KLASIFIKASI TRANSAKSI PENIPUAN PADA KARTU KREDIT MENGGUNAKAN METODE *RESAMPLING* DAN PEMBELAJARAN MESIN

OLEH:

MUKHLIS FEBRIADY

NIM 09042681721008

PROGRAM STUDI MAGISTER ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
TAHUN 2021

KLASIFIKASI TRANSAKSI PENIPUAN PADA KARTU KREDIT MENGGUNAKAN METODE *RESAMPLING* DAN PEMBELAJARAN MESIN

TESIS

Diajukan untuk melengkapi salah satu syarat
memperoleh gelar Magister

OLEH:

MUKHLIS FEBRIADY

NIM 09042681721008

PROGRAM STUDI MAGISTER ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
TAHUN 2021

LEMBAR PENGESAHAN

KLASIFIKASI TRANSAKSI PENIPUAN PADA KARTU KREDIT MENGGUNAKAN METODE *RESAMPLING* DAN PEMBELAJARAN MESIN

TESIS

Diajukan untuk melengkapi salah satu syarat
memperoleh gelar Magister

OLEH:
MUKHLIS FEBRIADY
NIM 09042681721008

Palembang, Desember 2021

Pembimbing I,	Pembimbing II,
Samsuryadi, S.Si., M.Kom., Ph.D.	**Dian Palupi Rini, M.Kom., Ph.D**
NIP. 197102041997021003	NIP. 197802232006042002

Mengetahui,
Koordinator Program Magister Ilmu Komputer,

Dian Palupi Rini, M.Kom., Ph.D
NIP. 197802232006042002

LEMBAR PERSETUJUAN

Pada hari Kamis tanggal 30 Desember 2021 telah dilaksanakan ujian sidang Tesis secara daring oleh Magister Ilmu Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Mukhlis Febriady

NIM : 09042681721008

Judul : Klasifikasi Transaksi Penipuan Pada Kartu Kredit Menggunakan Metode *Resampling* Dan Pembelajaran Mesin.

1. Pembimbing I

   Samsuryadi, S.Si., M.Kom., Ph.D. .....
   NIP. 197102041997021003

2. Pembimbing II

   Dian Palupi Rini, M.Kom., Ph.D. .....
   NIP. 197802232006042002

3. Penguji I

   Dr. Ermatita, M.Kom. .....
   NIP. 196709132006042001

4. Penguji II

   Hadipurnawan Satria, Ph.D. .....
   NIP. 198004182020121001

Mengetahui,
Koordinator Program Studi Magister Ilmu Komputer,

Dian Palupi Rini, M.Kom., Ph.D
NIP. 197802232006042002

LEMBAR PERNYATAAN

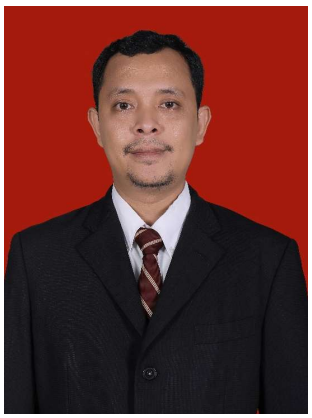
Yang bertanda tangan dibawah ini :

Nama : Mukhlis Febriady
NIM : 09042681721008
Program Studi : Magister Ilmu Komputer
Judul : Klasifikasi Transaksi Penipuan Pada Kartu Kredit Menggunakan Metode *Resampling* Dan Pembelajaran Mesin.

Hasil pengecekan Software iThenticate/Turnitin : **14%**

Menyatakan bahwa laporan tesis saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan tesis ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.



Palembang, Januari 2022

Mukhlis Febriady
NIM. 09042681721008

KATA PENGANTAR

Puji dan syukur penulis haturkan kehadirat Allah SWT yang telah melimpahkan rahmat, hidayah, dan karunia kesehatan kepada penulis sehingga dapat menyelesaikan Tesis yang berjudul **"Klasifikasi Transaksi Penipuan pada Kartu Kredit menggunakan Metode *Resampling* dan Pembelajaran Mesin".**

Tujuan dari penulisan tesis ini adalah untuk memenuhi syarat dalam memperoleh gelar Magister Ilmu Komputer Universitas Sriwijaya.

Dalam proses penulisan tesis ini, penulis banyak mendapat bimbingan dan dukungan dari berbagai pihak sehingga penulisan tesis ini dapat terselesaikan tepat waktu. Oleh karena itu, ucapan terima kasih yang sebesar-besarnya dan penghargaan setinggi-tingginya penulis sampaikan kepada :

1. Orang tua penulis, Almarhum Ayah dan Ibu yang tidak bisa di balas jasa-jasa beliau berdua dari lahir hingga sekarang ini, selalu memberikan do'a yang terbaik untuk penulis khususnya.
2. Istri dan anak tercinta yang selalu mendoakan dalam setiap langkah dan semangat kepada penulis, baik secara moril, suka duka, selalu memberikan dorongan untuk dapat menyelesaikan tesis.
3. Mertua, Almarhum Ayah dan Ibu yang telah memberikan bantuan dan dukungan motivasi serta semangat untuk menyelesaikan tesis.
4. Saudara-saudaraku, kakak-kakak, adik-adik yang tidak bisa di sebutkan satu persatu selalu memberikan motivasi dan doa agar cepat selesai.
5. Bapak Prof. Saparudin, M.T., Ph.D. selaku penasehat sekaligus pembimbing yang selalu memberikan arahan dan motivasi kepada penulis.
6. Ibu Dian Palupi Rini, S.Si., M.Kom., Ph.D. selaku Koordinator Program Studi Magister Ilmu Komputer Universitas Sriwijaya dan pembimbing II atas kebijakan, bimbingan dan arahan kepada penulis dalam penyelesaian tesis saya.
7. Bapak Samsuryadi, S.Si., M.Kom., Ph.D. selaku pembimbing I yang telah memberikan masukan dan arahan terhadap tesis saya.
8. Bapak Dr. Bambang Tutuko, M.T. selaku ketua ujian sidang komprehensif.
9. Ibu Dr. Ermatita, M.Kom. selaku penguji I dan Bapak Hadipurnawan Satria, Ph.D. selaku penguji II yang telah memberikan masukan untuk penulisan tesis.

10. Semua Dosen program studi Magister Ilmu Komputer yang telah melimpahkan ilmunya kepada penulis selama belajar mengajar di Fakultas Ilmu Komputer Universitas Sriwijaya.
11. Admin Program Studi Magister Ilmu Komputer, serta staf dan karyawan di Fakultas Ilmu Komputer Universitas Sriwijaya yang telah banyak membantu mempelancar kegiatan akademik.
12. Semua pihak yang telah membantu secara langsung maupun tidak langsung yang tidak bisa penulis sebutkan satu persatu.

Penulis menyadari bahwa masih banyak kekurangan dalam penulisan tesis ini. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan demi kemajuan karya tulis khususnya yang berkenaan dengan tesis ini. Penulis berharap semoga tesis ini dapat bermanfaat bagi semua pihak peneliti dan khususnya mahasiswa Magister Ilmu Komputer Universitas Sriwijaya sebagai bahan acuan maupun sebagai panduan dalam penyelesaian Tesis.

Palembang, Januari 2022

Penulis

ABSTRACT

The high number of credit card fraud causes a lot of losses for both users and credit card service providers. Because the rate of credit card transactions is very fast, it is necessary to detect credit card fraud as early as possible. However, another challenge that is no less important is the unbalanced amount of data (balance data) between valid and invalid transactions. One solution to the problem of data imbalance is to use a *resampling* method that can improve the quantity of data so that the accuracy results are better. In this study, three types of *resampling* methods were applied, namely SMOTE, bootstrap, and Jackknife. Furthermore, to validate the success of the *resampling* method, three types of machine learning methods were used, namely SVM, ANN, and *Random Forest*. The test results show that the combination of SMOTE and *Random Forest resampling* methods produces the best performance with accuracy, precision, recall and F1-score values of 99,95%, 81,63%, 90,91% and 86,02%, respectively.

Keywords: imbalance data, *resampling* method, credit card fraud, machine learning, credit card.

ABSTRAK

Tingginya angka penipuan kartu kredit menyebabkan banyak kerugian baik dari sisi pengguna maupun penyedia layanan kartu kredit. Karena laju transaksi kartu kredit sangat cepat, maka perlu dilakukan deteksi penipuan kartu kredit sedini mungkin. Namun tantangan lain yang tidak kalah penting adalah jumlah data yang tidak seimbang (*imbalance data*) antara transaksi valid dan tidak valid. Salah satu solusi untuk permasalahan imbalance data adalah menggunakan metode *resampling* yang dapat memperbaiki kuantitas data sehingga hasil akurasi semakin baik. Pada penelitian ini menerapkan tiga jenis metode *resampling*, yaitu SMOTE, *bootstrap*, dan *Jackknife*. Selanjutnya untuk memvalidasi keberhasilan metode *resampling*, maka tiga jenis metode pembelajaran mesin digunakan, yaitu SVM, ANN, dan *Random Forest*. Hasil pengujian memperlihatkan bahwa kombinasi metode *resampling* SMOTE dan *Random Forest* menghasilkan kinerja terbaik dengan nilai akurasi, presisi, recall dan F1-score masing-masing sebesar 99,95%, 81,63%, 90,91% dan 86,02%.

Kata Kunci: *imbalance* data, metode *resampling*, penipuan kartu kredit, pembelajaran mesin, kartu kredit

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

Bab ini menjelaskan mengenai masalah yang melatar belakangi penelitian yang dilakukan, kemudian disusun menjadi suatu permasalahan dengan batasan yang jelas sehingga dapat diselesaikan dengan merumuskan beberapa metode penyelesaian yang sesuai. Metode yang digunakan adalah metode yang sejalan dengan tujuan pada penelitian ini, sehingga hasil yang diperoleh merupakan hasil yang terbaik dan efektif dalam menyelesaikan permasalahan yang dibahas.

1.1 Latar Belakang

Kemudahan dalam mengakses informasi dapat menyebabkan penyalahgunaan informasi terutama pada tindak kejahatan mulai dari penipuan, penyerangan dan berbagai kasus lainnya (Dornadula & Geetha, 2019; Pourhabibi, Ong, Kam, & Boo, 2020). Pelaku kejahatan dapat dengan mudah melakukan melakukan aktivitas kejahatan karena informasi dapat mereka disembunyikan pada *the mountains of data.* Kemudahan ini menimbulkan peluang bagi penipu untuk terus memanipulasi data sehingga mereka mendapat keuntungan yang lebih banyak (Dornadula & Geetha, 2019).

Salah satu bentuk manipulasi data pada bidang *e-commerce* adalah penipuan pada kartu kredit. Transaksi kartu kredit adalah metode pembayaran yang paling umum dalam beberapa tahun terakhir. Meskipun kartu kredit bukanlah alat pembayaran yang paling diminati di Indonesia. Namun jumlah masyarakat pengguna kartu kredit di Indonesia tidaklah sedikit, Bank Indonesia (BI) mencatat pada bulan Januari 2013 jumlah pemegang kartu kredit telah mencapai 14.591.371. Pada awal tahun 2013 ini, nilai transaksinya mencapai Rp 17,96 triliun (Prasetyo, 2017).

Banyaknya pengguna kartu kredit saat ini, menyebabkan penipuan kartu kredit menjadi salah satu yang paling banyak terjadi, karena risiko yang dihadapi sangatlah kecil bahkan bisa dikatakan tidak ada sama sekali (Asha & Kumar, 2020), sehingga aktivitas penipuan meningkat pesat. Perusahaan dan lembaga publik menghadapi masalah besar karena kerugian finansial yang sangat besar disebabkan oleh aktivitas penipuan. Penipuan

kartu kredit dapat dikategorikan dalam berbagai macam(Shakya, 2013). Menurut (Dornadula & Geetha, 2019) penipuan kartu kredit dapat dibedakan berdasarkan strategi yang digunakan. Mereka membaginya menjadi 2 (dua) yaitu penipuan aplikasi dan penipuan perilaku. Pada penipuan aplikasi, penipu mengajukan permohonan untuk kartu kredit dengan ID palsu, sedangkan pada penipuan perilaku penipu menemukan cara untuk mendapatkan kredensial pemegang kartu untuk dapat menggunakan kartu kredit yang sudah ada sebelumnya.

Dengan berbagai macam kasus penipuan kartu kredit yang telah terjadi, bank berusaha meningkatkan keamanan dengan cara beralih pada kartu *Europay, MasterCard, Visa* (EMV). Kartu EMV merupakan *smart card* yang menyimpan datanya pada sirkuit yang terintegrasi, bukan lagi pada strip. Selain itu, solusi atas kecurangan dapat dikategorikan menjadi pencegahan, yaitu mencegah terjadinya kecurangan pada sumbernya sendiri dan pendeteksiannya, yaitu tindakan yang dilakukan setelah terjadinya peristiwa tersebut. Teknologi seperti *Address Verification Service* (AVS) dan *Cardholder Verification Method* (CVM) biasanya dioperasikan untuk mencegah penipuan. Pada dasarnya, filter berbasis aturan dan metode data mining digunakan untuk pencegahan.

Namun, jika penipuan tidak bisa dicegah, maka harus segera dideteksi sedini mungkin, dan tindakan yang diperlukan harus diambil untuk melawannya. Klasifikasi transaksi penipuan adalah proses mendeteksi apakah suatu transaksi sah atau tidak (Sam Maes, et.al., 1993). Sistem klasifikasi penipuan otomatis diperlukan terutama mengingat lalu lintas data transaksi yang besar, dan tidak mungkin bagi manusia untuk memeriksa secara manual setiap transaksi satu per satu apakah itu curang atau tidak. Sistem klasifikasi penipuan otomatis dengan menggunakan teknik pembelajaran mesin dan metode lain sudah banyak berkembang.

Beberapa metode yang telah dikembangkan untuk melakukan klasifikasi transaksi kartu kredit sah atau tidak telah dimulai sejak lama, penelitian menggunakan metode pembelajaran mesin yang dilakukan pada tahun 2013 oleh (Shakya, 2013). Penelitian ini menggunakan algoritma pembelajaran mesin *Random Forest* sebagai model klasifikasinya. Metode *Random Forest* menerapkan konsep *bootstrap* sehingga dapat menghindari terjadinya *overfitting*. Selanjutnya Yu, Li, Dong, & Zheng (2020) mengimplementasikan metode *Artificial Neural Network* (ANN) pada kasus klasifikasi penipuan kartu kredit. Metode ANN memiliki kelebihan dalam mempelajari pola dari

data untuk memperkirakan hubungan non linier antara informasi input dan output akhir. Selain itu ANN memiliki kemampuan untuk menangkap fitur abstrak di seluruh kumpulan data. Pada tahun 2019 dilakukan penelitian dengan mengkombinasikan metode *supervised learning* dan *unsupervised learning* (Carcillo et al., 2019).

Demi mendapat hasil akurasi terbaik dalam pembangunan model klasifikasi transaksi pada kartu kredit, penelitian-penelitian sejenis terus dilakukan. Beberapa metode yang kembali dikembangkan, diantaranya dengan menggunakan metode pembelajaran mesin (Dornadula & Geetha, 2019; Sadgali et al., 2019; Zhu et al., 2020), metode *pipeling and ensemble learning* (Bagga, Goyal, Gupta, & Goyal, 2020), dengan menggunakan metode *Graph Based Anomaly* (GBA) (Pourhabibi et al., 2020), serta dengan menggunakan metode penghapusan fitur secara rekursif dan algoritma klasifikasi *Support Vector Machine* (SVM) untuk melakukan klasifikasi kasus penipuan kartu kredit. (Rtayli & Enneya, 2020). Salah satu keunggulan metode SVM adalah memiliki kinerja yang baik pada kasus klasifikasi kelas biner (dua kelas). Selain itu, metode SVM lebih efektif pada kasus data berdimensi tinggi.

Berdasarkan uraian dari beberapa penelitian sebelumnya, belum didapat hasil pasti nilai akurasi terbaik yang dapat digunakan sebagai metode pembangunan model klasifikasi transaksi kartu kredit. Hal ini juga dikarenakan data yang ada merupakan data yang tidak seimbang (*imbalanced data*) (Sadgali et al., 2019; Zhu et al., 2020). Tidak seimbangan data dapat mempengaruhi hasil akhir dalam memperoleh nilai akurasi. Maka diperlukan metode *resampling* yang dapat memperbaiki kuantitas data sehingga hasil akurasi semakin baik. Metode *resampling* yang paling sering digunakan adalah metode *Synthetic Minority Oversampling Technique* (SMOTE) (Douzas & Bacao, 2019; Elreedy & Atiya, 2019; Rtayli & Enneya, 2020; Sadgali et al., 2019). Padahal masih ada beberapa metode *resampling* lain yang dapat digunakan seperti metode *jackknife* dan *bootstrap* (Sinharay, 2010), serta algoritma residual *resampling* (Hosseini & Jamali, 2019).

Dari karakteristik data kartu kredit yang termasuk ke dalam data *imbalanced*, sehingga dalam penelitian ini akan dilakukan sebuah proses data *resampling* dan klasifikasi data. Metode *resampling* yang digunakan diantaranya SMOTE, *jackknife* dan *bootstrap* . Selain itu untuk menghasilkan sebuah model yang dapat membedakan transaksi kartu kredit yang *valid* dan *invalid*, maka beberapa metode pembelajaran mesin

seperti ANN, *Random Forest*, dan SVM akan dibandingkan untuk mendapatkan kinerja model yang terbaik.

1.2 Perumusan Masalah

Perumusan masalah yang terdapat dalam penelitian ini didasarkan pada latar belakang yang telah dijelaskan diatas yaitu " Bagaimana mendapatkan hasil akurasi yang terbaik dengan menggunakan metode pembelajaran mesin dan metode *resampling* apa yang dapat digunakan untuk mengoptimalkan data yang tidak seimbang?" Sehingga, dari rumusan masalah tersebut, dapat diuraikan menjadi :

1. Bagaimana metode pembelajaran mesin (ANN, SVM dan *Random Forest*) dapat digunakan untuk memperoleh hasil terbaik dalam kasus klasifikasi transaksi kartu kredit dengan memadukan metode *resampling*.
2. Bagaimana kinerja metode pembelajaran mesin dan metode *resampling* dalam melakukan klasifikasi transaksi penipuan kartu kredit.

1.3 Batasan Masalah

Batasan masalah dalam sistem klasifikasi yang dikembangkan pada Tesis ini adalah:

1. Metode Pembelajaran mesin yang digunakan adalah metode ANN, SVM dan *Random Forest*.
2. Metode *resampling* yang digunakan adalah SMOTE, *Jackknife* dan *Bootstrap.*
3. Metode pengukuran kinerja menggunakan akurasi, *recall, precision,* dan *F-1 Score.*
4. Dataset yang digunakan sebagai masukan berasal dari https://www.kaggle.com/mlg-ulb/creditcardfraud dengan jumlah data sebanyak 284.807 transaksi.

1.4 Tujuan

Tujuan penelitian ini adalah ini sebagai berikut:

1. Mendapatkan perpaduan metode pembelajaran mesin dengan metode *resampling* untuk menentukan klasifikasi transaksi penipuan kartu kredit.
2. Melakukan pengukuran kinerja klasifikasi pada metode pembelajaran mesin dan metode *resampling* pada kasus klasifikasi transaksi penipuan kartu kredit menggunakan pengukuran akurasi, presisi, dan sensitivitas.

3. Menentukan metode pembelajaran mesin dengan metode *resampling* yang terbaik dalam klasifikasi transaksi penipuan kartu kredit berdasarkan akurasi, presisi, dan sensitivitas.

1.5 Manfaat Penelitian

Manfaat penelitian ini adalah sebagai berikut:

1. Metode pembelajaran mesin berguna untuk klasifikasi transaksi kartu kredit dengan kinerja yang tinggi.
2. Kerangka kerja dan metode yang dibuat dalam penelitian ini dapat dijadikan referensi untuk penelitian selanjutnya.
3. Membantu pihak-pihak terkait seperti bank atau perusahaan penyedia jasa keuangan untuk mengklasifikasi transaksi penipuan kartu kredit.
4. Metode *resampling* dapat mengoptimalkan ketidakseimbangan data yang tersedia.
5. Dapat mengukur kinerja klasifikasi pada metode pembelajaran mesin dan metode *resampling* pada kasus klasifikasi transaksi penipuan kartu kredit.
6. Memberikan solusi penanganan data tidak seimbang *(imbalanced)* pada kasus klasifikasi transaksi penipuan kartu kredit.

1.6 Sistematika Penulisan

Sistematika penulisan bertujuan untuk lebih memudahkan dalam menyusun dan memperjelas isi dari setiap bab yang ada pada penelitian ini yang dirangkum sebagai berikut :

1. **BAB I Pendahuluan**

   Bab ini berisi tentang latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, dan sistematika penulisan.

2. **BAB II Tinjauan Pustaka**

   Bab ini berisi tentang seluruh penjelasan mengenai landasan teori yang berhubungan dengan permasalahan yang dibahas pada penulisan tesis ini..

3. **BAB III Metodologi Penelitian**

   Bab ini berisi penjelasan secara bertahap dan terperinci tentang langkah-langkah (metodologi) yang digunakan untuk membuat kerangka berfikir dan kerangka kerja dalam menyelesaikan tesis.

4. **BAB IV Hasil dan Analisa**

   Bab ini membahas implementasi hasil dari analisis yang dirancang pada bab III. Sehingga dapat melakukan pengujian terhadap metode yang diusulkan.

5. **BAB V Kesimpulan**

   Pada bab ini penulis merangkum hasil dan analisis yang telah dilakukan pada bab IV. Selain itu penulis juga membahas usulan solusi yang dapat digunakan pada penelitian selanjutnya.

DAFTAR PUSTAKA

Ali, Azad, Centeno, Hao, & van Moorsel. (2019). Consumer-facing technology fraud: Economics, attack methods and potential solutions. *Future Generation Computer Systems*, *100*.

Aral, K. D. (2009). *Prescription fraud detection via data mining: a methodology approach*.

Asha, & Kumar, S. (2020). Credit Card Fraud Detection Using Artificial Neural Network. *Global Transitions Proceedings*, 0–8. https://doi.org/10.1016/j.gltp.2021.01.006

Bagga, S., Goyal, A., Gupta, N., & Goyal, A. (2020). Credit Card Fraud Detection using Pipeling and Ensemble Learning. *Procedia Computer Science*, *173*(2019), 104–112. https://doi.org/10.1016/j.procs.2020.06.014

Carcillo, F., Le Borgne, Y. A., Caelen, O., Kessaci, Y., Oblé, F., & Bontempi, G. (2019). Combining unsupervised and supervised learning in credit card fraud detection. *Information Sciences*, (xxxx). https://doi.org/10.1016/j.ins.2019.05.042

Chawla, Bowyer, Hall, & Kegelmeyer. (2002). Smote: Synthetic minority over-sampling technique. *Journal of Artificial Intelligence Research 16*.

Chouiekh, A., & El Haj, E. H. I. (2018). ConvNets for fraud detection analysis. *Procedia Computer Science*, *127*, 133–138. https://doi.org/10.1016/j.procs.2018.01.107

Chrome Web Store. (n.d.). Credit Card Generator Tool.

Delamaire, Abdou, & Pointon. (2009). Credit card fraud and detection techniques: a review. *Banks and Bank Systems.*

Dornadula, V. N., & Geetha, S. (2019). Credit Card Fraud Detection using Machine Learning Algorithms. *Procedia Computer Science*, *165*, 631–641. https://doi.org/10.1016/j.procs.2020.01.057

Douzas, G., & Bacao, F. (2019). Geometric SMOTE a geometrically enhanced drop-in replacement for SMOTE. *Information Sciences*, *501*, 118–135. https://doi.org/10.1016/j.ins.2019.06.007

Elreedy, D., & Atiya, A. F. (2019). A Comprehensive Analysis of Synthetic Minority Oversampling Technique (SMOTE) for handling class imbalance. *Information Sciences*, *505*, 32–64. https://doi.org/10.1016/j.ins.2019.07.070

Fossi, & Gianini. (2019). Managing a pool of rules for credit card fraud detection by a

game theory based approach. *Future Generations Computer Systems.*

Gershunskaya, J., Jiang, J., & Lahiri, P. (2009). *Resampling* Methods in Surveys. In *Handbook of Statistics* (Vol. 29). https://doi.org/10.1016/S0169-7161(09)00228-4

Ghosh, & Reilly. (1994). Credit card fraud detection with a neural-network. *IEEE Proceedings of the Twenty-Seventh Hawaii International Conference on System Sciences.*

Guo, & Berkhahn. (2016). Entity embeddings of categorical variables. *CoRR.*

Hordri, N. F., Sophiayati, S., Firdaus, N., & Mariyam, S. (2018). Handling Class Imbalance in Credit Card Fraud using *Resampling* Methods. *International Journal of Advanced Computer Science and Applications*, *9*(11). https://doi.org/10.14569/IJACSA.2018.091155

Hosseini, S. S., & Jamali, M. M. (2019). *Resampling* methods combined with rao-blackwellized monte carlo data association algorithm. In the Handbook *of Probabilistic Models*. https://doi.org/10.1016/B978-0-12-816514-0.00018-7

Laleh, & Azgomi. (2009). A taxonomy of frauds and fraud detection techniques. *International Conference on Informa- Tion Systems, Technology and Management.*

Mqadi, N., Naicker, N., & Adeliyi, T. (2021). A SMOTe based Oversampling Data-Point Approach to Solving the Credit Card Data Imbalance Problem in Financial Fraud Detection. *International Journal of Computing and Digital Systems*, *10*(1), 277–286. https://doi.org/10.12785/ijcds/100128

Muhammad, Y. (2020). #7 Artificial Neural Network (ANN) — Part 2 (Single Layer Perceptron).

Noghani, & Moattar. (2015). Ensemble classification and extended feature selection for credit card fraud detection. *Journal of AI and Data Mining.*

Patidar, R, & Sharma. (2011). Credit card fraud detection using neural network. *International Journal of Soft Computing and Engineering (IJSCE).*

Pourhabibi, T., Ong, K. L., Kam, B. H., & Boo, Y. L. (2020). Fraud detection: A systematic literature review of graph-based anomaly detection approaches. *Decision Support Systems*, *133*(April), 113303. https://doi.org/10.1016/j.dss.2020.113303

Prasetyo, S. N. (2017). Rumusan Pengaturan Credit Card Fraud Dalam Hukum Pidana Indonesia Ditinjau Dari Asas Legalitas. *Jurnal Ilmiah Hukum LEGALITY*, *24*(1), 101. https://doi.org/10.22219/jihl.v24i1.4260

Rodliyah, & Iesyah. (2016). Perbandingan Metode Bootstrap Dan Jackknife (Comparison of Bootstrap and Jackknife Methods To. *Jurnal Matematika Dan Pendidikan Matematika*, *I*(1), 76–86.

Rtayli, N., & Enneya, N. (2020). Enhanced credit card fraud detection based on SVM-recursive feature elimination and hyper-parameters optimization. *Journal of Information Security and Applications*, *55*(September), 102596. https://doi.org/10.1016/j.jisa.2020.102596

Russac, Caelen, & He-Guelton. (2018). Embed- dings of categorical variables for sequential data in fraud context. *International Conference on Advanced Machine Learning Technologies and Applications.*

Sadgali, I., Sael, N., & Benabbou, F. (2019). Performance of machine learning techniques in the detection of financial frauds. *Procedia Computer Science*, *148*(Icds 2018), 45–54. https://doi.org/10.1016/j.procs.2019.01.007

Sam Maes, Karl Tuyls, Bram Vanschoenwinkel, and B. M. (1993). Credit card fraud detection using bayesian and neural networks. *Maciunas RJ, Editor. Interactive Image-Guided Neurosurgery. American Association Neurological Surgeons*, pages 261–270.

Shakya, R. (2013). *Application of Machine Learning Techniques in Credit Card Fraud Detection*. (December), 1–67.

Sinharay, S. (2010). Jackknife methods. *International Encyclopedia of Education*, 229–231. https://doi.org/10.1016/B978-0-08-044894-7.01338-5

Ying, X. (2019). An Overview of Overfitting and its Solutions. *Journal of Physics: Conference Series*, *1168*, 022022. https://doi.org/10.1088/1742-6596/1168/2/022022

Yu, X., Li, X., Dong, Y., & Zheng, R. (2020). A Deep Neural Network Algorithm for Detecting Credit Card Fraud. *2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*, 181–183. https://doi.org/10.1109/ICBAIE49996.2020.00045

Zhu, H., Liu, G., Zhou, M., Xie, Y., Abusorrah, A., & Kang, Q. (2020). Optimizing Weighted Extreme Learning Machines for imbalanced classification and application to credit card fraud detection. *Neurocomputing*, *407*, 50–62. https://doi.org/10.1016/j.neucom.2020.04.078