BAB 1 PENDAHULUAN

1.1 Latar Belakang

Kartu kredit merupakan salah satu metode pembayaran yang umum di dunia finansial maupun bisnis. Penipuan kartu kredit adalah kejadian dimana penipu menggunakan identitas kartu kredit milik orang lain untuk melakukan transaksi. Jumlah penipuan transaksi kartu kredit meningkat setiap tahunnya, khususnya di Amerika Serikat. Pada tahun 2014, terjadi 55.553 penipuan kartu kredit, sedangkan pada tahun 2018, jumlahnya meningkat menjadi 157.688 kasus penipuan [4]. Jumlah kerugian yang diakibatkan oleh transaksi kartu kredit di seluruh dunia pada tahun 2018 sangat besar, yaitu sebesar 24,26 miliar dollar Amerika Serikat [4]. Penipuan kartu kredit dapat terjadi ketika penipu menggunakan informasi palsu untuk melakukan transaksi kartu kredit, dan pihak penerbit kartu kredit menerima transaksi tersebut atau ketika kartu kredit diterbitkan dengan benar namun transaksi melibatkan aktivitas yang bersifat curang atau penipuan. Deteksi penipuan kartu kredit memiliki tantangan tersendiri, karena dari banyaknya transaksi kartu kredit yang terjadi, hanya beberapa transaksi yang dapat dikategorikan kedalam penipuan. Oleh karena itu, diperlukan sebuah sistem yang sensitif untuk mendeteksi transaksi penipuan kartu kredit [5], [6], [7], [8], [9].

Penelitian [5] bertujuan untuk mendeteksi anomali atau *outlier* dengan menggunakan algoritme *Local Outlier Factor* dan *Isolation Forest*. Kedua algoritme ini mampu mengukur nilai anomali untuks setiap sample data. *Dataset* merupakan data transaksi kartu kredit berjumlah 285 ribu data. Hasil penelitian dengan menggunakan 10% dari *dataset*, *Isolation Forest* memperoleh *precision*, *recall*, dan *f1-score* tertinggi untuk mendeteksi kelas positif *(fraud)* dengan nilai 28%, 29%, dan 28%. Sedangkan jika keseluruhan *dataset* digunakan, *Isolation Forest* memperoleh *precision*, *recall*, dan *f1-score* tertinggi dengan nilai 33%, 33%, dan 33%. Perlu diperhatikan bahwa *recall* seharusnya menjadi ukuran dalam deteksi penipuan kartu kredit karena *recall* menekan terjadinya klasifikasi *false negative*, yang berarti bahwa transaksi diklasifikasikan sebagai transaksi bukan penipuan, tetapi sebenarnya merupakan transaksi penipuan.

Penelitian [6] bertujuan untuk mendeteksi penipuan dalam transaksi

kartu kredit dengan menggunakan pendekatan *Hybrid Classification* yaitu klasifikasi dengan menggunakan metode *K-nearest neighbors* (KNN) dan *Naive Bayes*. Algoritme KNN akan melakukan klasifikasi transaksi kartu kredit. Hasil klasifikasi dari KNN akan menjadi masukkan bagi algoritme *Naive Bayes*, sehingga hasil sesungguhnya merupakan keluaran dari algoritme *Naive Bayes*. *Dataset* pada penelitian ini diambil dari *UCI Machine Learning Repository*. *Dataset* berisi 284,807 transaksi, dengan 492 (0.172%) diantaranya merupakan transaksi penipuan. Hasil pengujian menunjukkan bahwa *Hybrid Classification* memperoleh nilai *recall* sebesar 36%, akurasi sebesar 100% dan *precision* sebesar 100%.

Penelitian [7] bertujuan untuk mendeteksi penipuan dalam transaksi kartu kredit dengan menggunakan *Light Gradient Boosting Machine* (LightGBM) dan *Bayesian-based hyperparameter optimization* yang digunakan sebagai metode *Hyperparameter tuning* dan menggunakan 2 buah *dataset*. *Dataset* pertama 284 ribu data transaksi kartu kredit dengan 492 merupakan transaksi penipuan. Sedangkan *dataset* kedua diambil dari *University of California Data Mining Contest* yang berisi data transaksi *E-commerce* berjumlah 94.683 data transaksi dengan 2,094 diantaranya merupakan transaksi penipuan. Data tersebut diambil dari 73.729 kartu kredit selama 98 hari. *Cross validation* dengan jumlah *5-fold* diterapkan agar memperoleh hasil pengukuran yang lebih akurat. Pada *dataset* kedua, LightGBM memperoleh akurasi 98,40%, *recall* 40,59%, *precision* 97,34%, dan *f1-score* 56,95%. Pada *dataset* pertama, LightGBM memperoleh akurasi 98,35%, *recall* 28,33%, *precision* 91,72%, dan *f1-score* 43,27%.

Penelitian [8] bertujuan untuk melakukan pengujian algoritme klasifikasi *machine learning* dengan metode klasifikasi *imbalance*. Algoritme klasifikasi yang digunakan adalah C5.0, *Support Vector Machine* (SVM), *Artificial Neural Network* (ANN), *Naive Bayes* (NB), *Bayesian Belief Network* (BBN), *Logistic Regression* (LR), *K-Nearest Neighbor* (KNN), dan *Artifiical Immune System* (AIS). Sedangkan untuk menangani *dataset* yang *imbalance*, digunakan metode *Random Oversampling* (RO), *One-Class Classification* (OCC) yang terdiri dari *One-Class Classification SVM* (OCC SVM) dan *Auto Associative Neural Network* (AANN), dan *Cost-sensitive models* (CS). *Dataset* penelitian ini berisi 10 juta data transaksi kartu kredit. Evaluasi pengukuran yang digunakan pada penelitian ini adalah akurasi, *precision*, *sensitivity* (*recall)* dan *area under the precision-recall curve*

(AUPRC). Hasil terbaik pada pengujian penelitian ini menunjukkan bahwa akurasi tertinggi diperoleh oleh C5.0, ANN dan SVM sebesar 96% sedangkan *recall* tertinggi diperoleh RO C5.0 dengan nilai 66% dan AUPRC tertinggi diperoleh oleh SVM dengan nilai 63%.

Penelitian [9] menguji *Synthetic Minority Oversampling Technique* (SMOTE) sebagai metode *oversampling* dengan menggunakan algoritme klasifikasi *K-Nearest Neighbors* (KNN), *Decision Tree*, *Logistic Regression*, Random Forest, dan *Extreme gradient boosting* (XGBoost). *Dataset* transaksi penipuan kartu kredit berjumlah 285 ribu data. Hasil penelitian menunjukkan bahwa akurasi tertinggi diperoleh oleh semua algoritme dengan nilai 99%. Algoritme *Random Forest* memperoleh *precision* tertinggi dengan nilai 90%. XGBoost memperoleh *recall* dan *f1-score* tertinggi dengan nilai 79% dan 84%. Pada masalah transaksi kartu kredit, evaluasi yang paling tepat digunakan adalah *recall*. Oleh karena itu, XGBoost akan digunakan dalam penelitian ini karena memiliki nilai *recall* tertinggi.

Penelitian ini akan berfokus kepada pengujian *hyperparameter Extreme gradient boosting* (XGBoost). Selain itu, metode *k-fold cross validation* akan diterapkan dalam pengujian dengan tujuan untuk melihat performa model untuk memprediksi data yang tidak ada dalam proses *training*. Metode *Synthetic Minority Oversampling Technique* (SMOTE) untuk menangani *dataset* yang *imbalance*.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas penulis merumuskan masalah sebagai berikut:

1. Bagaimana konfigurasi *hyperparameter* terbaik pada algoritme klasifikasi XGBoost?
2. Berapa nilai akurasi, *recall* dan *f-measure* terbaik algoritme XGBoost dan SMOTE?

1.3 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah menguji algoritme klasifikasi XGBoost dengan menggunakan *hyperparameter tuning*.

1. Mencari nilai *hyperparameter* terbaik XGBoost untuk klasifikasi transaksi penipuan kartu kredit.
2. Mengetahui hasil kinerja model klasifikasi *machine learning* XGBoost

dengan *k-fold cross-validation* dan SMOTE sebagai metode *oversampling*.

1.4 Batasan Masalah

Dalam penelitian ini, peneliti akan membatasi masalah yang akan diteliti, antara lain:

1. Sistem deteksi transaksi penipuan kartu kredit bekerja secara *offline* sehingga tidak dapat digunakan pada kasus *real-time*.
2. Masukan berupa *dataset* transaksi kartu kredit yang diambil dari ULB Machine Learning Group yang dapat diakses melalui situs *kaggle* [10].

1.5 Kontribusi Penelitian

Dengan dilakukannya penelitian ini, diharapkan dapat mengetahui *hyperparameter* terbaik pada XGBoost dengan menggunakan SMOTE sebagai teknik *oversampling*.

1.6 Metodologi Penelitian

Metode penelitian yang dilakukan dalam penelitian ini adalah sebagai berikut:

1. Studi Literatur
   Penulisan ini dimulai dengan studi kepustakaan yaitu mengumpulkan bahan-bahan referensi baik dari jurnal, paper, dan buku mengenai deteksi transaksi penipuan kartu kredit.
2. Data *Sampling*
   Data *sampling* yang akan digunakan berupa data transaksi pembayaran menggunakan kartu kredit dan akan diambil dari beberapa penyedia data terbuka di internet.
3. Analisis Masalah
   Pada tahap ini dilakukan analisis permasalahan yang ada, batasan yang dimiliki dan kebutuhan yang diperlukan.
4. Perancangan dan Implementasi *Algoritme*
   Pada tahap ini dilakukan pendefinisian beberapa aturan dalam teknik klasifikasi data transaksi, serta perancangan pada algoritma yang akan dipakai untuk menyelesaikan masalah berdasarkan metode yang telah dipilih.
5. Pengujian
   Pada tahap ini dilakukan pengujian terhadap aplikasi yang telah dibangun.
6. Dokumentasi
   Pada tahap ini dilakukan pendokumentasian hasil analisis dan

implementasi secara tertulis dalam bentuk laporan skripsi.

1.7 Sistematika Pembahasan

Pada penelitian ini peneliti menyusun berdasarkan sistematika penulisan sebagai berikut:

Bab I Pendahuluan

Pendahuluan yang berisi latar belakang, rumusan masalah, tujuan penelitian, batasan masalah, kontribusi penelitian, serta metode penelitian.

Bab II Landasan Teori

Landasan teori yang berisi penjelasan dasar teori yang mendukung penelitian ini.

Bab III Analisis dan Perancangan

Analisis dan perancangan yang berisi analisis berupa algoritma yang digunakan.

Bab IV Implementasi dan Pengujian

Implementasi dan pengujian yang berisi implementasi pengujian dengan berbagai data *testing* beserta hasilnya.

Bab V Kesimpulan dan Saran

Penutup yang berisi kesimpulan dari penelitian dan saran untuk penelitian lebih lanjut di masa mendatang.