KLASIFIKASI LALU LINTAS *DARKNET* MENGGUNAKAN METODE *ADABOOST CLASSIFIER*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH :

RIZKY ELINDA SARI

09011282025084

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

LEMBAR PENGESAHAN

KLASIFIKASI LALU LINTAS *DARKNET* MENGGUNAKAN METODE *ADABOOST CLASSIFIER*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

RIZKY ELINDA SARI
09011282025084

Palembang, 26 Agustus 2024

Pembimbing I,

Prof. Deris Stiawan, M.T., Ph.D.
NIP. 197806172006041002

Pembimbing II,

Nurul Afifah, M.Kom.
NIP. 199211102023212049

Mengetahui,
Kepala Jurusan Sistem Komputer

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

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Selasa

Tanggal : 30 Juli 2024

Tim Penguji :

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

Mengetahui, 26/8/24
Ketua Jurusan Sistem Komputer

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

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Rizky Elinda Sari

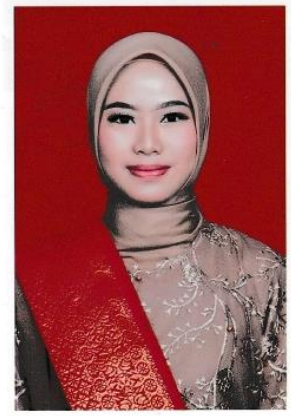
NIM : 09011282025084

Judul : Klasifikasi Lalu Lintas *Darknet* Menggunakan Metode *AdaBoost Classifier*

Hasil Pengecekan *Software iThenticate/Turnitin* : 3%

Menyatakan bahwa laporan skripsi saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam laporan skripsi ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaan dari siapapun.



Palembang, 12 Agustus 2024

Rizky Elinda Sari

NIM. 09011282025084

KATA PENGANTAR

Assalamu'alaikum Warhmatullahi Wabarokatuh

Puji syukur penulis panjatkan kepada Allah Ta'ala atas rahmat, hidayah dan karunia-Nya sehingga penulis dapat menyelesaikan penyusunan skripsi ini dengan judul "**Klasifikasi Lalu Lintas *Darknet* Menggunakan Metode *AdaBoost Classifier***". Sholawat dan salam tak terhingga kepada Nabi Muhammad Shalallaahu Alaihi Wassalaam, yang telah membawa umatnya dari jaman kegelapan ke jaman yang terang benderang ini.

Penulisan skripsi ini merupakan salah satu syarat dalam menyelesaikan studi pada Jurusan Sistem Komputer, Universitas Sriwijaya. Terselesaikannya penulisan skripsi ini tak lepas dari bantuan, bimbingan dan arahan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada :

1. Allah SWT yang telah memberikan nikmat kesehatan dan kesempatan kepada penulis untuk menyelesaikan proposal tugas akhir.
2. Kedua orang tua dan keluarga yang selalu mendoakan dan memberikan semangat kepada penulis.
3. Bapak Prof. Dr. Erwin, S.Si., M.Si. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
5. Bapak Muhammad Ali Buchari, M.T. selaku Dosen Pembimbing Akademik.
6. Bapak Prof. Deris Stiawan, M.T., Ph.D. selaku Dosen Pembimbing I.
7. Ibu Nurul Afifah, M.Kom. selaku Dosen Pembimbing II .
8. Mba Renny, Pak Yoppy dan Kak Angga selaku Admin Jurusan Sistem Komputer.
9. Nurul Fitria, Septiani Kusuma Ningrum, Vijiantika Fajaria Sastri, Zuli Yanti, teman-teman SKB 2020 dan teman-teman COMNETS di Indralaya.
10. Seluruh pihak yang tidak dapat penulis sebutkan satu persatu, yang telah memberikan semangat
11. Almamater.

Penulis menyadari bahwa penyusunan skripsi ini masih perlu perbaikan dan penyempurnaan. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun dari pihak-pihak terkait agar lebih baik dikemudian hari.

Akhir kata, penulis berharap semoga penulisan skripsi ini dapat memberikan manfaat secara langsung maupun tidak langsung bagi semua pihak khususnya mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya.

Wassalamu'alaikum Warahmatullahi Wabarakatuh

Palembang, 12 Agustus 2024
Penulis,

Rizky Elinda Sari
NIM. 09011282025084

KLASIFIKASI LALU LINTAS *DARKNET* MENGGUNAKAN METODE *ADABOOST CLASSIFIER*

Rizky Elinda Sari (09011282025084)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer

Universitas Sriwijaya

Email : 09011282025084@student.unsri.ac.id

ABSTRAK

Darknet dikenal karena kemampuannya yang dapat memberikan anonimitas yang sering digunakan untuk kegiatan ilegal. Laporan monitor keamanan dari BSSN menunjukkan bahwa 290.556 data kredensial akun dari instansi di Indonesia telah terekspos di *darknet*. Teknik klasifikasi merupakan pendekatan penting dalam mempelajari dan mengidentifikasi lalu lintas *darknet.* Penelitian ini mengusulkan *AdaBoost Classifier* sebagai metode dalam klasifikasi darknet. Penggunaan variasi dari *n_estimator* memberikan dampak yang signifikan terhadap hasil klasifikasi pada penelitian ini. Berdasarkan hasil evaluasi model *AdaBoost* menggunakan *Confusion Matrix,* performa model terbaik diperoleh pada nilai *n_estimator* 500 dengan akurasi 99,70%. Berhasilnya penelitian ini memberikan kontribusi dalam mengembangkan model klasifikasi dan evaluasi *AdaBoost* dalam hal klasifikasi *darknet*.

Kata Kunci : Klasifikasi, *Darknet, AdaBoost, n_estimator*, SMOTE-ENN

CLASSIFICATION OF DARKNET TRAFFIC USING THE ADABOOST CLASSIFIER METHOD

Rizky Elinda Sari (09011282025084)

Department of Computer System, Faculty of Computer Science

Sriwijaya University

Email : 09011282025084@student.unsri.ac.id

ABSTRACT

Darknet is famous for its ability to provide anonymity which is often used for illegal activities. A security monitor report from BSSN highlights that 290,556 credential data from institution in Indonesia have been exposed on the darknet. Classification techniques are important for studying and identifying darknet traffic. This study proposes the utilization of the AdaBoost Classifier in darknet classification. The use of variable estimator values significantly impact classification results. The best performance was obtained with an estimator value of 500 with an accuracy of 99.70%. The contribution of this research lies in the development of classification models and the evaluation of AdaBoost models in the context of darknet traffic classification.

***Keyword** : Classification, darknet, AdaBoost, n_estimator, SMOTE-ENN*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Internet menyediakan platform sistem informasi yang dikenal sebagai *World Wide Web* (WWW), di mana pengguna dapat mengakses dan berbagi berbagai jenis informasi yang kemudian ditukar secara luas ke seluruh dunia. Namun, terkadang pengguna internet tidak menyadari adanya lapisan internet yang tersembunyi yang memberikan anonimitas dan platform yang sebagian besar digunakan untuk aktivitas ilegal dan kejahatan siber yang dikenal sebagai *Darknet* [1].

Darknet merupakan sub set dari *deep web* yang tidak dapat diakses oleh mesin pencari biasa [2]. *Darknet* merupakan teknologi jaringan terenkripsi yang memberikan anonimitas kepada pengirim dan penerima. *Darknet* hanya dapat diakses menggunakan teknologi anonimitas seperti *Virtual Private Network* (VPN) atau *The Onion Router* (Tor) [3], [4]. *Darknet* menjadi tempat dimana kemungkinan akan menemukan file atau data yang dicuri untuk dijual, serta dijualnya produk tidak sah lainnya [5]. *Malware* seperti *keylogger*, *botnet*, dan *ransomware* juga dapat ditemukan di *Darknet* dari sumber yang tidak dikenal [6].

Darknet berpotensi menyebabkan *darknet exposure*, yaitu kondisi ketika terdapat data atau informasi kredensial akun pada suatu instansi tertentu terekspos di *darknet*. Berdasarkan laporan hasil monitor keamanan siber BSSN bulan Agustus 2023 [7], di Indonesia ditemukan 290.556 data *exposure* dari 431 instansi terdampak. Sebagai upaya dalam menghadapi darknet, klasifikasi dapat dilakukan sebagai dasar untuk mempelajari dan membedakan lalu lintas darknet.

Klasifikasi lalu lintas *darknet* telah diterapkan penelitian terdahulu. Penelitian oleh Habibi Laskhari [8] dkk menerapkan pendekatan CNN sebagai metode dalam mengklasifikasi lalu lintas darknet. Pendekatan ini mampu membedakan lalu lintas darknet dengan akurasi 86%. Berdasarkan keberhasilan CNN dalam klasifikasi lalu lintas *darknet*, penelitian ini mengusulkan metode yang berbeda dalam mengklasifikasikan lalu lintas darknet yaitu AdaBoost Classifier.

AdaBoost classifier merupakan salah satu metode ensemble learning yang cukup populer [9]. *AdaBoost* atau *adaptive boosting* menghasilkan pembelajaran

yang lebih kuat dengan menambahkan pembelajaran lemah (*weak learners*) secara berulang [10]. Metode ini meningkatkan bobot secara iteratif. Penggunaan metode *AdaBoost* telah dilakukan beberapa penelitian terdahulu.

Penelitian Rehman Javed [11] dkk menerapkan metode *AdaBoost* dalam mengklasifikasikan *botnet* pada connected vehicles. Hasil dari penelitian ini menunjukkan metode *AdaBoost* mampu mencapai akurasi sebesar 99,1%. Hasil ini membuktikan metode yang digunakan cukup efisien dalam klasifikasi *botnet*.

Selanjutnya, penelitian Mohammed dkk menerapkan *AdaBoost* dalam klasifikasi serangan siber. Penelitian dilakukan dengan dataset CICIDS2019. Penelitian ini menerapkan PCA dalam pemilihan fitur. Hasil penelitian ini menunjukkan AdaBoost mampu mencapai klasifikasi terbaik dengan akurasi sebesar 99,1%.

Berdasarkan uraian di atas, penelitian ini mengusulkan *AdaBoost* sebagai pendekatan dalam mengklasifikasikan lalu lintas *darknet.* penelitian ini bertujuan untuk mengukur bagaimana pengaruh variasi nilai parameter terhadap performa model. Penelitian ini diharapkan dapat memberikan kontribusi sebagai dasar mengembangkan metode klasifikasi dan memberikan evaluasi terhadap performa *AdaBoost* dalam mengklasifikasikan lalu lintas *darknet*.

1.2 Rumusan Masalah

Dari penjelasan yang telah diuraikan pada latar belakang di atas, rumusan masalah yang diambil dari penelitian ini adalah :

1. Bagaimana cara klasifikasi lalu lintas *Darknet* dan *Benign* menggunakan metode *AdaBoost Classifier*?
2. Bagaimana tingkat akurasi metode *AdaBoost Classifier* dalam mengklasifikasikan lalu lintas *Darknet* dan *Benign.*
3. Bagaimana pengaruh variasi parameter *AdaBoost* seperti nilai *n_estimator* terhadap kinerja model klasifikasi.

1.3 Batasan Masalah

Agar penelitian mengarah pada pemaparan yang diharapkan, maka diperlukan batasan masalah dalam penelitian. Adapun batasan masalah dari penelitian ini adalah sebagai berikut :

1. Penelitian dilakukan pada dataset yang berasal dari *Canadian Intitute for Cybersecurity* (CIC) yaitu dataset CIC-*Darknet*2020.
2. Klasifikasi yang dilakukan adalah mengklasifikasikan lalu lintas ke dalam dua kelas, yaitu kelas "*Darknet"* dan "*Benign"*.
3. Penelitian ini hanya berfokus kepada klasifikasi, tidak melibatkan analisa lanjutan dan cara pencegahan terhadap aktivitas mencurigakan dalam lalu lintas *Darknet*.

1.4 Tujuan

Adapun tujuan yang hendak dicapai dari penelitian ini adalah:

1. Mengimplementasikan metode *AdaBoost Classifier* untuk membedakan *Darknet* dan *Benign* pada dataset CIC-Darknet2020.
2. Mengukur tingkat akurasi dari metode *AdaBoost Classifier* dalam mengklasifikasi lalu lintas *Darknet* dan *Benign*.
3. Menganalisis pengaruh variasi parameter AdaBoost terhadap hasil klasifikasi lalu lintas Darknet dan *Benign*.

1.5 Manfaat

Hasil dari penelitian ini dapat dijadikan landasan dalam pengembangan klasifikasi lalu lintas *Darknet* pada penelitian selanjutnya. Adapun manfaat lain dari penelitian ini adalah sebagai berikut:

1. Mampu menerapkan metode *AdaBoost Classifier* dalam membedakan lalu lintas *Darknet* dan *Benign*.
2. Menambah pemahaman tentang kinerja dan efektivitas metode *AdaBoost* dalam klasifikasi lalu lintas *Darknet* dan *Benign*.
3. Menambah pemahaman mengenai pengaruh variasi parameter terhadap hasil klasifikasi.

1.6 Metodologi Penelitian

Pada penelitian ini diterapkan beberapa tahapan metodologi. Adapun tahapan metodologi tersebut adalah sebagai berikut :

1. Tahap Pertama (Studi Pustaka/Literatur)

   Tahap ini dilakukan pencarian referensi atau literatur terkait dengan topik yang diangkat dari judul. Tujuannya untuk mendukung penelitian dengan informasi dan konsep dari berbagai sumber yang relevan terhadap penelitian.

2. Tahap Kedua (Perancangan Sistem)

   Selanjutnya tahap perancangan sistem, sistem dirancang berdasarkan perumusan masalah yang telah ditetapkan. Proses ini melibatkan pembangunan dan penerapan metode yang akan dilakukan pada proses penelitian, serta menyiapkan perangkat lunak dan perangkat keras yang mendukung. Konfigurasi dan penulisan kode juga dilakukan untuk implementasi metode yang digunakan pada tugas akhir ini.

3. Tahap Ketika (Pengujian)

   Pada tahap pengujian, dilakukan pengujian pada dataset yang berasal dari *Canadian Institute for Cybersecurity* (CIC) dengan nama CIC-*Darknet*2020 menggunakan metode *AdaBoost Classifier.*

4. Tahap Keempat (Analisis)

   Setelah data dari proses pengujian diperoleh, tahapan selanjutnya yaitu melakukan analisa dan pengolahan data sesuai dengan metode yang telah ditetapkan. Analisa dilakukan untuk membantingkan hasil penelitian ini dengan penelitian sebelumnya.

5. Tahap Kelima (Kesimpulan dan Saran)

   Tahap terakhir ialah menarik kesimpulan dari tahapan penelitian mulai dari studi pustaka, pengujian dan analisis hasil pengujian. Selain itu, saran untuk penelitian selanjutnya juga disusun berdasarkan hasil analisa yang telah dilakukan.

1.7 Sistematika Penulisan

Dalam penulisan tugas akhir ini akan dibagi menjadi beberapa bagian bab dengan sistematika sebagai berikut :

BAB I Pada bab pertama akan menjelaskan tentang latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat penelitian.

BAB II Pada bab ini berisikan *literatur review* tentang teori-teori pendukung yang berkaitan dengan lalu lintas *darknet*.

BAB III Pada bab ini dijelaskan kerangka kerja dari penelitian, perancangan sistem, dan tahapan-tahapan metodologi dalam proses penelitian.

BAB IV Pada bab ini menjelaskan tentang hasil dari pengujian yang telah dilakukan, dari hasil tersebut akan dilakukan analisa agar mendapat data yang akurat

BAB V Pada bab dijelaskan kesimpulan yang merupakan hasil dari penelitian yang telah dilakukan, serta saran yang diharapkan dapat membantu pengembangan penelitian selanjutnya.

DAFTAR PUSTAKA

[1] A. Anju *et al.*, "A Mysterious And Darkside Of The Darknet : A Qualitative Study," *Webology*, vol. 18, no. 4, pp. 285–294, 2021.

[2] K. Demertzis, K. Tsiknas, D. Takezis, C. Skianis, and L. Iliadis, "Darknet traffic big-data analysis and network management for real-time automating of the malicious intent detection process by a weight agnostic neural networks framework," *Electron.*, vol. 10, no. 7, 2021, doi: 10.3390/electronics10070781.

[3] H. Mohanty, A. H. Roudsari, and A. H. Lashkari, "Robust stacking ensemble model for darknet traffic classification under adversarial settings," *Comput. Secur.*, vol. 120, p. 102830, 2022, doi: 10.1016/j.cose.2022.102830.

[4] A. Almomani, *Darknet traffic analysis, and classification system based on modified stacking ensemble learning algorithms*, no. 0123456789. Springer Berlin Heidelberg, 2023. doi: 10.1007/s10257-023-00626-2.

[5] Q. A. Al-Haija, M. Krichen, and W. A. Elhaija, "Machine-Learning-Based Darknet Traffic Detection System for IoT Applications," *Electron.*, vol. 11, no. 4, 2022, doi: 10.3390/electronics11040556.

[6] F. Horasan and A. H. Yurttakal, "Darknet Web Traffic Classification via Gradient Boosting Algorithm," *Int. J. Eng. Res. Dev.*, vol. 14, no. 2, pp. 794–798, 2022.

[7] BSSN, "Laporan Bulanan Agustus 2023," 2023, [Online]. Available: www.idsirtii.or.id

[8] A. H. Lashkari, "DIDarknet : A Contemporary Approach to Detect and Characterize the Darknet Traffic using Deep Image Learning," pp. 1–13.

[9] Y. Zhang, J. Liu, and W. Shen, "A Review of Ensemble Learning Algorithms Used in Remote Sensing Applications," *Appl. Sci.*, vol. 12, no. 17, 2022, doi: 10.3390/app12178654.

[10] B. Thilagavathi, K. Suthendran, and K. Srujanraju, "Evaluating the AdaBoost Algorithm for Biometric-Based Face Recognition," *Lect. Notes Data Eng. Commun. Technol.*, vol. 63, pp. 669–678, 2021, doi: 10.1007/978-981-16-0081-4_67.

[11] A. Rehman Javed, Z. Jalil, S. Atif Moqurrab, S. Abbas, and X. Liu, “Ensemble Adaboost classifier for accurate and fast detection of botnet attacks in connected vehicles,” *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 10, pp. 1–18, 2022, doi: 10.1002/ett.4088.

[12] M. Coutinho Marim *et al.*, “Darknet traffic detection and characterization with models based on decision trees and neural networks,” *Intell. Syst. with Appl.*, vol. 18, no. February, p. 200199, 2023, doi: 10.1016/j.iswa.2023.200199.

[13] N. Rust-Nguyen, S. Sharma, and M. Stamp, “Darknet traffic classification and adversarial attacks using machine learning,” *Comput. Secur.*, vol. 127, 2023, doi: 10.1016/j.cose.2023.103098.

[14] M. B. Sarwar, M. K. Hanif, R. Talib, M. Younas, and M. U. Sarwar, “DarkDetect: Darknet Traffic Detection and Categorization Using Modified Convolution-Long Short-Term Memory,” *IEEE Access*, vol. 9, no. Dl, pp. 113705–113713, 2021, doi: 10.1109/ACCESS.2021.3105000.

[15] E. F. Fernandez, R. A. V. Carofilis, F. J. Martino, and P. B. Medina, “Classifying Suspicious Content in Tor Darknet,” 2020, [Online]. Available: http://arxiv.org/abs/2005.10086

[16] X. Tong, C. Zhang, J. Wang, Z. Zhao, and Z. Liu, “Dark-Forest: Analysis on the Behavior of DarkWeb Traffic via DeepForest and PSO Algorithm,” *C. - Comput. Model. Eng. Sci.*, vol. 135, no. 1, pp. 561–581, 2023, doi: 10.32604/cmes.2022.022495.

[17] R. Niranjana, V. A. Kumar, and S. Sheen, “Darknet Traffic Analysis and Classification Using Numerical AGM and Mean Shift Clustering Algorithm,” *SN Comput. Sci.*, vol. 1, no. 1, pp. 1–10, 2020, doi: 10.1007/s42979-019-0016-x.

[18] Z. Mohamud Omar and J. Ibrahim, “An Overview of Darknet, Rise and Challenges and Its Assumptions,” *Artic. Int. J. Comput. Sci. Inf. Technol.*, vol. 7, no. July, pp. 110–116, 2020, [Online]. Available: www.researchpublish.com

[19] D. P. F. Möller, “Machine Learning and Deep Learning,” *Adv. Inf. Secur.*, vol. 103, pp. 347–384, 2023, doi: 10.1007/978-3-031-26845-8_8.

[20] P. C. Sen, M. Hajra, and M. Ghosh, *Supervised Classification Algorithms in Machine Learning: A Survey and Review*, vol. 937. Springer Singapore, 2020. doi: 10.1007/978-981-13-7403-6_11.

[21] M. Zounemat-Kermani, O. Batelaan, M. Fadaee, and R. Hinkelmann, "Ensemble machine learning paradigms in hydrology: A review," *J. Hydrol.*, vol. 598, no. December 2020, p. 126266, 2021, doi: 10.1016/j.jhydrol.2021.126266.

[22] N. Thomas Rincy and R. Gupta, "Ensemble learning techniques and its efficiency in machine learning: A survey," *2nd Int. Conf. Data, Eng. Appl. IDEA 2020*, 2020, doi: 10.1109/IDEA49133.2020.9170675.

[23] J. M. Ferreira *et al.*, "Identification of Daily Activites and Environments Based on the AdaBoost Method Using Mobile Device Data: A Systematic Review," *Electronics*, vol. 9, no. 1, p. 192, 2020, doi: 10.3390/electronics9010192.

[24] D. C. Feng, Z. T. Liu, X. D. Wang, Z. M. Jiang, and S. X. Liang, "Failure mode classification and bearing capacity prediction for reinforced concrete columns based on ensemble machine learning algorithm," *Adv. Eng. Informatics*, vol. 45, no. May, p. 101126, 2020, doi: 10.1016/j.aei.2020.101126.

[25] L. B. V. de Amorim, G. D. C. Cavalcanti, and R. M. O. Cruz, "The choice of scaling technique matters for classification performance," *Appl. Soft Comput.*, vol. 133, pp. 1–37, 2023, doi: 10.1016/j.asoc.2022.109924.

[26] C. Kaope and Y. Pristyanto, "The Effect of Class Imbalance Handling on Datasets Toward Classification Algorithm Performance," *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 22, no. 2, pp. 227–238, 2023, doi: 10.30812/matrik.v22i2.2515.

[27] M. S. Kraiem, F. Sánchez-Hernández, and M. N. Moreno-García, "Selecting the suitable resampling strategy for imbalanced data classification regarding dataset properties. An approach based on association models," *Appl. Sci.*, vol. 11, no. 18, 2021, doi: 10.3390/app11188546.

[28] Y. Zhu, Y. Hu, Q. Liu, H. Liu, C. Ma, and J. Yin, "A Hybrid Approach for Predicting Corporate Financial Risk: Integrating SMOTE-ENN and

NGBoost," *IEEE Access*, vol. 11, pp. 111106–111125, 2023, doi: 10.1109/ACCESS.2023.3323198.

[29] F. Yang, K. Wang, L. Sun, M. Zhai, J. Song, and H. Wang, "A hybrid sampling algorithm combining synthetic minority over-sampling technique and edited nearest neighbor for missed abortion diagnosis," *BMC Med. Inform. Decis. Mak.*, vol. 22, no. 1, pp. 1–14, 2022, doi: 10.1186/s12911-022-02075-2.