E-ISSN 2808-5841
P-ISSN 2808-7283

Pendeteksian Spam pada E-mail menggunakan Pendekatan *Natural Language Processing*

Ikbar Athallah Taufik[1], Dimas Dzaky Daniswara[2], Amri Muhaimin[3]
[1, 2, 3,] *Program Studi Sains Data, Fakultas Ilmu Komputer, UPN "Veteran" Jawa Timur*
[1]20083010027@student.upnjatim.ac.id[2]20083010006@student.upnjatim.ac.id[3] amri.muhaimin.stat@upnjatim.ac.id
Corresponding author email: 20083010027@student.upnjatim.ac.id

Abstract: *Natural Language Processing (NLP) is a branch of computer science that deals with the processing of human natural language by machines or computers. In this study, detection was performed on a dataset containing spam and non-spam emails. Email or electronic mail is a common communication medium used on the internet as a means for exchanging information. The NLP approach used in this study involves data preprocessing, such as removing punctuation, irrelevant common words, tokenizing, stemming, and others, as well as classification techniques such as Support Vector Classifier (SVC), Naive Bayes, etc. Among various models tested, one model showed a higher precision rate of 0.98 compared to other models. The study indicates that the NLP approach yields better performance in detecting spam compared to other methods. However, further technological advancements and the development of more complex detection methods are still required to improve the performance and accuracy of email spam detection models.*
Keywords: *NLP, Spam, Email, Machine Learning, Detection*

Abstrak: Natural Language Processing (NLP) adalah sebuah cabang ilmu komputer yang berkaitan dengan pemrosesan bahasa alami manusia oleh mesin atau komputer, pada penelitian ini telah dilakukan pendeteksian pada sebuah dataset yang berisikan spam dan bukan spam pada email. Email atau surel adalah media komunikasi yang umum digunakan dalam internet sebagai sarana seseorang untuk bertukar informasi. Metode yang digunakan dalam pendekatan NLP ini meliputi preprocessing data, seperti penghapusan tanda baca, kata-kata umum yang tidak relevan, tokenize, stemming, dan lainnya, serta teknik-teknik klasifikasi, seperti Support Vector Classifier (SVC), Naive Bayes, dll. Dari berbagai model yang telah dilakukan uji, terdapat satu model yang menunjukan angka lebih tinggi dari model lainnya dengan presisi 0,98. Penelitian menunjukkan bahwa pendekatan NLP menghasilkan kinerja yang lebih baik dalam mendeteksi spam dibandingkan dengan metode-metode lain. Namun, peningkatan teknologi dan pengembangan metode deteksi yang lebih kompleks masih diperlukan untuk meningkatkan kinerja dan akurasi dari model deteksi spam email.
Kata kunci: NLP, Spam, Email, Pembelajaran Mesin, Pendeteksian

I. PENDAHULUAN

Perkembangan teknologi saat ini terhadap surat menyurat sudah sangat berkembang, manusia sudah jarang sekali ditemukan mengirim surat melalui kantor pos atau manusia tidak lagi menggunakan surat berbentuk fisik hanya untuk berbicara dengan satu sama lainnya. Surat saat ini bukan lagi berbentuk fisik / hardfile melainkan dalam bentuk digital atau yang bisa disebut dengan E- mail. Adanya e-mail memudahkan manusia untuk mengirimkan surat atas dasar kepentingan tertentu kepada seseorang [1].

Email atau surel adalah media komunikasi yang umum digunakan dalam internet sebagai sarana seseorang untuk bertukar informasi dan kebutuhan pribadi. Kemudahan penggunaannya menjadikan email tetap populer hingga saat ini, bahkan digunakan sebagai sarana untuk memverifikasi identitas pengguna aplikasi dan dapat memastikan informasi data pengguna media sosial seperti Tiktok, Instagram, Twitter, dan Facebook benar-benar sama. Meskipun email memiliki dampak positif yang besar, penggunaannya juga bisa terkena dampak dari sisi negatif

E-ISSN 2808-5841
P-ISSN 2808-7283

email jika tidak menggunakannya dengan baik dan tepat. Banyak penyalahgunaan email yang dapat merugikan pengguna lain, seperti spam atau email sampah yang berisi iklan, scam [2].

Spam yang berarti *stupid pointless annoying messages* juga memiliki beberapa jenisnya diantaranya seperti, iklan, phising, virus malware, scam dan yang lainnya [3]. Spam juga dapat dibedakan dengan non-spam, terutama dilihat pada subjek dan body dari surat, subjek berarti judul dari isi surat biasanya pada spam judul berisikan kata-kata promosi sepert "Diskon untuk Anda", dan body berarti isi atau inti dari surat yang dikirim oleh spammer tersebut. [4],

Perkembangan e-mail juga memiliki masalahnya, dimana e-mail pada akun seseorang bisa terkena spam, hal ini mengakibatkan pengguna tidak mengetahui apakah email tersebut berbahaya atau hanya sekedar sampah. Di dalam spam pada email dapat berupa file sampah, dokumen yang tidak penting dan bahkan spam pada email bisa saja menjadi berbahaya jika di dalamnya terdapat virus atau*malware* yang dapat membahayakan pengguna [5].

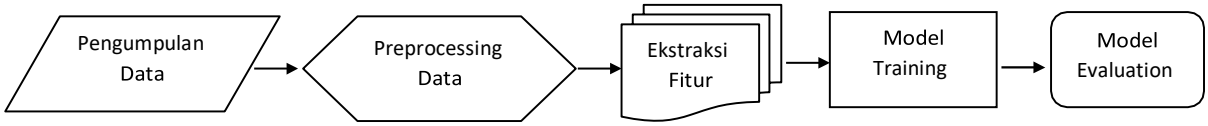
Untuk mengatasi masalah ini, metode deteksi spam email dengan menggunakan pendekatan NLP atau *Natural Language Processing* telah dikembangkan. NLP adalah satu diantara teknologi kecerdasan buatan yang memungkinkan komputer untuk memahami, menganalisis, dan memanipulasi bahasa manusia dengan cara yang mirip seperti manusia. Dalam deteksi spam email, NLP digunakan untuk memeriksa konten pesan email dan mengidentifikasi apakah email tersebut masuk dalam kategori spam atau bukan.

Penjelasan mengenai deteksi spam banyak ditemukan dari berbagai sumber lainnya, dimana mereka mencoba mendeteksi spam dengan bermacam-macam metode untuk menemukan model deteksi yang akurat atau mendapatkan model pengklasifikasian yang presisi, seperti pada [6]. dijelaskan disitu bahwa mereka menemukan tingkat keakuratan model machine learning yang gunakan.

Penelitian yang dilakukan pada artikel ini, membahas mengenai deteksi spam email dengan menggunakan NLP. Selain daripada itu, dalam artikel ini akan membahas juga tentang teknik-teknik NLP yang digunakan dalam deteksi spam email, serta keunggulan dan kelemahan dari metode ini. Penelitian ini diharapkan dapat memberikan manfaat dan kontribusi bagi pengguna email dalam mengatasi masalah spam email dan memaksimalkan produktivitas dalam penggunaan email.

II. METODE PENELITIAN

Secara umum, setiap pemrosesan pada NLP terdiri dari lima fase utama yaitu, pengumpulan data,pra-pemrosesan data, ekstraksi fitur, pelatihan model, dan evaluasi model. Gambar di bawah menunjukkan alur untuk fase-fase tersebut yang digunakan sebagai metode dalam pendeteksian spam pada e-mail. [7]



Gambar 1 Alur metode penelitian

Berikut adalah penjelasan metode penelitian yang dapat dilakukan dalam pendeteksian spam email dengan Natural Language Processing (NLP):

2.1 Pengumpulan Data

Pertama-tama, data email yang akan digunakan untuk pelatihan dan pengujian algoritma

E-ISSN 2808-5841
P-ISSN 2808-7283

deteksi spam email harus dikumpulkan. Data ini harus mencakup berbagai jenis email, termasuk email spam dan non-spam. Pengumpulan data dapat dilakukan dengan melakukan crawling pada berbagai sumber atau menggunakan dataset yang tersedia secara publik. Pada Artikel ini data diperoleh dari situs publik yang memberikan akses untuk mengambil dataset [8], Dari dataset terhitung keseluruhan data memiliki 6046, dengan total spam sebanyak 1896, dan ham sebanyak 4150, data yang terhitung dimuali dari 0 sampai 6046 [9].

2.2 Data Preprocessing

Setelah data email dikumpulkan, langkah selanjutnya adalah melakukan preprocessing data. Hal ini meliputi cleaning, penghapusan karakter-karakter khusus, konversi semua huruf kecil, penghapusan kata-kata umum, dan lain sebagainya. Data email yang sudah dipreprocessing ini akan membantu dalam membangun model deteksi spam email yang akurat [10].

2.2.1 Cleaning data:

Pembersihan pada data diperlukan karena data yang tidak bearturan atau tidak terstuktur dapat mempengaruhi hasil akurasi maka, dilakukanlah pembersihan pada data dari simbol, tanda baca, hashtag, karakter khusus, dan karakter lainnya yang menggangu struktur kata pada data, juga melakukan konversi teks ke huruf kecil [4]. Kata-kata semisal"Buku" dan "buku" mempunyai makna yang sama, namun apabila tidak dikonversi menjadi huruf kecil, kedua kata tersebut direpresentasikan sebagai dua kata yang berbeda dalam model ruang vektor (yang menghasilkan lebih banyak dimensi) [11].

2.2.2 Tokenize:

Tokenize memecah kalimat menjadi kata-kata sehingga membuat dokumen terpecah menjadikannya bagian-bagian yang lebih kecil sehingga pada saat proses analisa nantinya akan lebih mudah [3].

2.2.3 Menghilangkan stopwords:

Menghapus kata-kata yang tidak memiliki pengertian jika tidak ada kata lain seperti: dan, saya, atau. [4]

2.2.4 Stemming data:

Mengubah kata-kata yang memiliki imbuhan menjadi tidak ada imbuhannya atau kembali menjadi kata dasar aslinya.[4]

2.3 Feature Extraction

Setelah data email dipreprocessing, langkah selanjutnya adalah melakukan ekstraksi fitur. Fitur- fitur yang dapat digunakan dalam deteksi spam email meliputi kata kunci tertentu, frekuensi kemunculan kata, dan panjang email. Fitur-fitur ini akan menjadi input dalam model deteksi spam email. [4]

2.4 Pembuatan Model

Setelah fitur-fitur diekstraksi, selanjutnya adalah membangun model deteksi spam email. Model dapat dibuat dengan menggunakan algoritma Machine Learning seperti Gaussian NB (NaïveBayes), Multinominal NB, Bernouliie NB, Decision Tree, KNeighbors, Support Vector Classifier (SVC), Logistic Regression, dan (SGDC) Stochastic Gradient Descent Classifier. Model ini akan dilatih menggunakan data email yang sudah dipreprocessing dan diekstraksi

E-ISSN 2808-5841
P-ISSN 2808-7283

fiturnya.

2.5 Evaluasi Model

Setelah model selesai dibuat, langkah selanjutnya adalah melakukan evaluasi model. Evaluasi ini bertujuan untuk mengukur kinerja model dalam mendeteksi email spam dan non-spam. Metrik yang dapat digunakan untuk evaluasi model meliputi akurasi, dan presisi [6].

2.6 Uji Coba

Setelah model berhasil diuji dan terbukti akurat dalam mendeteksi spam email, langkah selanjutnya adalah mengujinya pada dataset email yang belum pernah dilihat sebelumnya. Uji coba ini akan membantu untuk mengevaluasi kemampuan model dalam mendeteksi spam email secara umum.

Dengan menggunakan metode penelitian di atas, diharapkan dapat menghasilkan model deteksi spam email yang akurat dan dapat membantu pengguna email dalam mengatasi masalah spam email.

III. HASIL DAN PEMBAHASAN

Deteksi spam email menggunakan Natural Language Processing (NLP) merupakan salah satu metode yang dapat digunakan untuk memfilter email yang masuk ke dalam kotak masuk pengguna. Dalam penelitian ini, dilakukan pengimplementasian beberapa teknik NLP seperti klasifikasi teks dan pemrosesan bahasa alami untuk melakukan deteksi spam email.

Pada tahap awal, dilakukan pengumpulan data email yang bersumber dari web dimana data sudah dalam bentuk dataset, dari dataset tersebut dilakukan import ke dalam bahasa pemrograman yang dilanjut dengan mengimport beberapa library yang dibutuhkan untuk melakukan pengerjaan NLP. Data yang sudah masuk dapat dilakukan analisis sederhana dengan melihat varibel, besarnya data, dan tipe dari data. Data kemudian dilakukan pembersihan untuk menghindari kesalahan dalam melakukan proses NLP, dilakukan juga exploratory data analysis untuk mengetahui diagram dan heat map pada data.

Pemrosesan berikutnya yaitu dengan melakukan preprocessing pada data tersebut seperti konversi ke lowercase, tokenize, menghapus karakter khusus, stopword removal, dan stemming untuk memperoleh data yang lebih bersih dan terstruktur. Selanjutnya, dilakukan proses ekstraksi fitur menggunakan metode TF-IDF untuk mengonversi setiap email menjadi vektor fitur yang dapat digunakan oleh model [3]. Proses ekstrasi yang telah selesai dilanjutkan dengan membagi data menjadi data untuk dilatih dan data untuk percobaan.

Pengerjaan dari tahap-tahap sebelumnya yang telah berhasil dilakukan, membawa pada tahap selanjutnya dimana, setelah data melewati beberapa metode sehingga, didapat data train dan data test maka, dilakukan implementasi model yang mana, mengimplementasikan beberapa algoritma klasifikasi seperti Gaussian NB, Multinominal NB, Bernouliie NB, Decision Tree, KNeighbors, Support Vector Classifier (SVC), Logistic Regression, dan SGDClassifier untuk melakukan pengklasifikasian spam dan bukan spam pada email dari dataset sehingga, dapat dilihat hasil akurasi dan presisi dari masing-masing model.

Tabel 1. Tabel Hasil Modeling

Model	Accuracy	Precision
GaussianNB	0,90	0,83

MultinomialNB	0,93	0,89
BernoulliNB	0,94	0,98
SVC	0,95	0,90
KNeighbors	0,39	0,33
Decision Tree	0,88	0,79
Logistic Regression	0,93	0,88
SGDClassifier	0,96	0,90

Evaluasi kinerja model dilakukan dengan menggunakan metrik akurasi, dan presisi. Hasil evaluasi menunjukkan bahwa algoritma Bernouliie Naive Bayes dengan akurasi 0,94 dan presisi sebesar 0,98 memberikan kinerja yang lebih baik dibandingkan dengan algoritma lainnya. Akurasi dan presisi terkecil ada pada model KNeighbors dengan akurasi 0,39 dan presisi sebesar 0,33 sehingga, model ini kurang baik untuk dapat dijadikan model pendeteksian spam pada e-mail.

Dalam penelitian ini, dipertimbangkan juga kelemahan dari teknik deteksi spam email dengan NLP. Salah satu kelemahan utama adalah kurangnya kemampuan untuk memahami konteks email dankonten yang dinamis. Hal ini dapat mengakibatkan kesalahan klasifikasi email yang seharusnyadianggap sebagai spam namun terdeteksi sebagai email biasa dan sebaliknya.

IV. KESIMPULAN

Dalam kesimpulannya, pendekatan NLP menjadi salah satu metode yang efektif dalam mendeteksi spam pada email. Dalam pengembangan teknologi di masa depan, pendekatan NLP ini dapat dikembangkan lebih lanjut untuk mengatasi masalah-masalah baru dan meningkatkan keamananinformasi pada email.

Pendekatan NLP dapat memberikan hasil yang lebih akurat dalam pendeteksian spam pada email dibandingkan dengan pendekatan konvensional. Namun, peningkatan teknologi dan pengembangan metode deteksi yang lebih kompleks masih diperlukan untuk meningkatkan kinerja dan akurasi dari model deteksi spam email.

Secara keseluruhan, teknik deteksi spam email dengan NLP dapat memberikan solusi yang efektif untuk mengatasi masalah spam email. Dalam pengembangan teknologi di masa depan, pendekatan NLP ini dapat dikembangkan lebih lanjut untuk mengatasi masalah-masalah baru dan meningkatkan keamanan informasi pada email

Selain itu, dalam perkembangannya teknik NLP dapat dikembangkan lebih lanjut dengan menggunakan metode deep learning seperti convolutional neural network (CNN) dan recurrent neural network (RNN) untuk meningkatkan akurasi dan efektivitas pendeteksian spam pada email.

UCAPAN TERIMA KASIH

Ucapan terima kasih disampaikan kepada semua yang telah membantu dalam menyelesaikan artikel ini. Terima kasih kepada orang tua yang memberikan dukungan doa dan memfasilitasi untuk bisa menyelesaikan penulisan ini. Ucapan terimakasih kepada dosen-dosen yang memberikan masukan dan ilmu yang berharga. Terima kasih kepada tim yang selalu mendukung dalam menyelesaikan penulisan ini.

Ucapan terima kasih juga kepada pembaca artikel ini yang telah meluangkan waktunya untuk membaca tulisan ini. Semoga artikel ini dapat memberikan manfaat dan kontribusi bagi pengembangan ilmu pengetahuan di bidang Sains Data atau bidang yang berkaitan dengan pembahasan tulisan ini

E-ISSN 2808-5841
P-ISSN 2808-7283

REFERENSI

[1] E. G. Dada, J. S. Bassi, H. Chiroma, S. M. Abdulhamid, A. O. Adetunmbi, and O. E. Ajibuwa, "Machine learning for email spam filtering: review, approaches and open research problems," *Heliyon*, vol. 5, no. 6, 2019, doi: 10.1016/j.heliyon.2019.e01802.

[2] F. Z. Ruskanda, "Study on the Effect of Preprocessing Methods for Spam Email Detection," *Indones. J. Comput.*, vol. 4, no. 1, p. 109, 2019, doi: 10.21108/indojc.2019.4.1.284.

[3] E. P. Laksono and A. Wicaksono, "Penyaringan Spam email menggunakan," vol. 5, no. 2, pp. 26–32.

[4] F. Rahma, A. Z. Farmadiansyah, and A. F. Hidayatullah, "Deteksi Surel Spam dan Non Spam Bahasa Indonesia Menggunakan Metode Naïve Bayes," *Automata*, vol. 2, no. 2, 2021.

[5] R. S. Lutfiyani and N. Retnowati, "Implementasi Pendeteksian Spam Email Menggunakan Metode TextMining Dengan Algoritma Naïve Bayes Dan Decision Tree J48," *J. Komput. dan Inform.*, vol. 9, no. 2, pp. 244–252, 2021, doi: 10.35508/jicon.v9i2.5304.

[6] S. K. Arts and S. K. Arts, "Performance Evaluation of Machine Learning Algorithms for Email SpamDetection," pp. 1–4, 2020.

[7] I. AbdulNabi and Q. Yaseen, "Spam email detection using deep learning techniques," *Procedia Comput. Sci.*, vol. 184, no. 2019, pp. 853–858, 2021, doi: 10.1016/j.procs.2021.03.107.

[8] nitisha bharathi, "Email Spam Dataset," *kaggle*, 2020.https://www.kaggle.com/datasets/nitishabharathi/email-spam-dataset.

[9] N. Q. Fitriyah, H. Oktavianto, and H. Hasbullah, "Deteksi Spam Pada Email Berbasis Fitur Konten Menggunakan Naïve Bayes," *JUSTINDO (Jurnal Sist. dan Teknol. Inf. Indones.*, vol. 5, no. 1, pp. 1–7, 2020, doi: 10.32528/justindo.v5i1.3414.

[10] S. Khairunnisa, A. Adiwijaya, and S. Al Faraby, "Pengaruh Text Preprocessing terhadap Analisis Sentimen Komentar Masyarakat pada Media Sosial Twitter (Studi Kasus Pandemi COVID-19)," *J. Media Inform. Budidarma*, vol. 5, no. 2, p. 406, 2021, doi: 10.30865/mib.v5i2.2835.

[11] M. A. Ghani and H. Sulaiman, "Deteksi Spam Email dengan Metode Naive Bayes dan Particle Swarm Optimization (PSO)," *Infotek J. Inform. dan Teknol.*, vol. 6, no. 1, pp. 11–20, 2023, doi: 10.29408/jit.v6i1.7049.