

MENDETEKSI KECURANGAN PADA TRANSAKSI KARTU KREDIT UNTUK VERIFIKASI TRANSAKSI MENGGUNAKAN METODE SVM

Yazid

Magister Teknik Informatika
Universitas Amikom Yogyakarta
Email: ntyazid@gmail

Arga Fiananta

Magister Teknik Informatika
Universitas Amikom Yogyakarta
Email : argafiananta@gmail.com

ABSTRAK

Kartu kredit merupakan salah satu metode pembayaran yang sangat populer dan banyak digunakan pada transaksi online. Sejalan dengan banyaknya pengguna kartu kredit dan bahkan menjadi metode pembyaran sehari-hari, keamanan dalam mem-verifikasi setiap transaksi juga sangat penting untuk ditingkatkan. Metode data mining merupakan salah satu yang dapat membantu dalam pemecahan masalah dalam keamanan transaksi kartu kredit. Penelitian ini bertujuan untuk merancang sebuah sistem verifikasi transaksi kartu kredit, yang dapat membantu pihak perbankan dalam mengetahui kemungkinan kecurangan yang terjadi. Penelitian ini menggunakan metode *support vector machine* (SVM) untuk mendeteksi kecurangan berdasarkan *outlier*/anomali pada data transaksi. Sample data sejumlah 100 data, dengan menggunakan atribut nomor akun sebagai label, bulan, dan nominal transaksi sebagai data training. Testing dilakukan dengan melakukan simulasi transaksi pada form, dengan mengisi nomor akun, bulan, dan nominal transaksi. Sistem akan mendeteksi apakah transaksi dengan nomor akun tersebut masuk dalam kelas yang sudah ditentukan pada model atau tidak. Jika keluar dari kelas maka transaksi dihentikan sementara.

Kata kunci: Kartu Kredit, SVM, *Outlier*, Verifikasi.

ABSTRACT

Credit cards are one of the most popular and many used payment methods on online transactions. In line with the large number of credit card users and even become a daily payment method, the security in verifying every transaction is also very important to be improved. Data mining is one of the most method that can assist in solving problems in credit card transaction security. This research purpose to design a verification system of credit card transactions, which can help the banks in knowing the possibility of fraud that occurred. This research uses support vector machine (SVM) method to detect fraud based on outlier / anomaly on transaction data. Sample data of 100 rows, using attribute of account number as label, month, and transaction nominal as training data. Testing is done by simulating a transaction on the form, by filling in the account number, month, and transaction nominal. The system will detect whether transaction with the account number is entered in the designated in the model class. If out of the class then the transaction is suspended.

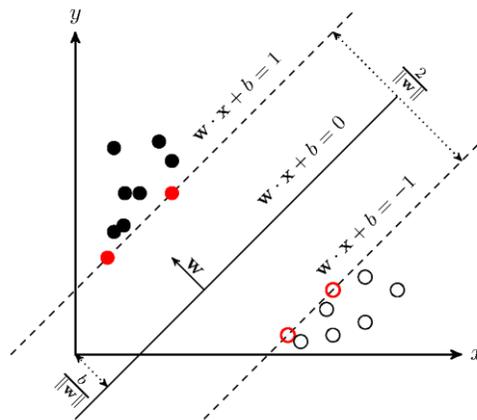
Keywords: Credit Card, SVM, *Outlier*, Verification.

1. PENDAHULUAN

Perkembangan teknologi modern dan cara komunikasi global yang sangat tinggi menyebabkan kecurangan finansial meningkat secara drastis [9]. Kecurangan dalam pembayaran elektronik digolongkan dalam tindakan ilegal yang dapat merugikan pihak perbankan ataupun nasabah [8]. Metode keamanan pada

transaksi kartu kredit terus dikembangkan guna mengurangi kecurangan dan penipuan yang terjadi. Metode data mining merupakan salah satu yang dapat membantu dalam pendeteksian kecurangan yang terjadi dengan mengenali pola transaksi (*pattern*) [1] [2] [8] [9].

Data mining adalah proses untuk mencari informasi yang berguna dari sebuah dataset yang berukuran besar. Data mining adalah pengestrakan data berukuran besar untuk menemukan keteraturan, pola, atau hubungan untuk diolah menjadi informasi yang dapat digunakan dalam pengambilan keputusan [4] [6]. Salah satu metode data mining yang populer adalah *support vector machine* (SVM) yang masuk dalam metode klasifikasi. SVM adalah metode yang berakar dari teori pembelajaran statistik. Cara kerja SVM adalah mencari *hyperplane* terbaik yang berfungsi sebagai pemisah dua buah kelas data pada *input space* [5]. *Hyperplane* (batas keputusan) pemisah terbaik antara kedua kelas dapat ditemukan dengan mengukur margin *hyperplane* tersebut dan mencari titik maksimalnya. Margin adalah jarak antara *hyperplane* tersebut dengan data terdekat dari masing-masing kelas. Data yang paling dekat disebut sebagai *support vector*.



Gambar 1. Margin Hyperplane [5]

Garis solid pada gambar 1 menunjukkan *hyperplane* terbaik yaitu yang terletak ditengah-tengah kedua kelas, sedangkan data lingkaran dengan merah penuh dan merah putih yang dilewati garis batas margin (garis putus-putus) adalah *support vector* [5].

Penelitian ini membahas bagaimana metode SVM dapat mendeteksi kecurangan pada transaksi kartu kredit, dengan mencari anomali/*outlier* pada dataset sebagai dasar dalam menentukan kecurangan transaksi tersebut. Perancangan sistem ini menggambarkan implementasi metode SVM pada sistem pendukung pengambilan keputusan (SPPK) untuk pihak perbankan dalam proses transaksi kartu kredit. SPPK dalam hal ini digunakan sebagai verifikasi setiap terjadi transaksi kartu kredit. Sistem ini akan membantu pihak perbankan dalam mengetahui indikasi kecurangan yang terjadi, sehingga dapat melakukan tindakan cepat, seperti melakukan pemberhentian transaksi atau pemblokiran sementara.

Penelitian yang berkaitan dengan kecurangan kartu kredit juga sudah pernah dilakukan oleh penelitian sebelumnya. Seperti penelitian Vaishali yang mengembangkan metode untuk pendeteksian kecurangan kartu kredit menggunakan algoritma *k-means clustering*. Sistem mendeteksi transaksi tersebut merupakan transaksi legal atau ilegal (*fraud*), kemudian *cluster* membagi tingkat kecurangan menjadi empat kategori, yaitu kecurangan tingkat rendah, tingkat tinggi, beresiko, dan beresiko tinggi. Penelitian ini menggunakan lima variabel yaitu *transaction id*, *transaction amount*, *transaction country*, *transaction date*, dan *credit card number*. Kecurangan kartu kredit tidak dapat dideteksi dengan akurasi 100%, karena jenis kecurangan selalu berganti sehingga mempersulit dalam pengkategorian kecurangan tersebut [8].

Metode pendeteksian kecurangan kartu kredit juga pernah dilakukan pada dataset yang tidak seimbang dan *anonymous*. Pendeteksian yang diusulkan adalah dengan menemukan pola transaksi legal dan *fraud* untuk setiap pelanggan dengan menggunakan frekuensi *itemset mining*. Metode yang diusulkan dapat berjalan dengan baik dan dapat menangani ketidakseimbangan kelas. Database pola penipuan dan transaksi legal dibuat terpisah, dan *update* data antara keduanya tidak sama, sehingga dapat mengurangi

keakurasian dalam pendeteksian. Oleh karena itu dibuat *update* secara berkala baik sekali dalam tiga bulan atau enam bulan atau bahkan setiap kali terjadi transaksi [7].

Penelitian lain dengan permasalahan yang sama mengusulkan metode yang berbeda sebagai pendeteksian kecurangan kartu kredit. Metode yang digunakan adalah *principal component analysis* (PCA) sebagai pendeteksi *outlier*. Data diambil dari dataset standar *german credit card fraud* yang ada pada *UCI machine learning repository*. Data terdiri dari 20 atribut yang akan dikurangi setelah menerapkan PCA. Teknik ini akan mempercepat proses deteksi dan memerlukan sedikit memori, karena atribut yang diproses hanya atribut yang penting saja dan merupakan atribut utama [3].

Penelitian sekarang mengusulkan sebuah perancangan sistem pendukung pengambilan keputusan yang membantu pihak perbankan dalam mengenali kecurangan pada transaksi kartu kredit, metode yang digunakan adalah metode *support vector machine* (SVM) yang masuk dalam metode klasifikasi. Teknik yang digunakan sama dengan penelitian sebelumnya yaitu dengan mendeteksi outlier dari dataset yang diproses.

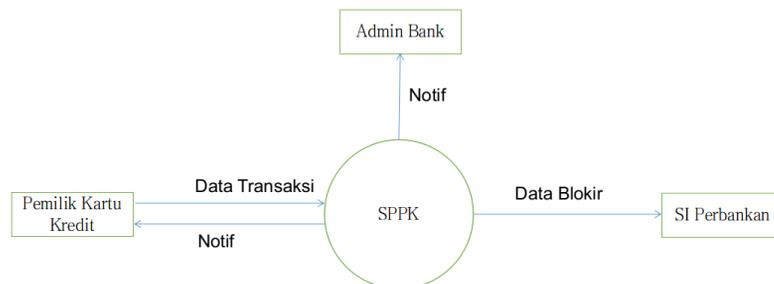
2. METODOLOGI PENELITIAN

Penelitian ini dilakukan dengan melakukan tahapan berikut:

1. Melakukan *literatur review* untuk mengetahui *state of the art problem* dari penelitian sejenis.
2. Menentukan variabel yang akan digunakan dalam klasifikasi.
3. Merancang sistem pendukung pengambilan keputusan secara keseluruhan.
4. Melakukan *training* pada dataset
5. Melakukan *testing* dan simulasi transaksi.

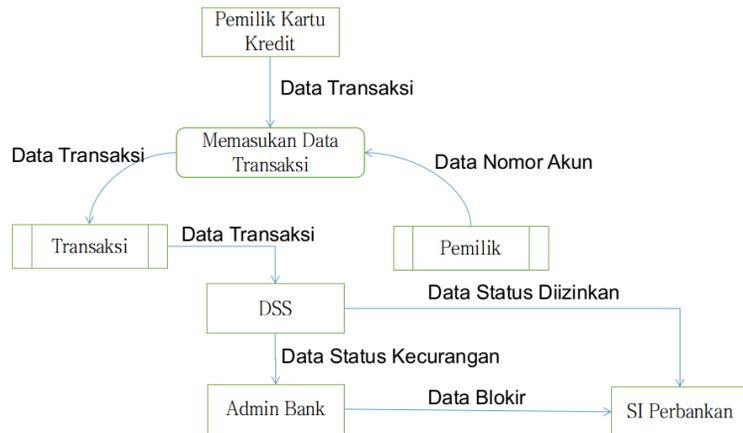
3. HASIL DAN PEMBAHASAN

Penelitian ini memberikan gambaran mengenai implementasi sistem pendukung pengambilan keputusan pada dunia perbankan. Sistem ini nantinya akan terintegrasi dengan sistem perbankan yang ada. Gambaran sistem secara keseluruhan dapat dilihat pada gambar 2, yang merupakan DFD level 0 dari sistem. DFD level 0 menggambarkan hubungan sistem dengan entitas eksternal.



Gambar 2. DFD Level 0

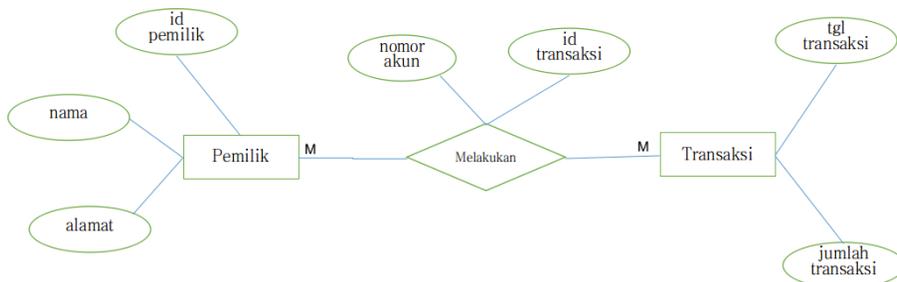
DFD level 0 kemudian dideskripsikan lagi lebih detail dengan DFD level 1 yang menjelaskan entitas, proses, *store*, dan *output* dari hasil proses sistem.



Gambar 3. DFD Level 1

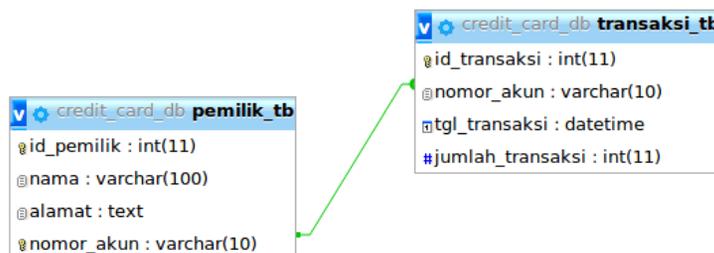
Gambar 3 memperlihatkan posisi dari SPPK pada proses transaksi kartu kredit, setiap terjadi transaksi akan melewati SPPK sebagai bentuk verifikasi. SPPK akan melakukan pengecekan apakah transaksi yang dilakukan masuk dalam klasifikasi transaksi legal atau merupakan sebuah kecurangan (*fraud*).

Setelah dilakukan pemilihan atribut yang akan digunakan pada SPPK, maka dapat dirancang dalam bentuk ERD diagram untuk menggambarkan hubungan antar entitas dan juga atribut.



Gambar 4. ERD Diagram

ERD Diagram yang digambarkan bukan ERD sistem secara keseluruhan, tapi hanya yang berhubungan langsung dengan SPPK. ERD diagram tersebut kemudian direpresentasikan dalam bentuk relasi tabel yang terlihat pada gambar5.



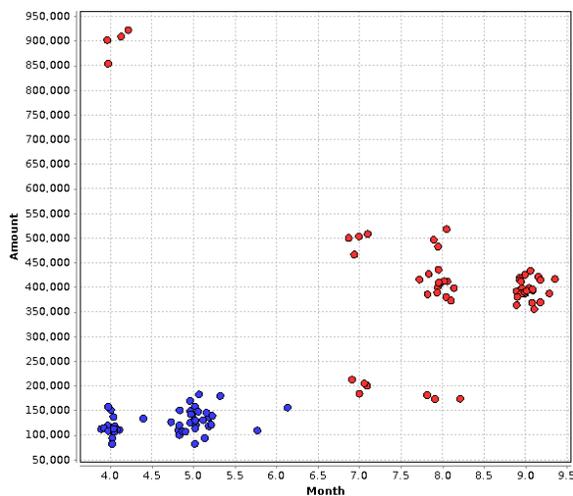
Gambar 5. Relasi Tabel

Data yang digunakan untuk melakukan training sejumlah 100 data. Atribut yang digunakan dalam proses klasifikasi dengan menggunakan SVM adalah nomor akun sebagai label, bulan dan nominal transaksi sebagai *values*.

Tabel 1. Sample Data

<i>Account Number</i>	<i>Month</i>	<i>Transaction Amount</i>
78374	5	103200
78374	5	123000
78374	4	104000
78374	4	120400
78374	5	110000
78374	5	102000
78374	5	200200
78374	5	112700
78374	4	132000
78374	5	200030
78374	4	123020
78374	4	130050
78374	5	124040
78374	5	129303
78374	5	120301
78374	5	103200
...

Metode SVM diimplementasikan menggunakan bahasa pemrograman java, dan smile library sebagai library algoritma SVM yang bersifat *open source* dengan lisensi *apache*. Langkah pertama adalah melakukan training terhadap 100 baris data, dan akan divisualisasikan dalam bentuk *plot*.



Gambar 6. Plot Training Data

Dalam proses pendeteksian kecurangan transaksi yang dilakukan metode SVM adalah dengan deteksi *outlier* atau anomali data. *Outlier* adalah data atau transaksi yang jauh berbeda dengan riwayat transaksi-transaksi sebelumnya yang sudah dimodelkan pada data training. Semakin banyak data pada data training maka akan semakin tinggi tingkat akurasi. Pendeteksian dilakukan tiap transaksi berdasarkan tiap *account number* pemilik kartu kredit. Setiap kali ada transaksi terjadi, data transaksi langsung diklasifikasikan kedalam kelas, kemudian setelah itu dilakukan pengecekan pada data tersebut, jika data jauh dari model yang ada maka data tersebut digolongkan sebagai *outlier*.

4. KESIMPULAN

Hasil uji coba pada desain SPPK yang diusulkan, sistem dapat mendeteksi data *outlier* yang dijadikan sebagai kecurangan (*fraud*). Hasil deteksi tersebut yang akan menjadi data yang akan dikirimkan pada pihak perbankan sebagai notifikasi kecurangan. Data training yang masih relatif sedikit kurang bisa menggambarkan tingkat akurasi dan kecepatan. Penelitian selanjutnya dapat melakukan implementasi pada data *real* perbankan dengan skala data lebih besar.

DAFTAR PUSTAKA

- [1] Devaki R., Kathiresan V., Gunasekaran S., 2014. "Credit Card Fraud Detection using Time Series Analysis", *International Conference on Simulations in Computing Nexus*
- [2] Nipane V.B., Kalinge P.S., et. all., 2016. "Fraudulent Detection in Credit Card System Using SVM & Decision Tree", *IJSDR Volume 1, Issue 5*
- [3] Pawar A.D., Kalavadekar P.N., Tambe S.N., 2014. "A Survey on Outlier Detection Techniques for Credit Card Fraud Detection", *IOSR Journal of Computer Engineering, Volume 16, Issue 2*
- [4] Prasetyo, E., 2012, Data Mining: Konsep dan Aplikasi Menggunakan Matlab, C.V Andi Offset Yogyakarta
- [5] Prasetyo, E., 2014, Data Mining: Mengelola Data Menjadi Informasi Menggunakan Matlab, Andi Yogyakarta
- [6] Santosa B., 2007, Data Mining: Teknik Pemanfaatan Data Untuk Keperluan Bisnis, Graha Ilmu Yogyakarta
- [7] Seeja K.R. & Zareapoor M., 2014. "FraudMiner: A Novel Credit Card Fraud Detection Model Based on Frequent Itemset Mining", *Hindawi Publishing Corporation The Scientific World Journal*
- [8] Vaishali, 2014. "Fraud Detection in Credit Card by Clustering Approach", *International Journal of Computer Applications (0975-8887) Volume 98-No.3*
- [9] Zareapoor M., Seeja K.R., Alam M.A., 2012. "Analysis of Credit Card Fraud Detection Techniques: based on Certain Design Criteria", *International Journal of Computer Applications (0975-8887) Volume 52-No.3*