Optimasi Logistic Regression untuk Deteksi Serangan DoS pada Keamanan IoT

Nauval Dwi Primadya[1], Adhitya Nugraha[2], Ardytha Luthfiarta[3], Sahrul Yudha Fahrezi[4]
Fakultas Ilmu Komputer, Program Studi Teknik Informatika
Universitas Dian Nuswantoro
Semarang, Indonesia
e-mail: [1]primadya021@gmail.com, [2]adhitya@dsn.dinus.ac.id, [3]ardytha.luthfiarta@dsn.dinus.ac.id,
[4]yudhafahrezi30@gmail.com

Diajukan: 23 Desember 2023; Direvisi: 19 Januari 2024; Diterima: 20 Januari 2024

Abstrak

Keamanan perangkat Internet of Things (IoT) merupakan prioritas utama karena potensi risiko kerusakan perangkat dan kebocoran data yang dapat berdampak serius. Perangkat IoT telah membawa manfaat signifikan ke berbagai sektor, seperti kesehatan, transportasi, dan industri, namun tingkat serangan terhadapnya terus meningkat. Dalam mengatasi tantangan ini, pendekatan machine learning digunakan dengan memanfaatkan dataset CIC IOT ATTACKS 2023 dari University of New Brunswick. Untuk menghasilkan data yang berkualitas, dilakukan random undersampling untuk mengatasi ketidakseimbangan data, dan seleksi fitur menggunakan Recursive Feature Elimination untuk mendapatkan fitur terbaik. Pemilihan Logistic Regression sebagai algoritma pemodelan dipilih dengan pertimbangan yang matang. Logistic Regression dipilih karena kemampuannya memberikan interpretasi yang jelas terhadap kontribusi relatif setiap fitur terhadap prediksi keamanan perangkat IoT. Selain itu, model ini efisien secara komputasional, mengatasi ketidakseimbangan data, dan tahan terhadap overfitting, yang semuanya merupakan faktor krusial dalam konteks keamanan IoT. Hasil penelitian menunjukkan bahwa penggunaan Logistic Regression bersamaan dengan seleksi fitur memberikan tingkat akurasi tertinggi mencapai 97%, dengan waktu pemrosesan yang efisien sekitar 11 detik. Dari hasil ini, dapat disimpulkan bahwa kombinasi teknik random undersampling dan seleksi fitur menggunakan Recursive Feature Elimination secara positif memengaruhi akurasi pada model Logistic Regression, menjadikannya pilihan yang sesuai untuk meningkatkan keamanan perangkat IoT.

Kata kunci: *CIC IOT Attack 2023, Random Under Sampling, Recursive Feature Elimination.*

Abstract

Security in Internet of Things (IoT) devices is a top priority due to the potential risks of device damage and data leaks that can have serious consequences. IoT devices have brought significant benefits to various sectors, including healthcare, transportation, and industry, but the level of attacks against them continues to rise. In addressing this challenge, a machine learning approach is employed using the CIC IOT ATTACKS 2023 dataset from the University of New Brunswick. To produce high-quality data, random undersampling is applied to address data imbalance, and feature selection is performed using Recursive Feature Elimination to obtain the best features. The choice of Logistic Regression as the modeling algorithm is made after careful consideration. Logistic Regression is selected for its ability to provide clear interpretations of the relative contributions of each feature to the prediction of IoT device security. Additionally, the model is computationally efficient, addresses data imbalance, and is resistant to overfitting—crucial factors in the context of IoT security. The research results indicate that the use of Logistic Regression in combination with feature selection achieves the highest accuracy rate of up to 97%, with an efficient processing time of around 11 seconds. From these findings, it can be concluded that the combination of random undersampling and feature selection using Recursive Feature Elimination positively influences accuracy in the Logistic Regression model, making it a suitable choice for enhancing IoT device security.

Keywords*: CIC IOT Attack 2023, Random Under Sampling, Recursive Feature Elimination.*

1. Pendahuluan

Internet of Things (IoT) merupakan ide mengenai objek fisik yang terkoneksi dengan internet dan dapat berinteraksi satu sama lain. Ide ini semakin berkembang popularitasnya dalam beberapa tahun terakhir karena memiliki potensi untuk meningkatkan efisiensi dan produktivitas di berbagai sektor [1]. Namun, seiring berjalannya waktu dan kemajuan teknologi, keamanan IoT menjadi semakin krusial. Hal ini disebabkan oleh kenyataan bahwa IoT selalu terkoneksi dengan internet. Rentannya perangkat IoT dapat mengakibatkan kerusakan pada perangkat itu sendiri dan berpotensi menyebabkan pencurian data pribadi pada perangkat IoT [2].

Denial of Service (DoS) adalah salah satu bentuk serangan yang merupakan ancaman keamanan yang sering terjadi. Jenis serangan ini dapat membuat perangkat IoT menjadi tidak responsif, bahkan hingga tidak dapat digunakan [3]. Untuk menjaga perangkat IoT dari berbagai jenis serangan, bukan hanya DDoS, diperlukan *dataset* yang dapat digunakan sebagai pelatihan model *mechine learning* untuk mendeteksi ancaman tersebut.

Random Under Sampling merupakan metode yang digunakan untuk mengatasi ketidakseimbangan kelas pada data. Pendekatan ini dilakukan dengan menghapus sejumlah *instance* dari kelas mayoritas, sehingga jumlah *instance* pada kelas mayoritas sejajar dengan jumlah *instance* pada kelas minoritas. Pendekatan ini telah sering diterapkan dalam berbagai penelitian dan aplikasi [4], [5].

Recursive Feature Elimination (RFE) merupakan salah satu metode seleksi fitur yang diterapkan dalam pembentukan model data. Pendekatan ini beroperasi dengan menghapus fitur yang dianggap kurang signifikan secara berurutan, sehingga diperoleh *subset* fitur yang paling relevan. RFE telah menjadi populer dalam berbagai penelitian dan aplikasi [6].

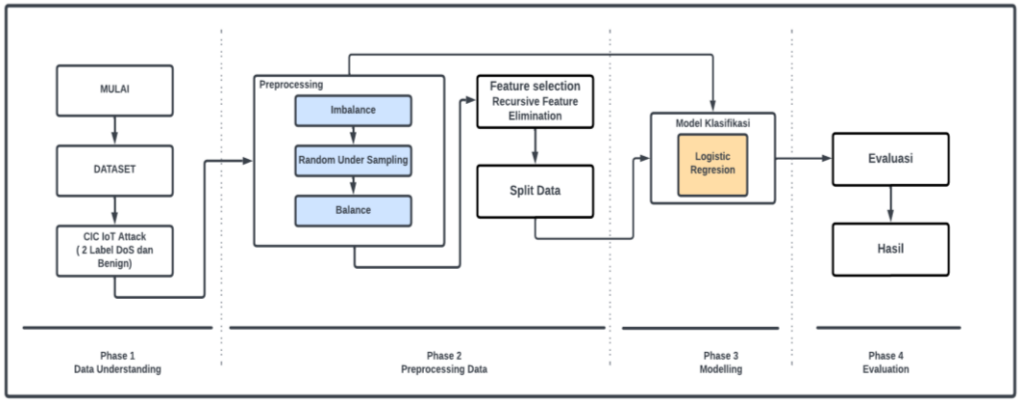
Dua metode tersebut sangat umum digunakan dalam proses pemodelan data. Dengan menggunakan *Random Under Sampling*, maka data yang semula tidak seimbang akan menjadi seimbang mengikuti kelas minoritas. Seleksi fitur menggunakan RFE akan mengambil fitur atau atribut yang penting tanpa mengurangi informasi data tersebut. Kedua metode tersebut dapat meningkatkan waktu pemrosesan yang digunakan [7].

Penelitian yang dilakukan oleh Li et al. (2021). Penelitian tersebut mengulas pemanfaatan *Random Under Sampling* dan *Recursive Feature Elimination* untuk meningkatkan kinerja model prediksi dalam konteks data keuangan. Hasil studi menunjukkan bahwa penggunaan *Random Under Sampling* dan *Recursive Feature Elimination* dapat meningkatkan akurasi model prediksi dengan mengurangi jumlah variabel yang tidak relevan. Kesimpulan yang diambil dari penelitian ini adalah bahwa penggunaan *Random Under Sampling* dan *Recursive Feature Elimination* dapat menjadi solusi untuk meningkatkan kinerja model prediksi dalam analisis data keuangan [8].

Penelitian lain yang mencakup topik *Random Under Sampling* dan *Recursive Feature Elimination* telah dilakukan oleh Zhang et al. (2019). Studi ini membahas penerapan algoritma Random Forest-*Recursive Feature Elimination* (RF-RFE) untuk meningkatkan kinerja model prediksi pada data kesehatan. Temuan dari penelitian tersebut menunjukkan bahwa penggunaan RF-RFE dapat meningkatkan akurasi model prediksi dengan mengurangi jumlah variabel yang tidak signifikan. Kesimpulan dari penelitian ini adalah bahwa RF-RFE dapat menjadi metode yang efektif dalam meningkatkan kinerja model prediksi pada analisis data kesehatan [9].

Penelitian yang telah dilakukan oleh Darst et al. Penelitian ini membahas penerapan algoritma Random Forest-*Recursive Feature Elimination* (RF-RFE) dalam penanganan variabel yang saling berkorelasi pada data omik dengan dimensi yang tinggi. Hasil penelitian menunjukkan bahwa RF-RFE mampu mengurangi signifikansi variabel yang berkorelasi, tetapi sekaligus juga mengurangi signifikansi variabel yang bersifat kausal, sehingga deteksinya menjadi sulit. Kesimpulan yang diambil dari penelitian ini adalah bahwa RF-RFE mungkin kurang sesuai untuk penggunaan pada data yang memiliki dimensi yang tinggi [10].

2. Metode Penelitian

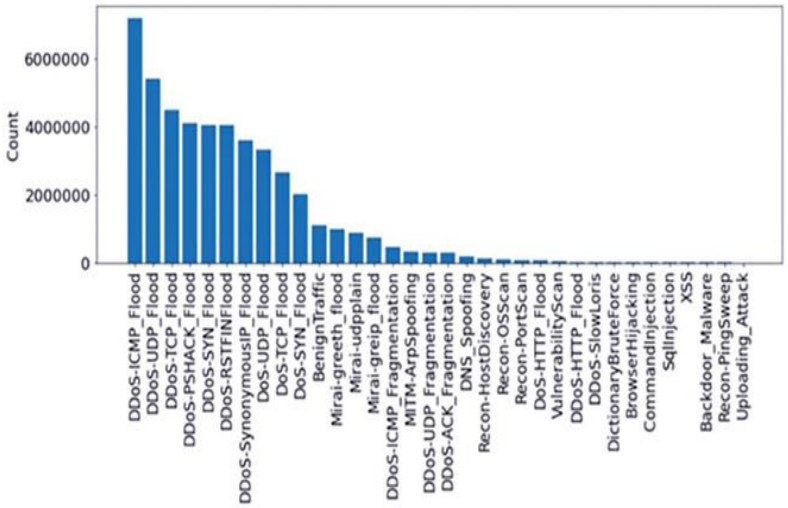


Gambar 1. Diagram Penelitian

Penelitian ini diawali dengan pengambilan data dari *University of New Brunswick*, yang terdiri dari 32 label, dengan pemfokusan pada *DoS* dan *Benign* sebagai variabel utama. Penelitian sebelumnya oleh Euclides Carlos Pinto Neto et al. tidak memberikan penjelasan yang mendalam mengenai langkah-langkah *preprocessing*, menimbulkan kekhawatiran akan ketidakseimbangan data dalam penelitian tersebut. Meskipun akurasi hasil penelitian sebelumnya relatif tinggi, diperkirakan bahwa hal ini mungkin disebabkan oleh kurangnya tahapan *balancing* data [1]. Oleh karena itu, penelitian ini berusaha menambahkan *balancing* data dan melakukan seleksi fitur dengan tujuan mencapai tingkat akurasi yang optimal tanpa mengesampingkan fitur-fitur kritis. Optimasi dilakukan melalui penerapan *Random Under Sampling* dan *Recursive Feature Elimination*. Penerapan *Random Under Sampling* bertujuan untuk mengurangi ketidakseimbangan antara kelas mayoritas dan minoritas, sehingga dapat meningkatkan kinerja model. Sementara itu, *Recursive Feature Elimination* digunakan untuk mengurangi dimensi data dan menghilangkan fitur-fitur yang tidak relevan, dengan harapan dapat meningkatkan kinerja model secara keseluruhan [11].

2.1. Pengambilan Data

Data yang digunakan pada penelitian ini adalah *dataset* yang diambil dari *University of New Brunswick*, dengan jumlah data sebesar 46.686.579 baris, 32 label jenis serangan IoT, dan 47 fitur. Data berbentuk CSV *file* yang akan digunakan pada penelitian ini [1]. Dengan sebaran data seperti pada gambar 2.



Gambar 2. Sebaran Data CIC IoT Attacks 2023

2.2. DoS

Serangan *Denial-of-Service* (DoS) adalah bentuk serangan yang bertujuan untuk membuat sumber daya sistem tidak dapat diakses. Pada konteks *Internet of Things* (IoT), serangan DoS memiliki potensi untuk menyebabkan kerusakan yang signifikan pada perangkat IoT dan infrastruktur terkait [12].

2.3. Pre-Processing

Preprocessing dalam *mechine learning* merupakan tahap pengolahan data yang dilakukan sebelum data tersebut dimasukkan ke dalam model *mechine learning*. Tujuan dari proses preprocessing adalah untuk mempersiapkan data agar dapat diolah secara efektif oleh model *mechine learning* dan menghasilkan hasil yang akurat. Beberapa metode *preprocessing* yang umum digunakan dalam *mechine learning* mencakup normalisasi dan penanganan data yang hilang [13].

2.4. *Random Under Sampling*

Strategi pengambilan sampel *Random Under Sampling* (RUS) merupakan metode yang digunakan untuk menangani ketidakseimbangan dalam *dataset* dengan mengurangi jumlah sampel dari kelas mayoritas. Dalam pendekatan ini, sampel-sampel dipilih secara acak dari kelas mayoritas sehingga mencapai keseimbangan dengan jumlah sampel di kelas minoritas. Implementasi RUS terbukti sangat efektif dalam menangani ketidakseimbangan kelas dalam *dataset* dan dapat meningkatkan kinerja model *mechine learning* [14].

2.5. *Recursive Feature Elimination*

Teknik seleksi fitur yang dikenal sebagai *Recursive Feature Elimination* (RFE) digunakan dalam pembentukan model data. Pendekatan ini bekerja dengan menghapus fitur yang dianggap kurang signifikan secara bertahap hingga diperoleh *subset* fitur yang paling relevan. RFE telah diterapkan luas dalam berbagai penelitian dan aplikasi [15], [16].

2.6. Logistic Regressione

Logistic Regression merupakan salah satu metode statistika yang digunakan untuk memprediksi hasil biner dari suatu variabel dependen berdasarkan satu atau lebih variabel independen. Pendekatan ini telah menjadi sangat populer dalam analisis data yang melibatkan variabel kategorial dan memiliki penerapan yang luas di berbagai bidang disiplin ilmu, termasuk ekonomi, kedokteran, dan ilmu sosial [17].

$$Ln\left(\frac{p}{1-p}\right) = B_o + B_1 X \quad (1)$$

$B_o = Konstanta$
$B_1 = The\ coefficient\ of\ each\ variable$

The value of p or chance (Y=1) can be found in the equation

$$p = \frac{e^{(B_o + B_1 X)}}{(1 + e^{(B_o + B_1 X)})} \quad (2)$$

2.7. Confusion Matrix

Confusion Matrix adalah alat evaluasi performa dalam *machine learning* untuk mengukur akurasi model dalam klasifikasi. Matriks ini terdiri dari empat elemen utama: *True Positive* (TP), *False Positive* (FP), *True Negative* (TN), dan *False Negative* (FN). Secara rinci, TP mencakup jumlah data positif yang benar-benar diklasifikasikan dengan benar, FP adalah jumlah data negatif yang keliru diklasifikasikan sebagai positif, TN adalah jumlah data negatif yang diklasifikasikan dengan benar, dan FN adalah jumlah data positif yang keliru diklasifikasikan sebagai negatif [17].

Tabel 1. Confusion Matrix

Predict class	Actual class	
	+	-
+	True positive (TP)	False positive (FP)
-	False negative (FN)	True negative (TN)

Untuk menghitung akurasi, gunakan rumus berikut:

$$Akurasi = \frac{(TP+TN)}{(TP+TN+FP+FN)} \quad (3)$$

Precision adalah istilah yang merujuk pada sejauh mana item yang relevan dipilih dibandingkan dengan semua item yang dipilih. Dalam konteks ini, presisi mencerminkan sejauh mana jawaban terhadap permintaan informasi cocok dengan permintaan tersebut. Rumus presisi yang digunakan untuk pengukuran adalah sebagai berikut:

$$Precision = \frac{TP}{(TP+FP)} \quad (4)$$

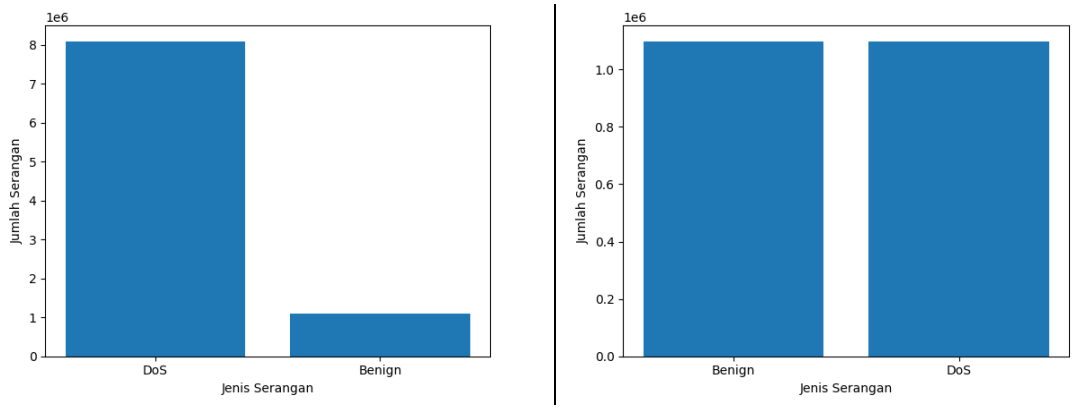
Recall adalah istilah yang merujuk pada sejauh mana item yang relevan dipilih dibandingkan dengan total jumlah item yang relevan yang tersedia. Perhitungan *recall* dilakukan menggunakan rumus berikut:

$$Recall = \frac{TP}{(TP+FN)} \quad (5)$$

3. Hasil dan Pembahasan

3.1. Imbalance *Dataset*

Dalam fase penanganan ketidakseimbangan *dataset*, dilakukan pendekatan *Random Under Sampling*. Jumlah data yang dihasilkan sesuai dengan kelas minoritas, yakni *Benign* dengan jumlah 1.098.195. Awalnya, *dataset* terdiri dari 8.090.738 sampel untuk kelas DoS dan 1.098.195 sampel untuk kelas *Benign*. Sebagaimana tampak pada gambar 3, perbandingan antara hasil sebelum dan setelah penerapan *Random Under Sampling* dapat dilihat.



Gambar 3. Perbandingan Sebelum dan Sesudah *Random Under Sampling*

Setelah dilakukan *Random Under Sampling*, data yang telah diolah selanjutnya disimpan sebagai *dataset* baru. Langkah ini bertujuan untuk mempermudah proses selanjutnya. Tahap berikutnya melibatkan pengujian *dataset* baru dengan dua pendekatan yang berbeda. Pendekatan pertama melibatkan seleksi fitur, sementara pendekatan kedua tidak melibatkan seleksi fitur.

3.2. Seleksi Fitur

Data yang telah melewati proses *preprocessing* akan melanjutkan ke tahap seleksi fitur. Seleksi fitur merupakan langkah untuk memilih atribut pada *dataset*, dengan tujuan mendapatkan jumlah atribut yang lebih sedikit tanpa menghilangkan data penting yang dapat memengaruhi hasil pengujian. Awalnya, terdapat 47 fitur dengan jabaran sebagai berikut:

Tabel 2. Fitur pada *Dataset*

Feature	
flow_duration	SSH
Header_Length	IRC
Protocol type	TCP
Duration	UDP
Rate	DHCP
Srate	ARP
Drate	ICMP
fin_flag_number	IPv
syn_flag_number	LLC
rst_flag_number	Tot sum
psh_flag_number	Min
ack_flag_number	Max
ece_flag_number	AVG
cwr_flag_number	Std
ack_count	Tot size
syn_count	IAT
fin_count	Number
urg_count	Magnitue
rst_count	Radius
HTTP	Covariance
HTTPS	Variance
DNS	Weight
Telnet	label
SMTP	

Setelah melalui tahap seleksi fitur menggunakan metode *Recursive Feature Elimination* with Cross-Validation (RFECV) dengan nilai KFold 5, fitur terpilih adalah sebagai berikut:

Tabel 3. Fitur terpilih setelah RFECV

Feature
flow_duration
Header_Length
urg_count
rst_count
Tot sum
Min
Max

AVG
Std
Tot size
Radius
Weight
label

Dari jumlah fitur yang terpilih, dilakukan pengujian menggunakan algoritma *Logistic Regression* untuk mengukur tingkat akurasi setelah dilakukan seleksi fitur, dan dilakukan perbandingan waktu pemrosesan sebelum dan sesudah seleksi fitur.

3.3. Klasifikasi dan Evaluasi

Guna memperoleh pemahaman menyeluruh mengenai klasifikasi dari dua *dataset* yang telah disiapkan, dilakukan pengujian menggunakan algoritma *Logistic Regression*. Hasil pengujian mencakup tingkat akurasi dan waktu pemrosesan, dengan tujuan memungkinkan perbandingan antara keduanya.

Tabel 4. Hasil Uji

RASIO	Akurasi		Waktu	
	Logistic Regression - RFECV	Logistic Regression	Logistic Regression - RFECV	Logistic Regression
70 : 30	97.80 %	93.47 %	10.695 detik	14.229 detik
80 : 20	97.80 %	93.43 %	11.038 detik	13.408 detik
90 : 10	97.85 %	93.44 %	12.572 detik	13.153 detik

Tampak pada tabel 4 perbandingan antara algoritma *Logistic Regression* (LR) yang memanfaatkan *dataset* dengan seleksi fitur dan *dataset* tanpa seleksi fitur. Dari kedua perbandingan tersebut, dengan membagi rasio data *train* dan *test*, terlihat bahwa tingkat akurasi yang diperoleh dari *dataset* yang mengalami seleksi fitur lebih unggul dibandingkan dengan yang tidak mengalami seleksi fitur. Rata-rata peningkatan akurasi mencapai 4%. Perbedaan waktu pemrosesan berkisar antara 1 hingga 4 detik.

4. Kesimpulan

Dari masalah yang dijelaskan pada bagian pendahuluan, terungkap bahwa perlu dilakukan pengolahan data yang lebih efektif dan efisien untuk meningkatkan kecepatan dalam proses pengambilan keputusan. Salah satu pendekatan untuk meningkatkan efisiensi dalam proses klasifikasi adalah melalui seleksi fitur, yang menghasilkan *dataset* dengan jumlah atribut yang lebih terbatas. Evaluasi terhadap hasil klasifikasi pada *dataset* yang telah mengalami seleksi fitur menunjukkan peningkatan kinerja dibandingkan dengan *dataset* tanpa seleksi fitur.

Bukti perbandingan tersebut terlihat pada akurasi akhir *Logistic Regression*. Tanpa seleksi fitur, akurasi rata-rata mencapai 93% dengan waktu pemrosesan rata-rata selama 13 detik. Sebaliknya, dengan menggunakan seleksi fitur, akurasi meningkat menjadi 97%, sementara waktu pemrosesan rata-rata hanya 11 detik.

Daftar Pustaka

[1] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment," *Sensors*, vol. 23, no. 13, Jul. 2023, doi: 10.3390/s23135941.

[2] M. Zolanvari, M. A. Teixeira, and R. Jain, "Effect of Imbalanced Datasets on Security of Industrial IoT Using Machine Learning."

[3] IEEE Communications Society, Global IT Research Institute, and Institute of Electrical and Electronics Engineers, *The 24th International Conference on Advanced Communication Technology : conference proceedings : Phoenix Park, Pyeongchang, Korea (South) (on-line conference) : Feb. 13-16, 2022*.

[4] N. Noorhalim, A. Ali, and S. M. Shamsuddin, "Handling Imbalanced Ratio for Class Imbalance Problem Using SMOTE," in *Proceedings of the Third International Conference on Computing,*

Mathematics and Statistics (iCMS2017), Springer Singapore, 2019, pp. 19–30. doi: 10.1007/978-981-13-7279-7_3.

[5] A. Ilham[1], "KOMPARASI ALGORITMA KLASIFIKASI DENGAN PENDEKATAN LEVEL DATA UNTUK MENANGANI DATA KELAS TIDAK SEIMBANG," *Jurnal Ilmiah Ilmu Komputer*, vol. 3, no. 1, 2017, [Online]. Available: http://ejournal.fikom-unasman.ac.id

[6] A. Mudi, P. 1∗, W. Febri, R. Sudirman, R. J. Musridho, and F. Amalia, "Impurity-Based Important Features for feature selection in Recursive Feature Elimination for Stock Price Forecasting," 2023, doi: 10.31004/jutin.v6i4.17726.

[7] E. F. Saraswita, D. P. Rini, and A. Abdiansah, "Analisis Sentimen E-Wallet di Twitter Menggunakan Support Vector Machine dan Recursive Feature Elimination," *JURNAL MEDIA INFORMATIKA BUDIDARMA*, vol. 5, no. 4, p. 1195, Oct. 2021, doi: 10.30865/mib.v5i4.3118.

[8] A. Rezaei Barzani, P. Pahlavani, O. Ghorbanzadeh, and P. Ghamisi, "How the recursive feature elimination affects the SVM and RF for wildfire modeling? A mountainous case study area", doi: 10.5194/egusphere-2022-1294.

[9] S. Xia and Y. Yang, "A Model-Free Feature Selection Technique of Feature Screening and Random Forest-Based Recursive Feature Elimination," *International Journal of Intelligent Systems*, vol. 2023, 2023, doi: 10.1155/2023/2400194.

[10] B. F. Darst, K. C. Malecki, and C. D. Engelman, "Using recursive feature elimination in random forest to account for correlated variables in high dimensional data," *BMC Genet*, vol. 19, Sep. 2018, doi: 10.1186/s12863-018-0633-8.

[11] F. Abbasi, M. Naderan, and S. E. Alavi, "Anomaly detection in Internet of Things using feature selection and classification based on Logistic Regression and Artificial Neural Network on N-BaIoT dataset," in *Proceedings of 2021 5th International Conference on Internet of Things and Applications, IoT 2021*, Institute of Electrical and Electronics Engineers Inc., May 2021. doi: 10.1109/IoT52625.2021.9469605.

[12] S. H. Lee, Y. L. Shiue, C. H. Cheng, Y. H. Li, and Y. F. Huang, "Detection and Prevention of DDoS Attacks on the IoT," *Applied Sciences (Switzerland)*, vol. 12, no. 23, Dec. 2022, doi: 10.3390/app122312407.

[13] B. Hakim, "Analisa Sentimen Data Text Preprocessing Pada Data Mining Dengan Menggunakan Machine Learning," *JBASE - Journal of Business and Audit Information Systems*, vol. 4, no. 2, Aug. 2021, doi: 10.30813/jbase.v4i2.3000.

[14] A. Syukron and A. Subekti, "Penerapan Metode Random Over-Under Sampling dan Random Forest untuk Klasifikasi Penilaian Kredit," *JURNAL INFORMATIKA*, vol. 5, no. 2, 2018.

[15] H. Jeon and S. Oh, "Hybrid-recursive feature elimination for efficient feature selection," *Applied Sciences (Switzerland)*, vol. 10, no. 9, May 2020, doi: 10.3390/app10093211.

[16] M. G. Ismail, M. A. El Ghany, and M. A. M. Salem, "Enhanced Recursive Feature Elimination for IoT Intrusion Detection Systems," in *2022 International Conference on Microelectronics, ICM 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 193–196. doi: 10.1109/ICM56065.2022.10005438.

[17] W. A. Setyati, S. Sunaryo, A. Rezagama, A. K. Widodo, and M. F. A. Yulianto, "PENERAPAN REGRESI LOGISTIK DALAM PENENTUAN FAKTOR YANG MEMPENGARUHI JUMLAH WISATAWAN ECOTOURISM DESA BEDONO," *JURNAL ENGGANO*, vol. 5, no. 1, pp. 11–22, Apr. 2020, doi: 10.31186/jenggano.5.1.11-22.