DETEKSI TRANSAKSI ANOMALI PADA *BLOCKCHAIN* DENGAN MENGGUNAKAN METODE *GATED RECURRENT UNIT (GRU)*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

Oleh :

Faisal Soultan Muhammad

09011381924123

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

LEMBAR PENGESAHAN

DETEKSI TRANSAKSI ANOMALI PADA *BLOCKCHAIN* DENGAN MENGGUNAKAN METODE *GATED RECURRENT UNIT (GRU)*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Program Studi Sistem Komputer
Jenjang S1

Oleh:

Faisal Soultan Muhammad
09011381924123

Palembang, Mei 2024

Pembimbing I	Pembimbing II
Prof. Deris Stiawan, M.T., Ph.D.	**Huda Ubaya, M.T.**
NIP. 197806172006041002	**NIP. 198106162012121003**

Mengetahui, 4/6/24
Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.
NIP. 196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada

Hari : Rabu

Tanggal : 22 Mei 2024

Tim Penguji

1. Ketua : Kemahyanto Exaudi, M.T.
2. Sekretaris : Nurul Afifah, M.Kom.
3. Penguji : Dr. Ahmad Zarkasi, M.T.
4. Pembimbing I : Prof. Deris Stiawan, M.T., Ph.D.
5. Pembimbing II : Huda Ubaya, M.T.

Mengetahui

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama	:	Faisal Soultan Muhammad
NIM	:	09011381924123
Judul	:	Deteksi Transaksi Anomali Pada *Blockchain* Dengan Menggunakan Metode *Gated Recurrent Unit* (GRU)

Hasil Pengecekan Plagiat/Turnitin: 12%

Menyatakan bahwa laporan tugas akhir ini adalah hasil karya saya sendiri dan tidak mengandung unsur penjiplakan atau plagiat. Saya sepenuhnya menyadari bahwa jika terbukti adanya penjiplakan atau plagiat dalam laporan tugas akhir ini, saya siap menerima sanksi akademik dari Universitas Sriwijaya. Pernyataan ini saya buat dengan kesadaran penuh dan tanpa adanya paksaan dari pihak manapun.

Palembang, 29 Mei 2024

Faisal Soultan Muhammad

NIM. 09011381924123

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh,

Puji dan syukur penulis panjatkan kepada Allah SWT yang telah melimpahkan rahmat dan karunianya yang sangat besar dan tidak berhenti, sehingga penulis dapat menyelesaikan Tugas Akhir ini yang berjudul "**Deteksi Transaksi Anomali Pada *Blockchain* Dengan Menggunakan metode *Gated Recurrent Unit* (GRU)"**. Serta shalawat serta salam yang kita curahkan kepada junjungan kita Nabi Muhammad Shallallahu 'Alaihi Wasallam beserta keluarga, sahabat dan para pengikutnya yang insyaallah istiqomah hingga akhir zaman.

Selesainya penyususan Tugas Akhir ini tidak terlepas dari peran semua pihak atas ide, bimbingan, dan saran serta bantuannya dalam menyelesaikan penulisan Proposal Tugas Akhir ini, antara lain:

1. Allah SWT yang telah memberikan berkah serta nikmat kesehatan dan kesempatan kepada penulis sehingga dapat menyelesaikan Tugas Akhir ini.
2. Kepada kedua orang tua saya tercinta yang telah membesarkan dan mendidik saya dengan penuh kasih sayang, serta telah memberikan motivasi dan dukungan baik secara moril, material maupun spiritual selama ini.
3. Bapak Prof. Dr. Erwin, S.Si., M.Si. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. H. Sukemi, M.T., selaku ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Huda Ubaya, M.T. selaku Sekretaris Jurusan dan Dosen Pembimbing 2 Tugas Akhir Sistem Komputer Universitas Sriwijaya.
6. Bapak Prof. Deris Stiawan, M.T., Ph.D. selaku Dosen Pembimbing 1 Tugas Akhir dan selaku Dosen Pembimbing Akademik Jurusan Sistem Komputer.
7. Ibu Nurul afifah, M.Kom. selaku dosen Sistem Komputer yang telah membantu dan memberikan masukan selama pengerjaan Tugas Akhir.
8. Bapak, Ibu dosen jurusan Sistem Komputer yang telah memberikan ilmu dan pengalamannya kepada saya.
9. Mbak Sari selaku admin Jurusan Sistem Komputer yang telah membantu penulis dalam hal administrasi selama perkuliahan.
10. Teman – teman seperjuangan Jurusan Sistem Komputer Angkatan 2019.

11. Seluruh pihak yang tergabung dalam Comnets terutama Muhammad Triwahyudi, Galih Bayu Permana, M Imam dan Muhammad Sholahudin yang menjadi anggota dalam tim penelitian ini.
12. Teman – teman saya yang terdapat pada Grup BACOD Mobile yang selalu memberikan dukungan kepada penulis.
13. Kakak-kakak tingkat yang satu riset dengan terimakasih telah membantu saya menyelesaikan tugas akhir ini.
14. Seluruh pihak yang tidak dapat penulis sebutkan satu persatu, yang telah memberikan semangat serta do'anya dalam penyelesaian Tugas Akhir.
15. Jurusan Sistem Komputer.
16. Almamater.

Penulis menyadari bahwa dalam penyusunan laporan ini masih sangat jauh dari kata sempurna. Oleh karena itu penulis mengharapkan kritik dan saran yang membangun untuk penulis, semoga Proposal Tugas Akhir ini dapat bermanfaat dan berguna bagi siapa saja yang membacanya.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Palembang, Mei 2024
Penulis,

Faisal Soultan Muhammad
NIM. 09011381924123

DETEKSI TRANSAKSI ANOMALI PADA *BLOCKCHAIN* DENGAN MENGGUNAKAN METODE *GATED RECURRENT UNIT* (GRU)

FAISAL SOULTAN MUHAMMAD (09011381924123)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer

Universitas Sriwijaya

Email : faisalsoultan27@gmail.com

ABSTRAK

Aktivitas ilegal seperti pencucian uang menggunakan *cryptocurrency* yang diwakili oleh bitcoin telah bermunculan. Dalam penelitian ini, digunakan jaringan saraf *Gated Reccurent Unit* (GRU) untuk mengidentifikasi pola transaksi anomali dalam dataset. Dataset dibuat dengan mengambil data mentah berdasarkan parameter tahun untuk mengekstrak subset data. Subset ini mewakili data dari tahun 2011 hingga 2013 dan diekstrak dengan menulis kode *python snippet*. Dikarenakan datanya yang tidak seimbang dataset diseimbangkan kelasnya menggunakan teknik *oversampling* dan *undersampling*. Model terbaik mencapai akurasi sebesar 90,31%. Kemudian, melalui validasi *k-fold*, model tersebut menunjukkan konsistensi yang baik, dengan akurasi rata-rata mencapai 86,29%. Hasil ini mengindikasikan bahwa model memiliki kinerja yang dapat diandalkan dalam tugas deteksi.

Kata Kunci : *Blockchain*, Deteksi Anomali, *Gated Reccurent Unit*

ANOMALOUS TRANSACTION DETECTION ON BLOCKCHAIN USING GATED RECURRENT UNIT (GRU)

FAISAL SOULTAN MUHAMMAD (09011381924123)

Computer Engineering Department, Computer Science Faculty

Sriwijaya University

Email : faisalsoultan27@gmail.com

ABSTRACT

Illegal activities such as money laundering using cryptocurrencies represented by Bitcoin have emerged. In this study, a Gated Recurrent Unit (GRU) neural network is used to identify anomalous transaction patterns in the dataset. The dataset is created by taking raw data based on yearly parameters to extract a subset of data. This subset represents data from the years 2011 to 2013 and is extracted by writing a Python code snippet. Due to the imbalance of the data, the dataset's classes are balanced using oversampling and undersampling techniques. The best model achieved an accuracy of 90.31%. Then, through k-fold validation, the model showed good consistency, with an average accuracy of 86.29%. These results indicate that the model has reliable performance in the detection task.

Keywords : *Anomaly Detection, Blockchain, Gated Reccurent Unit*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada Penelitian [1] *Blockchain* adalah basis data terdistribusi yang menyimpan daftar catatan data yang terus bertambah dan datanya didesentralisasi, dicadangkan bersama, dan ditautkan ke dalam rantai yang saling bertautan sehingga tidak dapat dirusak. Pada penelitian [2] bitcoin adalah mata uang digital *peer-to-peer*, dengan menggunakan mana pengguna dapat mengirim dan menerima bentuk uang elektronik satu sama lain secara anonim tanpa memerlukan perantara apa pun.

Pada penelitian [3] *Cryptocurrency* adalah sistem pertukaran digital *peer-to-peer* di mana kriptografi digunakan untuk menghasilkan dan mendistribusikan unit mata uang. Proses ini membutuhkan verifikasi transaksi terdistribusi tanpa otoritas pusat. Verifikasi transaksi mengonfirmasi jumlah transaksi, dan apakah pembayar memiliki mata uang yang ingin mereka belanjakan sembari memastikan bahwa unit mata uang tidak dibelanjakan dua kali. Proses verifikasi ini disebut mining. *Cryptocurrency* berhubungan dengan *blockchain* karena *cryptocurrency* dibuat dengan menggunakan teknologi *blockchain*.

Pada penelitian [4] aktivitas ilegal seperti pencucian uang menggunakan *cryptocurrency* yang diwakili oleh bitcoin telah bermunculan. Anonimitas, konvertibilitas dua arah, dan bitcoin digunakan untuk "mencuci" pendapatan ilegal. Beberapa insiden pencurian bitcoin juga dikaitkan dengan pencucian uang. Peretas “mencuci” bitcoin yang dicuri dan akhirnya mengubahnya menjadi properti legal.

Pada penelitian [5] membahas transaksi bitcoin yang terdapat data anomali. Lalu data dari transaksi tersebut diekstrak kemudian digunakan teknik unsupervised machine learning untuk dianalisa dan mendeteksi transaksi abnormal. Terdapat metode algoritma seperti *deep autoencoder* menghasilkan akurasi 98.84%, *histogram based outlier score* (HBOS) menghasilkan akurasi 87.12%, *principal component analysis* (PCA) menghasilkan akurasi 88.18%,

isolation forest menghasilkan akurasi 96.99%, K-means menghasilkan akurasi 86.52%, *ensemble classification* menghasilkan akurasi 94.89% dan *cluster based local outier factor* (CBLOF) menghasilkan akurasi 84.89%. Pada riset [6] teridentifikasi transaksi abnormal pada platform cryptocurrency seperti Binance, Kraken, Coinbase dan houbi. Data yang di kumpukan dari etherscans kemundian dianalisis dengan deep learning LSTM.

Pada riset [7] dibahas performa mendeteksi data *anomaly* pada metode LSTM dan *Gated Recurrent Unit* (GRU). Kedua metode tersebut memiliki algoritma simpel dan mudah digunakan. Secara keunggulan GRU memiliki presiksi *short-term precipitation* dan prediksi *traffic flow* yang cukup konsisten dan rinci.

Dari pembahasan tersebut, penulis akan melakukan penelitian dengan judul "*Deteksi Transaksi Anomali Pada Blockchain Dengan Menggunakan metode Gated Recurrent Unit* (GRU)".

1.2 Tujuan

Tujuan penelitian ini ditetapkan berdasarkan rumusan masalah, yang meliputi:

1. Membedakan data pada transaksi mana yang data normal dan data anomali dalam dataset.
2. Penyeimbangan dataset dan menerapkan dataset dengan teknik oversampling dan teknik undersampling.
3. Melakukan deteksi pada data anomali dalam transaksi *blockchain* dengan metode GRU.

1.3 Manfaat

Di bagian manfaat ini yang dapat diperoleh dari penelitian ini, antara lain:

1. Mampu membedakan antara transaksi data mana yang normal dan transaksi data mana yang anomali di dalam dataset transaksi bitcoin.
2. Mengatasi permasalahan dataset yang tidak seimbang dengan menerapankan teknik oversampling dan undersampling membuat dataset menjadi seimbang.

3. Mampu secara efektif mendeteksi transaksi yang normal dan anomali dalam jaringan *blockchain* dengan mengimplemetasikan metode GRU.

1.4 Rumusan Masalah

Berdasarkan informasi diatas, rumusan masalah dalam penelitian ini dapat disimpulkan sebagai berikut:

1. Bagaimana persiapan untuk memproses dataset sebelum deteksi transaksi anomali?
2. Bagaimana cara melakukan deteksi transaksi anomali pada data blockchain dengan mengunakan metode GRU*?*
3. Bagaimana cara mengatasi *imbalance* pada data untuk mencapai performa yang optimal?

1.5 Batasan Masalah

Batasan masalah menjadi titik fokus pada penelitian tugas akhir ini meliputi:

1. *Bitcoin Network Transactional Metadata* 2011 - 2013 digunakan sebagai dataset.
2. Menggunakan dataset dimana data normal dan anomali belum seimbang.
3. Penggunaan *Gated Recurrent Unit* (GRU) sebagai algoritma untuk mendeteksi anomali.
4. Melatih model GRU menggunakan 4 *layer* terdiri dari 3 ReLU dan 1 Sigmoid berfungsi sebagai aktivasi, *optimizer* yaitu *adam*, *loss function* yaitu *MSE* dan terakhir *metrics binary accuracy*

1.6 Metodologi Penelitian

1. Metode Studi Pustaka dan Literatur

   Pada literatur dan studi pustaka ini merupakan langkah awal dalam proses penelitian. Dalam metode ini, penulis akan melakukan pencarian dan pengumpulan refrensi dari berbagai jenis literatur yaitu buku, jurnal ilmiah, dan sumber internet yang relevan dengan topik penelitian. Tujuannya untuk membangun kerangka metodologi penelitian yang akan dijalankan.

2. Metode Konsultasi

Pada metode konsultasi ini, penulis akan bertemu dengan narasumber yang memiliki pengetahuan tentang penelitian ini secara langsung atau melalui komunikasi tidak langsung saat proses konsultasi. Tujuan dari pertemuan ini untuk mendapatkan pemahaman yang mendalam tentang masalah yang akan muncul dalam penelitian ini.

3. Metode Perancangan Sistem

Pada metode perencangan sistem ini adalah tahap kunci dari penelitian, yang berfokus pada proses pembangunan metode untuk sistem Tugas Akhir. Metode akan menjelaskan menyeluruh semua langkah yang diperlukan untuk membangun sistem termasuk *software* yang dipakai, alat apa pun yang digunakan, dan proses konfigurasi metode yang relevan dengan Tugas Akhir.

4. Metode Pengujian dan Validasi

Proses pengujian dan validasi, dimana dataset yang dikumpulkan akan diuji menggunakan metode *machine learning* untuk mencapai tingkat akurasi yang diinginkan. Proses pengujian melibatkan langkah evaluasi terhadap kinerja model untuk menentukan baik atau buruk.

5. Metode Analisis

Hasil penelitian ini akan di analisis terhadap kelebihan dan kekurangan secara menyeluruh yang bertujuan untuk pemahaman yang lebih baik tentang kinerja metode dan untuk pengembangan lebih lanjut.

1.7 Sistematika Penulisan

Proses sistematika pada penulisan untuk menulis pada Tugas Akhir ini secara keseluruhan, meliputi:

BAB I PENDAHULUAN

Dalam BAB I, dikenalkan dengan landasan topik penelitian yang dimulai dari latar belakang yang memperkenalkan konteks masalah, rumusan masalah yang menidentifikasi pertanyaan penelitian, batasan masalah yang

menetapkan penelitian, tujuan yang diharapkan, manfaat yang diantisipasi, dan metodologi penelitian yang merinci langkah yang digunakan, serta sistematika penulisan yang mengatur struktur dan isi pada Tugas Akhir.

BAB II TINJAUAN PUSTAKA

Dalam BAB II, rangkuman penelitian yang relevan dengan topik, menjelaskan teori yang mendukung antara lain konsep *blockchain*, konsep *bitcoin*, konsep *anomaly detection*, konsep *deep learning*, serta metode *Gated Recurrent Unit* (GRU).

BAB III METODOLOGI PENELITIAN

Dalam BAB III, penjelasan peracangan ruang pengujian yang disiapkan untuk penelitian ini. Selain itu, membahas perancangan model GRU yang dirancang dengan tujuan mendeteksi anmali pada transaksi bitcoin.

BAB IV HASIL DAN ANALISA

Dalam BAB IV, akan memaparkan hasil dari rangkaian pengujian yang telah dilakukan, serta analisis dan pembahasan pada data yang diperoleh.

BAB V KESIMPULAN DAN SARAN

Dalam BAB V, penarikan kesimpulan yang diambil berdasarkan hasil penelitian. Selain itu, ada saran-saran yang bertujuan untuk para penulis yang akan mengembangkan penelitian ini kedepannya.

DAFTAR PUSTAKA

[1] M. Di Pierro, "What Is the Blockchain?," in Computing in Science & Engineering, vol. 19, no. 5, pp. 92-95, 2017, doi: 10.1109/MCSE.2017.3421554.

[2] S. Nakamoto, "Bitcoin: Sebuah Sistem Uang Tunai Elektronik Peer-to-Peer," *Bitcoin*, pp. 1–10, 2008, [Online]. Available: www.bitcoin.org

[3] A. V. Singh, J. Shaw, V. Mishra, and A. Singh, "A Systematic Analysis on Cryptocurrencies as a Financial Asset," *2022 Int. Conf. Interdiscip. Res. Technol. Manag. IRTM 2022 - Proc.*, 2022, doi: 10.1109/IRTM54583.2022.9791804.

[4] L. Yang, X. Dong, S. Xing, J. Zheng, X. Gu, and X. Song, "An abnormal transaction detection mechanim on bitcoin," *Proc. - 2019 Int. Conf. Netw. Netw. Appl. NaNA 2019*, pp. 452–457, 2019, doi: 10.1109/NaNA.2019.00083.

[5] Omer Shafiq, "Anomaly Detection inBlockchain," no. December, 2019.

[6] Z. Gu, D. Lin, and J. Wu, "On-chain analysis-based detection of abnormal transaction amount on cryptocurrency exchanges," *Phys. A Stat. Mech. its Appl.*, vol. 604, p. 127799, 2022, doi: 10.1016/j.physa.2022.127799.

[7] C. Tang, L. Xu, B. Yang, Y. Tang, and D. Zhao, "GRU-Based Interpretable Multivariate Time Series Anomaly Detection in Industrial Control System," *Comput. Secur.*, vol. 127, p. 103094, 2023, doi: 10.1016/j.cose.2023.103094.

[8] T. Ashfaq *et al.*, "A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism," *Sensors*, vol. 22, no. 19, pp. 1–20, 2022, doi: 10.3390/s22197162.

[9] R. Fu, Z. Zhang, and L. Li, "Using LSTM and GRU neural network methods for traffic flow prediction," *Proc. - 2016 31st Youth Acad. Annu. Conf. Chinese Assoc. Autom. YAC 2016*, no. December, pp. 324–328, 2017, doi: 10.1109/YAC.2016.7804912.

[10] M. Rwibasira and S. R, "ADOBSVM: Anomaly detection on block chain using support vector machine," *Meas. Sensors*, vol. 24, no. October, p.

100503, 2022, doi: 10.1016/j.measen.2022.100503.

[11] J. Audibert, P. Michiardi, F. Guyard, S. Marti, and M. A. Zuluaga, “Do deep neural networks contribute to multivariate time series anomaly detection?,” *Pattern Recognit.*, vol. 132, p. 108945, 2022, doi: 10.1016/j.patcog.2022.108945.

[12] P. Nerurkar, S. Bhirud, D. Patel, R. Ludinard, Y. Busnel, and S. Kumari, “Supervised learning model for identifying illegal activities in Bitcoin,” *Appl. Intell.*, vol. 51, no. 6, pp. 3824–3843, 2021, doi: 10.1007/s10489-020-02048-w.

[13] P. Monamo, V. Marivate, and B. Twala, “Unsupervised learning for robust Bitcoin fraud detection,” *2016 Inf. Secur. South Africa - Proc. 2016 ISSA Conf.*, pp. 129–134, 2016, doi: 10.1109/ISSA.2016.7802939.

[14] A.-T. Nechiti, “Anomaly Detection in Blockchain Networks,” Tampere University, 2023.

[15] C. Y. Lin, H. K. Liao, and F. C. Tsai, “A Systematic Review of Detecting Illicit Bitcoin Transactions,” *Procedia Comput. Sci.*, vol. 207, no. Kes, pp. 3211–3219, 2022, doi: 10.1016/j.procs.2022.09.379.

[16] F. Fang *et al.*, “Cryptocurrency trading: a comprehensive survey,” *Financ. Innov.*, vol. 8, no. 1, 2022, doi: 10.1186/s40854-021-00321-6.

[17] Y. Yuan and F. Y. Wang, “Blockchain and Cryptocurrencies: Model, Techniques, and Applications,” *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 48, no. 9, pp. 1421–1428, 2018, doi: 10.1109/TSMC.2018.2854904.

[18] O. Shafiq, “Bitcoin Transactions Data 2011-2013.” [Online]. Available: https://ieee-dataport.org/open-access/bitcoin-transactions-data-2011-2013

[19] R. M. A. Ilyasa, “Legalitas Bitcoin Dalam Transaksi Bisnis Di Indonesia,” *Lex Sci. Law Rev.*, vol. 3, no. 2, pp. 115–128, 2019, doi: 10.15294/lesrev.v3i2.35394.

[20] Z. Munawa and N. I. Putri, “Keamanan IoT Dengan Deep Learning dan Teknologi Big Data,” *Temat. J. Teknol. Inf. Komun.*, vol. 7, no. 2, pp. 161–185, 2020.

[21] Ulrich Wake, “Kesalahan Scaling Data di Machine Learning Menggunakan Scikit-Learn.”

[22] ashwinsharmap, “StandardScaler, MinMaxScaler and RobustScaler techniques – ML.”

[23] M. S. Shelke, P. R. Deshmukh, and P. V. K. Shandilya, “A Review on Imbalanced Data Handling Using Undersampling and Oversampling Technique,” *Int. J. Recent Trends Eng. Res.*, vol. 3, no. 4, pp. 444–449, 2017, doi: 10.23883/ijrter.2017.3168.0uwxm.

[24] N. A.-R. Al-Serw, “Undersampling dan oversampling: Pendekatan lama dan baru.”

[25] R. Mohammed, J. Rawashdeh, and M. Abdullah, “Machine Learning with Oversampling and Undersampling Techniques: Overview Study and Experimental Results,” *2020 11th Int. Conf. Inf. Commun. Syst. ICICS 2020*, pp. 243–248, 2020, doi: 10.1109/ICICS49469.2020.239556.

[26] N. M. Mqadi, N. Naicker, and T. Adeliyi, “Solving Misclassification of the Credit Card Imbalance Problem Using near Miss,” *Math. Probl. Eng.*, vol. 2021, 2021, doi: 10.1155/2021/7194728.

[27] A. R. Hassan and M. I. H. Bhuiyan, “Automated identification of sleep states from EEG signals by means of ensemble empirical mode decomposition and random under sampling boosting,” *Comput. Methods Programs Biomed.*, vol. 140, pp. 201–210, 2017, doi: 10.1016/j.cmpb.2016.12.015.

[28] R. Blagus and L. Lusa, “SMOTE for high-dimensional class-imbalanced data,” *BMC Bioinformatics*, vol. 14, 2013, doi: 10.1186/1471-2105-14-106.

[29] A. Ghazikhani, H. S. Yazdi, and R. Monsefi, “Class Imbalance Handling Using Wrapper-based Random Oversampling,” pp. 1–6, 2010, doi: 10.1109/IranianCEE.2012.6292428.

[30] P. Singh, N. Singh, K. K. Singh, and A. Singh, “Diagnosing of disease using machine learning,” *Mach. Learn. Internet Med. Things Healthc.*, pp. 89–111, 2021, doi: 10.1016/B978-0-12-821229-5.00003-3.