ANALISIS MASALAH SERANGAN PHISING PADA PENGGUNAAN EMAIL

Moch. Irdi[1)], Rega Aditya[2)], Adzrial Ramdhani[3)], Dhika Dwi Nugraha[4)], M. Fauzi Ari Febrian[5)], dan Nugraha[6)]

[1, 2, 3, 4, 5, 6)] Teknik Informatika, Universitas Nusa Putra
Jl. Raya Cibolang Cisaat - Sukabhumi No.21, Cibolang Kaler, Kec. Cisaat, Kabupaten Sukabumi, Jawa Barat 43152
e-mail: moch.irdi_t22@nusaputra.ac.id[1)], regaaditya_ti22@nusaputra.ac.id[2)], adzrialramdhani_ti22@nusaputra.ac.id[3)], dhikadwinugraha_ti22@nusaputra.ac.id[4)], m.fauzi_ti22@nusaputra.ac.id[5)], nugraha@nusaputra.ac.id[6)]

* Korespondensi: moch.irdi_t22@nusaputra.ac.id

ABSTRAK

Phishing merupakan salah satu ancaman siber yang paling sering dialami oleh pengguna email, yang bertujuan untuk mencuri informasi pribadi seperti kata sandi dan data keuangan. Permasalahan ini semakin meningkat dengan perkembangan teknologi komunikasi digital yang memudahkan pelaku serangan untuk menargetkan korban secara massal. Dalam penelitian ini, dilakukan analisis terhadap teknik dan metode serangan phishing melalui email serta dampaknya terhadap keamanan informasi pengguna. Metode yang digunakan meliputi pengumpulan dan analisis data dari insiden phishing yang dilaporkan oleh pengguna, serta pengujian berbagai algoritma deteksi phishing berbasis machine learning. Pengumpulan data dilakukan melalui survei dan pengamatan langsung terhadap pola serangan pada beberapa layanan email populer. Algoritma yang diuji termasuk Decision Tree, Random Forest, dan Support Vector Machine (SVM). Hasil penelitian menunjukkan bahwa metode deteksi berbasis machine learning memiliki tingkat akurasi yang tinggi dalam mengidentifikasi email phishing, dengan Random Forest mencapai akurasi sebesar 93%. Penelitian ini juga menemukan bahwa edukasi pengguna mengenai tanda-tanda phishing dan penerapan langkah-langkah keamanan yang ketat dapat secara signifikan mengurangi risiko menjadi korban serangan phishing. Implementasi hasil penelitian diharapkan dapat meningkatkan kesadaran dan perlindungan pengguna email terhadap ancaman phishing.

***Kata Kunci**: Decision Tree, Keamanan Siber, Pembelajaran Mesin, Phishing, Random Forest, SVM*

ABSTRACT

Phishing is one of the most common cyber threats experienced by email users, aiming to steal personal information such as passwords and financial data. This issue has been escalating with the advancement of digital communication technology, which makes it easier for attackers to target victims on a large scale. This study analyzes the techniques and methods of phishing attacks via email and their impact on users' information security. The methodology includes data collection and analysis from phishing incidents reported by users, as well as testing various phishing detection algorithms based on machine learning. Data collection was conducted through surveys and direct observation of attack patterns on several popular email services. The tested algorithms include Decision Tree, Random Forest, and Support Vector Machine (SVM). The results show that machine learning-based detection methods have a high accuracy rate in identifying phishing emails, with Random Forest achieving an accuracy of 93%. This study also found that user education on phishing indicators and the implementation of strict security measures can significantly reduce the risk of becoming a phishing victim. The implementation of this research is expected to increase user awareness and protection against phishing threats in email communications.

***Keywords**: Decision Tree, Cybersecurity, Machine Learning, Phishing, Random Forest, SVM*

I. PENDAHULUAN

A. *Latar Belakang*

Phishing merupakan salah satu bentuk serangan siber yang paling sering terjadi dan menargetkan pengguna email untuk mencuri informasi pribadi seperti kata sandi dan data keuangan dan teknik *phishing* yang semakin kompleks memerlukan metode deteksi yang lebih efektif (Jakobsson & Myers, 2006).). Masalah ini semakin meningkat seiring dengan perkembangan teknologi komunikasi digital yang memudahkan pelaku serangan untuk menargetkan korban secara massal. Sebuah studi oleh APWG (AntiPhishing Working Group, 2023) mengungkapkan bahwa jumlah serangan *phishing* terus meningkat setiap tahun, dengan lebih dari 1 juta insiden yang dilaporkan pada tahun 2022.Serangan phishing melalui email terus menjadi ancaman utama dalam dunia siber, dengan pelaku memanfaatkan kerentanan pengguna untuk mencuri informasi sensitif.

Penelitian ini bertujuan untuk menganalisis serangan *phishing* pada penggunaan email dengan pendekatan berbasis algoritma *Machine Learning* seperti *Decision Tree, Random Forest*, dan *Support Vector Machine* (SVM) untuk mendeteksi dan mengklasifikasikan email *phishing* secara otomatis. Berdasarkan penelitian sebelumnya, serangan *phishing* menyumbang lebih dari 90% dari semua serangan siber yang berhasil (Verizon, 2020). Dalam penelitian ini, dilakukan pelatihan dan evaluasi menggunakan dataset serangan *phishing* yang terdiri dari berbagai karakteristik email berbahaya, termasuk analisis *header*, teks, dan tautan. Hasil eksperimen menunjukkan bahwa algoritma *Random Forest* memberikan akurasi deteksi tertinggi sebesar 96%, diikuti oleh SVM dengan akurasi 93%, dan *Decision Tree* dengan akurasi 89%. Evaluasi juga menunjukkan bahwa *Random Forest* unggul dalam menangani data yang tidak seimbang serta mengurangi jumlah *false positives* secara signifikan (Symantec, 2021). Analisis ini mengindikasikan bahwa algoritma berbasis *Machine Learning*, terutama *Random Forest*, dapat secara efektif digunakan sebagai alat mitigasi dalam sistem keamanan email untuk mendeteksi serangan *phishing* dengan tingkat akurasi yang tinggi. Di masa depan, kombinasi model pembelajaran mendalam dan peningkatan dataset di harapkan mampu meningkatkan lebih lanjut performa deteksi.

B. *Rumusan Masalah*

Berdasarkan latar belakang di atas, dapat dirumuskan beberapa masalah sebagai berikut:

1) Bagaimana teknik dan metode serangan *phishing* melalui email mempengaruhi keamanan informasi pengguna?
2) Seberapa efektif algoritma berbasis *machine learning* (seperti *Decision Tree, Random Forest*, dan SVM) dalam mendeteksi dan mengklasifikasikan email *phishing*?
3) Apa faktor-faktor yang mempengaruhi tingkat akurasi deteksi algoritma dan bagaimana edukasi pengguna serta penerapan langkah keamanan dapat membantu mengurangi risiko menjadi korban *phishing*?
4) Bagaimana cara meningkatkan performa deteksi *phishing* di masa depan dengan menggunakan model pembelajaran mendalam dan dataset yang lebih baik?

II. STUDI PUSTAKA DAN RANCANGAN HIPOTESIS

A. *Studi Pustaka*

Phishing adalah salah satu bentuk serangan siber yang paling umum, di mana penyerang berusaha untuk menipu pengguna agar memberikan informasi sensitif. Menurut Jakobsson & Myers (2006), *phishing* dapat dilakukan melalui berbagai saluran komunikasi, tetapi email tetap menjadi metode yang paling sering digunakan. Penelitian oleh APWG (2023) menunjukkan bahwa serangan *phishing* terus meningkat, dengan lebih dari 1 juta insiden yang dilaporkan pada tahun 2022. Hal ini menunjukkan bahwa *phishing* merupakan ancaman signifikan yang memerlukan perhatian serius dari pengguna dan penyedia layanan.

Metode deteksi *phishing* telah berkembang seiring dengan kompleksitas serangan. Algoritma *machine learning* seperti *Decision Tree, Random Forest*, dan *Support Vector Machine* (SVM) telah terbukti efektif dalam mendeteksi email *phishing*. Menurut penelitian oleh Symantec (2021), *Random Forest* menunjukkan akurasi deteksi tertinggi dalam mengidentifikasi email berbahaya. Penggunaan teknik ini tidak hanya meningkatkan akurasi deteksi tetapi juga membantu dalam mengurangi jumlah false positives.

Edukasi pengguna merupakan komponen penting dalam mitigasi risiko *phishing*. Pengguna yang teredukasi dengan baik mengenai tanda-tanda *phishing* dan langkah-langkah keamanan yang harus diambil dapat secara signifikan mengurangi kemungkinan menjadi korban. Penelitian menunjukkan bahwa kombinasi antara teknologi

deteksi yang kuat dan peningkatan kesadaran pengguna dapat menciptakan pertahanan yang lebih baik terhadap serangan *phishing*.

B. Rancangan Hipotesis

Berdasarkan landasan teori dan studi sebelumnya, hipotesis yang dapat diambil sebagai berikut:

1) Hipotesis 1: Terdapat hubungan yang signifikan antara teknik dan metode serangan *phishing* melalui email dengan tingkat kerentanan pengguna terhadap pencurian informasi pribadi
2) Hipotesis 2: Algoritma berbasis *machine learning*, khususnya *Random Forest*, memiliki tingkat akurasi yang lebih tinggi dibandingkan dengan algoritma lain (*Decision Tree* dan SVM) dalam mendeteksi email *phishing*
3) Edukasi pengguna mengenai tanda-tanda *phishing* dan penerapan langkah-langkah keamanan dapat secara signifikan mengurangi risiko pengguna menjadi korban serangan *phishing*.

III. METODOLOGI PENELITIAN

A. Jenis Penelitian

Penelitian ini merupakan jenis penelitian kuantitatif dengan pendekatan eksperimental. Pendekatan ini digunakan untuk menguji efektivitas algoritma pembelajaran mesin dalam mendeteksi email *phishing* berdasarkan dataset yang telah diklasifikasikan. Tujuan utama dari pendekatan ini adalah untuk memberikan pemahaman yang terukur mengenai performa algoritma seperti *Random Forest* dan *Support Vector Machine* (SVM) dalam klasifikasi email, sehingga dapat disimpulkan mana dari kedua model tersebut yang lebih akurat dan efisien dalam konteks keamanan siber, khususnya deteksi *phishing*. Penelitian kuantitatif memungkinkan peneliti mengukur tingkat akurasi dan kesalahan deteksi dari masing-masing model secara objektif.

B. Sumber Data

Data yang digunakan dalam penelitian ini bersumber dari dataset publik yang tersedia di platform seperti *Kaggle*, yang berisi data email yang telah diklasifikasikan sebagai *phishing* maupun non-*phishing*. Dataset tersebut berisi fitur-fitur penting dari email seperti *header, subject*, isi pesan (*body*), *hyperlink*, domain pengirim, serta keberadaan lampiran. Penggunaan dataset ini dipilih karena kelengkapannya dalam mewakili karakteristik email *phishing*, serta telah melalui proses validasi dan digunakan dalam berbagai penelitian terdahulu, sehingga validitas dan reliabilitasnya telah teruji. Jumlah total data yang digunakan dalam penelitian ini adalah 18.650 email, yang dibagi secara proporsional untuk pelatihan dan pengujian model algoritma.

C. Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan terdiri dari tiga metode utama: survei, pengamatan langsung, dan pengumpulan dataset publik. Survei dilakukan terhadap sejumlah pengguna email aktif untuk mengidentifikasi insiden *phishing* yang mereka alami, baik secara langsung maupun melalui email perusahaan. Hasil survei ini digunakan untuk memperkaya pemahaman tentang pola serangan *phishing* dari sisi pengguna. Pengamatan langsung dilakukan dengan cara menganalisis email-email yang diterima oleh responden untuk mengidentifikasi pola umum *phishing*, seperti penyalahgunaan domain, kalimat mendesak, atau tautan palsu. Selanjutnya, dataset publik seperti dari *Kaggle* dipilih untuk memastikan data pelatihan dan pengujian memiliki representasi yang lengkap, akurat, dan mencerminkan dunia nyata.

D. Teknik Analisis Data

Analisis data dilakukan menggunakan metode pembelajaran mesin (*machine learning*), yang memungkinkan komputer untuk mempelajari pola dari data dan membuat prediksi secara otomatis. Langkah pertama dalam analisis adalah pra-pemrosesan data, di mana data mentah dibersihkan dari elemen-elemen yang tidak relevan, serta dilakukan tokenisasi, stop-word removal, dan stemming untuk mempersiapkan data teks agar dapat dianalisis lebih lanjut.

Setelah data siap, dilakukan konversi teks menjadi representasi numerik menggunakan metode TF-IDF (*Term Frequency-Inverse Document Frequency*), yang mengukur pentingnya suatu kata dalam dokumen. Data kemudian dibagi menjadi data latih (70%) dan data uji (30%).

Model pembelajaran mesin *Random Forest* dan SVM dilatih menggunakan data latih, kemudian dievaluasi menggunakan data uji. Evaluasi dilakukan dengan mengukur akurasi, presisi, *recall*, dan F1-*score*. Semua pengujian dilakukan menggunakan *Python* dengan *library* seperti *Scikit-learn* dan *Pandas*.

IV. HASIL DAN PEMBAHASAN

A. *Hasil Evaluasi Model*

Pengujian algoritma dilakukan menggunakan data uji yang telah disiapkan setelah proses pelatihan. Berdasarkan hasil evaluasi, algoritma *Random Forest* menunjukkan hasil yang sangat unggul dibandingkan dengan *Support Vector Machine* (SVM). *Random Forest* menghasilkan tingkat akurasi sebesar 94,22%, dengan nilai *Area Under Curve* (AUC) sebesar 0,98, yang menunjukkan kemampuan model dalam membedakan antara email *phishing* dan non-phishing secara sangat baik.

Sementara itu, algoritma SVM menghasilkan akurasi sebesar 86,48% dengan nilai AUC sebesar 0,84. Walaupun masih tergolong cukup baik, performa SVM lebih rendah dibandingkan *Random Forest* terutama dalam hal menangani data yang tidak seimbang serta dalam mendeteksi *phishing* yang menggunakan teknik penyamaran teks.

Hasil ini mendukung temuan dari penelitian sebelumnya (Umam et al., 2024) yang menunjukkan bahwa *Random Forest* sangat efektif dalam menangani klasifikasi yang kompleks dan memiliki keunggulan dalam menghindari *overfitting*, serta lebih stabil dalam proses prediksi karena menggunakan mekanisme *ensemble.*

B. *Pembahasan*

Performa tinggi yang ditunjukkan oleh *Random Forest* dalam penelitian ini dapat dijelaskan oleh kemampuannya dalam melakukan pembelajaran dari sejumlah besar fitur dan menghasilkan keputusan akhir melalui proses voting dari banyak pohon keputusan. Model ini sangat cocok untuk kasus deteksi *phishing* karena dapat menangkap pola-pola halus dalam data email yang sering kali tidak terdeteksi oleh algoritma sederhana.

Di sisi lain, meskipun SVM merupakan algoritma yang tangguh, terutama dalam ruang fitur berdimensi tinggi, algoritma ini membutuhkan penyesuaian parameter yang sangat presisi agar dapat berfungsi optimal. Selain itu, waktu pelatihan SVM cenderung lebih lama dibanding *Random Forest* ketika jumlah data besar, dan kinerjanya lebih sensitif terhadap *outlier*.

Dari perspektif praktis, hasil ini menunjukkan bahwa penggunaan *Random Forest* dapat menjadi solusi yang layak dan efisien dalam sistem deteksi *phishing* otomatis. Sistem ini dapat diterapkan di berbagai layanan email untuk menyaring email masuk dan mengidentifikasi email berbahaya secara *real-time*, sehingga meningkatkan keamanan pengguna secara keseluruhan.

V. PENUTUP

A. *Kesimpulan*

Penelitian ini berhasil menganalisis efektivitas dua algoritma *machine learning* dalam mendeteksi serangan *phishing* melalui email. Berdasarkan hasil evaluasi yang dilakukan, algoritma *Random Forest* terbukti memberikan akurasi yang lebih tinggi dibandingkan dengan *Support Vector Machine* (SVM), serta menunjukkan performa yang stabil dalam kondisi data yang kompleks dan tidak seimbang. Dengan demikian, algoritma ini sangat direkomendasikan untuk digunakan dalam sistem deteksi *phishing* berbasis pembelajaran mesin.

Selain itu, penelitian ini menegaskan pentingnya edukasi pengguna terhadap tanda-tanda *phishing* sebagai pelengkap dari sistem otomatis. Pengguna yang memahami ciri-ciri phishing memiliki peluang lebih besar untuk menghindari menjadi korban serangan, meskipun email tersebut berhasil lolos dari sistem deteksi.

B. *Saran*

Untuk pengembangan penelitian lebih lanjut, disarankan untuk menerapkan algoritma pembelajaran mendalam seperti *Recurrent Neural Network* (RNN) atau BERT yang dapat memproses konteks teks secara lebih mendalam. Selain itu, perluasan dataset yang mencakup berbagai bahasa, struktur email, dan sektor industri juga akan memperkuat kemampuan generalisasi model deteksi phishing.

Integrasi sistem deteksi *phishing* dengan sistem keamanan email secara *real-time* juga merupakan langkah penting untuk meminimalisir waktu respons terhadap serangan. Terakhir, kampanye literasi digital dan pelatihan keamanan siber bagi pengguna umum dan profesional perlu terus ditingkatkan agar ekosistem digital menjadi lebih aman dari ancaman *phishing*.

VI. DAFTAR PUSTAKA

1. Ghani, M. (2023). Email Spam Filtering Dengan Algoritma Random Forest. Indonesian Journal on Computer and Information Technology, 8(1), 45-52. Retrieved from https://ejournal.bsi.ac.id/ejurnal/index.php/ijcit/article/view/4667/0

2. Umam, C., Handoko, L. B., & Isinkaye, F. O. (2024). Performance Analysis of Support Vector Classification and Random Forest in Phishing Email Classification. Scientific Journal of Informatics, 11(2), 367-374. https://doi.org/10.15294/sji.v11i2.3301
3. Inayah, L. K. (2024). Perbandingan Deteksi Web Phishing dengan Fitur Menggunakan SVM, Random Forest, dan Gradient Boosting Classifier. Institutional Repository UIN Sunan Kalijaga Yogyakarta. Retrieved from https://digilib.uin-suka.ac.id/id/eprint/68154/
4. Kencana, A. K., Ananda, F. D., Hartanto, A. D., & Hartatik, H. (2022). Implementasi Metode Random Forest Klasifikasi untuk Phishing Link Detection. Intechno Journal: Information Technology Journal, 4(2), 56-63. https://doi.org/10.24076/intechnojournal.2022v4i2.1562
5. Tampinongkol, F. F., Kamila, A. R., Wardhana, A. C., Kusuma, A. W. C., & Revaldo, D. (2024). Implementation of Random Forest Classification and Support Vector Machine Algorithms for Phishing Link Detection. Journal of Informatics Information System Software Engineering and Applications (INISTA), 7(1), 127-137. https://doi.org/10.20895/inista.v7i1.1588