ESCAF 4th 2025
p-ISSN : 2962-7710
e-ISSN : 3021-8594

Penerapan Random Forest Dan Naive Bayes Untuk Deteksi Phishing Dan Serangan Social Engineering Pada Email

Ulya Kurniati[1*], M.Agus Syamsul Arifin[2], Nelly Khairani Daulay[3]
[1]Program Studi Informatika, Universitas Bina Insan, Lubuklinggau

e-mail: *[1]2102020022@mhs.univbinainsan.ac.id, [2]mas.arifin@univbinainsan.ac.id, [3]nellykhairanilestari@gmail.com
*Corresponding Author

Abstrak

Phishing dan serangan social engineering merupakan ancaman signifikan dalam komunikasi digital berbasis email.Proses penelitian dimulai dengan tahap preprocessing data yang meliputi data cleaning, case folding, stopwords removal, dan tokenizing. Fitur teks diekstraksi menggunakan metode TF-IDF untuk menghasilkan representasi numerik. Dataset yang digunakan dibagi menjadi data latih (80%) dan data uji (20%) untuk memastikan evaluasi yang adil.Model dikembangkan menggunakan algoritma Random Forest dan Naive Bayes. Evaluasi dilakukan dengan metrik seperti accuracy, precision, recall, dan F1-score. Hasil penelitian menunjukkan bahwa algoritma Random Forest memberikan performa terbaik dengan akurasi 0,8996, precision 0,90, recall 0,90, dan F1-score 0,90. Sementara itu, algoritma Naive Bayes menghasilkan akurasi 0,6048, precision 0,65, recall 0,60, dan F1-score 0,59.Penelitian ini membuktikan bahwa Random Forest lebih unggul dalam mendeteksi phishing dan serangan social engineering dibandingkan Naive Bayes. Sistem yang dikembangkan dapat menjadi solusi efektif untuk meningkatkan keamanan komunikasi berbasis email. Hasil penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan teknologi deteksi ancaman siber di masa depan.

Kata kunci: Phishing; Social Engineering; Random Forest;Naive Bayes;Deteksi Email

Abstract

Phishing and social engineering attacks are significant threats in email-based digital communications. The research process begins with the data preprocessing stage which includes data cleaning, case folding, stopwords removal, and tokenizing. Text features are extracted using the TF-IDF method to produce a numerical representation. The dataset used is divided into training data (80%) and test data (20%) to ensure fair evaluation. The model was developed using Random Forest and Naive Bayes algorithms. Evaluation is carried out with metrics such as accuracy, precision, recall, and F1-score. The research results show that the Random Forest algorithm provides the best performance with an accuracy of 0.8996, precision 0.90, recall 0.90, and F1-score 0.90. Meanwhile, the Naive Bayes algorithm produces an accuracy of 0.6048, precision 0.65, recall 0.60, and F1-score 0.59. This research proves that Random Forest is superior in detecting phishing and social engineering attacks compared to Naive Bayes. The system developed can be an effective solution for increasing the security of email-based communications. It is hoped that the results of this research can contribute to the development of cyber threat detection technology in the future.

Keywords: *Phishing;Social Engineering; Random Forest; Naive Bayes; Email Detection.*

ESCAF 4th 2025
p-ISSN : 2962-7710
e-ISSN : 3021-8594

I. PENDAHULUAN

Dalam era digital yang semakin berkembang pesat dan cepat, email telah menjadi salah satu sarana komunikasi yang paling banyak di gunakan di seluruh dunia baik untuk keperluan pribadi ataupun bisnis.Dalam berapa tahun terakhir email telah berkembang dari alat sederhana menjadi platform kompleks yang mendukung berbagai fungsi,seperti pengiriman dokumen,kolaborasi proyek,dan pemasaran digital. Namun di balik kemudahan yang di tawarkan,email juga menjadi target utama bagi penyerang siber yang berupaya mengeksploitasi keretanan dalam sistem dan perilaku manusia,menjadikan nya salah satu vektor serangan yang paling umum dan berbahaya[1].

Salah satu ancaman utama yang sering terjadi dalam dunia komunikasi berbasis email adalah serangan phishing dan social engineering. Phishing dan social engineering merupakan metode serangan siber yang sering digunakan untuk mencuri data pribadi melalui email. Serangan ini di lakukan dengan cara mengelabui korban melalui pesan yang tampak meyakinkan untuk mengklik tautan berbahaya atau membocorkan informasi sensitif. Seiring meningkatnya jumlah serangan phishing, sistem deteksi yang lebih efektif sangat diperlukan[2].

Dalam konteks ini,penelitian kami berfokus pada deteksi phishing dan serangan social engineering pada email menggunakan algoritma machine learning Random Forest dan naive bayes.Dua algoritma ini di pilih karna metode yang terkenal dan terbukti kuat dalam menganalisis data dan melakukan klasifikasi.Random forest merupakan algoritma ensembel berbasis pohon keputusan,menawarkan keunggulan dalam memproses data dengan akurasi tinggi. Pendekatan ini dapat memberikan prediksi yang lebih stabil dan tahan terhadap overfitting, sedangkan Naive Bayes yang di dasarkan pada probabilistik sederhana,sangat cepat dan efisien dalam menangani data dalam jumlah besar, membuatnya cocok dalam analisis real time[3].

Penelitian yang di lakukan oleh Januar al-amien,dkk (2022) menyimpulkan bahwa permasalahan dalam penelitian nya ialah bagaimana menyaring email spam yang masuk dan penelitian ini bertujuan untuk memfilter spam email secara otomatis menggunakan algoritma naive bayes yang terhubug dengan mail server,metode penelitian ini menggunakan algoritma naive bayes.hasil dari penelitian ini adalah pengujian dataset dengan pemodelan mendapatkan akurasi sebesar 98.00%[4].Kemudian penelitian yang di lakukan oleh Gishma paulson (2023) menyimpulkan bahwa pokok permasalahan penelitian ini mengeksplorasi alasan peningkatan kasus phishing data di kuwait sejak tahun 2020 dan temuan nya di dukung oleh statistik menggunkan pembelajaran mesin dan bahasa phyton,bahasa mesin yang di gunakan pada peneltian ini yaitu menggunkan metode algoritma Random Forest.Dan adapun hasil dari penelitian ini yaitu menunjukkan bahwa hipotesis nol itu benar dan ada sekitar 82% kemungkinan jika pengguna telepon pintar menginstal aplikasi yang tidak terenskripsi data nya di perangkat[5].Lalu penelitian yang di lakukan oleh Ratnam dodda,dkk(2023) menyimpulkan pada penelitian ini memiliki pokok permasalah menyelidiki dan menganalisis metrik presisi,dengan mempertimbangkan pertukaran antara hasil positif yang benar dan hasil positif yang salah.Studi komparatif ini memberikan wawasan tentang kekuatan dan keterbatasan masing-masing algoritma dalam mengidentifikasi email spam secara efektif.Pada penelitian ini peneliti menggunkan metode penelitian CNN,Regresi logistik,LSTM,Naive Bayes,dan machine learning.Hasil dari penelitian ini merupakan CNN yang di rancang untuk hirarki spesial pada data seperti gambar,mengungguli model lain dengan tingkat akurasi 99,82% pada data pelatihan dan 98,65% yang luar biasa pada data pengujian[1].

Penelitian ini bertujuan untuk mengembangkan model yang dapat mendeteksi dan mengklasifikasikan phishing dan serangan social engineering dengan akurasi tinggi.Penelitian ini juga

ESCAF 4th 2025
p-ISSN : 2962-7710
e-ISSN : 3021-8594

membandingkan performa algoritma Random Forest dan naive bayes dalam mendeteksi phisihing dan serangan social engineering pada email.Performa model akan diukur menggunakan beberapa metrik evaluasi yang umum di gunakan dalam machinelearning,yaitu.Akurasi,precision,re call,dan f-1 score.Untuk memastikan keandalan dan generasasi model,validasi di lakukan menggunakan teknik cross-validation 10-fold.Dalam teknik ini,Dataset dibagi menjadi 10 subnet (fold),dan model di latih sebnyak 10 kali setiap kali menggunkan 9 subnet sebagai data latih dan 1 subnet sebagai data uji.Proses ini berulang sebanyak 10 kali dengan setiap subnet berperan sekali sebagai data uji.Teknik ini membantu dalam mengurangi bias yang mungkin muncul dari pembagian data secara acak dan memberikan gambaran yang lebih akurat tentang performa model pada data yang tidak terlihat seblumnya[6].

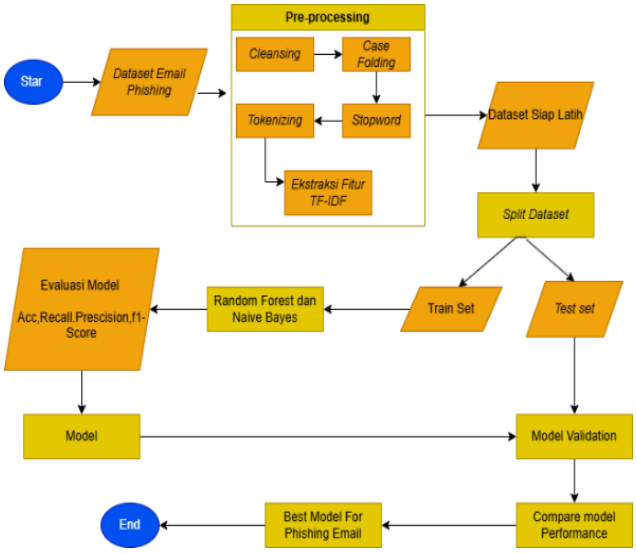
Hasil dari penelitian ini di harapkan dapat memberikan wawasan yang yang mendalam mengenai efektifitas pengunaan algoritma random forest dan naive bayes dalam mendeteksi email phishing dan serangan social engineering dengan membandingkan performa kedua algoritma ini,penelitian ini dapat membantu dalam pengembangan sistem deteksi email phishing dan serangan social engineering yang lebih efektif dan efisien.

II. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Gambar 1 berikut menunjukkan alur yang digunakan dalam penelitian ini untuk menentukan model terbaik dalam mendeteksi serangan phishing dan serangan social engineering pada email.Dataset email phishing merupakan dataset mentah dengan format CSV dan memiliki 7 dataset csv,kemudian di lakukan tahap preprocessing,tahap preprosessing di perlukan untuk memproses datayang dibutuhkan serta membersihkan data dari elemen yang tidak di perlukan dengan tujuan ketika masuk pada tahap klasifikasi dengan suatu algoritma yang lebih optimal dalam perhitungan nya.Adapun tahapan preprocesing terdiri dari beberapa langka seperticleaansing,casefolding,stopword,toke nezing dan selanjut nya yaitu ekstraksi fitur nlp dengan fitur TF-IDF[7].Selanjutnya Setelah melakukan preprocessing dan ekstraksi fitur menggunakan tf-idf dataset siap digunakan untuk melatih model machine learning,karna dataset sudah sesuai dengan persyatan input model seperti format,struktur,dan tipe data.selanjutnya data set di bagi dua menjadi data test dan data train,kemuidan di lakukan memilih model klasifikasi yang di gunakan antara algoritma random forest dan naive bayes agar nanti mendapatkan algoritma mana yang lebih efisien.Lalu Selanjutnya evalusi model menggunkan test set dan metrik sepertiakurasi,precision,f1score,recall.Selan jutnya model diuji dengan K-Fold Cross Validation untuk menentukan hasil yang konsisten,dan juga menggunkan confusion matrix untuk melihat kesalahan klasifikasi[8]. Selanjutnya proses validasi di lakukan untuk memastikan bahwa model bekerja dengan baik pada data yang belum pernah di lihat sebelumnya. Lalu bandingkan hasil evaluasi antara Random forest dan Naive bayes untuk menentukan mana yang memiliki performa terbaik. Setelah kita melakukan tahapan-tahapan diatas, kita akan mendapatkan model terbaik untuk deteksi phishing pada email.

ESCAF 4th 2025
p-ISSN : 2962-7710
e-ISSN : 3021-8594



Gambar1. Flowchat pembuatan model deteksi email phishing

Penelitian ini menggunakan dataset dari sumber terbuka yang telah di akui secara luas,yaitu di peroleh langsung dari kaggle yang terdiri dari 7 dataset scv dengan total keseluruhan 165.283.

2.2 Random Forest

Random forest merupakan suatu algoritma yang menggunakan pendekatan pemisahan rekursif biner untuk mencapai simpul akhir dalam struktur pohon,berdasarkan konsep pohon klasifikasi dan regresi. Random forest adalah algoritma supervised learning yang di keluarkan Random Forest biasa di gunakan untuk menyelesaikan masalah yang berhubungan dengan klasifikasi,regresi dan sebagainya[3].Setiap pohon tumbuh pada sample bootstrap yang berbeda di ambil dari data lain secara acak.Dalam setiap node split selama pembentukan decision tree,sebagai sample dari m variabel di pilih dari kumpulan data asli dan kemudian yang terbaik akan di gunakan dalam node tersebut.Atau bisa di sebut *desicion tree* di mana setiap *tree* bergantung pada nilai random vector yang di jadikan sample secara bebas dan merata pada semua tree dalam forest tersebut. Hasil prediksi Random Forest di dapatkan melalui hasil terbanyak dari setiap individual decision tree(voting untuk klasifikasi dan rata-rata untuk regresi)[9].

2.3 Naive Bayes

Pengklasifikasi bayes merupakan salah satu pengklasifikasi statistik,di mana penglasifikasi ini dapat memprediksi probabilitas kelas satu data tuple yang akan masuk kedalam kelas tertentu, sesuai dengan perhitunganprobabilitas[10]. Pengklasifikasi bayes di dasari oleh teorema bayes yang di temukan oleh Thomas Bayes pada abad ke-18. Dalam studi perbandingan algoritma telah di temukan simple bayesian atau yang biasa di kenal dengan *Naive Bayes classifier*.*Naive Bayes classifier* menunjukkan akurasi dan kecepatan yang tinggi bila di terapkan pada database yang besar[11]. Metode ini sering di gunakan dalam menyelesaikan masalah dalam bidang mesin pembelajaran karena metode ini di kenal memiliki tingkat akurasi yang tinggi dengan perhitungan sederhana[12].

III. HASIL DAN PEMBAHASAN

Jumlah data pada dataset setelah proses normalisasi adalah 165.283 dengan data phishing berjumlah 82.450 data, non-phishing 79.190 data, dan social_engineering 3.332 data. Sub bab 3.1 akan menjabarkan hasil dari performa ektraksi fitur nlp dengan fitur TF-IDF menggunakan machine learning dengan Random Forest dan naïve bayes yang menggunakan dataset email phishing publik sekaligus hasil validasi dari model machine learning yang dibuat dan sub bab 3.2 akan menjabarkan pembahasan hasil dari performa ektraksi fitur nlp dengan fitur naïve bayes pada dataset email phishing publik.

ESCAF 4th 2025
p-ISSN : 2962-7710
e-ISSN : 3021-8594

3.1 Hasil

Dari pengujian yang dilakukan performa ektraksi nlp dengan fitur TF-IDF yang dibangun menggunakan algoritma random forest dan naïve bayes mendapatkan perbandingan hasil yang mana lebih baik pada data uji, namun pada data latih performa kedua model machine learning yang digunakan mendapatkan hasil yang berbeda. gambar 1 berikut menunjukkan perbandingan performa ektraksi nlp dengan TF-IDF yang menggunakan algoritma random forest dan naïve bayes pada data latih dan gambar 2 menggunakan data uji.

Gambar 1. Perbandingan performa ektrasi fitur nlp dengan fitur TF-IDf yang menggunakan algoritma random forest dan naïve bayes pada data latih

```
=== Data Latih (Training Data) ===
       subject   body  cleaned_subject  emails_from_subject  \
53608    37833  67240            26896                   46
34423    38903  72704            29152                   46
50425    41101  18847            20082                   46
81427     2983  24198             6758                   46
54709    42210  62074            37315                   46

       urls_from_subject  cleaned_body  emails_from_body  urls_from_body
53608                 21         44937              7406           15095
34423                 21         61694              7406           15095
50425                 21         28602              7406           15095
81427                 21         16682              2459           10185
54709                 21         36138              7406           15095
53608    non-phishing
34423    non-phishing
50425    non-phishing
81427        phishing
54709    non-phishing
Name: label, dtype: object
```

Gambar 2. Perbandingan performa ektrasi fitur nlp dengan fitur TF-IDf yang menggunakan algoritma random forest dan naïve bayes pada data uji

```
=== Data Uji (Test Data) ===
       subject   body  cleaned_subject  emails_from_subject  \
3031     25506  67874             6631                   46
79376    40109  61739             6796                   46
47593    36866  55553            24938                   46
63061     4356  12157            11725                   46
29582     2983  23265             6758                   46

       urls_from_subject  cleaned_body  emails_from_body  urls_from_body
3031                  21         45597              7406           15095
79376                 21         37456              7406           15095
47593                 21         22218              7406           15095
63061                 21         57263              7406            6888
29582                 21         15750              2500            8268
3031         phishing
79376        phishing
47593    non-phishing
63061        phishing
29582        phishing
Name: label, dtype: object
```

Gambar 3. Word cloud. Data yang sudah di cleaned tersebut

Adapun juga hasil dari setiap accuracy, precision, recall, f1-score untuk algoritma naïve bayes dan random forest. Gambar 4 berikut akan menunjukkan hasil dari naïve bayes yaitu accuracy,precision,recall,f1-score sedangkan untuk gambar 5 menampilkan dari algoritma random forest.

Gambar 4. Classification Naïve Bayes

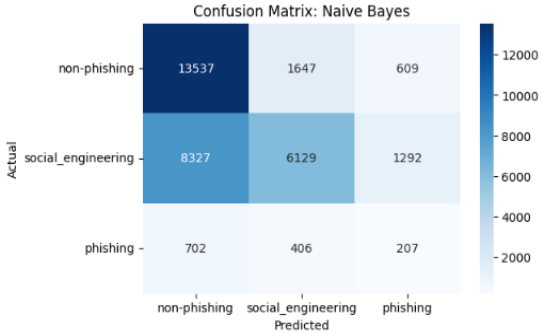
```
=== Random Forest Model ===
Accuracy Random Forest: 0.8996225955685415
                    precision    recall  f1-score   support

        non-phishing       0.90      0.91      0.91     15793
            phishing       0.90      0.91      0.90     15748
social_engineering       0.87      0.70      0.77      1315

            accuracy                           0.90     32856
           macro avg       0.89      0.84      0.86     32856
        weighted avg       0.90      0.90      0.90     32856
```

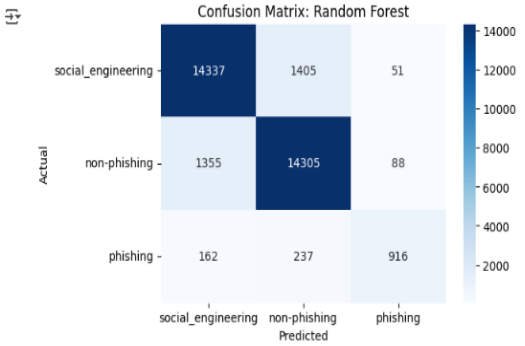
Gambar 5. Classification Random Forest

Kami menggunakan grafik confusion matrix untuk melihat hasil dari phishing, non-phishing dan social_engineering. Gambar 6 berikut menunjukkan confusion matrix Naïve Bayes hasil dari Classification phishing,non-phishing dan social_engineering sedangkan Gambar 7 menunjukkan confusion matrix Random Forest hasil dari Classification phishing,non-phishing dan social_engineering.



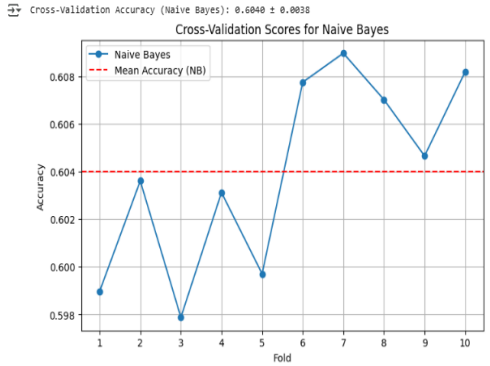
Gambar 6. Confusion Matrix: Naïve Bayes

ESCAF 4th 2025
p-ISSN : 2962-7710
e-ISSN : 3021-8594

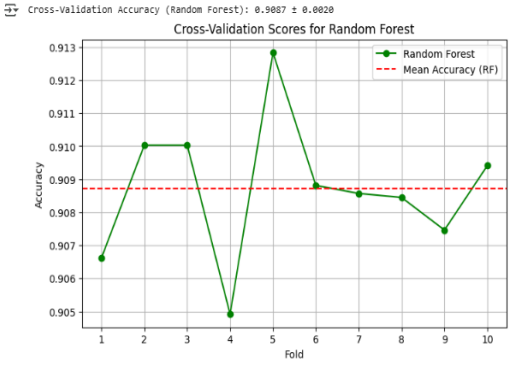


Gambar 7. Confusion Matrix: Random Forest

Gambar 8 berikut menunjukkan kurva ROC untuk mengukur kemampuan algoritma naïve bayes dan random forest yang dibuat dalam melakukan klasifikasi phishing, non-phishing, social_engineering, yang sama juga Gambar 9 menunjukkan hasil cross-validation dari algoritma naïve bayes dan random forest untuk melihat model yang dibuat tersebut.



Gambar 8. Cross-Validation scores for naïve bayes



Gambar 9. Cross-Validation for Random Forest

3.2 Pembahasan

Algoritma random forest ini memberikan hasil yang sangat baik dengan akurasi tertinggi (0,8996),Precision dan recall yang tinggi menunjukkan kemampuan model dalam mendeteksi phishing dan email normal tanpa banyak kesalahan.Dan sangat cocok untuk dataset dengan jumlah data yang besar dan kompleks,dapat di lihat pada visualisasi hasil confusion matrix dan ROC,pada confusion matrix menunjukkan kesalahan klasifikasi yang minimal, dengan prediksi yang akurat pada kelas phishing dan normal,sedangkan pada roc menunjukan hasil yang hampir sempurna, sedangkan Algoritma naive bayes ini memberikan hasil yang baik dengan akurasi 0,6048 yang sedikit lebih rendah dari Random Forest.Meskipun lebih cepat dalam melakukan prediksi, performanya dipengaruhi oleh distribusi data yang tidak seimbang.dapat di lihat pada visualisasi hasil confusion matrix dan ROC,pada confusion matrix Kesalahan klasifikasi sedikit lebih tinggi dibandingkan Random Forest.

Berdasarkan hasil pengujian, algoritma Random Forest lebih unggul dalam mendeteksi phishing dan serangan social engineering dibandingkan Naive Bayes, baik dari segi akurasi maupun stabilitas prediksi. Namun, Naive Bayes tetap menjadi pilihan yang cepat dan efisien untuk implementasi pada dataset yang lebih kecil atau membutuhkan respons waktu nyata

IV. KESIMPULAN

Berdasarkan penelitian yang dilakukan dengan menggunakan metode Random Forest dan Naive Bayes untuk deteksi phishing dan serangan social engineering pada email, dapat

ESCAF 4th 2025
p-ISSN : 2962-7710
e-ISSN : 3021-8594

disimpulkan dalam beberapa hal.Algoritma Random Forest menunjukkan performa yang unggul dalam mendeteksi phishing dan serangan social engineering, dengan akurasi mencapai 0,8996. Algoritma ini mampu memberikan prediksi yang stabil dan andal dengan precision dan recall yang tinggi.Sedangkan algoritma Naive Bayes, meskipun memiliki akurasi yang sedikit lebih rendah 0,6048, tetap menunjukkan hasil yang baik dan efisien. Algoritma ini lebih cepat dalam pemrosesan data namun lebih sensitif terhadap data yang tidak seimbang.Evaluasi menggunakan metrik seperti accuracy, precision, recall, dan F1-score menunjukkan bahwa kedua algoritma memiliki kemampuan deteksi yang baik.Random Forest memiliki keunggulan lebih tinggi dalam hal akurasi dan kestabilan dibandingkan Naive Bayes.

Dengan hasil evaluasi yang positif, sistem yang dikembangkan menggunakan algoritma Random Forest dan Naive Bayes dapat diimplementasikan sebagai solusi deteksi phishing dan serangan social engineering pada email. Pendekatan ini memberikan alternatif yang akurat dan efisien untuk meningkatkan keamanan komunikasi berbasis email.Penelitian ini menunjukkan bahwa kombinasi teknik preprocessing teks, pemilihan fitur yang relevan (TF-IDF), serta penggunaan algoritma pembelajaran mesin dapat menghasilkan model deteksi yang andal.Penelitian ini diharapkan menjadi referensi bagi pengembangan sistem deteksi ancaman siber di masa mendatang.

V. SARAN

Penelitian selanjutnya dapat menggunakan dataset yang lebih besar dan lebih beragam untuk meningkatkan generalisasi model. Pengumpulan dataset real-time dari berbagai sumber dapat membantu meningkatkan kemampuan model dalam mendeteksi ancaman baru.Penelitian dapat diperluas dengan membandingkan algoritma lain seperti Support Vector Machine (SVM) atau Deep Learning untuk meningkatkan akurasi deteksi.

Parameter tuning lebih lanjut pada algoritma Random Forest dan Naive Bayes dapat dilakukan untuk mendapatkan performa yang lebih optimal.

Diharapkan hasil penelitian ini dapat menjadi dasar pengembangan lebih lanjut dalam upaya meningkatkan keamanan komunikasi digital.

VI. DAFTAR PUSTAKA

[1] G. Mujtaba, L. Shuib, R. G. Raj, N. Majeed, and M. A. Al-Garadi, “Email Classification Research Trends: Review and Open Issues,” *IEEE Access*, vol. 5, pp. 9044–9064, 2017, doi: 10.1109/ACCESS.2017.2702187.

[2] H. Gurung, R. Nepal, and S. Nepal, “Phishing URL Detection Using CNN-LSTM and Random Forest Classifier,” *Int J Med Net*, vol. 2, no. 5, pp. 1–15, 2023, [Online]. Available: https://www.

[3] R. Ageng, R. Faisal, and S. Ihsan, “Random Forest Machine Learning for Spam Email Classification,” *J. Dinda Data Sci. Inf. Technol. Data Anal.*, vol. 4, no. 1, pp. 8–13, 2024, doi: 10.20895/dinda.v4i1.1363.

[4] H. Mukhtar, J. Al Amien, and M. A. Rucyat, “Filtering Spam Email menggunakan Algoritma Naïve Bayes,” *J. CoSciTech (Computer Sci. Inf. Technol.*, vol. 3, no. 1, pp. 9–19, 2022, doi: 10.37859/coscitech.v3i1.3652.

[5] G. Paulson, “Assessing data phishing risks associated with unencrypted apps on smartphones with non-parametric test and random forest model: Insights from Kuwait phishing scam calls,” *J. Eng. Res.*,

ESCAF 4th 2025
p-ISSN : 2962-7710
e-ISSN : 3021-8594

no. May, Sep. 2023, doi: 10.1016/j.jer.2023.09.017.

[6] N. Bybin, P. Gopan, R. K, R. S. Jimmy, A. Eldho, and R. R. Meckmalil, "Naive Bayes - Random Forest Ensemble Model Analysis and Heart Disease Prediction," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 12, no. 5, pp. 2853–2859, 2024, doi: 10.22214/ijraset.2024.62177.

[7] J. McAlaney and P. J. Hills, "Understanding Phishing Email Processing and Perceived Trustworthiness Through Eye Tracking," *Front. Psychol.*, vol. 11, no. July, pp. 1–13, 2020, doi: 10.3389/fpsyg.2020.01756.

[8] S. Salloum, T. Gaber, S. Vadera, and K. Shaalan, "A Systematic Literature Review on Phishing Email Detection Using Natural Language Processing Techniques," *IEEE Access*, vol. 10, pp. 65703–65727, 2022, doi: 10.1109/ACCESS.2022.3183083.

[9] T. Gangavarapu, C. D. Jaidhar, and B. Chanduka, "Applicability of machine learning in spam and phishing email filtering: review and approaches," *Artif. Intell. Rev.*, vol. 53, no. 7, pp. 5019–5081, 2020, doi: 10.1007/s10462-020-09814-9.

[10] A. Gayathri, J. Aswini, and A. Revathi, "Classification Of Spam Detection Using Naive Bayes Algorithm Over K-Nearest Neighbors Algorithm Based On Accuracy," *Volatiles Essent. Oils*, vol. 8, no. 5, pp. 8516–8530, 2021.

[11] A. T. Zy, A. T. Sasongko, and A. Z. Kamalia, "Penerapan Naïve Bayes Classifier, Support Vector Machine, dan Decision Tree untuk Meningkatkan Deteksi Ancaman Keamanan Jaringan," *Media Online)*, vol. 4, no. 1, pp. 610–617, 2023, doi: 10.30865/klik.v4i1.1134.

[12] M. F. Shahzad, S. Xu, W. M. Lim, X. Yang, and Q. R. Khan, "Artificial intelligence and social media on academic performance and mental well-being: Student perceptions of positive impact in the age of smart learning," *Heliyon*, vol. 10, no. 8, Apr. 2024, doi: 10.1016/j.heliyon.2024.e29523.