Jurnal
ILMU KEPOLISIAN
ISSN : 2620-5025

Volume 17 / Nomor 3 / Desember 2023

PENERAPAN METODE MULTIPLE MACHINE LEARNING (HYBRID MODEL) UNTUK MENDETEKSI LINK PHISHING SEBAGAI UPAYA PREVENTIF DALAM MEMINIMALISIR KORBAN PENCURIAN DATA

[1]Mokhamad Fikri Alfawaid, [2]Jarot Prianggono
[1,2]Program Studi S1 Ilmu Kepolisian, Sekolah Tinggi Ilmu Kepolisian, Jakarta 12160
e-mail: alfawaidfikri@gmail.com

Abstrak

Hegemoni yang dihasilkan dari meluasnya penggunaan teknologi dan media sosial tidak dapat dibendung. Di sisi lain, efek negatif dari dunia yang saling terhubung selalu ada di benak semua pengguna. Seperti halnya teknologi, kejahatan berevolusi dari waktu ke waktu, menciptakan ruang-ruang baru yang sebelumnya tidak berpenghuni. *Phishing*, salah satu bentuknya, telah menjadi momok yang menakutkan di dunia digital karena mengeksploitasi kerentanan terbesar di dunia maya: manusia. Tulisan ini bertujuan untuk memaparkan hasil penelitian penulis dalam mengembangkan model *machine learning* (ML) untuk membantu mendeteksi dan mengenali tautan *phishing*, sekaligus mengusulkan penggunaan ML oleh Kepolisian Negara Republik Indonesia (Polri) untuk membantu masyarakat dalam menghindari kejahatan *phishing*. Penelitian dilakukan dengan menggunakan pendekatan ML dengan tiga (3) metode, yaitu Support Vector Machine (SVM), Decision Tree, dan Random Forest secara terpisah dan kombinasinya (hybrid model) dalam empat (4) area penilaian, yaitu tingkat akurasi, presisi, *recall*, dan nilai f1. Hasil penelitian menunjukkan bahwa model *hybrid* yang merupakan gabungan dari ketiga model ML, yaitu Decision Tree, Random Forest dan Support Vector Machine (SVM) mampu menunjukan performa yang lebih unggul dibandingkan dengan masing-masing model berdiri sendiri. Penulis merekomendasikan penggunaan model gabungan dan para peneliti yang berniat untuk melakukan penelitian yang serupa untuk memperkaya jumlah dataset yang digunakan agar hasil klasifikasi dan performa ML yang dihasilkan lebbih baik.

Kata kunci: phishing; Machine Learning; Support Vector Machine (SVM); Decision Tree; Random Forest; Hybrid Model

Abstract

The hegemony resulting from the widespread use of technology and social media cannot be stopped. On the other hand, the negative effects of an interconnected world are always present in the minds of all users. As with technology, crime evolves over time, creating new spaces that were previously uninhabited. Phishing, one of its forms, has become a terrifying spectre in the digital world because it exploits the greatest vulnerability in cyberspace: humans. This journal aims to present the results of the author's research into developing a machine learning (ML) model to assist in detecting and recognizing phishing links, while also proposing the use of ML by the National Police to assist citizens in avoiding phishing crimes. The research was conducted using the ML approach with three (three) methods, namely Support Vector Machine (SVM), Decision Tree, and Random Forest separately and their combination (hybrid model) in four (four) assessment areas, namely the level of accuracy, precision, recall, and scores f1. The research results show that the hybrid model which is a combination of three ML models, namely Decision Tree, Random Forest and Support Vector Machine (SVM) is able to show superior performance compared to each model standing alone. The author recommends the use of combined models and researchers who intend to conduct similar research to enrich the number of datasets used so that the resulting classification results and ML performance are better.

Keywords: phishing: machine learning; Support Vector Machine (SVM); decision tree; random forest; hybrid model.

Pendahuluan

Phishing merupakan salah satu bentuk serangan siber yang paling sering digunakan oleh para pelaku kejahatan siber. *Phishing* sudah menjadi sebuah masalah yang berkepanjangan di dalam ruang maya sejak pertama kali serangan tersebut terjadi dan menyerang sebuah web portal America Online (AOL) sebagai pada tahun 1995 (James, 2006, dalam Chiew, Yong & Tan, 2018). Metode yang pertama digunakan adalah dengan berusaha mencuri data password penggunanya dan men-generate nomor kartu kredit secara random menggunakan algoritma tertentu. Kemudian akun tersebut digunakan untuk mengirimkan email *phishing* secara acak ke beberapa pengguna lain untuk mendapatkan data sensitif milik mereka. Pada akhirnya AOL berhasil menggagalkan serangan tersebut dengan mengaplikasikan langkah-langkah keamanan untuk mencegah metode yang sama terjadi.

Link *phishing* adalah link yang digunakan untuk menipu korban agar memberikan informasi sensitif, seperti kata sandi, nomor kartu kredit, atau data pribadi lainnya. Link phishing biasanya dikirim melalui email, pesan teks, atau media sosial. Link tersebut sering kali disamarkan sebagai link dari sumber yang tepercaya, seperti bank, perusahaan e-commerce, atau layanan pemerintah. Pencurian data adalah tindakan mengambil data sensitif dari seseorang atau organisasi tanpa izin. Data yang dicuri dapat digunakan untuk berbagai tujuan yang merugikan, seperti penipuan, pemerasan, atau pencurian identitas.

Link phishing biasanya memiliki ciri-ciri sebagai berikut:

1. Tautan yang mencurigakan: Tautan phishing biasanya memiliki URL yang tidak lazim atau terlihat mencurigakan. Misalnya, URL yang mengandung simbol atau huruf yang tidak biasa, atau URL yang tidak sesuai dengan domain situs web yang diklaimnya.
2. Pesan yang mendesak: Pesan phishing biasanya berisi pesan yang mendesak korban untuk bertindak segera, seperti "Akun Anda akan diblokir jika Anda tidak memperbarui informasi Anda sekarang."
3. Gaya bahasa yang tidak formal: Pesan phishing biasanya ditulis dengan gaya bahasa yang tidak formal atau tidak profesional.

Berdasarkan laporan investigasi kebocoran data Verizon, serangan *phishing* masih menjadi jenis serangan yang paling sering digunakan dan berhasil dengan lebih dari 80% laporan insiden keamanan dan kebocoran data (Data Breach Investigations Report, 2021). Serangan *phishing* juga merupakan jenis serangan siber yang mengalami peningkatan pada tahun 2020 sebanyak 65% dibandingkan dengan tahun sebelumnya berdasarkan laporan Anti-*Phishing* Working Group (APWG, 2021). Selain dari jumlah serangan yang terus meningkat, keadaan semakin diperparah dengan fakta bahwa serangan *phishing* tidak hanya memiliki dampak pada kerugian materiil namun juga non-materiil. Salah satu contoh kerugian materiil yang ditimbulkan oleh serangan *phishing* diantaranya laporan IBM mengenai Cost of Data Breach tahun 2022 (IBM, 2022) dimana, *phishing* memiliki proporsi jumlah serangan terbanyak kedua sebesar 16% dengan nominal kerugian $ 4.91 juta sepanjang tahun 2022. Sedangkan dampak non-materiilnya yaitu terjadinya 3.7 juta kebocoran data perbulan sejak Agustus 2020 hingga Juli 2021 di Amerika Serikat dengan 58.8% diantaranya terjadi pada penyedia jasa layanan kesehatan di Amerika Serikat (HIPAA, 2021).

Selama masa pandemi COVID-19 telah terjadi peningkatan tajam sebanyak 4-5 kali lipat terhadap tindak kejahatan siber melalui serangan *phishing* hal tersebut berdasarkan pada laporan transparansi Google (Google Transparency Report, 2021) Berbagai situs website mulai dari e-commerce, sosial media hingga situs perbankan tidak luput dari serangan *phishing*. Dalam melakukan serangan *phishing*, penyerang mencoba untuk memperoleh informasi sensitif dari

korban, seperti *username*, *password*, nomor kartu kredit, atau informasi keuangan penting lainnya dengan memperdaya korbannya menggunakan link yang menipu. Link *phising* tersebut pada umumnya dikirim melalui email, pesan instan, atau media sosial.

Phishing tidak hanya digunakan sebagai bentuk serangan utama seorang pelaku kejahatan dunia maya dalam melakukan serangan. Tetapi *phishing* juga dapat dilakukan sebagai serangan pembuka untuk mengirimkan *payload* seperti *malware* baik itu *ransomware* maupun *spyware*. Selain itu, *phishing* juga kerap digunakan untuk digunakan sebuah *entry point* untuk memudahkan melakukan serangan pada target yang sebenarnya.

Sudah terdapat berbagai metode untuk menangani permasalahan terkait *phishing* tersebut, salah satu diantaranya adalah metode yang terbilang masih tradisional untuk mendeteksi link *phising* yaitu menggunakan metode blacklist dan whitelist untuk mengidentifikasi tautan yang aman atau tidak aman. Namun sayangnya, metode ini memiliki banyak keterbatasan dalam mendeteksi tautan *phising* yang baru dan seringkali tidak efektif dalam mengenali tautan *phising* yang tersembunyi di balik URL yang valid. Sehingga, dalam beberapa tahun terakhir, penggunaan ML hadir sebagai solusi untuk mendeteksi tautan *phising* secara akurat dan otomatis.

Dalam penelitian ini, algoritma ML dilatih untuk mengenali pola dan karakteristik dari tautan *phising* sehingga dapat mengklasifikasikan tautan yang mencurigakan. Dimana, penulis menerapkan 3 algoritma ML yaitu *Support Vector Machine, Decision Tree, dan Random Forest* yang kemudian dikolaborasikan untuk menciptakan sebuah algoritma hybrid dalam mendeteksi tautan *phishing*. Penelitian ini ditujukan untuk meneliti dan menciptakan sebuah metode baru menggunakan penggabungan hasil dari 3 algoritma ML yang lebih efektif dan efisien dalam mendeteksi tautan palsu yang kerap digunakan dalam serangan *phishing*. Selain itu, penelitian tentang pengaplikasian ML untuk alat deteksi tautan *phising* ini diharapkan dapat memberikan kontribusi besar dalam upaya pencegahan kejahatan siber dan perlindungan informasi sensitif baik bagi individu maupun organisasi yang dapat digunakan dan diaplikasikan pada institusi Polri.

Penelitian ini dilakukan menggunakan bahasa pemrograman Python untuk membuat algoritma ML dengan menggunakan 1.677 *dataset* yang berisi 827 tautan *phishing* dan 850 tautan *non-phishing* untuk melatih model ML yang dibuat dengan rasio 80:20 untuk data *training* dan *test*. Dataset tersebut penulis dapatkan dari database milik Phishtank (Phishtank, 2021). Sebelum melatih model ML, penulis terlebih dahulu melakukan ekstraksi fitur dari masing-masing dataset dalam sebuah ekosistem *sandbox* pada OS Linux dengan menggunakan jaringan TOR. Selanjutnya, sebuah *pilot software* yang berbasis ekstensi *Google Chrome* dapat dibuat untuk menguji pengaplikasian model ML yang dibuat dalam kasus nyata.

Pada awal penelitian, penulis menggunakan 10.000 dataset *phishing* dan non-*phishing* URL. Namun, dalam proses ekstraksi fitur pertama kali terjadi beberapa kendala diantaranya lama waktu yang diperlukan untuk memproses ekstraksi fitur yang tidak kunjung berakhir, dimana hal tersebut disebabkan oleh beberapa faktor seperti halaman web dari tautan yang sudah tidak aktif dan sistem keamanan yang cukup sensitif. Sehingga, hasil ekstraksi fitur pada percobaan pertama tidak begitu kuat untuk mengidentifikasi link *phising* dan non-*phishing*. Oleh sebab itu, penulis menetapkan *time-limit* pada percobaan yang kedua dan berhasil menghasilkan 1.677 dataset.

Tinjauan Literatur

Teori Difusi Inovasi

Teori difusi inovasi adalah teori yang menjelaskan bagaimana ide dan teknologi baru menyebar dalam suatu sistem sosial. Teori ini menjelaskan proses komunikasi dan adopsi inovasi melalui saluran tertentu dalam suatu sistem sosial sepanjang waktu. Teori ini dipopulerkan oleh Everett

Rogers pada tahun 1964 melalui bukunya yang berjudul *Diffusion of Innovations*. Teori difusi inovasi didasarkan pada asumsi bahwa inovasi adalah suatu hal yang baru dan belum banyak diketahui, dan adopsi inovasi adalah proses yang kompleks yang dipengaruhi oleh berbagai faktor, baik internal maupun eksternal.

Pada dasarnya, teori ini mengasumsikan bahwa adopsi inovasi oleh masyarakat terjadi dalam pola yang bisa diprediksi. Beberapa kelompok orang akan mengadopsi inovasi segera setelah mereka mendengar tentang inovasi tersebut, sementara kelompok lainnya membutuhkan waktu lebih lama untuk mengadopsinya. Ketika sebuah inovasi banyak diadopsi oleh sejumlah orang, hal itu dikatakan sebagai difusi inovasi yang berhasil. Teori Difusi Inovasi juga mengidentifikasi beberapa faktor yang mempengaruhi kecepatan dan tingkat adopsi inovasi, seperti saluran komunikasi, ciri-ciri sistem sosial, kegiatan promosi, dan peran pemuka pendapat atau opinion leader.

Rogers membagi proses difusi inovasi menjadi lima tahap, yaitu:

1. Kesadaran (*awareness*): Tahap ini ditandai dengan munculnya kesadaran akan adanya inovasi.
2. Pemahaman (*interest*): Tahap ini ditandai dengan munculnya ketertarikan untuk mempelajari lebih lanjut tentang inovasi.
3. Evaluasi (*evaluation*): Tahap ini ditandai dengan munculnya penilaian terhadap manfaat dan risiko inovasi.
4. Percobaan (*trial*): Tahap ini ditandai dengan mencoba inovasi dalam skala kecil.
5. Adopsi (*adoption*): Tahap ini ditandai dengan penerimaan dan penggunaan inovasi secara penuh.

Rogers juga membagi individu-individu yang mengadopsi inovasi menjadi lima kategori, yaitu:

1. *Pioneer* (pelopor): Individu yang pertama kali mengadopsi inovasi.
2. *Early adopter* (pengadopsi awal): Individu yang mengadopsi inovasi setelah pelopor, tetapi masih dalam kelompok awal.
3. *Early majority* (mayoritas awal): Individu yang mengadopsi inovasi setelah pengadopsi awal.
4. *Late majority* (mayoritas akhir): Individu yang mengadopsi inovasi setelah mayoritas awal.
5. *Laggard* (yang tertinggal): Individu yang mengadopsi inovasi paling akhir.

Teori difusi inovasi telah digunakan untuk menganalisis penyebaran berbagai macam inovasi, seperti teknologi baru, ide-ide baru, dan perilaku baru. Teori ini telah diterapkan dalam berbagai bidang, seperti pemasaran, komunikasi, dan pengembangan masyarakat. Beberapa contoh penerapan teori difusi inovasi digunakan untuk:

1. Pemasaran: Teori difusi inovasi dapat digunakan untuk memahami bagaimana konsumen mengadopsi produk dan layanan baru.
2. Komunikasi: Teori difusi inovasi dapat digunakan untuk memahami bagaimana informasi dan ide-ide baru menyebar dalam masyarakat.
3. Pengembangan masyarakat: Teori difusi inovasi dapat digunakan untuk memahami bagaimana inovasi sosial menyebar di masyarakat.

Dalam konteks penerapan teori ini, difusi inovasi dapat terjadi dalam berbagai bidang, termasuk teknologi, pendidikan, kesehatan, dan bisnis. Teori ini memberikan pemahaman tentang bagaimana inovasi dapat diterima dan menyebar di masyarakat, serta membantu dalam merencanakan strategi komunikasi dan pemasaran yang efektif untuk mempercepat adopsi inovasi.

Teori Difusi Inovasi adalah teori yang menjelaskan bagaimana ide atau gagasan baru dan teknologi tersebar dalam suatu kebudayaan melalui saluran tertentu sepanjang waktu. Teori ini mengidentifikasi faktor-faktor yang mempengaruhi adopsi inovasi dan memberikan pemahaman tentang proses difusi inovasi dalam berbagai konteks. Teori difusi inovasi merupakan alat yang bermanfaat untuk memahami penyebaran inovasi. Teori ini dapat digunakan untuk memprediksi tingkat adopsi inovasi, serta untuk mengembangkan strategi untuk mempercepat penyebaran inovasi.

Machine Learning (ML) untuk Deteksi *Phishing* URL

Machine Learning adalah cabang ilmu komputer yang mengeksplorasi algoritma dan strategi untuk mengotomatiskan solusi dari masalah rumit yang sulit diprogram menggunakan teknik pemrograman standar (Rebala, Ravi and Churiwala, 2019). ML bekerja dengan cara yang mirip. Algoritma ML dilatih pada set data yang besar dan terstruktur yang berisi contoh-contoh yang telah diberi label. Algoritma tersebut kemudian mempelajari pola dan hubungan dalam data tersebut sehingga dapat membuat prediksi atau keputusan baru pada data yang belum pernah dilihat sebelumnya.

Data adalah elemen kunci dalam *machine learning*. Model-*machine learning* dipelajari dari data yang diberikan. Data ini dapat berupa berbagai jenis informasi, termasuk gambar, teks, suara, atau angka. Model-machine learning adalah struktur matematis atau komputasional yang digunakan untuk mewakili pengetahuan atau pola yang ditemukan dalam data. Model ini dapat berupa jaringan saraf tiruan, pohon keputusan, regresi, atau berbagai jenis struktur lainnya.

Algoritma *machine learning* adalah langkah-langkah matematis atau perhitungan yang dijalankan oleh model untuk mempelajari pola dari data. Algoritma ini mencakup proses pelatihan (*training)* di mana model dipelajari dari data, dan proses pengujian *(testing)* di mana model diuji pada data baru untuk melakukan prediksi atau klasifikasi. Dalam supervised learning, model dilatih dengan menggunakan data yang sudah diberi label, yang berarti bahwa setiap contoh data sudah diketahui output yang seharusnya. Tujuan model adalah untuk mempelajari hubungan antara input dan output sehingga dapat melakukan prediksi pada data baru.

Unsupervised learning tidak menggunakan label pada data pelatihan. Tujuan model adalah untuk menemukan pola atau struktur tersembunyi dalam data, seperti pengelompokan (*clustering*) atau reduksi dimensi. Reinforcement learning melibatkan model yang belajar melalui interaksi dengan lingkungan. Model menerima umpan balik (*reward* atau hukuman) berdasarkan tindakan yang diambilnya, dan tujuannya adalah untuk memaksimalkan kumulatif *reward*. Proses identifikasi dan pemilihan fitur (*features*) yang paling relevan dari data untuk memperbaiki kinerja model.

Beberapa literatur tentang penelitian terdahulu pada pemanfaatan ML dalam mendeteksi *phishing* telah diteliti dan dipelajari, antara lain:

1. Subasi, Molah, Almkallawi and Chaudhery (2017) meneliti performa beberapa model ML diantaranya ANN, KNN, SVM, Random Forest, dan C4.5 dalam mendeteksi *phishing*. Mereka berhasil memproduksi angka akurasi yang cukup tinggi dalam mendeteksi tautan *phishing*; model Random Forest adalah model yang paling akurat dengan tingkat akurasi 97.26%. *Dataset* yang digunakan dalam penelitiannya didapatkan dari University of California's UCI repository dengan 30 fitur. Penelitian ini menguji performa masing-masing model ML berdasarkan akurasi, *f-measure and Receiver Operating Characteristics* (ROC).

2. Pandey, Gill, Sai Prasad Nadendla and Thaseen (2019) dalam penelitiannya menggabungkan model SVM dan Random Forest untuk menciptakan sebuah model hybrid. Model tersebut kemudian dilatih dan diuji pada 1.353 dataset URL dari *University of California, Irvine's ML Repository*. Model *Random Forest* merupakan model yang paling akurat diantara kedua model tersebut (RF and SVM). Namun, jika dibandingkan antara model *hybrid* yang diciptakan dengan masing-masing model secara berdiri sendiri, model *hybrid* menunjukkan signifikansi dalam hal keakuratan. Selain akurasi tes yang dilakukan juga meliputi *f1, precision, correlation coefficient, true positive rate and true negative rate*.

Kemudian, dengan mempertimbangkan beberapa penelitian tersebut, penulis menetapkan untuk menggunakan 3 model ML dalam penelitian ini. Berikut adalah 3 model yang dipilih beserta alasan penggunaannya:

Tabel 1. Model *Machine Learning*

	ML Model	Alasan
1	*Support Vector Machine* (SVM)	Merupakan sebuag model *supervised learning* yang umum digunakan untuk kategorisasi, terkenal karena efisiensinya dalam mengkategorikan bidang dimensi yang beragam.
2	*Decision Tree*	Sebuah model ML yang banyak digunakan secara luas, model ini menggunakan struktur seperti pohon untuk mendeskripsikan peristiwa dan potensi konsekuensinya dalam berbagai konteks.
3	*Random Forest*	Model *ensemble learning* untuk klasifikasi, regresi dan masalah lainnya, dengan *output* berupa serangkaian pilihan acak untuk mewakili kelas mayoritas.

Sumber: Hasil Olahan Penulis

Dataset* dan *Data Pre-Processing

Penulis memperoleh himpunan data URL *phishing* dan non-*phising* dari repositori dari *Phishtank* dan *University of New Brunswick*. Penulis menggunakan 19 fitur untuk ekstraksi fitur yang telah dibuat oleh Lakshmi dan Vijaya (2021) dan Mohammad, Thabtah dan McCluskey (2012), sebagai berikut:

Tabel 2. Fitur Adress Bar Himpunan Dataset

	Fitur Pada Address Bar	**Indikator**	**Kesimpulan**
1	Menggunakan IP sebagai alamat URL	Jika ditemukan	*Phishing*
2	Menggunakan symbol '@' pada alamat URL	Jika ditemukan	*Phishing*
3	Panjang URL	Lebih dari 54 karakter	*Phishing*
4	Kedalaman URL	Hitung simbol '/'	-

5	URL redirection	Bila ditemukan posisi simbol "//" diluar dari urutan ke 6 dan 7	*Phishing*
6	HTTPS palsu	Jika ditemukan	*Phishing*
7	Menggunakan URL shortening	Jika ditemukan	*Phishing*
8	Terdapat prefiks maupun sufiks symbol '-'	Jika ditemukan	*Phishing*
9	Jumlah subdomain	> 2	*Phishing*
10	Jumlah parameter yang digunakan	Hitung jumlah query dalam URL	-
11	Jumlah period pada URL	Hitung jumlah simbol '.'	-
	Fitur pada Domain		
12	Lakukan pengecekan DNS	Jika tidak ditemukan	*Phishing*
13	Cek web traffic (Alexa Rating)	Ranking > 100.000	*Phishing*
14	Cek sertifikat SSL	Jika tidak ditemukan	*Phishing*
15	Cek umur domain	< 6 bulan	*Phishing*
	Fitur berbasis pada HTML dan Javascript		
16	Pengalihan Iframe	Jika ditemukan	*Phishing*
17	Kostumisasi bar status	Jika ditemukan	*Phishing*
18	Right-click dinonaktifkan	Jika ditemukan	*Phishing*
19	Website forwarding	Jika > 2	*Phishing*

Sumber: *Phistank and University of New Brunswick repository* dan 19 fitur untuk ekstraksi oleh Lakshmi dan Vijaya (2021) dan Mohammad, Thabtah dan McCluskey (2012)

Selanjutnya, untuk mengklasifikasikannya maka data yang sudah diekstrak akan diberikan kode 1 untuk fitur yang dicurigai merupakan sebuah *phishing* dan 0 untuk fitur non-*phishing*. Kemudian data yang sudah diekstrak penulis gunakan untuk melatih model ML.

Metode Pengujian Model ML

Pengujian model ML dilakukan dengan menguji performa berdasarkan 4 kriteria penilaian yaitu: akurasi, presisi, *recall, dan f1-score*. Dalam pengujian performa yang dilakukan penulis menitik beratkan pada didapatkannya performa model ML yang seimbang, oleh karena itu pengujian *f1-score* sangat dibutuhkan dalam pengujian ini (M.D. Hossain et al., 2020). Tabel dibawah menjelaskan masing-masing pengujian performa yang dilakukan beserta *confusion matrix*.

Tabel 3. Nilai Klasifikasi

	Nilai diklasifikasikan positif	**Nilai diklasifikasikan negatif**
Actual Positive	*True Positive*	*False Negative*
Actual Negative	*False Positive*	*True Negative*

Sumber : Hasil Olahan Penulis

Tabel 4. 4 Kriteria Penilaian

	Pengujian	**Formula**	**Deskripsi**
1	Akurasi	*True Positive* + True Negative *nsamples*	Akurasi adalah jumlah TAPI dibandingkan dengan banyaknya data

2	Presisi	*True Positive* *True Positive + False Positive*	Presisi dapat dinyatakan baik apabila FP memiliki pengaruh yang signnifikan
3	*Recall*	*True Positive* *True Positive + False Negative*	*Recall* dikatakan baik apabila FN memiliki pengaruh yang signifikan
4	*F1-Score*	Presisi x Recall Presisi + Recall	*F1-Score* diperlukan apabila model yang membutuhkan keseimbangan antara Presisi dan *Recall*

Sumber: Hasil Olahan Penulis

Teknologi yang Digunakan

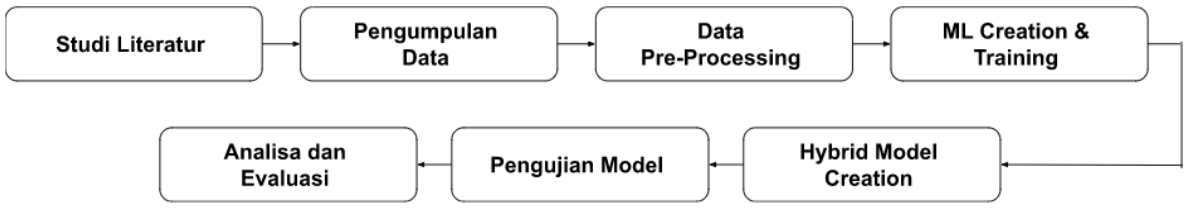
Figur di bawah menjelaskan berbagai perangkat lunak, baik teknologi maupun *environment* yang Penulis gunakan dalam penelitian ini, yaitu:

Sumber: Hasil Olahan Penulis

Gambar 1. Teknologi dan *Environment* yang digunakan Penulis pada penelitian ini

Metodologi Penelitian

Metode yang digunakan dalam penelitian ini adalah *Research and Development* (RnD). Metode penelitian *Research and Development* (R&D) adalah suatu pendekatan penelitian yang bertujuan untuk mengembangkan atau meningkatkan produk, proses, atau sistem. Penelitian ini terbagi atas beberapa bagian dalam prosesnya, yaitu: Pertama, melakukan pendalaman latar belakang termasuk di dalamnya studi literatur dengan membaca dan mempelajari beberapa penelitian terdahulu pada area penelitian yang sama serta menentukan teknologi yang akan digunakan. Kedua, proses pengumpulan dataset berupa link *phising* dan non-*phishing*. Ketiga, melakukan data pre-processing dengan metode ekstraksi fitur. Keempat, menyiapkan dan melatih 3 model ML (SVM, *Decision Tree, dan Random Forest*), Kelima, menyiapkan algoritma penggabungan 3 model ML untuk menciptakan model hybrid. Keenam, pengujian masing-masing model baik model yang berdiri sendiri maupun model hybrid berdasarkan 4 area penilaian (akurasi, presisi, *recall dan f1-score*). Ketujuh, analisis dan evaluasi hasil penelitian terhadap keempat model ML tersebut.



Sumber: Hasil Olahan Penulis

Gambar 2. Konsep Metode penelitian *Research and Development*(R&D)

Hasil dan Pembahasan

Link *phishing* dan pencurian data adalah bentuk serangan siber yang umum digunakan oleh penjahat dunia maya untuk mencuri informasi pribadi atau rahasia dari individu atau organisasi. Link *phishing* adalah teknik di mana penyerang mencoba untuk mendapatkan informasi rahasia, seperti nama pengguna, kata sandi, atau rincian keuangan, dengan menyamar sebagai entitas tepercaya. Ini sering dilakukan melalui email, pesan teks, atau media sosial, di mana korban diminta untuk mengklik tautan yang sebenarnya mengarah ke situs web palsu yang dirancang untuk mengekstrak informasi pribadi.

Link *phishing* sering digunakan sebagai salah satu metode untuk melakukan pencurian data. Pelaku *phising* akan mengirimkan *email*, pesan teks, atau pesan lain yang mengelabui pengguna agar mengklik tautan palsu yang mengarah ke situs web palsu yang menyerupai situs asli. Ketika pengguna memasukkan informasi pribadi mereka ke dalam situs palsu tersebut, data tersebut akan dicuri oleh pelaku *phising*. Cara umum di mana *link phishing* dapat dilakukan dengan:

1. *Email Phishing*: Penyerang mengirimkan email yang terlihat sah, sering kali menyamar sebagai layanan atau organisasi yang dikenal, dan meminta korban untuk mengklik tautan yang sebenarnya menuju situs palsu.
2. *Spear Phishing*: Jenis serangan ini melibatkan pendekatan yang lebih terfokus, di mana penyerang menargetkan individu atau organisasi tertentu dengan pesan yang dikustomisasi agar terlihat meyakinkan.
3. *Smishing (SMS Phishing)*: Serangan ini melibatkan penggunaan pesan teks atau SMS untuk mengarahkan korban ke situs *phishing*.
4. *Social Media Phishing*: Penyerang dapat menggunakan pesan atau tautan palsu di platform media sosial untuk mengecoh korban.

Pencurian data merupakan aksi mengambil, mengakses, atau mengumpulkan informasi pribadi atau rahasia tanpa izin, meliputi data pribadi, informasi keuangan, informasi medis, atau bahkan rahasia perusahaan. Pencurian data dapat terjadi melalui berbagai metode, termasuk serangan siber yang meliputi:

1. Serangan *Malware*: Penyebaran perangkat lunak berbahaya, seperti virus, trojan, atau ransomware, untuk mengakses dan mencuri data dari sistem korban.
2. Pengambilan Fisik: Pencurian perangkat penyimpanan, laptop, atau perangkat mobile yang berisi data sensitif.
3. Serangan *Man-in-the-Middle*: Penyerang mencuri atau menyadap data saat berpindah antara dua pihak yang berkomunikasi.
4. Pencurian Identitas: Penggunaan informasi pribadi seseorang untuk mendapatkan akses ke akun atau layanan lainnya.

Baik *link phishing* dan pencurian data, dapat menjadi ancaman serius terhadap keamanan informasi. Penting bagi individu dan organisasi untuk meningkatkan kesadaran akan risiko ini, mengadopsi praktik keamanan siber yang baik, dan menggunakan alat keamanan seperti perangkat lunak *antivirus, firewall*, dan enkripsi untuk melindungi data mereka (Clarke, 2010).

Pencurian data dapat memiliki konsekuensi serius bagi korban, termasuk pencurian identitas, penipuan keuangan, atau penggunaan data pribadi untuk tujuan jahat lainnya. Oleh karena itu, penting bagi pengguna untuk selalu waspada terhadap *link phishing* dan mengambil langkah-langkah untuk melindungi data pribadi mereka, seperti tidak mengklik tautan yang mencurigakan, menggunakan kata sandi yang kuat, dan mengaktifkan fitur keamanan tambahan seperti otentikasi dua faktor.

Link phishing adalah tautan palsu yang dirancang untuk menipu pengguna agar mengungkapkan informasi pribadi mereka, sementara pencurian data adalah tindakan mengambil atau mengakses data pribadi seseorang tanpa izin. *Link phishing* sering digunakan sebagai metode untuk melakukan pencurian data, dan pengguna perlu waspada dan melindungi data pribadi mereka dari ancaman ini.

Sedangkan *Machine Learning* (ML) adalah cabang dari kecerdasan buatan (*Artificial Intelligence*) yang berkaitan dengan pengembangan algoritma dan model komputer yang dapat belajar dari data dan melakukan tugas-tugas tertentu tanpa perlu secara eksplisit diprogram. Tujuan utama dari *machine learning* adalah untuk mengembangkan sistem yang dapat mengenali pola, membuat prediksi, dan mengambil keputusan berdasarkan data yang diberikan (Zhang dkk., 2014).

Pada dasarnya, *machine learning* melibatkan penggunaan algoritma dan model statistik untuk melatih komputer agar dapat mengenali pola dan membuat prediksi berdasarkan data yang diberikan. Proses ini melibatkan dua tahap utama: tahap pelatihan (*training*) dan tahap pengujian (*testing*). Pada tahap pelatihan, model machine learning diberikan data yang telah dilabeli (*labeled data*) dan menggunakan algoritma untuk menyesuaikan parameter agar dapat mengenali pola dalam data tersebut. Setelah pelatihan selesai, model tersebut dapat digunakan untuk melakukan prediksi atau mengklasifikasikan data baru pada tahap pengujian.

Ada beberapa jenis pendekatan dalam machine learning, termasuk *supervised learning, unsupervised learning,* dan *reinforcement learning*. Dalam *supervised learning*, model *machine learning* dilatih menggunakan data yang telah dilabeli dengan benar, sedangkan dalam *unsupervised learning*, model tersebut belajar dari data yang tidak dilabeli untuk menemukan pola atau struktur yang tersembunyi. Sementara itu, *reinforcement learning* melibatkan interaksi model dengan lingkungan untuk belajar melalui percobaan dan umpan balik.

Machine learning memiliki berbagai aplikasi yang luas, termasuk pengenalan wajah, pengenalan suara, analisis data, prediksi pasar, pengenalan pola, dan banyak lagi. Dalam beberapa tahun terakhir, perkembangan dalam teknologi komputasi dan ketersediaan data yang besar telah mendorong kemajuan pesat dalam bidang machine learning.

Multiple Machine Learning (Hybrid Model) merupakan pendekatan di mana dua atau lebih jenis metode atau model pembelajaran mesin digabungkan untuk meningkatkan kinerja dan keefektifan sistem. *Hybrid models* atau model hibrida mengintegrasikan kekuatan berbagai pendekatan pembelajaran mesin untuk menangani kompleksitas masalah yang lebih baik daripada model tunggal. Contoh umum dari *hybrid model* melibatkan kombinasi antara model parametrik dan model non-parametrik, model generatif dan model diskriminatif, atau bahkan gabungan antara pembelajaran terawasi dan tidak terawasi.

Dalam *multiple machine learning*, model-model yang berbeda dapat digunakan secara bersamaan atau secara bergantian. Misalnya, dapat digunakan kombinasi antara model regresi logistik, *decision tree*, dan *neural network* untuk meningkatkan kinerja prediksi. Pendekatan ini memungkinkan penggunaan berbagai teknik dan algoritma yang paling sesuai untuk setiap tugas atau masalah yang dihadapi. Salah satu contoh penerapan *multiple machine learning* adalah pada deteksi anomali. Dalam penelitian yang dilakukan oleh para peneliti, mereka menggunakan metode *multiple machine learning* yang menggabungkan *deep learning* dan *machine learning* tradisional untuk meningkatkan deteksi anomali.

Multiple machine learning, atau *hybrid model*, adalah teknik yang menggabungkan dua atau lebih model *machine learning* yang berbeda untuk meningkatkan kinerja. Teknik ini dapat digunakan untuk mengatasi berbagai macam tantangan dalam *machine learning*, seperti kurangnya data, data yang tidak seimbang dan kompleksitas data. *Hybrid model* dapat digunakan untuk

menggabungkan data dari berbagai sumber untuk meningkatkan kinerja model. *Hybrid model* dapat digunakan untuk menggabungkan model yang lebih baik dalam menangani data yang tidak seimbang. *Hybrid model* dapat digunakan untuk menggabungkan model yang lebih baik dalam menangani data yang kompleks. Beberapa contoh konsep *hybrid model* dalam konteks *machine learning*, antara lain:

1. *Ensemble Learning*: adalah salah satu bentuk *hybrid model* yang paling umum. *Ensemble learning* melibatkan penggabungan hasil dari beberapa model pembelajaran mesin untuk meningkatkan performa keseluruhan. Contoh termasuk *Random Forest*, yang menggabungkan beberapa pohon keputusan, dan *Boosting*, di mana model yang lemah digabungkan untuk membentuk model yang lebih kuat.
2. *Transfer Learning*: Model *transfer learning* menggunakan pengetahuan yang diperoleh dari satu tugas pembelajaran untuk meningkatkan kinerja pada tugas pembelajaran lainnya. Ini dapat melibatkan penggunaan model yang telah dilatih sebelumnya dan disesuaikan dengan tugas tertentu.
3. *Neuro-Fuzzy Systems*: *Hybrid model* ini menggabungkan konsep dari jaringan saraf (*neural networks*) dan sistem logika *fuzzy*. Sistem *neuro-fuzzy* dapat memanfaatkan kelebihan jaringan saraf, seperti kemampuan untuk memodelkan pola kompleks, dengan kelebihan sistem logika *fuzzy*, seperti kemampuan untuk menangani ketidakpastian dan ambiguitas.
4. *Genetic Algorithms + Machine Learning*: Algoritma genetika dapat digunakan untuk mengoptimalkan parameter model dalam konteks pembelajaran mesin. *Hybrid model* ini dapat membantu menemukan konfigurasi parameter yang optimal untuk model pembelajaran mesin.
5. *Rule-Based Learning + Neural Networks*: Dalam beberapa kasus, model hibrida dapat menggabungkan aturan-aturan berbasis pengetahuan dengan kemampuan pembelajaran mendalam dari jaringan saraf. Ini dapat membantu menggabungkan pengetahuan eksplisit manusia dengan kemampuan adaptasi dan generalisasi dari model *neural networks*.

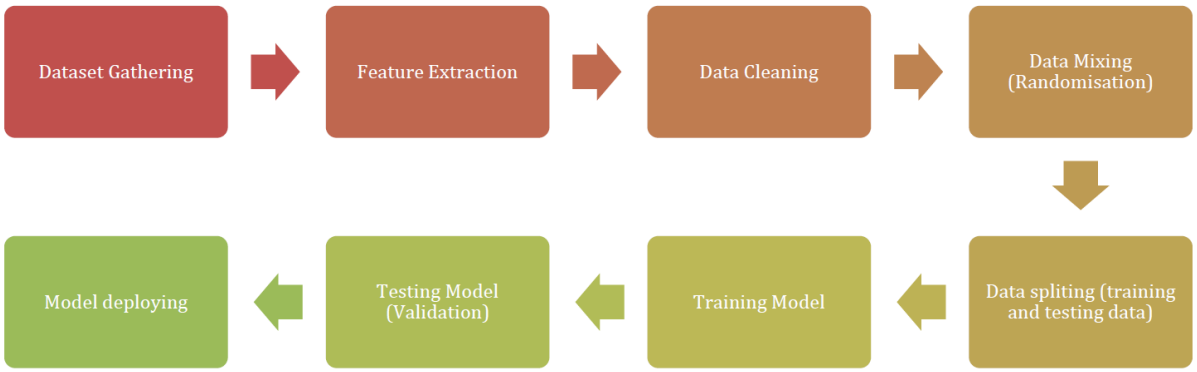
Dalam konteks lain, *multiple machine learning* juga dapat digunakan dalam analisis data tak terstruktur. Data tak terstruktur adalah data yang tidak memiliki format yang terstruktur seperti teks, gambar, atau suara. Dalam analisis data tak terstruktur, multiple machine learning dapat digunakan untuk menggabungkan berbagai teknik dan algoritma yang paling sesuai untuk menganalisis dan memahami data tersebut.

Multiple machine learning (hybrid model) adalah pendekatan dalam *machine learning* di mana beberapa metode atau model *machine learning* digabungkan untuk meningkatkan kinerja dan akurasi prediksi. Pendekatan ini memungkinkan penggunaan berbagai teknik dan algoritma yang paling sesuai untuk setiap tugas atau masalah yang dihadapi.

Alur ML *Deployment*

Proses penyusunan model ML dimulai dari pengumpulan dataset URL *phishing* dan non-*phishing*. Selanjutnya, penulis melakukan proses ekstraksi fitur terhadap dataset yang ada berdasarkan 19 fitur ada pada bagian data *pre-processing*. Data yang sudah diekstraksi kemudian dibersihkan untuk menghapus data dengan nilai *null* atau eror, setelah itu data dibagi menjadi 2 set untuk *training* dan *testing* dari model ML yang dibuat. Setelah data dibagi menjadi 2 set penulis melatih model ML yang dibuat menggunakan dataset untuk training serta men-*deploy* model ML tyang sudah dilatih. Figur di bawah mengilustrasikan *flowchart* dari proses pelatihan model ML, *testing*

hingga *deployment*. Dalam proses ekstraksi fitur penulis menyiapkan sebuah program berbasis bahasa *python* untuk mempercepat prosesnya menggunakan fungsi *looping* yang terotomatisasi. Proses ekstraksi fitur merupakan bagian terpenting untuk menghasilkan kualitas model ML yang baik. Dikarenakan proses ekstraksi fitur memerlukan *request* dan perintah *whois* pada *phishing* URL maka proses tersebut penulis lakukan pada sebuah *environment* terisolasi di dalam sebuah *sandbox*. Penulis menggunakan *Operating System (OS) Kali Linux* dalam sebuah *virtual box* dengan menggunakan jaringan *TOR* dan *Whonix gateway* yang dikombinasikan dengan *VPN* pada OS utamanya.



Sumber: Hasil Olahan Penulis

Gambar 3. Alur ML Deployment

Performa Model ML

Dalam proses pengujian performa model ML yang dibuat, pada proses data cleaning penulis menghapus beberapa fitur dari *dataset* untuk menghindari bias dari model ML untuk membedakan URL *Phishing* dan non-*Phishing*. Beberapa fitur yang dihapus dan alasan dihapusnya fitur rersebut diantaranya adalah sebagai berikut:

Tabel 5. Alasan fitur yang dihapus

	Fitur yang Dihapus	Alasan
	Jumlah tak tersembunyi	Hampir separuh data mengalami nilai timeout
	Jumlah hyperlink	Hampir separuh data mengalami nilai timeout
	Jumlah iframe	Hampir separuh data mengalami nilai timeout
	Script untuk menon-aktifkan *right-click*	Hampir tidak ada perbedaan antara URL *phishing* dan non-*phishing*

Sumber: Hasil Olahan Penulis

Selanjutnya, dataset dibagi menjadi 2 (dua) dengan rasio 80:20 untuk training dan testing terhadap 3 model ML yang sebelumnya sudah disampaikan pada bab sebelumnya. Kemudian masing-masing model yang telah dilatih dievaluasi tingkat akurasi, presisi, *recall* dan skor f1 nya dengan hasil sebagai berikut:

Tabel 6. Hasil Latihan model ML

No.	Model	Train Accuracy	Test Accuracy	Train Precision	Test Precision	Train Recall	Test Recall	Train F1-Score	Test F1-Score
1	DT	0.97912	0.925595	0.992272	0.948387	0.965414	0.896341	0.978659	0.921630
2	RF	0.97912	0.937500	0.990755	0.955414	0.966917	0.914634	0.978691	0.934579
3	SVM	0.90082	0.886905	0.946309	0.931507	0.848120	0.829268	0.894528	0.877419

Sumber: Hasil Olahan Penulis

Berdasarkan hasil pengujian tersebut, dapat dilihat bahwa model RF memiliki performa yang lebih baik dibandingkan dengan kedua model yang lain. Ketiga model ML tersebut selanjutnya dikombinasikan untuk menciptakan sebuah model ML baru, dan dilakukan pengujian yang sama terhadap model tersebut dengan hasil sebagai berikut:

Tabel 7. Hasil Uji Model ML Baru

No.	Model	Train Accuracy	Test Accuracy	Train Precision	Test Precision	Train Recall	Test Recall	Train F1-Score	Test F1-Score
1	Hybrid	0.97912	0.943452	0.992272	0.973856	0.965414	0.908537	0.978659	0.940063

Sumber: Hasil Olahan Penulis

Simulasi training model ML dan pengujian performa yang dilakukan dalam penelitian ini sudah diunggah secara online pada platform *IDE Google Colab* yang dapat dilihat dengan melakukan *scan* pada kode qr berikut atau dengan mengakses link berikut: https://tinyurl.com/y5ywr299.

Sumber: Hasil Olahan Penulis

Gambar 4. *Qr Code* Simulasi Training model ML

Kesimpulan dan Saran

Secara umum, model ML yang diciptakan dalam penelitian ini menunjukan hasil yang baik dengan performa yang mumpuni. Model hybrid yang merupakan gabungan dari ketiga model ML yaitu *Decision Tree, Random Forest dan Support Vector Machine* (SVM) mampu menunjukan performa

yang lebih unggul dibandingkan dengan masing-masing model berdiri sendiri. Skor yang didapatkan dari tes performa dari model hybrid yang dibuat diantaranya akurasi 94%, presisi 97% dan *recall* 96%. Model hybrid yang diciptakan juga mampu menunjukan skor f1 sebesar 94% yang mengindikasikan bahwa model tersebut memiliki keseimbangan antara presisi dan *recall*-nya.

Berkaca pada penelitian yang telah dilakukan oleh penulis, maka penulis menyarankan para peneliti yang berniat untuk melakukan penelitian yang serupa untuk memperkaya jumlah dataset yang digunakan agar hasil klasifikasi dan performa ML yang dihasilkan lebbih baik. Selain itu dalam data *pre-processing* peneliti juga dapat mengimbuhkan beberapa teknik ekstraksi fitur yang lain untuk meningkatkan kualitas dari ekstraksi fitur pada masing-masing URL seperti penggunaan citra dari tampilan suatu situs *web* agar diketahui ciri suatu situs web *phishing* tidak hanya dari URL saja.

Daftar Pustaka

Anti *Phishing* Working Group. (2016). *Phishing Activity Trends Report 4th 2016.*

Chiew, K.L., Yong, K.S.C. and Tan, C.L. (2018). A survey of phishing attacks: Their types, vectors and technical 'approaches', *Expert Systems with Applications, 106, pp. 1–20.*

Clarke, R. (2010). Situational Crime Prevention: Successful Case Studies, 2nd ed. Boulder: Lynne Rienner.

Google. (2021). *Google Transparency Report 2021.*

Hossain, M. D. et al. (2020). 'LSTM-Based Intrusion Detection System for In-Vehicle Can Bus 'Communications', *IEEE Access, 8, pp. 185489–185502.*

IBM. (2022). *Cost of Data Breach 2022.*

Journal, H. (2021). *July 2021 Healthcare Data Breach Report*. HIPAA Journal.

Kabir, M., Tayan, O., Alginahi, Y., Hasan, M. and Rahman, M. (2019). *On the development of a web extension for text authentication on Google Chrome 2019*. International Conference on Electrical, Computer and Communication Engineering (ECCE), Cox'sBazar.

Lakshmi, V. and Vijaya, M. (2012). Efficient prediction of phishing websites using supervised learning algorithms. *Procedia Engineering, 30, 798-805.*

Mohammad, R., Thabtah, F. and McCluskey, L. (2012). *Phishing Websites Features.* University Of Huddersfield Repository.

Pandey, A., Gill, N., Sai Prasad Nadendla, K. and Thaseen, I. (2019). Identification of Phishing Attack in Websites Using Random Forest-SVM Hybrid Model. *Advances In Intelligent Systems And Computing, 120-128.*

Phishtank. (2021). *Phishing Website Dataset. csv.*

Rebala, G., Ravi, A. and Churiwala, S. (2019). *Machine Learning Definition and Basics. An* introduction to machine learning. 1st ed. Springer, pp.1-17.

Rogers, Everett M. (1964). *Diffusion of innovations.* New York: Free Press of Glencoe.

Subasi, A., Molah, E., Almkallawi, F. and Chaudhery, T. (2017). *Intelligent phishing website detection using random forest classifier.* International Conference on Electrical and Computing Technologies and Applications (ICECTA). Ras Al Khaimah: IEEE.

Zhang, X., Zeng, Y., Jin, X. B., Yan, Z.W. and Geng, G. G. (2014). Boosting the Phishing Detection Performance by Semantic Analysis, in IEEE International Conference on Big Data (BIGDATA), 2014, pp. 1063-1070.