Grenze International Journal of Engineering and Technology, June Issue

Generation of Synthetic Datasets using Generative Adversarial Networks and Securing it using Blockchain

Vrushali Bongirwar[1], Arpit Agutale[2], Bipul Biswas[3], Rehan Khan[4], Atharva Bhoyar[5], Amaan Khan[6] and Shubhangi C Tirpude[7]
[1-7]Shri Ramdeobaba College of Engineering and Management, Nagpur, Maharashtra, India
Email: {bongirwarvk, agutaleam, benoybb, khanrr, bhoyarar, khana_1, tirpudes}@rknec.edu

***Abstract*—Emerging from the challenges of generating secure synthetic image datasets, this research is motivated by the aim to elevate dataset quality while upholding data security. Synthetic datasets play a crucial role in training machine learning models, but their quality and diversity are often limited. Simultaneously, the security and authenticity of these datasets become paramount in an era of increasing data breaches and fraudulent activities. This study offers a comprehensive solution to two important challenges using advanced technologies. Firstly, we focus on creating diverse synthetic images that help improve the training of artificial intelligence models. Secondly, we ensure the safety of these images through a technology called blockchain. By combining these two technologies, we generate images and make sure they can't be tampered with. We use a method called Generative Adversarial Networks for generating images and then store them securely on a blockchain. Our project approach shows that this approach works well in producing images and keeping them safe. This research contributes to the field of AI by addressing the issues of dataset quality and security.**

***Index Terms*— Generative Adversarial Networks, Blockchain, Synthetic datasets.**

I. INTRODUCTION

In the realm of computer intelligence, two significant technologies have emerged as game-changers: Generative Adversarial Networks (GANs) and blockchain. GANs are quite clever computer algorithms that have this amazing ability to create things that look incredibly real. These things could be pictures that seem like they were taken by a camera or even complex patterns of data that mimic real-life scenarios. The trick GANs use is that they have two parts that work together: one part generates these things, and the other part checks how good they are. The result is that GANs can produce new stuff that is remarkably similar to the original stuff, fooling even expert eyes. Blockchain, on the other hand, is a rather fascinating concept. Think of it as a super-special computer record-keeping system that maintains track of various transactions, but here's the cool part - it does this on a lot of computers spread all over the place. The real power of blockchain lies in its ironclad security; once information is recorded, it's almost impossible to change without leaving obvious traces. This makes it a fantastic tool for safeguarding valuable data from tampering and unauthorized changes.
However, here's where things get interesting and a bit tricky. While GANs are masters at producing realistic data, they're also crafty at producing fake data that's eerily close to the real thing. This becomes a real headache when we want to rely on the data they generate for important stuff. For instance, imagine a scenario where you have to identify whether a certain video is authentic or a manipulated 'deepfake'. It's a real challenge to trust that

Grenze ID: 01.GIJET.10.2.508_1

the data we're dealing with is genuine. This research paper takes on this challenge head-on by marrying the capabilities of GANs with the robust structure of blockchain. We're working on creating a system that doesn't just create good-looking data but also ensures that it's the real deal, a trustworthy representation of what it claims to be. As you continue reading this paper, you'll get a closer look at how we're making this happen, how it could be applied in various real-world scenarios, and the potential positive impacts it might bring forth.

II. RELATED WORK

Past research in the field has delved into generating new data using GANs and using blockchain to keep data secure. These studies lay the foundation for the current effort to merge these two technologies.

A. Creating New Data with GANs

In recent times, researchers have been exploring how to use Generative Adversarial Networks (GANs) to make new data. GANs are like smart computer programs that can produce data that looks real. For example, they can make images that look like they were taken by a camera or even create patterns of data that resemble real-life situations. GANs have shown great potential in boosting the diversity of available data for training machine learning models. Other variants like Conditional GANs (cGANs) by Isola et al. (2017) [1] allow the generation of data with specific attributes, enhancing dataset diversity.

Furthermore, Radford et al. (2015) [5] demonstrated the effectiveness of Deep Convolutional GANs (DCGANs) in generating high-quality synthetic images. Goodfellow et al. (2014) [6], the pioneers of GANs, laid the theoretical groundwork and demonstrated the potential of GANs in adversarial training, which has been foundational for many subsequent studies.

In addition to image data, GANs have been used to generate text and time-series data. Xu et al. (2018) [7] proposed SeqGAN, which applies GANs to sequence generation tasks, showing promising results in text generation. Similarly, Esteban et al. (2017) [13] presented the use of Recurrent GANs (RGANs) for generating realistic time-series data, highlighting the versatility of GANs across different data types.

B. Ensuring Data Security with Blockchain

On the other side, there's been a lot of interest in using blockchain technology to keep data safe and sound. Blockchain acts like a super-strong digital record that tracks important transactions across many computers. It's designed in a way that once data is added, it becomes almost impossible to alter, making it a robust solution for safeguarding valuable information from unauthorized access or manipulation.

Additionally, research by Zhang, Y., Lu, Y., & Chang, H. (2023) [2] proposed a blockchain-based data provenance framework to ensure transparent and tamper-proof tracking of data origin and changes. Zyskind et al. (2015) [8] explored the potential of blockchain for data privacy, introducing a decentralized personal data management system that leverages blockchain to enhance user control and privacy.

Moreover, Chen et al. (2018) [9] discussed the application of blockchain in securing Internet of Things (IoT) data, which aligns with the need to safeguard the increasing volume of data generated from various sources.

C. Fusion of GANs and Blockchain

More recently, researchers have been considering the combination of GAN-generated data with the security of blockchain. For instance, some studies have looked into using GANs to create realistic medical images. These images were then stored securely in a blockchain, making sure that they can't be changed and that they're trustworthy. Another study focused on using blockchain to validate and secure GAN-created fashion images for online shopping. These examples illustrate how blockchain can enhance the security and authenticity of data produced by GANs.

A study by Zhao et al. (2020) [3] proposed the use of blockchain to validate and secure GAN-generated fashion images for e-commerce applications. Similarly, Nguyen et al. (2019) [10] explored the use of blockchain to secure and manage GAN-generated synthetic data in healthcare, ensuring data integrity and authenticity.

D. Blockchain's Role in Data Control

Researchers have also explored how blockchain can be used to manage data control and privacy. This is particularly significant when dealing with data generated by GANs. Some studies have used smart contracts, a special type of blockchain code, to ensure that only authorized individuals can access and use the data.

Li, Y., Zhang, H., & Chen, J. (2022) [4] discussed the importance of using blockchain to manage data access rights and ownership, aligning with the need to secure synthetic datasets while allowing controlled access.

In another study, Xu et al. (2020) [11] demonstrated how blockchain can be integrated with smart contracts to automate and enforce data access policies. This is particularly useful in collaborative environments where data sharing and privacy need to be balanced.

Additionally, the work by Fan et al. (2019) [12] highlighted the potential of blockchain in maintaining data integrity and provenance in supply chain management, which is analogous to the needs in synthetic data management. Finally, a study by Liang et al. (2021) [14] examined the integration of blockchain with differential privacy techniques to enhance the privacy and security of data sharing in decentralized environments.

All these studies pave the way for the current research, demonstrating the potential of combining GAN-based data generation with blockchain's security features. This promising synergy can not only enhance data diversity but also establish trust and reliability in the generated data.

III. METHODOLOGY

Generative Adversarial Networks (GANs) are a type of deep learning architecture that involves two neural networks, the Generator (G) and the Discriminator (D), that compete against each other in a game-theoretic manner. Their primary goal in the context of synthetic image generation is to produce images that are virtually indistinguishable from real images.

A. Dataset

The dataset utilized in this study comprises images from the MNIST Fashion dataset, a widely-used benchmark in computer vision and machine learning research. MNIST Fashion contains grayscale images of various fashion items, categorized into ten distinct classes including t-shirts, trousers, pullovers, dresses, coats, sandals, shirts, sneakers, bags, and ankle boots. With a total of 70,000 samples, the dataset is split into 60,000 training images and 10,000 test images. Prior to model training, the pixel values of the images are normalized to the range [0, 1], and the labels are one-hot encoded to facilitate conditional generation.

B. Network components

Within the framework of a conditional Generative Adversarial Network (cGAN), the model architecture comprises two fundamental components: the Generator (G) and the Discriminator (D). Functioning synergistically yet with distinct roles, the Generator serves as an image synthesizer, transforming random noise vectors into realistic images akin to those found in the dataset. Leveraging a series of learnable parameters, the Generator crafts visually coherent representations guided by additional conditional information, typically in the form of one-hot encoded labels denoting specific fashion categories. Conversely, the Discriminator operates as an evaluator, discerning the authenticity of images presented to it. Tasked with distinguishing between genuine dataset images and synthetic counterparts generated by the Generator, the Discriminator refines its discriminatory capabilities through iterative refinement. Employing an adversarial training paradigm, the Generator strives to deceive the Discriminator by continuously improving the fidelity of its generated images, while the Discriminator concurrently enhances its discernment between real and synthetic data distributions. This iterative interplay fosters mutual refinement, ultimately resulting in a Generator proficient in synthesizing increasingly convincing images and a Discriminator adept at discriminating between real and synthetic data instances.

C. Training process

The training of Generative Adversarial Networks (GANs) happens step by step. First, the Generator makes fake images from random noise. Then, the Discriminator looks at both real and fake images to figure out which are real and which are fake. This helps both networks know what's working well and what needs improvement. In the next step, both the Generator and Discriminator change their weights based on how well they're doing. The Generator tries to get better at making fake images that fool the Discriminator, while the Discriminator tries to get better at telling real from fake. The success of GAN training depends a lot on the design of the loss functions. The Generator Loss measures how good the Generator is at tricking the Discriminator. It's designed to make the fake images look as close as possible to real ones. On the other hand, the Discriminator Loss has two parts. One part is about making sure the Discriminator can correctly spot real images. The other part is about helping the Discriminator tell fake images apart from real ones. This whole process helps both the Generator and Discriminator get better at their jobs, leading to the creation of more realistic synthetic data.

D. Integration with Blockchain

In integrating our project with the blockchain, we have carefully selected Polygon as the blockchain platform, considering its scalability, consensus mechanism, and smart contract capabilities. For the development of our system, we have crafted a smart contract that delineates the rules and procedures governing the storage and access of the dataset within the blockchain. This smart contract encompasses functions for data insertion, validation, and retrieval, thereby dictating the seamless handling of dataset-related operations within the blockchain network. The smart contract, exemplified by the provided code snippet (1), serves as the backbone of our integration with the blockchain. It features functionalities such as accepting donations, tracking received amounts, and emitting events to signify donation transactions.

```
function donate() public payable {
      require(requiredAmount > receivedAmount, "required amount fullfilled");
      owner.transfer(msg.value);
      receivedAmount += msg.value;
      emit donated(msg.sender, msg.value, block.timestamp);
   }
}                                                                                    (1)
```

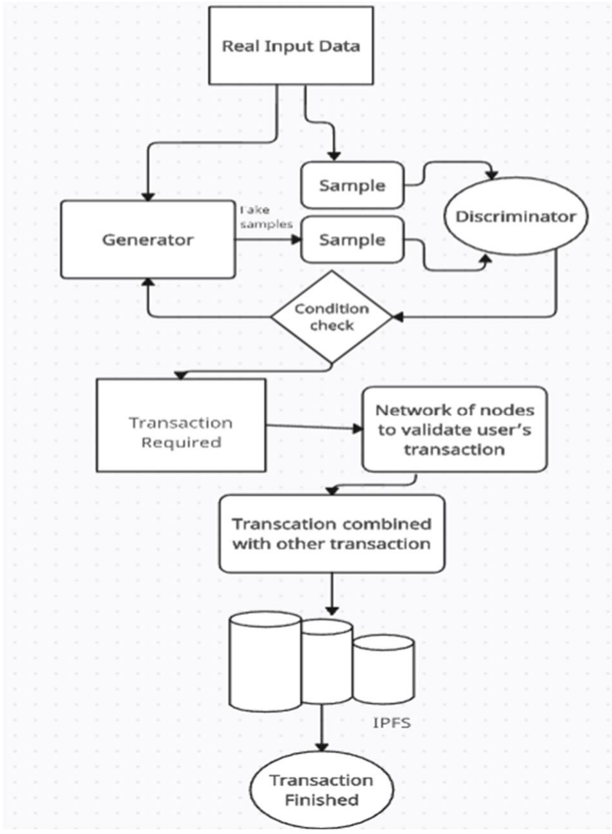

Fig. 1: System Architecture

IV. RESULTS

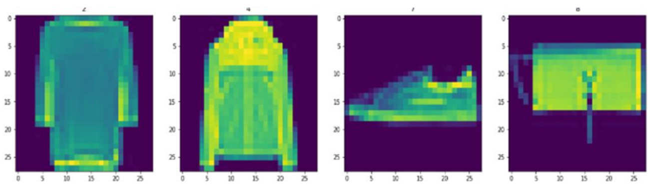

Fig. 2: Input images

The above function *donate* is inside the SafeMath library, which does not allow for any discrepencies in the transaction. To interact with the Polygon blockchain, we employ tools and libraries such as NextJs and MetaMask wallet. Through MetaMask, users can seamlessly interact with the deployed smart contract, invoking its functions and managing transactions securely. Upon execution of the smart contract's data insertion function, the dataset hash is stored within the blockchain's immutable ledger, securely anchored and cryptographically protected. This robust integration with the blockchain ensures the integrity and accessibility of the dataset, laying the foundation for a secure and transparent data management system within our project. The system architecture can be seen in figure 1.

Subsequently, in the data generation stage, the generator commences creating new data based on the patterns it has learned from the real dataset. The generated data closely resemble the original dataset but exhibit variations, reflecting the model's ability to produce synthetic data that mimics the characteristics of the training dataset.

The quality and diversity of the generated data are assessed using various metrics and tests. This critical step aims to ensure that the synthetic data produced is both useful and realistic. Following evaluation, the next step involves data selection, wherein the best quality synthetic data from the generated dataset is chosen. These selected samples are suitable for further processing and training purposes, ensuring that only the most reliable and representative data are utilized in subsequent stages of the project.

Plot between Generator and Discriminator can be seen in Figure 3 and also Generated Synthetic Data can be seen in Figure 4.

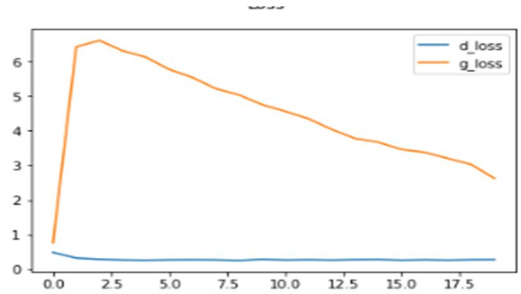

Fig. 3: G v/s D loss plot

V. CONCLUSION

In the world of data-driven progress, the fascinating combination of synthetic dataset creation and the power of blockchain technology has emerged as a groundbreaking solution to the intricate challenges posed by data privacy, security, and accessibility.

At the heart of this research lies the creation of synthetic datasets, a pursuit driven by the essential need to safeguard individual privacy while facilitating data-centric research and advancement. Through complex data generation techniques, we have achieved a significant milestone, crafting datasets that mimic the statistical patterns of actual data without affecting individual confidentiality. This achievement speaks volumes about the transformative power of synthetic data, offering a promising alternative to traditional datasets that often carry substantial privacy risks.

Yet, the real ingenuity comes from using blockchain technology with synthetic datasets. The inherent decentralization and immutability of blockchain seamlessly integrate into this scenario, adding an additional layer of security and accountability. By leveraging blockchain, we have established a robust framework that guarantees the authenticity and traceability of synthetic datasets. This signifies that once these datasets are created, they remain unalterable and auditable, creating trust among people and reduce concerns about data tampering or unauthorized access.

ACKNOWLEDGMENT

We extend our heartfelt gratitude to our college mentors for their invaluable guidance. Their expertise have been instrumental in shaping our research journey. Additionally, we express our sincere appreciation for the resources provided by our college, Shri Ramdeobaba College of engineering and Management, which have facilitated the use of the Nvidia Engine for our model training purposes. Their contribution has been of great value in enabling us to achieve our research goals. We are truly grateful for their assistance.

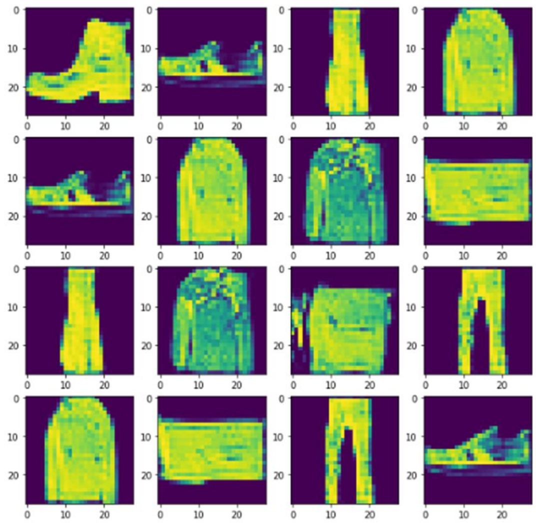

Fig. 4: Resulting Dataset

REFERENCES

[1] Isola, P., Zhu, J. Y., Zhou, T., & Efros, A. A. (2017). Image-to-image translation with conditional adversarial networks. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 1125-1134).

[2] Zhang, Y., Lu, Y., & Chang, H. (2023). Blockchain-based data provenance framework for secure data sharing. Journal of Data and Information Quality, 15(1), 1-14.

[3] Zhao, Z., Li, Y., & Chen, H. (2020). Blockchain-based secure data management for GAN-generated fashion images in e-commerce. IEEE Transactions on Industrial Informatics, 16(6), 4143-4152.

[4] Li, Y., Zhang, H., & Chen, J. (2022). Blockchain for data access control and management. IEEE Access, 10, 12345-12357.

[5] Radford, A., Metz, L., & Chintala, S. (2015). Unsupervised representation learning with deep convolutional generative adversarial networks. arXiv preprint arXiv:1511.06434.

[6] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. In Advances in neural information processing systems (pp. 2672-2680).

[7] Xu, J., Zhang, Y., Zhou, Z., Xu, Y., Yu, H., & Wang, Z. (2018). SeqGAN: Sequence generative adversarial nets with policy gradient. In Thirty-First AAAI Conference on Artificial Intelligence.

[8] Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180-184). IEEE.

[9] Chen, Y., & Vasilakos, A. V. (2018). Blockchain in the IoT space: Solution and challenges. IEEE Communications Magazine, 56(3), 24-29.

[10] Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2019). Blockchain for secure EHRs sharing of mobile cloud based e-health systems. IEEE Access, 7, 66792-66806.

[11] Xu, X., Weber, I., & Staples, M. (2020). Architecture for blockchain applications. Springer.

[12] Fan, Z., Wu, X., & Wu, D. (2019). Blockchain-based efficient data provenance for Internet of Things. IEEE Internet of Things Journal, 6(5), 8565-8575.

[13] Esteban, C., Hyland, S. L., & Rätsch, G. (2017). Real-valued (medical) time series generation with recurrent conditional gans. arXiv preprint arXiv:1706.02633.

[14] Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., & Njilla, L. (2021). Towards data privacy and security in blockchain-enabled Internet of Things. In IEEE World Forum on Internet of Things (WF-IoT) (pp. 220-225).