BAB I
PENDAHULUAN

1.1 Latar Belakang

Kartu kredit adalah kartu pembayaran yang diberikan oleh bank kepada nasabah (pemegang kartu) yang memenuhi syarat untuk melakukan transaksi sehari-hari. Dengan menggunakan kartu kredit, pemegang kartu dapat membayar barang dan jasa tanpa memiliki uang di rekening mereka dan dapat dibayar kemudian hari ke bank. Pengeluaran dari transaksi yang sah memberikan suatu pola. Jika kartu dicuri atau diakses oleh penipu, transaksi menunjukkan pola pengeluaran yang tidak normal dan transaksi tersebut disebut transaksi curang (*fraud*) (Kamaruddin & Ravi, 2016). Hal ini juga diatur oleh Otoritas Jasa Keuangan Republik Indonesia (OJK RI) dalam Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 39/POJK.03/2019 tentang Penerapan Strategi Anti *Fraud* Bagi Bank Umum.

Kecurangan (*fraud*) adalah tindakan kriminal yang dilakukan untuk keuntungan pribadi. Untuk mencegah kerugian yang terkait dengan *fraud*, terdapat dua metode yang dapat digunakan, yaitu deteksi dan pencegahan penipuan. Pencegahan penipuan merupakan strategi proaktif yang bertujuan untuk mencegah terjadinya penipuan sebelumnya. Sementara itu, deteksi penipuan diperlukan ketika penipu mencoba melakukan transaksi penipuan. *fraud* dengan menggunakan kartu kredit mengacu pada penggunaan informasi kartu kredit secara ilegal untuk melakukan pembelian. Transaksi kartu kredit dapat dilakukan baik secara fisik maupun digital. Dalam transaksi fisik, kartu kredit digunakan secara langsung. Sedangkan dalam transaksi digital, hal ini dapat dilakukan melalui telepon atau internet. Pemegang kartu kredit biasanya memberikan nomor kartu, tanggal kadaluwarsa, dan nomor verifikasi kartu melalui telepon atau situs web (Randhawa, dkk., 2018).

Kasus *fraud* terus meningkat seiring dengan meningkatnya penggunaan kartu kredit. Meskipun berbagai metode otorisasi telah digunakan, penipuan kartu kredit masih sulit untuk dihindari. Penipu sering memanfaatkan internet karena memungkinkan mereka untuk menyembunyikan identitas dan lokasi mereka.

Industri keuangan sangat terpengaruh oleh peningkatan kasus penipuan kartu kredit. Penipuan kartu kredit mengakibatkan kerugian global sebesar $21,84 miliar pada tahun 2015 (Randhawa, dkk., 2018). Selain menyebabkan kerugian finansial yang besar bagi pemilik kartu dan pihak bank, *fraud* juga dapat mempengaruhi kepercayaan masyarakat terhadap penggunaan kartu kredit. Meskipun kejadian *fraud* relatif jarang terjadi dibandingkan dengan jumlah transaksi yang sah, mendeteksi *fraud* tersebut tetap menjadi hal yang kompleks. Oleh karena itu, identifikasi transaksi penipuan menjadi permasalahan yang menarik bagi industri perbankan dan keuangan, komunitas penelitian, dan akademisi di bidang keuangan.

Salah satu cara mendeteksi *fraud* adalah dengan menggunakan data-data nasabah yang sudah ada, lalu diproses sehingga menemukan keteraturan, pola atau hubungan dalam data berukuran besar dengan menggunakan teknik pengenalan pola seperti statistik dan matematika. Proses tersebut dinamakan *Data Mining* (Prabowo & Muljono, 2018). *Data Mining* mengacu pada penggalian atau "*mining*" pengetahuan dari sejumlah besar data. Ada sejumlah teknik *mining* data seperti *Clustering*, *Neural Networks*, *Regression*, dan beberapa model prediksi. *Data Mining* dikaitkan dengan *supervised learning* berdasarkan *data training* tentang penipuan yang diketahui dan kasus yang sah dan *unsupervised learning* dengan data yang tidak dilabeli sebagai penipuan atau sah (Bhowmik, 2008).

Sejauh ini, terdapat beberapa algoritma klasifikasi *Data Mining* yang dapat digunakan untuk identifikasi transaksi penipuan, di antaranya *Naive Bayes* (NB), *Decision Trees* (DT) dan *Support Vector Machines* (SVM) (Prabowo & Muljono, 2018). Pada penelitian ini, algoritma yang digunakan adalah *Naive Bayes*. *Naive Bayes* yang merupakan teknik prediksi berbasis probabilistik sederhana yang berdasar pada penerapan teorema atau aturan Bayes dengan asumsi independensi yang kuat pada fitur, artinya bahwa sebuah fitur pada sebuah data tidak berkaitan dengan ada atau tidaknya fitur lain dalam data yang sama (Prasetyo, 2012). *Naive Bayes* memiliki kelemahan, yaitu atribut atau fitur independen sering salah dan hasil estimasi probabilitas tidak dapat berjalan optimal. Salah satu cara untuk mengatasi masalah tersebut yaitu menggunakan metode pembobotan atribut untuk meningkatkan akurasi dari *Naive Bayes*.

Untuk memperoleh pembobotan atribut yang tepat dapat dilakukan dengan menggunakan algoritma optimisasi, seperti *Particle Swarm Optimization* (PSO), *Genetic Algorithm* (GA), *Ant Colony Optimization* (ACO), dan *Adaboost*. *Particle Swarm Optimization* (PSO) adalah metode yang terinspirasi dari perilaku sosial sekelompok burung dan ikan. Seperti algoritma genetika, PSO melakukan pencarian menggunakan populasi (*swarm*) dari individu-individu (*particle*) yang diperbarui dari setiap iterasi yang dilakukan. Untuk menemukan solusi yang optimal, setiap partikel bergerak ke arah posisi terbaik yang sebelumnya (P_{best}) dan posisi global terbaik (G_{best}). PSO digunakan untuk menyeleksi fitur (*feature selection*) atau atribut, PSO menggunakan bobot atribut yang telah dihitung dan atribut yang telah diseleksi akan diprediksi menggunakan algoritma *Naive Bayes* (Prabowo & Muljono, 2018).

Metode PSO mudah diterapkan dan dapat memilih parameter yang sesuai. Pada penelitian yang telah dilakukan oleh Prabowo dan Muljono (2018) telah dibahas masalah nasabah yang berpotensi membuka simpanan deposito menggunakan *Naive Bayes* berbasis PSO. Hasil penelitian tersebut membuktikan bahwa algoritma PSO dapat meningkatkan akurasi sebesar 7,51% dan algoritma *Naive Baiyes* berbasis PSO tersebut dapat digunakan untuk *decision support system* nasabah yang berpotensi membuka deposito karena menjadi model algoritma yang terbaik. Dengan demikian dapat disimpulkan bahwa *Particle Swarm Optimization* (PSO) dapat diaplikasikan untuk menyelesaikan permasalahan sejenis yang terstruktur.

Berdasarkan pemaparan yang telah disampaikan, penulis tertarik untuk mengkaji lebih dalam mengenai deteksi *fraud* menggunakan metode *Naive Bayes* dan seleksi fitur dengan PSO. Fokus studi kasus dari penelitian ini yaitu mengidentifikasi *fraud* dalam transaksi kartu kredit pada *dataset* dari *Bank Simulation* atau BankSim. Hasil penelitian ini diharapkan dapat menjadi rujukan bagi pihak perbankan untuk mengidentifikasi *fraud* dalam transaksi kartu kredit.

1.2 Rumusan Masalah

Berdasarkan latar belakang penelitian yang telah diuraikan oleh penulis, maka permasalahan dalam penelitian ini dapat dirumuskan sebagai berikut:

1. Bagaimana mengidentifikasi kecurangan (*fraud)* dalam transaksi kartu kredit menggunakan metode *Naive Bayes* dan *Particle Swarm Optimization* (PSO)?
2. Bagaimana hasil optimisasi *Particle Swarm Optimization* (PSO) terhadap metode *Naive Bayes* untuk mengidentifikasi kecurangan (*fraud*) dalam transaksi kartu kredit?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk mengidentifikasi kecurangan (*fraud*) dalam transaksi kartu kredit menggunakan metode *Naive Bayes* dan *Particle Swarm Optimization* (PSO) yang selanjutnya akan dianalisis hasil optimisasi dari metode yang digunakan.

1.4 Manfaat Penelitian

Penelitian ini bermanfaat untuk menambah pengetahuan dalam masalah optimisasi khususnya dalam penerapan perbankan. Hasil penelitian ini juga dapat digunakan sebagai salah satu metode untuk mengidentifikasi kecurangan (*fraud*) dalam transaksi kartu kredit dan referensi bagi peneliti lain untuk mengembangkan metode tersebut untuk *dataset* yang lain.