator losses. This could indicate that the GANs model struggled more with the complexity and variability of the UNSW dataset which results in higher fluctuations and potentially slower convergence during training.

During QGANs training, the loss function progress of the generator and the discriminator (left column) is illustrated for real and synthetic datasets (UNSW), and the right column displays the convergence of the relative entropy for real and synthetic datasets. TABLE II presents the loss functions during the training of two networks, namely the Generator and Discriminator, for the UNSW dataset. The loss values are recorded as the minimum (Min. loss) and maximum (Max. loss) achieved during the training process. Additionally, the stability of each network is indicated by the Stable column. For the Generator network trained on real data, the minimum loss achieved is 0.602, while the maximum loss is 0.730, with a stable value of 0.693. The Discriminator network trained on real data exhibits a minimum loss of 0.688, a maximum loss of 0.698, and a stable value of 0.692.

TABLE II
LOSS FUNCTIONS-QGANS: (LEFT COL. (UNSW))

Networks	Dataset	Min. loss	Max. loss	Stable
Generator	Real	0.602	0.730	0.693
Discriminator	Real	0.688	0.698	0.692
Generator	Synthetic	0.666	0.806	0.694
Discriminator	Synthetic	0.692	0.697	0.694

TABLE III
LOSS FUNCTIONS (QGANS): (LEFT COL. (KDD))

Networks	Dataset	Min. loss	Max. loss	Stable
Generator	Real	0.675	0.753	0.693
Discriminator	Real	0.691	0.696	0.693
Generator	Synthetic	0.678	0.802	0.694
Discriminator	Synthetic	0.692	0.696	0.694

On the other hand, when the Generator network is trained on synthetic data, the minimum loss obtained is 0.666, while the maximum loss reaches 0.806. The stable value for the Generator network with synthetic data is 0.694. The Discriminator network, when trained on synthetic data, has a minimum loss of 0.692, a maximum loss of 0.697, and a stable value of 0.694. Overall, the presented table provides valuable information about the loss functions and stability of the Generator and Discriminator networks during the training process on the UNSW dataset.

TABLE IV
ENTROPY IN QGANS

Dataset-Name	Type	Epochs	Max. diff.	Min. diff.
UNSW	Real	100	0.56	0.21
	Real	500	1.19	0.07
	Synthetic	500	0.72	0.04
NSL-KDD	Real	100	0.48	0.21
	Real	500	0.52	0.02
	Synthetic	500	0.69	0.03

In the case of QGANs training, the loss function progress of the generator and the discriminator (left column) is illustrated for real and synthetic datasets (NSL-KDD), and the right column displays the convergence of the relative entropy for real and synthetic datasets. The provided TABLE III displays the loss functions observed during the training of two networks, the Generator and Discriminator, on the NSL-KDD dataset. It includes the minimum (Min. loss) and maximum (Max. loss) loss values achieved during the training process, along with the stability (Stable) of each network.

For the Generator network trained on real data from the NSL-KDD dataset, the minimum loss recorded is 0.675, while the maximum loss is 0.753. The stable value for the Generator network with real data is 0.693. The Discriminator network, when trained on real data, exhibits a minimum loss of 0.691, a maximum loss of 0.696, and a stable value of 0.693. Similarly, when the Generator network is trained on synthetic data from the NSL-KDD dataset, the minimum loss attained is 0.678, and the maximum loss is 0.802. The stable value for the Generator network with synthetic data is 0.694. On the other hand, the Discriminator network, when trained on synthetic data, demonstrates a minimum loss of 0.692, a maximum loss of 0.696, and a stable value of 0.694. In summary, the table provides a concise overview of the loss functions and the stability of the Generator and Discriminator networks during their training on the NSL-KDD dataset.

The TABLE IV presents a comparative analysis of entropy values across different datasets, data types, and epochs, providing insights into the level of uncertainty and randomness in the generated data and the discriminator's classification decisions during the training of the QGAN. In the case of UNSW dataset and epochs 500, the generator gets a minimum and maximum values of relative entropy were 0.07 and 1.19 and these values are 0.04 and 0.72 for the synthetic dataset. On the other hand, for the NSL-KDD dataset, a minimum and maximum relative entropy are 0.02 and 0.52 respectively. For the synthetic dataset, 0.03 and 0.69 are the values of minimum and maximum relative entropy respectively.

Based on the presented results, it can be concluded that QGANs demonstrate greater stability in generating synthetic datasets compared to traditional GANs when applied to cyber datasets. These research findings have significant implications in the realm of cybersecurity, as QGANs improved stability aids in preventing adversarial attacks by producing more reliable and robust synthetic data. By taking the advantages, QGANs offers promising solutions in enhancing the security and resilience of cyber systems against potential threats. These insights contribute to the advancement of data generation techniques and reinforce the importance of exploring quantum-based approaches for addressing challenges in cybersecurity.

V. Conclusions

This paper presented a comparative analysis of the stability of loss functions in GANs and QGANs for two prominent cybersecurity datasets. We investigated the convergence behavior and variability of loss functions during the training process. Experimental results indicate that the instability of the loss function is more pronounced in the UNSW dataset compared to the NSL-KDD dataset. The most important finding is that QGANs demonstrated significantly lower generator loss values, with ranges peaking at 0.5 to 1 for both datasets. The observed discrepancy in loss function behavior highlights the challenges associated with achieving stable convergence during training. The wider range of generator loss values in GANs indicates increased fluctuation and potentially slower convergence. Conversely, QGAN demonstrates superior stability, maintaining consistently lower generator loss values and exhibiting smaller variations for both datasets.

Acknowledgements

This work was partially supported by the National Science Foundation (NSF) Award#2433800, #1946442, and SERICS project (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

References

[1] F. Arute, K. Arya, R. Babbush, D. Bacon, J.C. Bardin, R. Barends, J.M. Martinis, "Quantum Supremacy using a Programmable Superconducting Processor". *Nature 574(7779)*, pp. 505-510, 2019.

[2] M.A. Rahman, H. Shahriar, V. Clincy, M.F. Hossain, M. Rahman, "A Quantum Generative Adversarial Network-based Intrusion Detection System". In: *47th IEEE Annual Computers, Software, and Applications Conference*, pp. 1810-1815, 2023.

[3] M.A. Rahman, M.S. Akter, E. Miller, B. Timofti, H. Shahriar, M. Masum, F. Wu, "Fine-tuned Variational Quantum Classifiers for Cyber Attacks Detection based on Parameterized Quantum Circuits and Optimizers". In: *48th IEEE Annual Computers, Software, and Applications Conference*, pp. 1810-1815, 2024.

[4] M.A. Rahman, "Detection of Distributed Denial of Service Attacks Based on Machine Learning Algorithms". *International Journal of Smart Home 14(2)*, pp. 15-24, 2020.

[5] M.A.K. Azad, A. Khatun, M.A. Rahman, "A Slotted-Sense Streaming MAC for Real-Time Multimedia Data Transmission in Industrial Wireless Sensor Networks". *International Journal of Advanced Engineering Research and Science 4(3)*, art. 237103, 2017.

[6] M.S. Akter, M.A. Rahman, H. Shahriar, M. Rahman, "Early Prediction of Cryptocurrency Price Decline: A Deep Learning Approach". In: *26th IEEE International Conference on Computer and Information Technology*, pp. 1-6, 2023.

[7] M.A. Rahman, H. Shahriar, "Clustering Enabled Robust Intrusion Detection System for Big Data using Hadoop-PySpark". In: *20th IEEE International Conference on Smart Communities: Improving Quality of Life using AI, Robotics and IoT*, pp. 249-254, 2023.

[8] I.J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, Y. Bengio, "Generative Adversarial Nets". *International Conference on Neural Information Processing Systems*, pp. 2672-2680, 2014.

[9] M.A. Rahman, H. Shahriar, "Towards Developing Generative Adversarial Networks based Robust Intrusion Detection Systems for Imbalanced Dataset using Hadoop-PySpark". In: *2024 International Conference on Innovations In Computing Research*, pp. 449–463, 2024.

[10] M. Mirza, S. Osindero, "Conditional Generative Adversarial Nets". CoRR abs/1411.1784, 2014.

[11] A. Radford, L. Metz, S. Chintala, "Unsupervised Representation Learning with Deep Convolutional Generative Adversarial Networks". In: *4th International Conference on Learning Representations*, 2016.

[12] X. Mao, Q. Li, H. Xie, R.Y.K. Lau, Z. Wang, S.P. Smolley, "Least Squares Generative Adversarial Networks". In: *2017 IEEE International Conference on Computer Vision*, pp. 2813-2821, 2017.

[13] M. Arjovsky, L. Bottou, "Towards Principled Methods for Training Generative Adversarial Networks". In: *5th International Conference on Learning Representations*, 2017.

[14] M. Arjovsky, S. Chintala, L. Bottou, "Wasserstein GAN". CoRR abs/1701.07875, 2017.

[15] M.A. Rahman, H. Shahriar, F. Wu, A. Cuzzocrea, "Applying Pre-trained Multilingual BERT in Embeddings for Improved Malicious Prompt Injection Attacks Detection". In: *2nd IEEE International Conference on Artificial Intelligence, Blockchain, and Internet of Things*, pp. 1-7, 2024.

[16] M.A. Rahman, F. Wu, A. Cuzzocrea, S.I. Ahamed, "Fine-tuned Large Language Models (LLMs): Improved Prompt Injection Attacks Detection". CoRR abs/2410.21337, 2024.

[17] M.A. Rahman, M.A. Barek, A.B.M. Riad, M. Rahman, M.B. Rashid, S. Ambedkar, S.I. Ahamed, "Embedding with Large Language Models for Classification of HIPAA Safeguard Compliance Rules". CoRR abs/2410.20664, 2024.

[18] M.A. Rahman, G. Francia, "Large Language Model can Reduce the Necessity of using Large Data Samples for Training Models". In: *25th IEEE Conference on Artificial Intelligence*, 2025.

[19] K. Mitarai, M. Negoro, M. Kitagawa, K. Fujii, "Quantum Circuit Learning". *Physical Review A 98(3)*, art. 032309, 2018.

[20] S. Lloyd, M. Mohseni, P. Rebentrost, "Quantum Principal Component Analysis". *Nature Physics 10(9)*, pp. 631-633, 2024.

[21] S.A. Stein, B. Baheri, D. Chen, Y. Mao, Q. Guan, A. Li, B. Fang, S. Xu, "QuGAN: A Quantum State Fidelity based Generative Adversarial Network". In: *2021 IEEE International Conference on Quantum Computing and Engineering*, pp. 71-81, 2021.

[22] H. Huang, Y. Du, M. Gong, Y. Zhao, Y. Wu, C. Wang, S. Li, F. Liang, J. Lin, Y. Xu, "Experimental Quantum Generative Adversarial Networks for Image Generation". *Physical Review Applied 16(2)*, art. 024051, 2021.

[23] A. Cuzzocrea, G. Fortino, O.F. Rana, "Managing Data and Processes in Cloud-Enabled Large-Scale Sensor Networks: State-of-the-Art and Future Research Directions". In *13th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing*, pp. 583-588, 2013.

[24] C.K. Leung, P. Braun, A. Cuzzocrea, "AI-Based Sensor Information Fusion for Supporting Deep Supervised Learning". *Sensors 19(6)*, art. 1345, 2019.

[25] R. Langone, A. Cuzzocrea, N. Skantzos, "Interpretable Anomaly Prediction: Predicting Anomalous Behavior in Industry 4.0 Settings via Regularized Logistic Regression Tools". *Data & Knowledge Engineering 130*, art. 101850, 2020.

[26] P. Howlader, K.K. Pal, A. Cuzzocrea, S.D.M. Kumar, "Predicting Facebook-Users' Personality Based on Status and Linguistic Features via Flexible Regression Analysis Techniques". In: *33rd Annual ACM Symposium on Applied Computing*, pp. 339-345, 2018.

[27] R.C. Camara, A. Cuzzocrea, G.M. Grasso, C.K. Leung, S.B. Powell, J. Souza, B. Tang, "Fuzzy Logic-Based Data Analytics on Predicting the Effect of Hurricanes on the Stock Market". In: *2018 IEEE International Conference on Fuzzy Systems*, pp. 1-8, 2018.

[28] M. Masum, H. Shahriar, H. Haddad, M.J. Faruk, M. Valero, M.A. Khan, M.A. Rahman, M.I. Adnan, A. Cuzzocrea, F. Wu, "Bayesian Hyperparameter Optimization for Deep Neural Network-Based Network Intrusion Detection". In: *2021 IEEE International Conference on Big Data*, pp. 5413-5419, 2021.

[29] N. Moustafa, J. Slay, "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems". In: *2015 IEEE Military Communications and Information Systems Conference*, pp. 1-6, 2015.

[30] L. Dhanabal, S.P. Shantharajah, "A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms". *International Journal of Advanced Research in Computer and Communication Engineering 4(6)*, pp. 446-452, 2015.