BAB II
KAJIAN LITERATUR

2.1 Tinjauan Pustaka

Pada bagian ini berisi landasan teori yang digunakan pada penelitian. Konsep penelitian dimulai dari pengenalan proses deteksi anomali. Adanya data yang tidak seimbang antara data normal dan data *fraud*, sehingga diperlukan teknik augmentasi data menggunakan *Conditional Tabular Generative Adversarial Networks* (CTGAN).

2.1.1 *Fraud* pada Transaksi Kartu Kredit

Dalam beberapa tahun terakhir, layanan transaksi online melalui telepon seluler dan aplikasi *web* semakin meningkat. Hal ini menyebabkan peningkatan jumlah transaksi pembayaran *online*. Penipuan dengan menggunakan kartu kredit telah mengakibatkan kerugian pendapatan bagi lembaga keuangan global dan menambah beban bagi pengguna kartu kredit. Menurut Asosiasi Kartu Kredit Indonesia, pada tahun 2023 terdapat jumlah kartu kredit sebesar 17.693.269 kartu, dengan jumlah transaksi sebesar 219.502.988 transaksi.

Pada gambar 2.1 di bawah ini, menampilkan data penipuan kartu kredit yang diproyeksikan secara global sampai 2027 [12]. Dapat dilihat bahwa kerugian penipuan kartu kredit mencapai hampir 30 miliar dollar pada tahun 2019 dan diperkirakan meningkat setiap tahun.

Gambar 2. 1 Data *Fraud* Secara Global

Dari data yang dilaporkan tersebut, penipuan kartu kredit menjadi ancaman besar bagi kestabilan bisnis. Namun, untuk mengatasi tantangan penipuan kartu kredit, sangat penting untuk mengerti mekanisme-mekanisme dalam melakukan *fraud*. Menurut [13], penipuan kartu kredit dapat dilakukan dalam beberapa cara, yaitu:

a. Tindakan penipuan kriminal dengan menggunakan akun dan/atau informasi pribadi yang tidak sah.
b. Penggunaan akun secara ilegal untuk keuntungan pribadi.
c. Pemalsuan informasi akun untuk mendapatkan barang atau jasa.

2.1.2 Deteksi *Fraud* Menggunakan *Machine Learning* (ML)

Penggunaan ML untuk mendeteksi *fraud* dapat melakukan klasifikasi terhadap transaksi yang bisa dikelompokkan sebagai transaksi normal atau *fraud* dengan berdasar pola transaksi sebelumnya. Peningkatan volume data transaksi kartu kredit dapat dimanfaatkan untuk menemukan anomali dalam data tersebut menggunakan metode seperti *Autoencoders, Long Short Term Memory* (LSTM) dan *Convolutional Neural Network* (CNN) [14]. *Decision Tree Classifier* juga bisa diimplementasikan dengan mudah pada deteksi *fraud* kartu kredit, tetapi memiliki kinerja yang cukup rendah dengan data kompleks. Di sisi lain, *Artificial Neural Network* (ANN) menunjukkan kinerja yang lebih baik dengan kumpulan data besar dan kompleksitas tinggi. Akan tetapi, ANN membutuhkan daya pemrosesan yang tinggi [15].

Sebuah studi perbandingan pada *Neural Network* (NN), *Multilayer Perception Layer* (MPL) dan CNN disajikan pada penelitian [16]. Fitur yang dipilih dalam pembuatan data adalah atribut umum yang diperoleh dari basis data lembaga keuangan. *Dataset* yang dipakai memiliki data yang *imbalance*. *Dataset* kemudian diseimbangkan dengan menggunakan *under-sampling*. Penggunaan *Neural Network* seperti *Autoencoders* dilakukan pada penelitian [17]. Metrik performa yang dipilih untuk evaluasi model adalah *confusion matrix*, *precision*, *recall* dan *accuracy*. Pada penelitian ini, *Autoencoders* memiliki hasil yang sangat memuaskan dan memiliki nilai F1 yang tertinggi.

Penelitian pada deteksi transaksi *fraud* juga dilakukan dengan membuat perbandingan antara CNN, *Stacked* LSTM (SLSTM) dan model hibrida yang menggabungkan CNN dan LSTM (CNN-LSTM) [18]. CNN efektif dalam mempelajari urutan jangka pendek dalam data, sementara LSTM mampu mempelajari urutan jangka panjang. *Dataset* yang digunakan berasal dari Bank Indonesia dan kelas mayoritas nilai penipuan diambil sampelnya (*under-sampling*) dalam 4 rasio berbeda untuk membuat 4

dataset pengujian. Penelitian ini merepresentasikan *features* berdasarkan waktu dan PCA digunakan untuk pengurangan dimensionalitas.

2.1.3 *Imbalanced Data* (Ketidakseimbangan Data)

Pada *dataset* transaksi kartu kredit ataupun data keuangan lain seperti klaim asuransi, ketidakseimbangan data merupakan masalah yang sering muncul. Hal ini menyebabkan distribusi data yang sangat timpang [19], [20]. Transaksi data *fraud* dengan kartu kredit sangat timpang jika dibandingkan dengan pembayaran yang sah. Ketimpangan data transaksi *fraud* ini perlu lebih banyak sampel untuk melatih model secara efektif agar dapat digeneralisasikan ke sebuah *dataset* [9]. Dengan kata lain, kasus penipuan kartu kredit termasuk minoritas jika dibandingkan dengan pembayaran legal, sehingga memunculkan ketidakseimbangan data. Hal ini menyebabkan kurang terwakilinya satu kelas jika dibandingkan kelas lain. Ketidakseimbangan kelas menghasilkan performa klasifikasi yang buruk dari pendekatan *machine learning* untuk kelas minoritas [21].

Para ahli berpendapat bahwa metode pembuatan data sintetis merupakan salah satu solusi paling efektif untuk mengatasi permasalahan *imbalanced data* [22], [23], [24]. Pendekatan dengan data sintetis juga dapat mengurangi permasalahan *overfitting* pada permodelan. *Imbalanced* data terjadi ketika jumlah data dari satu kelas atau beberapa kelas memiliki jumlah yang jauh lebih banyak dibandingkan jumlah data dari kelas lainnya dalam suatu kumpulan data. Untuk mengatasi ketidakseimbangan data, ada dua teknik yang umum digunakan, yaitu teknik *oversampling* dan teknik augmentasi.

Data *fraud* merupakan data *outliers* yang pada beberapa kasus dianggap tidak berpengaruh terhadap analisis. *Oversampling* bertujuan untuk meningkatkan jumlah data point di kelas minoritas dengan cara menyeimbangkan jumlah data point antara kelas mayoritas dan minoritas. Teknik *oversampling* yang sering digunakan dan memiliki performa cukup baik yaitu *Synthetic Minority Oversampling Technique* (SMOTE). SMOTE bekerja dengan mengidentifikasi tetangga terdekat dari data *point* minoritas yang ada dan kemudian melakukan penambahan data *point* yang baru disepanjang garis antara data *point* tersebut dan tetangganya [7], [8], [9], [10].

Pada teknik augmentasi data, difokuskan pada penambahan variasi yang dihasilkan dari data yang sudah ada, khususnya pada data minoritas. *Generative Adversarial Networks* (GANs) memiliki kemampuan untuk mengembangkan data sintetis. Pada penelitian perbandingan GANs dan teknik *resampling*, kemampuan model yang diusulkan berbasis

GANs memiliki performa yang lebih akurat dibanding teknik *resampling* seperti SMOTE, ADASYN dan B-SMOTE [25].

2.1.4 GAN dan CTGAN

Generative Adversarial Network (GAN) adalah model generatif yang didasarkan pada teori permainan *zero-sum*. GAN terdiri dari dua jaringan, yaitu *generator* (G) dan *discriminator* (D) [26]. Selama pelatihan, *generator* terus meningkatkan kemampuannya untuk menciptakan data palsu. Tujuannya adalah untuk menipu *discriminator*. Di pihak *discriminator*, berfungsi untuk menilai apakah data input tersebut nyata atau buatan. Kedua komponen tersebut secara *iterative* saling mengoptimalkan sehingga mencapai keseimbangan dinamis. *Generator* akhirnya menghasilkan sampel simulasi dan menyelesaikan augmentasi data. Fungsi *loss* dari GAN ditunjukkan pada persamaan 2.1 di bawah ini.

$$min_G max_D V(G,D) = E[logD(x)]_{x-p_{data}(x)} + E[\,log(1 - D(G(z)))]_{z-p(z)} \quad .....(2.1)$$

Dimana:

min_G = *minimum over* G (nilai loss yang dialami *generator*)

max_G = *maximum over* D (peningkatan nilai loss yang dialami *discriminator*)

E[ ] = Ekspektasi

D(x) = probabilitas *discriminator* mengklasifikasikan data input (x) sebagai data asli

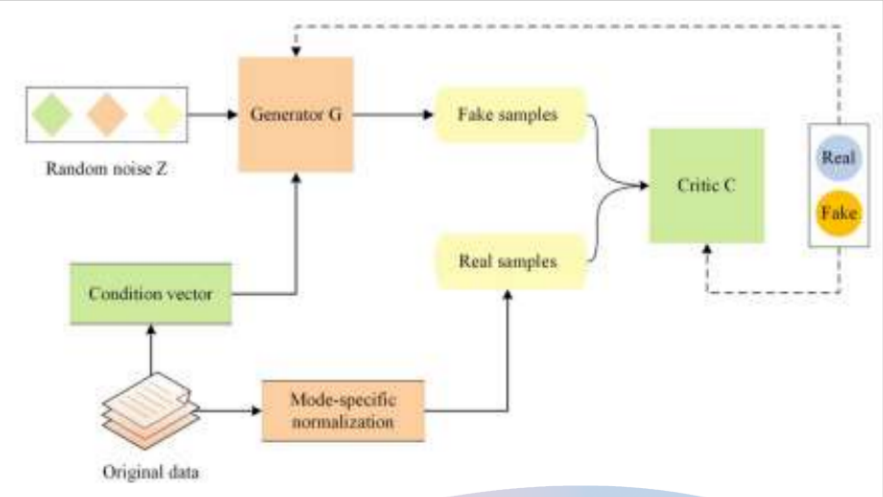
$p_{data(x)}$ = distribusi probabilitas sebenarnya dari data asli

G(z) = *output* dari *generator* berdasarkan vektor *noise input* (z)

D(G(z))= probabilitas *discriminator* mengklasifikasikan output *generator* sebagai data asli

p(z) = distribusi probabilitas vektor *noise input* (z) yang diberikan kepada G

Meskipun GAN dapat menghasilkan sampel data sintetis yang sesuai dengan distribusi data yang nyata, model ini tidak cocok untuk menghasilkan data tabular. CTGAN adalah model generatif berbasis GAN yang telah dioptimalkan untuk tugas pembuatan data tabular [11]. CTGAN mempertimbangkan informasi kondisional dalam data tabular dan menggunakan struktur *generator* khusus. Arsitektur dari CTGAN ditampilkan pada gambar 2.2.



Gambar 2. 2 Arsitektur *Conditional Tabular* GAN [6]

CTGAN terdiri dari dua jaringan saraf, yaitu *generator* (G) dan *critic* (C). Pada arsitektur GAN dikenal jaringan discriminator, pada CTGAN jaringan saraf *critic* berfungsi sama dengan *discriminator*. Untuk mengatasi distribusi *non-Gaussian* dan multi modal pada kolom kontinu di dalam data tabular, CTGAN menggunakan normalisasi mode-spesifik. Generator kondisional dan pelatihan berdasarkan sampel digunakan untuk mengatasi masalah kategori yang tidak seimbang dalam kolom diskrit. Fungsi *loss* CTGAN ditunjukkan pada persamaan 2.2 di bawah ini.

$$L = E_{G(z)\sim Pg}[D(G(z))] - E_{x\sim Pr}[D(x)] + \lambda E_{y\sim Py}[(\|\nabla_y D(y)\| - 1)2] \quad \text{..... (2.2)}$$

Dimana:

y = sampel yang diinterpolasi secara linier ke data nyata x

λ = faktor penalti gradien

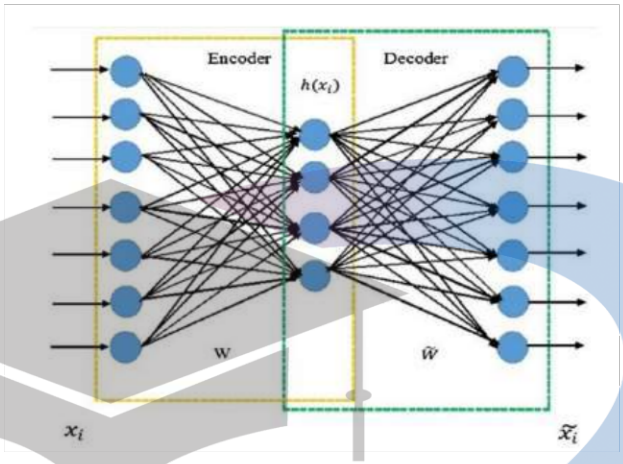
Pr = distribusi data nyata

Pg = distribusi data buatan

Dataset kartu kredit adalah tipe data tabular yang mengandung informasi data dan klasifikasi. CTGAN dirancang khusus untuk menghasilkan data tabular dan secara efektif dapat mempelajari distribusi data kartu kredit. Setelah itu CTGAN menghasilkan sampel sintetis yang sesuai dengan distribusi data nyata. Hal ini berguna untuk augmentasi data sambil tetap menjaga kegunaan data, sehingga data sintetis dan data sebenarnya tidak terlalu banyak perbedaan karakteristik.

2.1.5 *Autoencoders (AE)*

Autoencoders adalah jaringan saraf tiruan yang terdiri dari *encoder* dan *decoder*. Tujuan utama dari *autoencoders* adalah pembelajaran dengan melakukan rekonstruksi *features* sehingga dapat mengurangi dimensi. Seperti terlihat pada gambar 2.3 di bawah ini, *autoencoders* terdiri dari dua bagian. Bagian pertama adalah *encoder* dan bagian kedua adalah *decoder*.



Gambar 2. 3 Arsitektur Jaringan Saraf Tiruan *Autoencoders* [27]

Encoder mengurangi dimensi dari input data ke dimensi yang lebih rendah. Jaringan yang berada di tengah adalah *hidden layers* dari *autoencoder* yang melakukan kompresi data dan menyimpannya. *Autoencoders* yang sederhana bisa memiliki hanya satu *hidden layer*, tetapi pada tingkatan yang lebih jauh lagi, *autoencoders* bisa memiliki beberapa *hidden layers*. Jaringan *decoder* berfungsi untuk melakukan *decode* atau menambah dimensi data yang tersimpan pada *hidden layers*. *Reconstruction error* digunakan untuk melakukan evaluasi pada performa *autoencoder*, dengan cara mengukur seberapa baik *input* direkonstruksi berdasarkan perbedaan dari *input* dan *output* setelah di *decode*. Fungsi *loss* dari *autoencoder* dapat dilihat pada persamaan rumus di bawah ini.

$$J_{A,E} = \frac{1}{m} \sum_{i=1}^{m} \left(\frac{1}{2} \left|\left| \hat{X}_i - x_i \right|\right|^2\right) \quad \text{..... (2.3)}$$

Dimana :

m = jumlah dari *input* sampel

$\hat{X}$ = nilai yang diamati

x = nilai yang diprediksi

2.2 Penelitian Terdahulu

Penelitian ini mengacu dan terkait pada beberapa penelitian sebelumnya yang membahas mengenai deteksi anomali dan augmentasi pada *imbalanced data*.

Tabel 2. 1 Penelitian terdahulu mengenai deteksi anomali dengan *Machine Learning/Deep Learning*

No	Judul, Peneliti, Tahun	Metode	*Dataset* yang digunakan	Hasil/Temuan
1.	***Credit Card Fraud Detection Using Deep Learning*** Anu Maria Babu, A Pratap 2020	Metode yang digunakan melibatkan data transaksi yang tidak seimbang (*imbalanced*) dan CNN. Tujuan untuk memprediksi kecurangan di bawah 300 epochs dengan akurasi 99.62%	*Dataset* Kaggle untuk *machine learning* untuk deteksi kecurangan pada kartu kredit	Temuan utama dari penelitian ini adalah ketidakefisienan dari sistem deteksi anomali yang ada saat ini. Untuk hasil dengan akurasi yang tinggi dicapai oleh pendekatan menggunakan CNN seperti yang diusulkan.
2.	***A Bagged Ensemble Convolutional Neural Networks Approach to Recognize Insurance Claim Frauds*** Youness Abakarim, Mohamed Lahby, Abdelbaki Attioui 2023	*Data-driven* menggunakan *CNN models* (*AlexNet, InceptionV3* dan *Resnet101 model*) *Bagged Ensemble* dikombinasikan dengan SVM classifier untuk menghasilkan data	*Dataset* asli yang dikeluarkan oleh perusahaan Asuransi Amerika	Mencapai tingkat akurasi sebesar 98% dalam mengenali kecurangan pada klaim asuransi otomotif. *Brier score loss* sebesar 2%
3.	***Detection of Credit Card Fraud with Machine Learning Methods and Resampling Techniques*** Moh. Badris et al 2022	Menggunakan SMOTE sebagai teknik *resampling* pada data dengan ketidakseimbangan yang tinggi	*Dataset* transaksi kartu kredit dari situs Kaggle.com	*Gradient boosting model* menghasilkan tingkat nilai recall sebesar 92%. Model ini juga menjadi model yang terbaik untuk mendeteksi kecurangan pada transaksi kartu kredit

4.	***Fraud Detection and Analysis for Insurance Claim Using Machine Learning*** Vaishnavi Patil 2023	Menggunakan *Machine Learning* dan Analisis Data untuk mengevaluasi klaim asuransi. Menggunakan *random forest* untuk melakukan klasifikasi data kecurangan.	*Dataset* yang dikumpulkan dari berbagai sumber seperti Kaggle dan Google	Penelitian menghasilkan tingkat akurasi sebesar 65% untuk mendeteksi kecurangan dengan menggunakan *random forest*. Pentingnya untuk melakukan data *cleaning* dan *integration techniques* untuk meningkatkan kualitas *dataset*
5.	***Prediction of Insurance Fraud Detection using Machine Learning Algorithms*** Laiqa Rukhsar, Waqas Haider Bangyal, Kashif Nisar, Sana Nisar 2022	Analisis perbandingan dari algoritma klasifikasi seperi SVM, *Random Forest*, *Decision-Tree*, Adaboost, KNN dan lain-lain untuk mendeteksi kecurangan pada klaim asuransi. Evaluasi dilakukan menggunakan *metric performance*.	*Auto-insurance dataset*	*Decision Tree* (DT) merupakan algoritma dengan performa yang paling bagus untuk mendeteksi kecurangan.

Penelitian terdahulu yang terkait dengan deteksi anomali pada tabel di atas, dilakukan pada data transaksi untuk mencari transaksi yang dianggap transaksi *fraud.* Beberapa penelitian sudah menggunakan *deep learning* dan ada juga penelitian yang menggunakan *shallow machine learning model* (*traditional ML model* seperti Support Vector Machine, Random-Forest, Decision Tree dan lain-lain).

Pada penelitian [28], peneliti menggunakan *dataset unsupervised* dari transaksi kartu kredit. *Dataset* ini memiliki ketidakseimbangan data yang sangat tinggi dan hanya memiliki variabel data numerik yang dihasilkan dari PCA. Metode CNN digunakan untuk melakukan analisis deteksi kecurangan. Penelitian ini menghasilkan tingkat akurasi sebesar 99.62% pada model yang diusulkan menggunakan *Max Pooling Layer*. Namun pada penelitian ini tidak dijelaskan bagaimana mengatasi *highly imbalanced data* pada *dataset* yang digunakan, dimana ini sangat penting untuk meningkatkan akurasi dan performa model. Model hanya mengambil 300 data sampel *fraud* untuk melakukan pelatihan pada CNN.

Penelitian terkait selanjutnya [29] adalah metode *Bagged Ensamble* menggunakan 3 model CNN yaitu *AlexNet*, *Inception V3* dan *Restnet 101*. Penelitian ini mengusulkan

pendekatan *data-driven* untuk mendeteksi kecurangan pada *dataset* klaim asuransi. Untuk mengatasi *imbalanced data*, dilakukan augmentasi dengan teknik *analysis-based*. Dengan menggunakan *oversampling* data dengan kelas *fraud* diperbanyak setelah sebelumnya dilakukan cleaning dengan menghilangkan baris data yang kosong dan bernilai *null*. Model data CNN disusun secara paralel dengan metode *Bagged Ensamble.* Kemudian dilakukan deteksi *fraud* terhadap pada data klaim asuransi. Tingkat akurasi dari model ini mencapai 98% dan nilai *Brier Score Loss* yang cukup rendah yaitu 2%.

Pada penelitian yang menggunakan teknik *resampling* SMOTE [30], deteksi kecurangan dilakukan pada *dataset* yang memiliki ketidakseimbangan. Dengan menggunakan SMOTE, data sintetis dihasilkan pada data kelas yang minoritas. Kemudian dilakukan pelatihan pada data augmentasi ini dengan menggunakan beberapa model algoritma. Setelah melakukan data sintetis dengan menggunakan SMOTE, kemudian dilakukan klasifikasi terhadap data *fraud* dengan menggunakan model *machine learning* yaitu *XGBoost*, *GradientBoosting* dan *Adaboost*. Ketiga model ini dilatih pada data asli dan pada data yang sudah diseimbangkan menggunakan SMOTE.

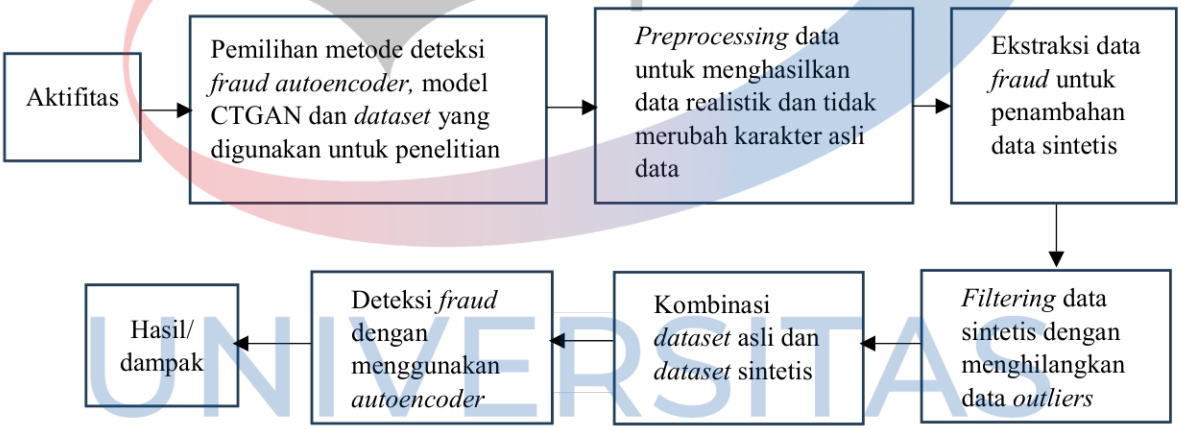
Pada penelitian [31] menggunakan *Random Forest* untuk klasifikasi data kecurangan pada klaim asuransi. Penelitian ini melakukan proses *cleaning* data dan teknik *interrogation* untuk meningkatkan kualitas *dataset*. Penelitian ini menghasilkan tingkat akurasi sebesar 65% dalam mendeteksi kecurangan. Metode analisis perbandingan terhadap beberapa model *machine learning* dilakukan pada penelitian [32] untuk mendeteksi anomali. Beberapa algoritma klasifikasi digunakan dalam penelitian ini, seperti SVM, *Random Forest*, *Decision-Tree*, *Adaboost* dan KNN. Model dilatih pada *dataset* dengan pembelajaran *supervised*. Evaluasi hasil diamati dengan melihat *performance metrics* seperti nilai *Precision*, nilai *Recall* dan *F1-Score*.

Penelitian terkait ini menjadi kondisi awal bagi penelitian yang dilakukan. Keterbatasan teknik *resampling* maupun *cleaning* adalah kualitas data yang dihasilkan tidak realistik dan rentan pada data berdimensi tinggi [33]. Khusus pada domain deteksi *fraud* pada kartu kredit, *dataset* yang digunakan merupakan data transaksi kartu kredit pada tahun 2013. Tentu saja untuk kondisi saat ini, *dataset* memiliki atribut tambahan yang menyesuaikan dengan teknologi terkini. Pada teknik *cleaning data* dan *interrogation* memiliki keterbatasan pada data yang bias, tidak akurat, *human error*, skalabilitas, waktu dan biaya. Berbeda dengan augmentasi data dengan menggunakan GAN/CTGAN yang mampu menghasilkan data yang realistik dan juga mampu menangani data yang kompleks [34].

Dari kajian yang dilakukan terhadap penelitian terdahulu, meskipun sudah ada yang melakukan penelitian deteksi anomali/*fraud* pada transaksi kartu kredit dengan kondisi *highly imbalanced data*, namun jumlah penelitian dengan menggunakan GAN/CTGAN untuk melakukan penambahan data sintetis dan dikombinasikan dengan *autoencoder* masih relatif sedikit. Hal ini diindikasikan dari hasil pencarian dengan menggunakan kombinasi kata kunci CTGAN dan *autoencoder* untuk deteksi *fraud* pada database jurnal ilmiah yang sering digunakan.

2.3 Kerangka Konseptual

Penelitian ini bertujuan untuk melakukan deteksi anomali pada data augmentasi untuk meningkatkan performa model. Kerangka konsep pemecahan masalah menggambarkan bagaimana masalah penelitian dapat diselesaikan. Kerangka konseptual pemecahan masalah penelitian dapat dilihat pada Gambar 2.4.



Gambar 2. 4 Kerangka Konseptual