ISSN: 2503-054X
Vol. 9 No: 2, Oktober 2024

Deteksi Ciri Link Phishing Menggunakan Algoritma Random Forest Untuk Meningkatkan Keamanan Cyber

Felliks Feiters Tampinongkol
Universitas Bunda Mulia
Jakarta Utara, Indonesia
ftampinongkol@bundamulia.ac.id

Rozali Ilham
Institut Pemerintahan Dalam Negeri
Padang Sumatra Barat, Indonesia
rozali@ipdn.ac.id

Ahya Radiatul Kamila
Universitas Bunda Mulia
Jakarta Utara, Indonesia
akamila@bundamulia.ac.id

Yunianto Purnomo
Universitas Bunda Mulia
Jakarta Utara, Indonesia
ypurnomo@bundamulia.ac.id

Cevi Herdian
Universitas Bunda Mulia
Jakarta Utara, Indonesia
cherdian@bundamulia.ac.id

Stella Virginia
Universitas Bunda Mulia
Jakarta Utara, Indonesia
stellavirginia02@gmail.com

Abstract*— Keamanan data digital diera teknologi yang semakin berkembang menjadi salah satu fokus utama yang harus diantisipasi agar tidak terjadi pencurian data atau privasi. Data privasi berupa pesan elektronik (*email*), nama, nomer *handphone*, *password* sampai pada nomer rekening bank tidak boleh sampai diketahui oleh orang yang tidak bertanggung jawab, karena akan menyebabkan dampak yang serius seperti pembobolan rekening bank dan tindak *cybercrime* yang lain. Salah satu tindak kejahatan *cyber* yang marak terjadi adalah *link phishing*, yang membuat korban dapat terkecoh apabila tidak melihat *link* dengan lebih teliti. Dengan memanfaatkan teknologi *Artificial Intelligence* (AI) dan *Machine Learning* (ML) dapat dibuat suatu *system* yang mampu mendeteksi apakah *link* tersebut terkategori sebagai *link phishing* atau *legitimate link*. Suatu *link* dapat dikatakan sebagai *phishing* atau *legitimate* itu dapat dilihat dari karakteristik *link* tersebut (*features*). Setiap *link* memiliki domain yang unik, keunikan dari domain ini yang digunakan sebagai nilai masukan pada *system* AI dan diproses menggunakan algoritma *Random forests classification*. Berdasarkan dengan hasil yang diperoleh *system* AI yang dirancang menggunakan *random forest classification* dapat memprediksi atau membedakan *link phishing* atau *legitimate* sebesar 0.77% sebagai nilai akurasi model, dengan menggunakan 6 *features* untuk digunakan sebagai *data training*. Penggunaan data link dan penambahan features yang akan digunakan sebagai data latih juga dapat dilakukan untuk meningkatkan akurasi dan presisi dari model yang telah diperoleh.

Kata kunci — Cyber, Features extraction, Link, Phishing, Random forests.

I. PENDAHULUAN

Keamanan data digital saat ini menjadi upaya yang serius dan terus dilakukan pencegahan agar data yang bersifat privasi pada dunia digital jauh dari serangan orang yang tidak bertanggung jawab atau biasa dikenal dengan *cyberattack* [1]. Penyerang cenderung memanfaatkan dan mengeksploitasi target (*user*) yang kurang memahami akan keamanan data digital, beserta dengan etika dalam lingkup dunia digital yang bertujuan untuk mengambil informasi dari pengguna [2]. Berbagai jenis serangan yang pernal dilakukan oleh pelaku kejahatan *cyber* dan menimbulkan dampak yang merugikan, mulai dari pencurian informasi data pribadi, gangguan layanan dalam berbagai sektor industri, sampai dengan kerugian harta dan benda [3]. Salah satu cara yang sering digunakan untuk mengambil data pengguna adalah dengan menggunakan *link phishing*.

Phishing link merupakan tindak kejahatan *cyber* yang memanfaatkan teknik psikologis manusia dan juga melakukan rekayasa sosial untuk memanipulasi tautan situs *website* tertentu agar menyerupai dengan *link* tautan asli [4]. Serangan *phishing* dapat dilakukan melalui berbagai media. Tiga media yang umum digunakan yaitu: internet, layanan pesan singkat, serta pesan suara [5]. Pelaku merancang tampilan situs internet dan tautan menjadi sangat mirip dengan situs asli, sehingga pengguna awam sulit mengidentifikasi originalitas dari suatu tautan. Pengguna akan diarahkan untuk memasuki tautan palsu lewat pesan singkat atau pesan suara dan meminta agar korban mengisi data diri seperti nama, kata sandi, kartu kredit, serta informasi pribadi lainnya [6]. Dengan meyakinkan korban bahwa *link* yang dikirim adalah milik instansi atau organisasi resmi, hal ini memungkinkan korban bersedia untuk melakukan tindakan tertentu tanpa sadar bahwa identitasnya telah diakses secara ilegal [7]. Semakin maraknya tindakan kejahatan seperti ini tentu menimbulkan kewaspadaan dalam mengakses suatu *link website*. Sehingga kejahatan dengan menggunakan *link phishing* harus disikapi dengan serius agar dapat mengurangi dampak yang serius seperti kerugian atau kehilangan data pribadi tanpa disadari dari pengguna media sosial.

Dengan memanfaatkan perkembangan teknologi informasi dalam keamanan suatu sistem pencegahan dan penanganan yang timbul akibat masalah *link phishing* dapat dikurangi. Salah satu upaya yang dapat dilakukan adalah dengan memberikan tambahan keamanan saat pengguna masuk untuk mengakses situs *website* seperti otentikasi data pengguna [8]. Namun tindakan pencegahan seperti ini memerlukan perangkat dan biaya tambahan sehingga kurang efisien untuk penerapan jangka panjang. Oleh karena itu, selain kesadaran masyarakat untuk melakukan identifikasi dan lebih berhati-hati terhadap suatu tautan *link*, perlu juga adanya sistem dari perangkat lunak yang dapat mendeteksi *link phishing* secara otomatis dengan menggunakan pendekatan *Artificial Intelligence* (AI) [9]. Berdasarkan dengan hasil penelitian yang telah dilakukan oleh [10] *link phishing* yang dibuat semirip mungkin dengan *link website* asli dapat memiliki penciri seperti slash, question mark, dots, hyphens, underscore, equal signs, semicolon, dan ampersands. Penciri tersebut dijadikan patokan bagi pelaku untuk merancang *link* (tautan) yang menyerupai instansi tertentu dengan harapan

ISSN: 2503-054X
Vol. 9 No: 2, Oktober 2024

pengguna awam dapat percaya bahwa situs tersebut adalah situs resmi. Secara umum akan sangat sulit membedakan suatu tautan merupakan situs asli atau phishing. Namun jika dibuatkan dalam bentuk suatu *system link phishing*, *link* akan dapat dideteksi berdasarkan dengan penciri yang terdapat dari *link phishing* atau bukan.

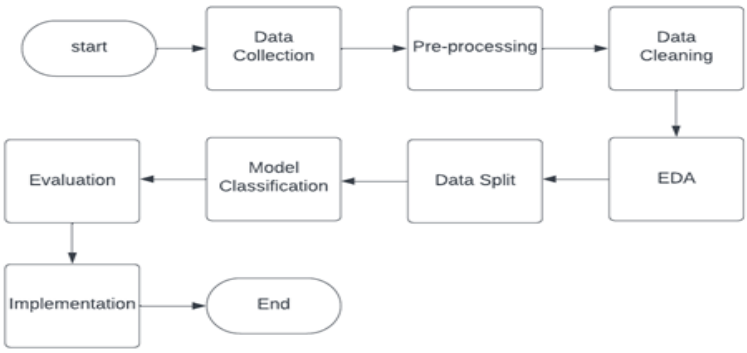
Pendekatan *supervised learning* dalam metode *Machine Learning* (ML) dapat digunakan dalam melakukan proses identifikasi dua atau lebih *object* target yang telah diketahui ciri pembedanya. *Ensemble Classification* merupakan salah satu metode dalam ML yang menggabungkan beberapa *training model* untuk meningkatkan hasil akurasi serta menurunkan kompleksitas dalam waktu bersamaan [11]. Dengan menggunakan metode ini algoritma klasifikasi dapat digabungkan untuk melakukan kombinasi acak, dan juga membandingkan prediksi terbaik. Sehingga, penelitian ini akan menggunakan algoritma *Random Forest* dengan metode *stacking ensemble classification* untuk mencari model yang sesuai yang dapat membedakan *link phishing* atau *legitimate*. *Random forest* merupakan algoritma ML yang menggunakan *tree* (pohon) sebagai cara untuk memisahkan *feature* (ciri) suatu *object* berdasarkan target yang sesuai [12]. Algoritma ini dikatakan *random* (acak) karena pada proses pembuatan *tree* dilakukan secara acak untuk memastikan setiap *tree* memiliki informasi yang berbeda. Setiap *tree* yang terbentuk melakukan kombinasi *features* dan baris data pada dataset untuk mendapatkan nilai prediksi setiap data *training*. Tahapan selanjutnya dari semua nilai prediksi yang dilakukan pendekatan mayoritas untuk melihat nilai hasil frekuensi *tree* yang paling banyak muncul. Nilai yang dipilih menunjukkan kemunculan *trees* paling banyak [13].

Penelitian ini bertujuan untuk mengembangkan system yang dapat mengidentifikasi *link phishing* berdasarkan dengan pendekatan *features* yang akan digunakan dengan data input berupa URL Website dan juga dapat meningkatkan kesadaran akan bahaya dari *link phishing*. Metode yang diterapkan pada penelitian ini adalah pendekatan ML menggunakan *ensemble classification*, yaitu algoritma *Random Forest*. Hasil penelitian diharapkan dapat menjadi salah satu cara mencegah serangan *phishing* yang banyak terjadi saat ini serta mengedukasi pengguna media sosial akan keamanan dalam melakukan kegiatan dalam dunia digital.

II. METODOLOGI PENELITIAN

A. *Serangan Phishing dan Tahapan Penelitian*

Serangan *phishing* merupakan salah satu serangan *cyber* yang memanfaatkan teknik rekayasa sosial untuk memanipulasi korban agar percaya dan masuk kedalam situs palsu, sehingga memungkinkan pelaku untuk mengambil informasi pribadi dari target [12]. Beberapa jenis phishing yang cukup banyak terjadi antara lain *phishing* konvensional, *spear phishing*, *whaling phishing*, *vishing*, *pharming*, *clone phishing*, *man-in-the-middle phishing*, *search engine phishing*, dan *session hijacking* [14]. Dalam penelitian ini serangan *phishing* yang merupakan objek pengamatan yang akan dimodelkan menggunakan metode *Random Forest*. Data yang digunakan berupa tautan *link website* yang terkonfirmasi sebagai *phishing* atau *legitimate*. Selanjutnya dilakukan *pre-processing* untuk memastikan ciri yang akan digunakan pada penelitian yang relevan serta berfokus pada ciri yang informatif untuk pembaca.



Gambar 1. *Flowchart* dan Tahapan Penelitian

Tahapan dalam penelitian ini data *link phishing* yang merupakan objek pengamatan akan diidentifikasi berdasarkan dengan tujuh tahapan yaitu: *pre-processing*, *data cleaning*, EDA (*exploratory data analysis*), *data split*, *classification model*, *evaluation* dan *implementation*. Sumber data yang digunakan dalam penelitian ini menggunakan sumber data dari website kaggle https://www.kaggle.com/ yang dapat diunduh secara gratis dan tambahan data *link* dari sumber yang lain. Dalam *pre-processing* data yang diperoleh diidentifikasi terlebih dahulu terkait dengan (*features*) penciri apa saja yang dapat digunakan dan yang dapat mendefinisikan *link* sebagai *phishing* atau *legitimate*. Tahapan penelitian dapat dilihat pada Gambar 1.

Tabel 1. *Features Explanation*

Features	Explanation
Panjang URL (length_url)	: Menghitung total panjang link URL
Panjang Hostname (length_hostname)	: Menghitung total panjang hostname URL
URL Ratio Digits (ratio_digits_url)	: Menghitung perbandingan nilai ratio digit pada URL
URL Ratio Host	: Menghitung perbandingan nilai ratio digit pada hostname
Domain com	: Terdapat .com atau tidak pada URL

ISSN: 2503-054X
Vol. 9 No: 2, Oktober 2024

Domain www	: Terdapt www atau tidak pada URL

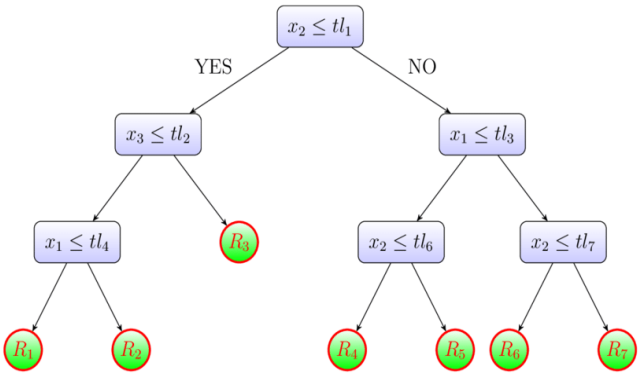
Proses *data cleaning* merupakan proses untuk membersihkan data yang diperoleh dari *features* yang tidak akan digunakan dalam melakukan pemodelan dalam *machine learning* (ML). Dalam penelitian ini terdapat 6 *features* yang akan digunakan dalam pemodelan terdiri dari *uniform resource locator* (*url*) *length*, *hostname length*, *ratio digits url*, *ratio digits host*, *com* dan *www*. Penjelasan setiap *features* dapat dilihat pada Tabel 1.

B. *Pre-processing and Data Cleaning*

Pre-processing merupakan tahapan awal yang dilakukan untuk mengolah data mentah menjadi data yang siap untuk diolah pada proses modeling data atau *training* data. Dalam tahapan *pre-processing* juga melakukan cleaning dataset berupa memilih penciri (*features*) yang akan digunakan, tidak semua *features* yang terdapat pada raw akan digunakan. Untuk *features* yang digunakan dapat dilihat pada Tabel 1. Pemilihan *features* di dasarkan pada studi literatur dan juga mempertimbangkan komputasi yang akan dihasilkan apabila semakin banyak *features* map yang digunakan [15]. *Pre-processing* dan *cleaning* data merupakan salah satu proses awal yang harus dilakukan untuk mengoptimalkan pemodelan data agar setiap *features* (penciri) dapat sesuai dengan model pengamatan yang akan dilakukan [16-17]. Penggunaan dataset yang tepat akan dapat mengurangi kesalahan dalam klasifikasi model, sehingga model yang dihasilkan dapat merepresentasikan data yang menjadi data masukan.

C. *Random Forests Classification*

Random Forest adalah salah satu algoritma pembelajaran terawasi (*supervised learning*) yang memanfaatkan data pelatihan (*training data*) yang terdiri dari variabel independen (*features*) dan variabel dependen (*label*). Algoritma *Random Forest* termasuk di antara algoritma *Machine Learning* (ML) yang paling *robust*, yang didasarkan pada konsep algoritma (*decision tree*) pohon keputusan. Dalam *Random Forest*, setiap *variable* dan sampel dataset dipilih secara acak dan beragam untuk membentuk satu pohon keputusan tunggal. Dari setiap variabel yang terpilih secara acak tersebut, algoritma *Random Forest* akan menentukan pemisah *optimal* untuk digunakan dalam proses klasifikasi [18].



Gambar 2. *Decision Tree Architecture*

Salah satu teknik yang digunakan dalam *Random Forest* adalah *Bagging*, dimana beberapa pohon keputusan dibangun berdasarkan sampel data yang diambil secara acak. Setiap pohon keputusan menggunakan sampel data yang diambil secara acak (*random*) dengan penggantian dari dataset asli, yang berarti beberapa sampel memiliki peluang muncul lebih dari satu kali, sementara yang lain mungkin tidak muncul sama sekali. Setiap sampel tersebut kemudian digunakan untuk membangun satu pohon Keputusan. Berdasarkan dengan hasil penelitian oleh [19] yang dapat dilihat pada gambar 2 menjelaskan proses yang terjadi pada setiap pohon dapat memiliki ketentuan pemilihan *feature* yang berbeda dan struktur yang unik berdasarkan *subset* data yang digunakan. Variable $x = [x_1, x_2, x_3]$ merupakan inputan data, yang akan dipisahkan (*split*) menggunakan *rules* $tl_1 - tl_7$ yang telah didefinisikan dan *leaf* yang didefinisikan sebagai $R_1 - R_7$ merupakn hasil *region* dari model *decision tree*. Setelah model-model (*trees*) terpisah terbentuk, masing-masing *tree* digunakan untuk membuat prediksi terhadap testing data atau data yang tidak digunakan dalam membangun model *tree* tersebut.

D. *Model Evaluation*

Tahapan terakhir penelitian dilakukan dengan melakukan evaluasi terhadap kinerja model. *Confusion matrix* merupakan salah satu teknik yang dapat digunakan untuk mengukur serta mengevaluasi kinerja model klasifikasi. Didalam *confusion matrix* terdapat empat parameter yang menjadi patokan pengukuran yaitu: *True Positive* (TP) menunjukkan jumlah prediksi yang benar dari data positif, *False Positive* (FP) menunjukkan banyak prediksi salah dari data positif, *False Negative* (FN) menunjukkan jumlah prediksi salah dari data negatif, dan *True Negative* (TN) yang menunjukkan jumlah data benar dari data negative [20]. Perhitungan dapat dilakukan berdasarkan dengan persamaan (1) *Accuracy*, (2) *Precision*, (3) *Recall* dan (4) F1-*Score*:

$$Accuracy = \frac{TP+TN}{(TP+FP+FN+TN)} \times 100\% \quad (1)$$

$$Precision = \frac{(TP)}{(TP+FP)} \times 100\% \quad (2)$$

ISSN: 2503-054X
Vol. 9 No: 2, Oktober 2024

Accuracy (akurasi) adalah nilai yang didapat untuk mengetahui tingkat keakuratan sistem klasifikasi data. *Precision* (presisi) adalah nilai untuk mengetahui jumlah data positif yang diklasifikasikan dengan benar dibagi dengan total data positif. *Recall* adalah nilai untuk mengetahui persentase data kategori positif yang diklasifikasikan dengan tepat oleh sistem yang dibuat. *F1-Score* adalah nilai *harmonic mean* dari presisi dan *recall*. Nilai *F1-Score* memiliki *range* [0-1].

$$Recall = \frac{TP}{(TP+FN)} \times 100\% \quad (3)$$

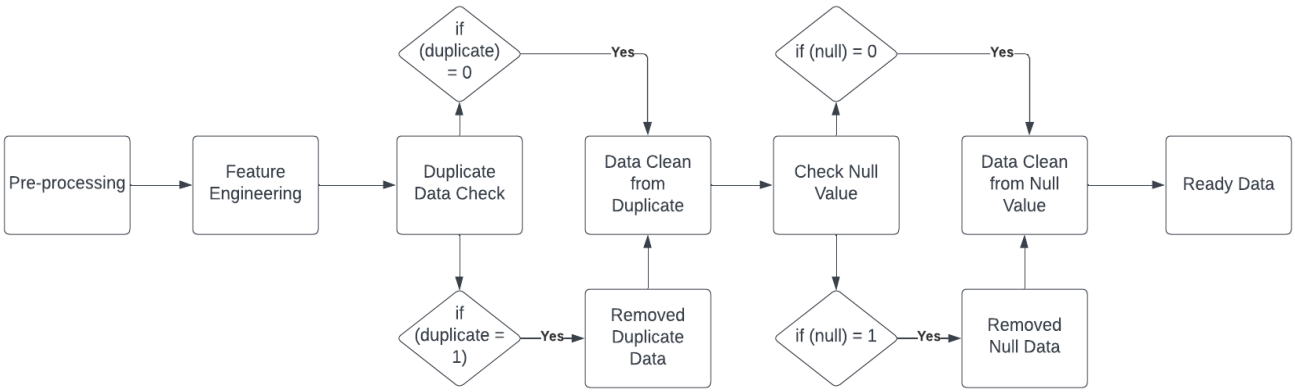
$$F1 - Score = \frac{2 \times Precision \times Recall}{Precision + Recall} \times 100\% \quad (4)$$

III. HASIL DAN PEMBAHASAN

Proses akuisi data dilakukan dengan mengambil data sekunder melalui halaman website https://www.kaggle.com/ yang bersifat terbuka (*opensource*) untuk semua *user*. Data yang digunakan dalam *website* berupa data tautan (URL) *uniform resource locator* yang terkonfirmasi *phishing* dan *legitimate*. Selain itu, diambil juga dataset dari sumber yang lain berdasarkan pada sumber *website* https://phishtank.org/ sebagai dataset ke-2 untuk mendapatkan model latih yang lebih bervariasi. Data *collection* seperti pada tahapan pertama dalam Gambar 1, merupakan tahapan awal untuk mengumpulkan informasi berupa link yang akan diolah. Selain menggunakan sumber dari dua *website* penyedia data *opensource*, penelitian ini juga menggunakan data primer yang dikumpulkan dari link URL perbakan *local*, *website* organisasi dan pemerintahan.

A. *Pre-processing*

Tahapan *pre-processing* dilakukan dengan membagi dataset keseluruhan yang diperoleh dari data *collection* menjadi data latih (data *train*) dan data uji (data *test*). Perbandingan antara data *train* dengan data *test* sebesar 80%:20%. Data train digunakan melatih model untuk memprediksi *link phishing* menggunakan model *machine learning* (ML) yang telah ditentukan, yaitu Random Forest, sedangkan data uji digunakan untuk menguji model berdasarkan model prediksi yang telah dibuat dari data train tersebut. Selanjutnya adalah proses pemetaan status untuk *dependent variable* dan *independent variable*. *Dependent variable* pada kasus ini adalah link *phishing*, pemetaan dilakukan dengan mengubah nilai status pada dataset dimana awalnya merupakan tipe data string (*phishing* dan *legitimate*) menjadi tipe data numerik. Bilangan '0' mewakili status *legitimate* serta '1' mewakili status *phishing*.



Gambar 3. *Flowchart Pre-processing*

Dalam Gambar 3 dapat dilihat proses yang dilakukan sebelum data siap untuk dimodelkan. *Raw* data dilakukan pengecekan untuk *duplicate data* apabila terjadi duplikasi maka, data tersebut akan dibuang (*drop out*) dari dataset. Selanjutnya melakukan pengecekan *missing value* atau *Null value* agar tidak akan terjadi kesalahan pengolahan pada *system*. Setelah semua proses selesai dilakukan maka dataset yang diperoleh merupakan dataset yang siap untuk dilakukan pemodelan. Tahapan awal terkait dengan *feature engineering* dapat dilihat pada Tabel 1.

B. *Features engineering*

Berdasarkan dataset yang digunakan untuk membangun model prediksi link *phishing*, terdapat dua variabel utama, yaitu URL dan status. Untuk menentukan parameter apa saja yang dapat dijadikan sebagai indikator dari suatu link (URL) *phishing* maka perlu dilakukan teknik *features engineering*. Rekayasa fitur pada kasus ini dilakukan dengan membuat perhitungan manual berdasarkan URL yang ada dan memilih penciri (*feature*) yang akan digunakan berdasarkan literasi jurnal dan publikasi. Penciri yang ditampilkan pada Tabel 1 merupakan variabel independen yang dibuat melalui perhitungan manual, selanjutnya status adalah variabel dependen yang telah ada berdasarkan pada dataset.

- URL Ratio Digits: merupakan perbandingan antara jumlah karakter *digit* dalam tautan dengan total panjang tautan. Rasio ini dapat dihitung menggunakan persamaan (5).

$$URL\ Rasio\ Digit = \frac{Jumlah\ Digit\ URL}{Total\ Panjang\ URL} \quad (5)$$

ISSN: 2503-054X
Vol. 9 No: 2, Oktober 2024

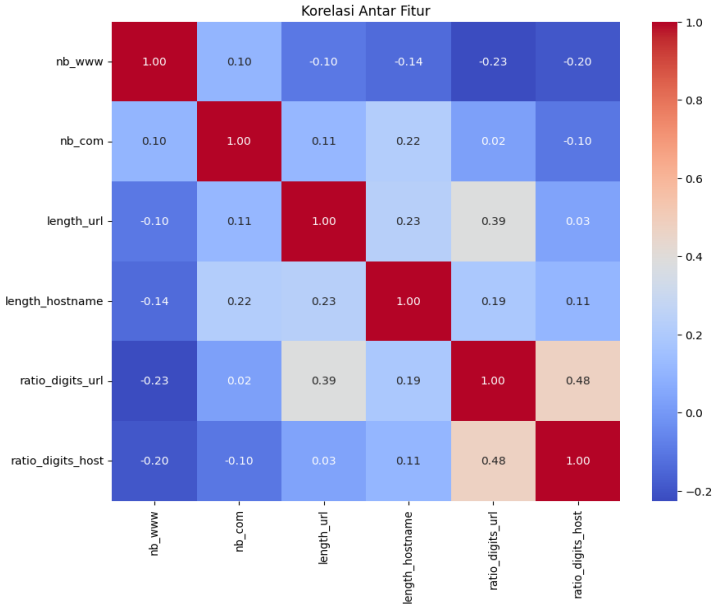
- URL Ratio Host: merupakan perbandingan antara jumlah karakter digit dalam URL *hostname* dengan total panjang *hostname*. Rasio ini dapat dihitung menggunakan persamaan (6).

$$URL\ Rasio\ Host\ = \frac{Jumlah\ Digit\ Hostname}{Total\ Panjang\ Hostname} \quad (6)$$

- Panjang URL: *Link website* seringkali menggunakan tautan yang panjang dan rumit dengan kombinasi huruf dan karakter, tujuan untuk mengecoh korban agar sulit teridentifikasi. Nilai Panjang URL dengan menghitung berapa jumlah karakter yang terdapat pada URL tersebut.
- Panjang Hostname: Hostname merupakan salah satu penciri yang merupakan *host* dari panjang suatu URL. Pelaku seringkali membuat domain yang sangat mirip dengan situs asli serta menyisipkan karakter ekstra untuk mengecoh korban. Nilai hostname diambil kemudian dikonversi menjadi objek string untuk memastikan panjang tautan sudah benar.
- Domain com: Keberadaan subdomain 'com' menjadi salah satu fitur yang digunakan dalam mendeteksi phishing. Nilai '1' mengindikasikan ditemukan '.com' didalam host URL, sedangkan nilai '0' mengindikasikan bahwa '.com' tidak ditemukan.
- Domain www: Keberadaan subdomain 'www' menjadi salah satu fitur yang digunakan dalam mendeteksi phishing. Sama seperti pada subdomain .com apabila bernilai 1 maka 'www' teridentifikasi dalam host dan '0' maka keberadaan 'www' tidak ditemukan dalam link tersebut.

C. EDA (*Exploratory Data Analysis*)

Analisis data eksploratif merupakan suatu proses awal dalam analisis data yang dilakuakan bertujuan untuk memahami karakteristik, menemukan pola, mendeteksi anomali, menguji hipotesis, dan memeriksa asumsi melalui metode statistik dan representasi secara visual. EDA membantu dalam mengidentifikasi struktur data, hubungan antar variabel, serta memberikan informasi awal yang digunakan dalam proses pemodelan data selanjutnya. Tahapan EDA yang dilakukan dalam penelitian ini adalah matriks korelasi dan penentuan.



Gambar 4. Matriks Korelasi

Matriks korelasi dapat dilihat pada gambar 4, terlihat korelasi atau hubungan antar setiap penciri yang terdapat pada dataset. Nilai 1 pada diagonal utama matriks korelasi mengartikan hubungan yang kuat antar dirinya sendiri. Sebaliknya, matrix yang memiliki korelasi rendah adalah matrix yang warna merah pudar atau biru. Berdasarkan grafik yang ditampilkan pada matriks korelasi, terdapat beberapa pasangan fitur yang memiliki korelasi signifikan untuk dapat digunakan sebagai parameter dalam sistem deteksi link phishing. Seperti korelasi yang terjadi antara ratio_digits_host dan ratio_digits_url yang memiliki nilai korelasi sebesar 0.48, selanjutnya nilai length_url dan ratio_digits_url juga memiliki hubungan sebesar 0.39. Informasi ini dapat menjadi masukan terhadap proses yang akan dilakukan selanjutnya.

D. *Model Classification*

Dalam tahapan ini model *classification* yang digunakan adalah *random forest calassification*. Berdasarkan dengan data dan informasi yang telah diperoleh selanjutnya dataset dilakukan pemodelan *training* data dengan perbandingan 80% data *train* dan 20% *testing* data dari keseluruhan data yang digunakan. *Training* model dilakukan menggunakan K-fold cross validation dengan menggunakan K = 5 sebagai iterasi dalam pembuatan model dapat dilihat pada Tabel 2.

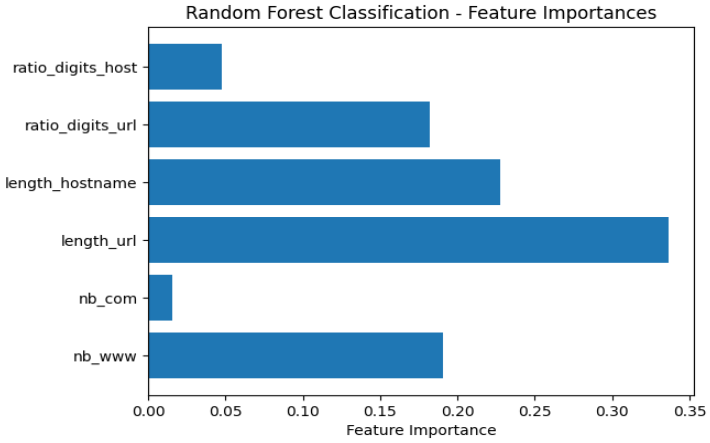
Tabel 2. K-*fold Cross Validation*

K-*fold*	Estimator	Akurasi
1	30	0.759142496847414

ISSN: 2503-054X
Vol. 9 No: 2, Oktober 2024

2	10	0.786885245901639
3	40	0.798234552332913
4	100	0.783102143757881
5	20	0.804539722572509

Berdasarkan algoritma yang digunakan juga dilakukan optimasi parameter untuk meningkatkan kinerja model dalam mendeteksi link phishing. Pencarian grid dilakukan untuk mencari kombinasi parameter terbaik yang memberikan nilai tertinggi untuk matrix evaluasi. Model pertama memiliki akurasi sebesar 0.7591 dengan jumlah estimator sebanyak 30. Model kedua memiliki akurasi sebesar 0.7868 dengan jumlah estimator sebanyak 10. Model ketiga memiliki akurasi sebesar 0.7982 dengan jumlah estimator sebanyak 40. Model keempat memiliki akurasi sebesar 0.7831 dengan jumlah estimator sebanyak 100. Model kelima memiliki akurasi sebesar 0.8045 dengan jumlah estimator sebanyak 20. Nilai rata-rata akurasi dari 5 model yang dihasilkan sebesar 0.7863. Berdasarkan hasil optimasi hyperparameter dapat dilihat bahwa model terbaik untuk deteksi link phishing adalah model kelima, dengan akurasi tertinggi yaitu 0.8045 atau 80.45%. Namun nilai rata-rata dari semua model cukup konsisten berada pada akurasi 0.7863 atau 78.63%, dan menunjukkan bahwa model memiliki kinerja yang relatif sama.



Gambar 5. *Features Importance*

Berdasarkan hasil *Feature Importance* pada Gambar 5, terdapat beberapa fitur yang memiliki pengaruh signifikan dalam mendeteksi link phishing, 3 dari 6 fitur diantaranya adalah panjang url, panjang hostname, dan rasio digit url. Panjang url (length_url) memiliki (penciri) *feature importance* tertinggi, menunjukkan bahwa link dengan panjang tidak proporsional dapat menjadi indikasi suatu link phishing. Panjang hostname (length_hostname) juga memiliki pengaruh signifikan, hostname yang memiliki panjang tidak biasa (terlalu pendek atau terlalu panjang) dapat menjadi penciri link phishing. Rasio digit url (rasio_digit_url) menjadi fitur signifikan yang berada pada urutan ke -3, yang menunjukkan bahwa rasio digit yang tinggi memiliki kecenderungan adanya manipulasi atau pemalsuan link. Hasil analisis data dapat disimpulkan bahwa 3 fitur tersebut memiliki peran yang sangat penting dalam deteksi link phishing. 3 fitur lain yang digunakan, yakni nb_www, rasio_digit_host, dan nb_com menunjukkan hasil yang sedikit, menunjukkan bahwa ketiga fitur tersebut memiliki pengaruh yang sedikit atau kurang signifikan. Atau dapat diartikan penciri tersebut tidak dapat dijadikan acuan awal sebagai parameter untuk mendeteksi link phishing.

E. *Model Evaluaation*

Evaluasi kinerja model Random Forest dilakukan menggunakan *confusion matrix*. Berdasarkan pada Tabel 3 *Confusion Matrix*, terdapat 643 link yang benar merupakan link phishing dan diprediksi benar oleh model sebagai phishing. Terdapat 201 link yang sebenarnya legitimate namun diprediksi phishing oleh model. Terdapat 158 link yang sebenarnya phishing namun diprediksi legitimate oleh model. Terdapat 592 link yang benar merupakan link legitimate dan diprediksi benar oleh model sebagai legitimate. Akurasi diperoleh berdasarkan hasil data yang benar diklasifikasikan phishing ditambah dengan data yang benar diklasifikasikan sebagai legitimate dibagi oleh keseluruhan data uji. Akurasi secara keseluruhan adalah 0.775, yang menunjukkan bahwa model berhasil memprediksi dengan benar 77.5% dari total data uji phishing.

Tabel 3. *Confusion Matrix*

		Actual	
		Phishing	**Legitimate**
Predicted	**Phishing**	643	158
	Legitimate	201	592

ISSN: 2503-054X
Vol. 9 No: 2, Oktober 2024

Precision didapat berdasarkan hasil data yang benar diklasifikasikan phishing dibagi dengan jumlah antara data yang benar klasifikasinya ditambah data phishing yang salah diprediksi sebagai legitimate. Untuk link phishing, presisi adalah 0.76, yang berarti 76% dari link yang diprediksi sebagai phishing oleh model sebenarnya adalah phishing. Untuk link yang sah, presisi adalah 0.79, yang berarti 79% dari link yang diprediksi sebagai *legitimate* dan model memprediksi sebagai link yang legitimate.

Recall didapat berdasarkan hasil data yang benar diklasifikasikan legitimate dibagi dengan jumlah antara data yang benar diklasifikasikan legitimate dengan data legitimate yang diklasifikasikan sebagai phishing. Untuk link phishing, recall adalah 0.80, yang berarti model berhasil mendeteksi 80% dari keseluruhan link phishing yang ada. Untuk link yang sah, recall adalah 0.75, yang berarti model berhasil mendeteksi 75% dari keseluruhan link legitimate. Nilai F1-Score data phishing adalah 78%, dan nilai F1-Score untuk legitimate adalah 77%.

Tabel 4. *Evaluation Tabel*

	Precision	**Recall**	**F1-Score**	**Support**
0	0.76	0.80	0.78	792
1	0.79	0.75	0.77	793
		Accuracy	0.77	1585
Macro avg	0.77	0.77	0.77	1585
Weighted avg	0.77	0.77	0.77	1585

IV. KESIMPULAN

Model machine learning yang digunakan dalam penelitian ini dapat mengidentifikasi status website sebagai phishing atau legitimate dengan akurasi sebesar 0.775% secara rata-rata dengan nilai precision 0.7% dan F1-*Score* diangka yang sama, yang mengartikan model sangat konsisten dalam mengidentifikasi pola dari 6 pencir (*feature*) yang digunakan dalam melakukan pemodelan dengan algoritma *random forest*. Dalam implementasi model juga mampu memprediksi dengan cukup baik terkait dengan URL yang dijadikan sebagai masukan untuk diprediksi, kesalahan model yang didapatkan ketika link URL terlalu panjang dengan kombinasi karakter yang banyak dan angka yang mana link tersebut merupakan link resmi (*legitimate*), tetapi diprediksi oleh model merupakan link phishing. Hal ini mungkin terjadi karena akurasi model yang masih diangka 0.78% dan *features* yang digunakan juga masih terlalu sedikit untuk dicoba. Untuk pengembangan selanjutnya disarankan untuk menambahkan features yang dapat merepresentasikan penciri dari link apakah phishing atau bukan.

PENGAKUAN

Makalah ini adalah sebagian dari Penelitian Hibah Kolaboratif Nasional milik anggota team penulis dan disponsori oleh Universitas Bunda Mulia (UBM). Penulis mengucapkan terima kasih untuk semua anggota team peneliti yang terlibat aktif dalam proses penelitian ini dan juga untuk kampus Universitas Bunda Mulia yang telah mensponsori penelitian ini sehingga dapat terlaksana dan dipublikasikan. Semua yang ditulis dalam makalah ini merupakan hasil pemikiran, diskusi dan analisis dari semua anggota tim peneliti. Semoga dapat menjadi bahan pertimbangan dan masukan oleh pembaca, dalam melakukan penelitian pada topik yang sama.

DAFTAR PUSTAKA

[1] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, "A comprehensive survey of AI-enabled phishing attacks detection techniques," Telecommun. Syst., vol. 76, no. 1, pp. 139–154, 2021, doi: 10.1007/s11235-020-00733-2.

[2] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," Front. Comput. Sci., vol. 3, no. March, pp. 1–23, 2021, doi: 10.3389/fcomp.2021.563060.

[3] N. Mtukushe, A. K. Onaolapo, A. Aluko, and D. G. Dorrell, "Review of Cyberattack Implementation, Detection, and Mitigation Methods in Cyber-Physical Systems," *Energies*, vol. 16, no. 13, pp. 1–25, 2023, doi: 10.3390/en16135206.

[4] R. Zieni, L. Massari, and M. C. Calzarossa, "Phishing or Not Phishing? A Survey on the Detection of Phishing Websites," *IEEE Access*, vol. 11, no. February, pp. 18499–18519, 2023, doi: 10.1109/ACCESS.2023.3247135.

[5] B. Naqvi, K. Perova, A. Farooq, I. Makhdoom, S. Oyedeji, and J. Porras, "Mitigation strategies against the phishing attacks: A systematic literature review," *Comput. Secur.*, vol. 132, p. 103387, 2023, doi: 10.1016/j.cose.2023.103387.

[6] M. F. Ansari, P. K. Sharma, and B. Dash, "Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training," *Int. J. Smart Sens. Adhoc Network.*, no. July, pp. 61–72, 2022, doi: 10.47893/ijssan.2022.1221.

[7] R. Alabdan, "Phishing attacks survey: Types, vectors, and technical approaches," *Futur. Internet*, vol. 12, no. 10, pp. 1–39, 2020, doi: 10.3390/fi12100168.

[8] S. Hawa Apandi, J. Sallim, and R. Mohd Sidek, "Types of anti-phishing solutions for phishing attack," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 769, no. 1, 2020, doi: 10.1088/1757-899X/769/1/012072.

[9] R. Alazaidah *et al.*, "Website Phishing Detection Using Machine Learning Techniques," *J. Stat. Appl. Probab.*, vol. 13, no. 1, pp. 119–129, 2024, doi: 10.18576/jsap/130108.

[10] C. Opara, Y. Chen, and B. Wei, "Look before you leap: Detecting phishing web pages by exploiting raw URL and HTML characteristics," *Expert Syst. Appl.*, vol. 236, no. August 2023, p. 121183, 2024, doi: 10.1016/j.eswa.2023.121183.

[11] M. S. Akhtar and T. Feng, "Comparison of Classification Model for the Detection of Cyber-attack using Ensemble Learning Models," *EAI Endorsed Trans. Scalable Inf. Syst.*, vol. 9, no. 5, pp. 1–11, 2022, doi: 10.4108/eai.1-2-2022.173293.

ISSN: 2503-054X
Vol. 9 No: 2, Oktober 2024

[12] T. O. Ojewumi, G. O. Ogunleye, B. O. Oguntunde, O. Folorunsho, S. G. Fashoto, and N. Ogbu, "Performance evaluation of machine learning tools for detection of phishing attacks on web pages," *Sci. African*, vol. 16, p. e01165, 2022, doi: 10.1016/j.sciaf.2022.e01165.

[13] R. Yang, K. Zheng, B. Wu, C. Wu, and X. Wang, "Phishing website detection based on deep convolutional neural network and random forest ensemble learning," *Sensors*, vol. 21, no. 24, pp. 1–18, 2021, doi: 10.3390/s21248281.

[14] A. Ferdita Nugraha, R. F. A. Aziza, and Y. Pristyanto, "Penerapan metode Stacking dan Random Forest untuk Meningkatkan Kinerja Klasifikasi pada Proses Deteksi Web Phishing," *J. Infomedia*, vol. 7, no. 1, p. 39, 2022, doi: 10.30811/jim.v7i1.2959.

[15] NaliniPriya, G. Damoddaram, K. Gopi, G. Nitish Kumar, R, "Phishing Attack Detection Using Machine Learning. In: Rathore, V.S., Piuri, V., Babo, R., Ferreira, M.C. (eds) Emerging Trends in Expert Applications and Security", ICETEAS 2023. Lecture Notes in Networks and Systems, vol 682. Springer, Singapore. https://doi.org/10.1007/978-981-99-1946-8_27.

[16] Herdian, C., Kamila, A., Tampinongkol, F. F., Kembau, A. S., & Budidarma, I. G. A. M.. "One-hot encoding feature engineering untuk label-based data studi kasus prediksi harga mobil bekas". 2024. Informasi Interaktif : Jurnal Informatika Dan Teknologi Informasi, 9(1), 10–16. https://doi.org/10.37159/jii.v9i1.41

[17] Tampinongkol, F. Basri, H. Herdian, C dan L. Halim, "Identifikasi Penyakit Daun Tomat Menggunakan Gray Level Co-occurrence Matrix (GLCM) dan Support Vector Machine (SVM)", Techno Xplore: Jurnal Ilmu Komputer dan Teknologi Informasi, Vol. 8, No. 1, April 2023, ISSN: 2503-054X.

[18] Zhe OuYang. "Research on the Diamond Price Prediction based on Linear Regression, Decision Tree and Random Forest", EMFRM 2023. Highlights in Business, Economics and Management, Vol 24.

[19] Akbari, Amir &Ng Lilian, and Bruno Solnik. "Drives of Economic and Financial Integration: A Machine Learning Approach", Journal of Empirical Finance 61. Oktober 2021. 10.1016/j.jempfin.2020.12.005.

[20] Tampinongkol, F.F., Herdiyeni Y., Herliyana E.N. "Feature extraction of Jabon (Anthocephalus sp) leaf disease using discrete wavelet transform"., 2020. TELKOMNIKA (Telecommunication Computing Electronics and Control) 18 (2), 740-751. http://doi.org/10.12928/telkomnika.v18i2.10714