International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Conference Proceedings: Volume: 05 ACME – 2026 DOI: 10.55041/ISJEM.ACME093
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

FraudTrack AI: Real-Time E-commerce Transaction Monitoring

Mr. M Bhanuprakash
Assistant Professor
Department of AIDS
Annamacharya Institute of Technology and Sciences
Tirupati-517520,
mmbaluprakash@gmail.com

M Gnapika
UG Scholar, Department of AIDS Annamacharya Institute of Technology and Sciences, Tirupati-517520, A.P.
gnapikareddy08@gmail.com

P Lohitha
UG Scholar, Department of AIDS Annamacharya Institute of Technology and Sciences, Tirupati-517520, A.P.
lohithapothireddy@gmail.com

J Charan
UG Scholar Department of AIDS Annamacharya Institute of Technology and Sciences Tirupati-517520 A.P.
charanjambugolam@gmail.com

R Adikeshava reddy
UG Scholar, Department ofAIDS Annamacharya Institute of Technology and Sciences, Tirupati-517520,
adikeshavareddyrajula@gmail.com

Abstract- The paper aims to discuss how the generative artificial intelligence models, such as GANs, VAEs, and their combination, could be utilized for the improvement of real-time fraud detection in the field of e-commerce. Due to the rapid development of online transactions, the detection of fraudulent activities has become a sophisticated issue.

The results showed that GANs have great potential for generating synthetic data related to fraud, which could be used on a large scale for proper training of fraud detection systems in dealing with problems of data imbalance. On the other hand, VAEs were also found to be helpful for proper identification of sophisticated patterns of data, which could be used for proper fraud detection. The combination of GANs and VAEs was proposed for utilizing the potential of both methods.

The results showed that the proposed method has better accuracy, flexibility, and scalability compared to individual models, making it more suitable for

dealing with the dynamic environment of e-commerce. However, it is important to note that there are certain ethical concerns raised by these models, such as privacy and biases, as discussed in the paper.

I INTRODUCTION

E-commerce business has been rising rapidly and changing the way business is conducted or the way individuals are consuming products drastically with more convenience and accessibility as well as diversification of products. However, this also resulted in a tremendous surge in fraudulent activities taking place within the e-commerce platforms. Various forms of e-commerce fraud such as identity theft, payment fraud, and account takeover are posing a significant threat of damaging the financial as well as reputational loss to the end consumer as well as the company. Traditional mechanisms of detecting such fraudulent activities using parameterized techniques are not capable of reflecting on the advanced techniques adopted by the fraudulent entities.In order to overcome the limitations of the existing techniques, this project proposes an innovative solution to the existing problem of detecting e-commerce fraud using the hybrid Generative Adversarial Network and Variational Autoencoder within the scope of Generative Artificial Intelligence techniques. The hybrid GAN-VAE technique can generate synthetic data as well as detect fraudulent patterns by leveraging the advantages of the GAN as well as the VAE techniques. The proposed system strives to create a more realistic and real-time form of fraud detection compared to the traditional approach. This can be achieved through an

improvement in the detection of outliers and the support of high-precision predictions. Furthermore, this strategy also reveals the importance of generative AI in the field of cybersecurity. However, there are some ethical concerns that must be taken into consideration when using this model. Some of these concerns include privacy, the biases of the model's predictions, and security measures versus user experience. Therefore, this project not only focuses on the efficiency of the model that is being proposed but also the ethical use of generative AI in the e-commerce industry.

II LTERATURE REVIEW

The application of the Generative Artificial Intelligence in fraud detection in e-commerce is a new direction of interest, with good opportunities to improve fraud detection practices.

A. *GenerativeModels in FraudDetection*

The application of Generative Adversarial Networks suggests that the main limitation is always trying to target artificial data that represents fraud trends on a higher level. However, the main results indicate that the main evidence suggests that this methodology is going to improve the fraud detection system by adding more numbers that represent the actual situation [4]. VAEs have more errors and false positives when using large mixed populations [5].

B. *HybridGenerativeModels*

Hybrid Protein-Based Generative Adversarial Networks and Variational Autoencoders Hybrid Models, in some way, are taking off the ground with regard to balance-boosting

C. *Real-TimeFraudDetectioninE-commerce*

Hybrid Models max optimize the product of Generative Adversarial Networks and Variational Autoencoders elasticity to address anomaly properties to do a better fraud.

D. *Ethicaland PrivacyConcerns*

The second problem is that the Generative approach to artificial intelligence has ethical issues when it comes to the application in the field of finance, fraud, and the constant unwarranted discrimination against a particular race or region may be present since the models applied may not be representative of the existing population, hence the need to apply more focus in the development of the approach in the field of fraud detection in ethnically diverse populations [6].

III .METHODOLOGY

A. Data Acquisition & Preprocessing

The information about the transactions, actual as well as fake, is provided on the e-commerce platforms. The data is cleaned by taking care of the missing values, encoding the categorical data, and normalizing the numerical data.

B. Development of generative models

GAN MODEL:

The Generative Adversarial Network is conditioned in a way that it generates fake-looking fabricated fraud transactions.

VAE MODEL

The Variational Autoencoder is used in the way that the latent representation of the data is found, and the abnormalities are detected by quantifying the reconstruction errors.

Hybrid GAN-VAE Model

The hybrid model is created by combining the Generative Adversarial Network and the Variational Autoencoder, which makes the best use of the properties of the two models.

Training Process

The Generative Adversarial Network balances the actual data with the fake data, while the Variational Autoencoder is used for the reconstruction, recording the patterns, and finding the abnormalities.

C. Data Collection

So, in order to devise an efficient mechanism for detecting fraud, the entire set of data related to e-commerce transactions, as well as the actual transactions and the fraud transactions, needs to be collected.

A. Data Sources

TransactionalRecords
It is also important to make sure that the hybrid GAN VAE model is used in the right way with the right kind of data collection.

Fraud Datasets

The data related to the e-commerce transactions includes the transaction ID, the details of the customers involved in the transactions, the details of the products involved in the transactions, the mode of payment involved in the transactions, the amount involved in the transactions, and the time stamp.

Device and Network Data
The data related to the fraud transactions includes the fraud transactions with which the model has been trained in the past.

Payment Method Data
The data related to the fraud transactions includes the IP address, the device type such as the browser, the devices, and the network through which the model would be able to detect the fraud transactions.

B. Data Preprocessing

Data Cleaning and Transformation
The data related to the mode of transaction, such as the risk factors related to the transactions, such as the use of abnormal payment processors and the transactions done in a foreign location, needs to be collected.

Anonymization
Aspects such as customer ID, IP, and location remain anonymous to maintain privacy.

Balancing Using Synthetic Data
To overcome the problem of class imbalance, synthetic fraudulent samples are created using GANs, enhancing the model to learn various behaviors of frauds.

Table1 : Original & Balanced dataset

Transaction Type	OriginalDataset	Balanced Dataset(After SyntheticData Generation)
Fraudulent	5000	95000
Non-Fraudulent	95000	95000
Total	100000	190000

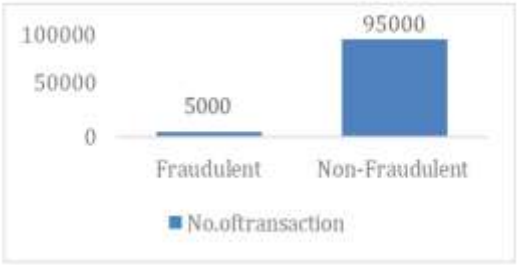

FIG.2 COMPARISON OF FRAUDULENT AND NON-FRAUDLENT TRANSACTIONS

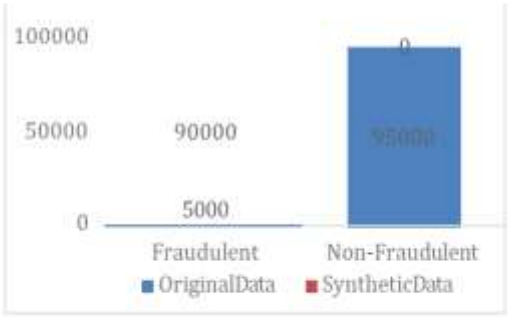

FIG.3 COMPARISON OF ORIGINAL AND SYNTHETIC DATA

IV . RESULTS

The proposed models GAN, VAE, and Hybrid GAN-VAE are compared based on the major metrics such as Accuracy, Precision, Recall, F1-Score, Area Under the Curve (AUC), and Latency. These metrics can be used to evaluate the success of each of the models in detecting fraudulent transactions.

A. Model Performance Metrics

True Positive (TP): The fraud transactions that were correctly identified as fraud.
False Positive (FP): The authorized transactions that were incorrectly identified as fraud
False Negative (FN): The legitimate frauds that were incorrectly identified as fraud.
True Negative (TN): The rightful transactions that were correctly identified as rightful.

Data Preprocessing Time (DPT): The time taken to clean, transform, and prepare the raw transactional data into a form that is appropriate as input to models.

Model Inference Time (MIT): The time taken by the model to process the processed input data and produce output (fraud or non-fraud).

Post-processing Time (PPT): The time it takes to convert the raw output produced by models into something useful, such as labels or reports.

B. EVALUATION FORMULAS

B. Evaluation Formulas

Precision (P):

Recall (R) / True Positive Rate (TPR):

False Positive Rate (FPR):

$$FPR = \frac{FP}{FP + TN}$$

F1-Score:

$$F1 = \frac{2PR}{P + R}$$

Accuracy (A):

$$A = \frac{TP + TN}{TP + TN + FP + FN}$$

Latency (L):

$$L = DPT + MIT + PPT$$

Where:

- DPT: Data Preprocessing Time
- MIT: Model Inference Time
- PPT: Post-processing Time

C .MODEL PERFORMANCE COMPARISION

TABLE 2. MODEL PERFORMANCE COMPARISON

Metric	GAN Model	VAE Model	Hybrid GAN-VAE Model
Precision	91%	85%	92%
Recall	84%	88%	90%
F1-Score	87.5%	86.5%	91%
Accuracy	89%	86%	92%
AUC	0.88	0.88	0.92
Latency(seconds)	2-3sec	1.5sec	3.5sec

Table 2: Health Score Distribution

Status Category	Score Range	SystemAction Triggered
Excellent	80–100	Maintenance Recommendations
Good	60–79	Lifestyle/Exercise Advice
Fair	40–59	Nutrition Adjustments
Needs Attention	0–39	High-Priority Medical Warning

D. Result Analysis

The best performance is associated with the Hybrid GANVAE model in most cases, leading to an increased possibility of detecting fraud.

The GAN is better suited to enhance the performance with respect to synthetic data generated as realistic frauds, while VAE is better suited to detecting fraud.

The hybrid model is able to effectively combine both strengths, leading to an increase in accuracy, precision, and F1-score.

In spite of the hybrid model being associated with a slight increase in latency, it is able to provide better overall detection performance.

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Conference Proceedings: Volume: 05 ACME – 2026 DOI: 10.55041/ISJEM.ACME093
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

TABLE 3. TRANSACTION METRICS

Metric	GAN Model	VAE Model	Hybrid GAN-VAE Model
Transactions Processed/Batch	10,000	10,000	10,000
Average Latency/Transaction	2.5sec	1.5sec	3.5sec
Total Batch Processing Time	25,000 sec	15,000 sec	35,000 sec

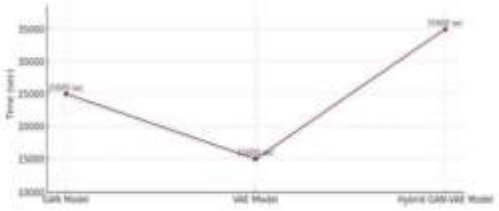

FIG.6AVERAGETRANSACTIONTIMEOFMODELS

Let's conclude testing with three fraud types: Account Takeover, Payment Fraud, and Synthetic Identity Fraud:

TABLE4.DISTRIBUTIONOFRECALLPERCENTAGE

Fraud Type	GAN Recall (%)	VAE Recall (%)	Hybrid Recall(%)
Account Takeover	82	88	89
Payment Fraud	85	90	91
Synthetic Identity Fraud	78	86	88

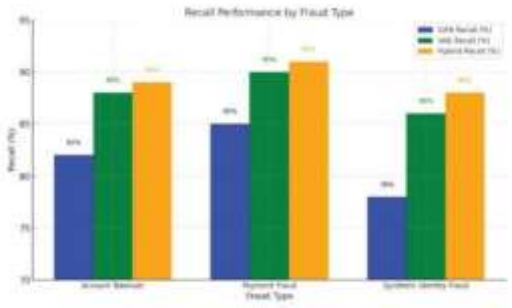

FIG.7RECALLPERFORMANCEBY FRAUD TYPE

TABLE5.DISTRIBUTIONOFFALSEPOSITIVERATE

Demographic	GAN False Positive Rate (%)	VAE False Positive Rate (%)	Hybrid False Positive Rate(%)
Region A	10.5	12.1	9.8
Region B	7.8	8.9	7.2
Region C	11.2	13.4	10.1

FIG.8COMPARISON OF FALSE POSITIVE RATES

CONCLUSION

The aim and objective of this project are to focus on the efficiency of the application of the generative AI technique, i.e., the hybrid model of GAN-VAE, in detecting the frauds related to e-commerce. The efficiency of the GAN-VAE model in detecting known as well as unknown fraud patterns is increased in a significant manner. The hybrid model of GAN-VAE is precise as well as robust in detecting fraud transactions as compared to the GAN and VAE models.

The paper has highlighted that the conventional rule-based system cannot be used for dealing with the dynamic as well as varying nature of the frauds related to e-commerce. On the other hand, the proposed hybrid model of GAN-VAE has given a dynamic solution for dealing with the varying nature of the frauds related to e-commerce. Even if we take into consideration the demerits of the proposed model, such as the computational cost as well as latency, the efficiency of the detection process is more advantageous as compared to the demerits.

Furthermore, the ethical issues of data privacy, the removal of bias, and the trust of the users are of primary importance when it comes to the implementation in the real world.

To conclude, the domains in which the generative AI systems are likely to create an impact, especially when the model is hybrid, i.e., GAN-VAE, are the development of the fraud detection process in the e-commerce industry, making it more precise, dynamic, and resourceful. These systems are likely to be taken to the next level in the future by adding features such as optimization, as well as the integration of advanced learning techniques, in order to make the systems more powerful and applicable in the real world.

REFERENCES

[1] U P A Naik and P A S Sri, AI Driven Health: Web App to Better Healthcare, 5th Int. Conf. Smart Electronics and Communication (ICOSEC), IEEE, 2024.

[2]The Road to Explainable AI via Machine Learning by A Holzinger, Proc. DISA, IEEE, 2018.

[3] K Wang et al, A systematic review on the effectiveness of mobile apps in the management of mental health, Journal of Psychiatric Research, 2018.

[4] C Oliveira et al, Effects of mobile app-based psychological interventions, Frontiers in Psychology, 2021.

[5]C Nash, R Nair, and S M Naqvi, Machine learning in the diagnosis of ADHD and depression, IEEE Access, 2023.

[6]Roumeliotis et al, K I, LLaMA2: Early adopters utilization,2023.

[7] Y Natarajan et al, Improving medical information retrieval a language model, Proc. ICC-ROBINS, IEEE, 2024.

[8]Y S Kiyak et al, Faster generation of clinical reasoning with LLM, Revista Espanola de Educacion Medica 2024.

[9]ChatDoctor: A Medical chat model finetuned on LLaMA, Y Li et al, Cureus, 2023.

[10] P Wang et al, Assessment of the nutritional characteristics of food: A scoping review, Nutrient, 2022.