

## ABSTRAK

Ketidakamanan transaksi kartu kredit menjadi perhatian utama dalam industri keuangan saat ini, dengan peningkatan kasus penipuan dan aktivitas ilegal yang mengancam integritas transaksi elektronik. Dalam rangka mengatasi tantangan ini, penelitian ini mengusulkan pendekatan yang menggabungkan metode Variational Autoencoder (VAE) dan Generative Adversarial Network (GAN) untuk mendeteksi fraud pada transaksi kartu kredit secara efektif. Metode VAE digunakan untuk melakukan representasi laten data transaksi kartu kredit, mengurangi dimensi data asli menjadi bentuk yang lebih terstruktur dan menghilangkan noise yang tidak penting. Selanjutnya, GAN digunakan untuk menghasilkan sampel-sampel data yang sebenarnya dari distribusi data asli, membantu dalam pembuatan data sintesis yang merepresentasikan pola transaksi normal. Proses ini membantu dalam mengatasi masalah ketidakseimbangan kelas antara transaksi normal dan fraud. Eksperimen dilakukan menggunakan dataset transaksi kartu kredit yang mencakup berbagai jenis transaksi, termasuk transaksi normal dan fraud. Hasil eksperimen menunjukkan bahwa pendekatan yang diusulkan mampu mengidentifikasi kasus fraud dengan tingkat akurasi yang signifikan. Metrik evaluasi seperti akurasi, presisi, recall, dan F1-score digunakan untuk mengukur kinerja model, dan hasilnya menunjukkan peningkatan dalam mendeteksi kasus fraud dibandingkan dengan metode pendekatan lainnya. Penelitian ini berhasil menggabungkan keunggulan Variational Autoencoder dalam ekstraksi fitur yang lebih baik dengan kemampuan Generative Adversarial Network dalam menghasilkan data sintesis yang realistis. Hasil eksperimen menunjukkan potensi pendekatan ini dalam mendeteksi fraud pada transaksi kartu kredit secara efektif, memberikan kontribusi dalam pengembangan solusi keamanan yang lebih kuat untuk industri keuangan.

Kata kunci:

Deteksi fraud; kartu kredit; deteksi kecurangan, Variational Autoencoder; Generative Adversarial Network

## **ABSTRACT**

*Credit card transaction insecurity is a major concern in today's financial industry, with an increase in cases of fraud and illegal activity that threaten the integrity of electronic transactions. In order to overcome this challenge, this study proposes an approach that combines Variational Autoencoder (VAE) and Generative Adversarial Network (GAN) methods to effectively detect fraud in credit card transactions. The VAE method is used to perform a latent representation of credit card transaction data, reducing the dimensions of the original data to a more structured form and eliminating unnecessary noise. Furthermore, GANs are used to generate actual data samples from the original data distribution, aiding in the creation of synthetic data that represents normal transaction patterns. This process helps in overcoming the problem of class imbalance between normal transactions and fraud. The experiment was conducted using a dataset of credit card transactions covering various types of transactions, including normal transactions and fraud. The experimental results show that the proposed approach is able to identify fraud cases with a significant degree of accuracy. Evaluation metrics such as accuracy, precision, recall, and F1-score were used to measure model performance, and the results showed an improvement in detecting fraud cases compared to other approach methods. This research successfully combines the advantages of Variational Autoencoder in better feature extraction with the ability of Generative Adversarial Network in producing realistic synthetic data. The experimental results demonstrate the potential of this approach in effectively detecting fraud in credit card transactions, contributing to the development of stronger security solutions for the financial industry.*

### **Keywords:**

*Fraud detection; credit card; fraud detection, Variational Autoencoder; Generative Adversarial Network*