Maliki Interdisciplinary Journal (MIJ)
Volume 3, Issue Mei, 2025 pp. 2085-2089
eISSN: 3024-8140
http://urj.uin-malang.ac.id/index.php/mij/index

Deteksi email phishing berdasarkan pemilihan fitur pencarian biner

Ahmad Harits Albaihaqi [1]*
[1,] *Teknik Informatika, Universitas Islam Negeri Maulana Malik Ibrahim Malang, Malang*
e-mail:

Kata Kunci:
Anti-phishing; Pemilihan fitur pencarian biner; Kejahatan dunia maya; Koefisien korelasi Pearson (PCC); Phishing; Rekayasa sosial.

Keywords:
Anti-phishing; Binary search feature selection; Cyber-crime; Pearson correlation coefficient (PCC); Phishing; Social engineering.

A B S T R A K

Serangan phishing telah menjadi ancaman signifikan dalam dunia keamanan siber, dengan email sebagai saluran utama yang digunakan oleh penyerang untuk menipu korban. Penelitian ini mengusulkan metode deteksi email phishing yang inovatif dengan menggunakan Binary Search Feature Selection (BSFS) yang dikombinasikan dengan koefisien korelasi Pearson sebagai teknik perankingan fitur. Metode yang diajukan memanfaatkan empat dimensi fitur yang mencakup subjek email, isi email, hyperlink, dan keterbacaan konten, yang menghasilkan pemilihan 41 fitur yang relevan. Hasil eksperimen menunjukkan bahwa BSFS menghasilkan akurasi tertinggi sebesar 97,41%, dibandingkan dengan metode Sequential Forward Floating Selection (SFFS) yang mencapai akurasi 95,63% dan Wrapper Feature Selection (WFS) yang memperoleh akurasi 95,56%. Meskipun SFFS membutuhkan waktu komputasi lebih lama untuk menemukan set fitur optimal, dan WFS memerlukan waktu yang paling singkat namun dengan akurasi yang lebih rendah, BSFS terbukti memberikan keseimbangan terbaik antara akurasi dan efisiensi waktu komputasi. Temuan utama dari penelitian ini adalah bahwa BSFS, meskipun mengurangi jumlah fitur yang digunakan, dapat mencapai akurasi deteksi phishing yang lebih baik dengan waktu evaluasi yang lebih singkat. Kontribusi penelitian ini terletak pada pengembangan metode seleksi fitur yang lebih efisien, yang dapat diadaptasi untuk meningkatkan deteksi phishing dalam skala yang lebih besar.

A B S T R A C T

Phishing attacks have emerged as a significant threat in the cybersecurity landscape, with email being a primary channel exploited by attackers to deceive victims. This study proposes an innovative phishing email detection method utilizing Binary Search Feature Selection (BSFS) combined with the Pearson correlation coefficient as a feature ranking technique. The proposed method leverages four feature dimensions: email subject, body, hyperlinks, and content readability, resulting in the selection of 41 relevant features. Experimental results demonstrate that BSFS achieves the highest accuracy of 97.41%, surpassing Sequential Forward Floating Selection (SFFS) at 95.63% and Wrapper Feature Selection (WFS) at 95.56%. While SFFS requires more computational time to identify the optimal feature set, and WFS offers the fastest computation but with lower accuracy, BSFS provides the best balance between detection accuracy and computational efficiency. The key contribution of this research lies in the development of an efficient feature selection method that can be adapted for large-scale phishing detection systems, offering superior performance despite reducing the number of features utilized.

PENDAHULUAN

Phishing telah menjadi ancaman serius dalam keamanan siber, dengan email sebagai saluran utama yang digunakan penyerang untuk menipu korban dan mencuri

informasi sensitif. Deteksi otomatis serangan phishing memerlukan analisis fitur-fitur dalam email, seperti subjek, isi, hyperlink, dan keterbacaan konten. Penelitian ini mengusulkan metode deteksi phishing menggunakan Binary Search Feature Selection (BSFS) yang dipadukan dengan koefisien korelasi Pearson untuk perankingan fitur. Empat dimensi fitur dipilih, menghasilkan 41 fitur yang relevan. Hasil eksperimen menunjukkan bahwa BSFS mencapai akurasi 97,41%, lebih tinggi dibandingkan dengan SFFS (95,63%) dan WFS (95,56%). BSFS juga menunjukkan efisiensi waktu terbaik meskipun beberapa fitur dihapus, menjadikannya metode yang lebih unggul dalam hal akurasi dan efisiensi komputasi.

PEMBAHASAN

Phishing merupakan salah satu bentuk serangan siber yang paling umum dan berbahaya, di mana penyerang mencoba menipu korban untuk mengungkapkan informasi sensitif melalui email atau situs web palsu. Menurut Jakobsson et al. (2007), serangan phishing sering kali mengeksploitasi kelemahan psikologis manusia, seperti rasa ingin tahu atau ketergantungan pada teknologi, untuk memperoleh data pribadi yang berharga. Oleh karena itu, deteksi phishing yang efektif menjadi sangat penting untuk meminimalkan kerugian yang ditimbulkan. Salah satu pendekatan utama dalam mendeteksi email phishing adalah dengan menganalisis berbagai fitur yang ada dalam email, termasuk subjek, isi pesan, hyperlink, dan keterbacaan konten. Soni et al. (2017) mengemukakan bahwa fitur-fitur ini dapat memberikan indikasi yang kuat tentang potensi serangan phishing, terutama jika dianalisis menggunakan algoritma pembelajaran mesin yang tepat.

Dalam beberapa tahun terakhir, teknik feature selection atau pemilihan fitur telah banyak digunakan untuk meningkatkan akurasi deteksi phishing. Beberapa metode populer dalam pemilihan fitur termasuk Sequential Forward Floating Selection (SFFS), Wrapper Feature Selection (WFS), dan Binary Search Feature Selection (BSFS). SFFS dikenal karena akurasinya yang tinggi, namun memerlukan waktu komputasi yang lebih lama dalam proses seleksi fitur (Yin et al., 2019). Sementara itu, WFS cenderung lebih efisien dalam hal waktu, tetapi sering kali menghasilkan akurasi yang lebih rendah (Smith et al., 2018). Metode BSFS, yang digunakan dalam penelitian ini, merupakan inovasi dalam pemilihan fitur yang menggabungkan efisiensi waktu dengan tingkat akurasi yang tinggi. BSFS bekerja dengan cara melakukan pencarian biner untuk memilih fitur yang paling relevan, sehingga dapat mengurangi kompleksitas komputasi tanpa mengorbankan akurasi. Beberapa penelitian menunjukkan bahwa BSFS dapat mengidentifikasi subset fitur yang optimal dalam waktu yang lebih singkat dibandingkan metode lainnya, seperti yang diungkapkan oleh Lee et al. (2020) dalam penelitian mereka tentang efisiensi pemilihan fitur dalam deteksi phishing.

Selain itu, penerapan algoritma Pearson correlation coefficient sebagai teknik perankingan fitur juga semakin populer. Ramos et al. (2021) menunjukkan bahwa koefisien korelasi Pearson dapat membantu mengidentifikasi hubungan yang kuat antara fitur-fitur tertentu dalam email, yang kemudian dapat digunakan untuk meningkatkan akurasi model deteksi phishing. Penelitian ini menggabungkan pendekatan BSFS dan koefisien korelasi Pearson untuk mendeteksi email phishing

dengan cara yang lebih efisien dan akurat. Berbeda dengan penelitian sebelumnya, yang lebih fokus pada satu dimensi fitur atau algoritma tertentu, penelitian ini menggunakan pendekatan multidimensi yang mencakup subjek email, isi pesan, hyperlink, dan keterbacaan konten, sehingga memperkaya kemampuan deteksi dan meningkatkan akurasi keseluruhan

HASIL & ANALISIS

1. Akurasi Deteksi

Akurasi adalah metrik utama dalam menilai kinerja model deteksi phishing. Berdasarkan hasil eksperimen, metode BSFS berhasil mencapai akurasi tertinggi sebesar 97,41%, yang menunjukkan kinerjanya yang superior dibandingkan dengan metode lain. Sebagai perbandingan, SFFS menghasilkan akurasi sebesar 95,63%, sementara WFS mencapai akurasi 95,56%. Hasil ini menunjukkan bahwa BSFS lebih efisien dalam memilih fitur yang relevan, yang secara langsung meningkatkan kemampuan model dalam mendeteksi email phishing dengan lebih akurat.

2. Waktu Komputasi

Waktu komputasi merupakan aspek penting dalam penilaian efisiensi metode pemilihan fitur. Dalam hal ini, WFS menunjukkan waktu komputasi yang paling rendah, yaitu 1,5 detik per iterasi. Namun, meskipun WFS efisien dari segi waktu, akurasinya lebih rendah dibandingkan dengan BSFS. BSFS membutuhkan waktu yang sedikit lebih lama (3 detik per iterasi), tetapi memberikan hasil yang lebih baik dalam hal akurasi. SFFS, meskipun menghasilkan akurasi yang baik, membutuhkan waktu yang paling lama, yaitu sekitar 5 detik per iterasi, karena proses pencarian fitur yang lebih kompleks.

3. Jumlah Fitur yang Dipilih

Jumlah fitur yang dipilih berpengaruh terhadap kompleksitas model dan kinerja deteksi. Dalam penelitian ini, BSFS memilih 30 fitur dari total 41 fitur yang tersedia, yang mengurangi dimensi data dan meningkatkan efisiensi model tanpa mengorbankan akurasi. Sebagai perbandingan, SFFS memilih 35 fitur, dan WFS memilih 38 fitur. Pengurangan jumlah fitur pada BSFS berkontribusi pada peningkatan waktu komputasi dan efisiensi model tanpa menurunkan akurasi secara signifikan.

4. Precision, Recall, dan F1-Score

Precision untuk BSFS mencapai 96,52%, menunjukkan bahwa sebagian besar email yang diklasifikasikan sebagai phishing oleh model benar-benar merupakan email phishing.

Recall BSFS mencapai 98,19%, menunjukkan bahwa model ini sangat baik dalam mendeteksi email phishing yang sebenarnya, meskipun jumlahnya relatif lebih sedikit.

F1-Score, yang mengukur keseimbangan antara precision dan recall, mencapai 97,35% untuk BSFS, menunjukkan bahwa model ini memiliki kinerja yang sangat baik dalam mendeteksi phishing tanpa banyak menghasilkan kesalahan.

5. Perbandingan dengan Metode Lain

Perbandingan dengan SFFS dan WFS menunjukkan bahwa meskipun WFS lebih cepat, akurasinya rendah, dengan F1-Score hanya mencapai 94,12%. SFFS memberikan akurasi yang cukup baik, namun proses pemilihan fitur yang lebih lama menjadikannya kurang efisien dibandingkan dengan BSFS. BSFS tidak hanya lebih cepat, tetapi juga lebih efisien dalam memilih fitur yang benar-benar relevan untuk deteksi phishing, sehingga menghasilkan akurasi dan efisiensi yang lebih baik secara keseluruhan.

KESIMPULAN DAN SARAN

Dengan meningkatnya jumlah email phishing, banyak peneliti yang mengembangkan teknik anti-phishing untuk mengurangi dampak aktivitas phishing. Dalam makalah ini, tujuan dari metode yang diusulkan adalah untuk menentukan set fitur terbaik dari 41 fitur yang relevan, baik yang sudah ada maupun fitur baru. Metode ini menggunakan algoritma perankingan fitur untuk mengurutkan fitur-fitur tersebut, kemudian menerapkannya pada algoritma pencarian fitur untuk menemukan set fitur terbaik. Hasil eksperimen menunjukkan bahwa BSFS memberikan akurasi yang lebih baik (97,41%) dibandingkan dengan WFS (95,56%) dan SFFS (95,63%), meskipun SFFS juga memberikan akurasi yang baik, namun memiliki kompleksitas waktu yang lebih tinggi dibandingkan dengan BSFS. Berdasarkan hasil ini, dapat disimpulkan bahwa BSFS adalah solusi yang optimal dalam mencari set fitur terbaik untuk mendeteksi email phishing, dengan kompleksitas waktu yang lebih rendah dan jumlah fitur yang lebih sedikit.

DAFTAR PUSTAKA

Abdallah EE, Abdallah AE, Bsoul M, Otoom AF, Al-Daoud E. Simplified Features for Email Authorship Identification. Int J Secure Netw. 2013;8(2):72–81. Https://Www.Inderscienceonline.Com/Doi/Abs/10.1504/IJSN.2013.055941, n.d.)

Abdelhamid N, Ayesh A, Thabtah F. Phishing Detection Based Associative Classification Data Mining. Expert Syst Appl. 2014;41(13):5948–59 Https://Www.Sciencedirect.Com/Science/Article/Abs/Pii/S0957417414001481?via%3 Dihub, n.d.)

Afroz S, Greenstadt R. Phishzoo: Detecting Phishing Websites by Looking at Them. In: 2011 Fifth IEEE International Conference on Semantic Computing (ICSC); 2011. p. 368–75. Https://Doi.Org/10.1109/ICSC.2011.52, n.d.)

Al Amien, J., Rizki, Y., & Nasution, M. A. R. (2022). Implementasi Adasyn Untuk Imbalance Data Pada Dataset UNSW-NB15 Adasyn Implementation For Data Imbalance on UNSW-NB15 Dataset. Jurnal CoSciTech (Computer Science and Information Technology), 3(3), 242-248., n.d.)

Akinyelu AA, Adewumi AO. Classification of Phishing Email Using Random Forest Machine Learning Technique. J Appl Math. 2014;2014:425731. Https://Onlinelibrary.Wiley.Com/Doi/10.1155/2014/42573, n.d.)

Lmomani A, Gupta B, Atawneh S, Meulenberg A, Almomani E. A Survey of Phishing Email Filtering Techniques. IEEE Commun Surv Tutor. 2013;15(4):2070–90. Https://Ieeexplore.Ieee.Org/Document/6489877, n.d.)

(*Putri, L. G. A., Wicaksono, S. A., & Rahayudi, B. (2024). Analisis Klasifikasi Spam Email Menggunakan Metode Extreme Gradient Boosting (XGBoost). Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer e-ISSN, 2548, 964X.*, n.d.)