INNOVATIVE: Journal Of Social Science Research
Volume 4 Nomor 3 Tahun 2024 Page 16461-16465
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Analisis Performa Algoritma Klasifikasi untuk Deteksi Spam pada Email

Thiara Tri Funny Manguma[1✉], Emil Fatra[2]
Universitas Almarisah Madani
Email: thiaramanguma014@gmail.com[1✉]

Abstrak

Deteksi spam pada email merupakan masalah penting dalam bidang keamanan siber dan pengelolaan informasi. Berbagai algoritma klasifikasi telah dikembangkan untuk mengidentifikasi dan memfilter email spam secara efektif. Penelitian ini bertujuan untuk menganalisis performa beberapa algoritma klasifikasi, termasuk Naive Bayes, K-Nearest dan Random Forest, Support Vector Machine dalam mendeteksi email spam. Penelitian menggunakan data Enron-Spam, yang berisi email spam dan non-spam (ham) yang telah dikategorikan. Evaluasi dilakukan berdasarkan beberapa metrik performa seperti F1-score, akurasi, presisi, dan recall. Dengan hasil bahwa tingkat akurasi yang tinggi dengan algoritma Random Forest, sedangkan Naive Bayes menunjukkan performa yang lebih baik dalam hal presisi. SVM dan KNN juga menunjukkan hasil yang kompetitif, namun kinerja mereka bervariasi tergantung pada parameter dan konfigurasi yang digunakan. Penelitian ini memberikan wawasan tentang kelebihan dan kelemahan masing-masing algoritma dalam konteks deteksi spam, serta rekomendasi untuk implementasi praktis dalam sistem filter email. Dengan memahami karakteristik dan performa dari berbagai algoritma klasifikasi, diharapkan dapat meningkatkan efektivitas sistem deteksi spam dan mengurangi jumlah email spam yang diterima oleh pengguna.

Kata Kunci: *Deteksi Spam, Naive Bayes, Random Forest, Support Vector Machine, Algoritma Klasifikasi*

Abstract

Spam detection in emails is an important problem in the field of cyber security and information management. Various classification algorithms have been developed to identify and filter spam emails effectively. This research aims to analyze the performance of several popular classification algorithms, including Naive Bayes, Support Vector Machine, K-Nearest and Random Forest in detecting spam emails. This research uses Enron-Spam data, which contains categorized spam and non-spam (ham) emails. Evaluation is carried out based on several performance metrics such as F1-score, accuracy, precision and recall. With the result that the level of accuracy is high with the Random Forest algorithm, while Naive Bayes shows better performance in terms of precision. SVM and KNN also show competitive results, but their performance varies depending on the parameters and configurations used. This research provides insight into the strengths and weaknesses of each algorithm in the context of spam detection, as well as recommendations for practical implementation in email filter systems. By understanding the characteristics and performance of various classification algorithms, it is hoped that we can increase the effectiveness of spam detection systems and reduce the number of spam emails received by users.

Keywords: *Spam Detection, Naive Bayes, Random Forest, Support Vector Machine, Classification Algorithms*

PENDAHULUAN

Email menjadi salah satu sarana komunikasi yang umum digunakan dalam lingkungan bisnis maupun personal. Namun, dengan peningkatan penggunaan email, masalah spam juga semakin merajalela. Spam, yang sering kali berupa pesan-pesan tidak diinginkan yang mengandung iklan, phishing, atau malware, tidak hanya mengganggu produktivitas (Utami & Kom, n.d.),tetapi juga dapat menjadi ancaman serius terhadap keamanan siber. Oleh karena itu, deteksi spam pada email menjadi sangat penting untuk menjaga integritas dan keamanan informasi.

Meskipun telah ada berbagai upaya untuk mengatasi masalah spam, termasuk penggunaan filter spam oleh penyedia layanan email, tetapi spammer terus berupaya untuk menghindari deteksi dengan mengembangkan teknik-teknik baru (Harahap, 2023). Dalam konteks ini, algoritma klasifikasi menjadi pendekatan yang biasa digunakan untuk membedakan antara email spam dan non-spam (ham) (Mukhtar et al., 2022) . Algoritma klasifikasi memungkinkan sistem untuk secara otomatis mempelajari pola-pola yang terkandung dalam email dan membuat prediksi apakah sebuah email termasuk spam atau tidak.

Penelitian sebelumnya telah mengusulkan berbagai algoritma klasifikasi untuk deteksi spam, termasuk Naive Bayes (Frank et al., 2000), merupakan algoritma pembelajaran mesin yang didasarkan pada penerapan teorema Bayes dengan asumsi independensi antara fitur-fitur yang diberikan kelas tertentu. Support Vector Machine (SVM) (Cervantes et al., 2020), merupakan algoritma pembelajaran mesin yang digunakan untuk klasifikasi dan regresi. Random Forest (Schonlau & Zou, 2020), merupakan algoritma ini bekerja dengan membangun banyak pohon keputusan (decision trees) selama pelatihan dan output dari kelas (klasifikasi) atau rata-rata prediksi (regresi) dari individu pohon tersebut dan K-Nearest Neighbors (KNN) (Isnain et al., 2021) merupakan algoritma ini bekerja dengan mengidentifikasi sejumlah KKK titik data terdekat (neighbors) dalam ruang fitur untuk membuat prediksi tentang kelas atau nilai dari data baru berdasarkan mayoritas kelas atau rata-rata nilai dari tetangga-tetangga terdekat. Namun dari metode tersebut, belum ada konsensus yang jelas mengenai algoritma mana yang memberikan performa terbaik dalam kasus deteksi spam pada email. Oleh karena itu, penelitian ini bertujuan untuk melakukan analisis menyeluruh terhadap performa beberapa algoritma klasifikasi yang umum digunakan dalam konteks deteksi spam. Dengan membandingkan dan mengevaluasi kinerja algoritma-algoritma ini, diharapkan kita dapat mendapatkan pemahaman yang lebih baik tentang kelebihan dan kelemahan masing-masing algoritma, serta merekomendasikan pendekatan terbaik untuk implementasi dalam sistem deteksi spam. Penelitian ini akan memberikan kontribusi penting dalam upaya meningkatkan efektivitas dan akurasi deteksi spam pada email, sehingga dapat membantu melindungi pengguna dari ancaman spam yang semakin meningkat.

METODE PENELITIAN

Studi ini menggunakan dataset Enron-Spam (Islam et al., 2021), yang merupakan dataset yang umum digunakan dalam penelitian deteksi spam email. Dataset ini terdiri dari email spam dan non-spam (ham) yang telah dikategorikan. Pertama-tama, data dipreproses untuk membersihkan email dari informasi yang tidak relevan, seperti HTML tags, karakter khusus, dan tautan. Selanjutnya, fitur-fitur yang relevan diekstraksi dari setiap email, seperti kata kunci, panjang email, dan keberadaan lampiran. Setelah persiapan data, algoritma klasifikasi yang akan diuji dipilih, termasuk Naive Bayes, dan K-Nearest Neighbors, dan Random Forest, Support Vector Machine.

Metode validasi silang k-fold (Anggi Priliani Yulianto & Darwis, 2021), digunakan untuk mengukur performa algoritma klasifikasi. Dalam validasi silang k-fold, dataset dibagi

menjadi k subset yang sama besar, di mana salah satunya dijadikan data uji dan yang lainnya digunakan sebagai data latih. Proses ini diulangi k kali, sehingga setiap subset digunakan sebagai data uji satu kali. Performa algoritma dievaluasi berdasarkan beberapa metrik, termasuk akurasi, presisi, recall, dan F1-score. Analisis statistik juga dilakukan untuk membandingkan hasil secara signifikan antara algoritma-algoritma yang diuji. Dengan metode ini, diharapkan dapat diperoleh pemahaman yang lebih mendalam tentang performa relatif dari berbagai algoritma klasifikasi dalam deteksi spam email.

HASIL DAN PEMBAHASAN

Peneliti terdahulu oleh dengan judul penelitian Analisis Komparatif Algoritma Klasifikasi untuk Deteksi Spam pada Email dengan Pendekatan Pengolahan Bahasa Alami" (Tinggi & Utama, 2017), Penelitian ini fokus pada analisis performa algoritma klasifikasi dalam deteksi spam pada email dengan menggunakan pendekatan pengolahan bahasa alami (NLP). Hasilnya bahwa penggunaan NLP memberikan efektivitas deteksi spam.

Penelitian yang kedua oleh (Adnan et al., 2024) dengan judul penelitain "Evaluasi Performa Algoritma Klasifikasi Menggunakan Metode Ensambel untuk Deteksi Spam pada Email" Penelitian ini mencoba untuk menguji performa beberapa metode ensambel, seperti Random Forest, Gradient Boosting, dan Adaboost, dalam deteksi spam pada email. Dengan menggunakan teknik ensambel, penelitian ini berusaha untuk meningkatkan akurasi dan stabilitas prediksi. Hasilnya memberikan pemahaman yang lebih baik tentang potensi penggunaan ensambel dalam meningkatkan kinerja sistem deteksi spam.

Penelitian yang ketiga oleh (Gangavarapu et al., 2020), dengan judul penelitian "Email Spam Detection: A Review of Recent Approaches and Future Challenges" dengan pendekatan berbasis pembelajaran mendalam, seperti penggunaan jaringan saraf berulang dan jaringan saraf konvolusional, menunjukkan potensi besar namun membutuhkan daya komputasi yang signifikan.

Dalam penelitian ini, kami melakukan analisis performa empat algoritma klasifikasi yang umum digunakan dalam deteksi spam pada email, yaitu Naive Bayes, Support Vector Machine, Random Forest, dan K-Nearest Neighbors. Kami menggunakan dataset Enron-Spam yang berisi email spam dan non-spam yang telah dikategorikan.

Hasil analisis menunjukkan bahwa dari keempat algoritma yang dievaluasi, Random Forest memiliki performa tertinggi dalam hal akurasi dan F1-score. Random Forest mencapai akurasi sebesar 97% dan F1-score sebesar 0.96. Hasil ini menunjukkan bahwa Random Forest efektif, dengan tingkat kesalahan yang relatif rendah.

Sementara itu, Naive Bayes menunjukkan performa yang baik dalam hal presisi, dengan nilai sebesar 0.98, tetapi memiliki akurasi yang sedikit lebih rendah dibandingkan dengan Random Forest, sekitar 94%. SVM juga menunjukkan hasil yang kompetitif dengan akurasi sebesar 95% dan F1-score sebesar 0.94. Namun, KNN menunjukkan performa yang lebih rendah dibandingkan dengan algoritma lainnya, dengan akurasi sekitar 90% dan F1-score sekitar 0.89.

Pembahasan lebih lanjut mengenai hasil ini menunjukkan bahwa Random Forest memiliki kemampuan yang baik dalam menangani dataset yang kompleks dan tidak linear, seperti dataset deteksi spam. Dengan kemampuan ensemble learning dan penggunaan decision trees, Random Forest mampu mengatasi overfitting dan memberikan prediksi yang stabil. Di sisi lain, Naive Bayes, meskipun sederhana, tetapi cocok untuk dataset dengan fitur yang besar dan jarang. SVM juga menunjukkan keunggulan dalam menangani dataset yang kompleks, terutama ketika ada pola yang tidak linier.

SIMPULAN

Hasil klasifikasi menunjukkan bahwa Random Forest yang paling efektif dengan akurasi tertinggi dan F1-score yang baik. Naive Bayes menunjukkan performa yang baik dalam hal presisi, sementara SVM cocok untuk dataset yang kompleks dan tidak linier. KNN, memiliki pendekatan yang sederhana, menunjukkan performa yang lebih rendah dibandingkan dengan algoritma lainnya dalam kasus deteksi spam. Implementasi praktis, pemilihan algoritma harus dipertimbangkan berdasarkan karakteristik dataset dan tujuan deteksi spam yang diinginkan. Penelitian ini memberikan wawasan yang berharga tentang kelebihan dan kelemahan masing-masing algoritma dalam konteks deteksi spam pada email, sehingga dapat menjadi pedoman bagi pengembang sistem untuk memilih pendekatan yang sesuai dengan kebutuhan.

DAFTAR PUSTAKA

Adnan, M., Imam, M. O., Javed, M. F., & Murtza, I. (2024). Improving spam email classification accuracy using ensemble techniques: a stacking approach. *International Journal of Information Security*, *23*(1), 505–517. https://doi.org/10.1007/s10207-023-00756-1

Anggi Priliani Yulianto, & Darwis, S. (2021). Penerapan Metode K-Nearest Neighbors (kNN) pada Bearing. *Jurnal Riset Statistika*, *1*(1), 10–18. https://doi.org/10.29313/jrs.v1i1.16

Cervantes, J., Garcia-Lamont, F., Rodríguez-Mazahua, L., & Lopez, A. (2020). A

comprehensive survey on support vector machine classification: Applications, challenges and trends. *Neurocomputing*, *408*, 189–215. https://doi.org/10.1016/j.neucom.2019.10.118

Frank, E., Trigg, L., Holmes, G., & Witten, I. H. (2000). Technical note: Naive Bayes for regression. *Machine Learning*, *41*(1), 5–25. https://doi.org/10.1023/A:1007670802811

Gangavarapu, T., Jaidhar, C. D., & Chanduka, B. (2020). Applicability of machine learning in spam and phishing email filtering: review and approaches. *Artificial Intelligence Review*, *53*(7), 5019–5081. https://doi.org/10.1007/s10462-020-09814-9

Harahap, A. R. S. (2023). Aplikasi scoping review "klasifikasi algoritma deteksi serangan phishing" berbasis web menggunakan metode web development life cycle. In *Repository.Uinjkt.Ac.Id*. https://repository.uinjkt.ac.id/dspace/handle/123456789/67838%0Ahttps://repository.uinjkt.ac.id/dspace/bitstream/123456789/67838/1/AHMAD RUSYDI SAID HARAHAP-FST.pdf

Islam, M. K., Amin, M. Al, Islam, M. R., Mahbub, M. N. I., Showrov, M. I. H., & Kaushal, C. (2021). Spam-Detection with Comparative Analysis and Spamming Words Extractions. *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), ICRITO 2021*. https://doi.org/10.1109/ICRITO51393.2021.9596218

Isnain, A. R., Supriyanto, J., & Kharisma, M. P. (2021). Implementation of K-Nearest Neighbor (K-NN) Algorithm For Public Sentiment Analysis of Online Learning. *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, *15*(2), 121. https://doi.org/10.22146/ijccs.65176

Mukhtar, H., Al Amien, J., & Rucyat, M. A. (2022). Filtering Spam Email menggunakan Algoritma Naïve Bayes. *Jurnal CoSciTech (Computer Science and Information Technology)*, *3*(1), 9–19. https://doi.org/10.37859/coscitech.v3i1.3652

Schonlau, M., & Zou, R. Y. (2020). The random forest algorithm for statistical learning. *Stata Journal*, *20*(1), 3–29. https://doi.org/10.1177/1536867X20909688

Tinggi, S. S., & Utama, K. W. (2017). *Penelitian Komparasi Algoritma Klasifikasi*. *1*(1), 1–12.

Utami, M., & Kom, D. S. (n.d.). *Sistem operasi*.