Identifikasi *Website Phishing* dengan Perbandingan Algoritma Klasifikasi

Agung Susilo Yuda Irawan[1*], Nono Heryana[2], Hopi Siti Hopipah[3], Dyas Rahma Putri[4]
[1,2,3,4] Jln. Hs. Ronggo Waluyo Puseurjaya Telukjambe Timur Karawang Jawa Barat
Email: *agung@unsika.ac.id

Abstrak. *Phishing* merupakan salah satu kejahatan siber yang bersifat mengancam dan menjebak seseorang dengan cara memancing korban untuk secara tidak langsung memberikan informasi kepada penjebak. Sebagian besar *phishing* menggunakan *link* yang mengarah pada *website* palsu untuk menjebak target. *Phishing* berpotensi menimbulkan kerugian baik dalam hal *privacy*, eksploitasi data, bahkan kerugian finansial. Jumlah website phishing yang merugikan pun tumbuh sangat cepat. Maka salah satu upaya yang dapat dilakukan yaitu melakukan penerapan klasifikasi untuk dapat mendeteksi *website phishing.* Penelitian ini bertujuan untuk mengetahui performa terbaik dalam penerapan algoritme klasifikasi yaitu *Support Vector Machine*, *Decision Tree*, *Random Forest*, dan *Multilayer Perceptron.* Berdasarkan hasil penelitian, performa terbaik terdapat pada algoritme *Multilayer Perceptron* dengan tingkat akurasi mencapai 93.15% dan nilai AUC 0.976.

Kata kunci: *klasifikasi, website phishing, multilayer perceptron.*

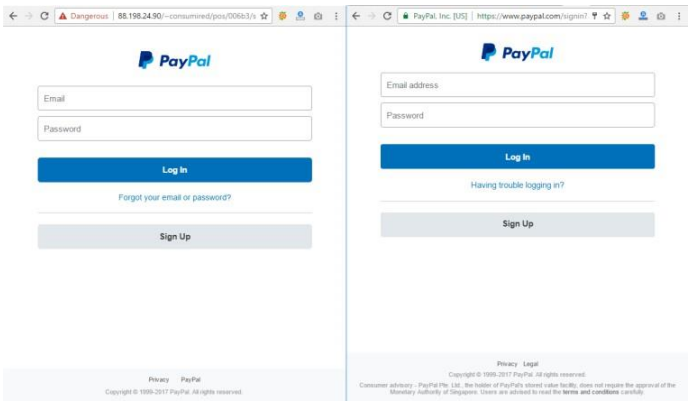
1 Pendahuluan

Kemajuan teknologi telah banyak membantu memudahkan aktivitas masyarakat. Khususnya dalam pemanfaatan internet, masyarakat menjadi lebih mudah dan efektif dalam berkomunikasi maupun mencari informasi [1]. Begitupun masyarakat Indonesia, 175,4 juta atau sekitar 64% penduduk Indonesia telah aktif menggunakan internet [2]. Seiring meningkatnya pengguna internet dan berkembangnya teknologi, ancaman terhadap keamanannya pun semakin beragam. Salah satunya adalah *phishing. Phishing* merupakan kegiatan yang bersifat mengancam dan menjebak seseorang dengan cara memancing target untuk secara tidak langsung memberikan informasi kepada penjebak (*pisher*) [3].

Phishing termasuk salah satu jenis kejahatan siber yang marak terjadi melalui jaringan komputer. Teknik ini rawan terjadi pada situs jejaring sosial seperti *facebook, instagram,* bahkan *email.* Sebagian besar *pisher* menjalankan aksinya melalui beberapa bentuk penipuan dengan membuat *link* yang mengarah pada situs *web* palsu [4]. *Link* tersebut dapat memikat pengguna untuk mengklik dan

Diterima 20 Mei 2021, Direvisi 25 Mei 2021, Diterima untuk publikasi 27 Mei 2021

memulai unduhan malware, atau memasukkan informasi pribadi ke situs web palsu yang memiliki tampilan mirip dengan yang asli.



Gambar 1 Perbandingan *Website Phishing* (kiri) dan yang otentik (kanan)

Maraknya *phising* tentunya berpotensi menimbulkan kerugian dalam hal *privacy*, bahkan mungkin terjadi penyalahgunaan (eksploitasi) data yang dapat merugikan finansial [4]. Menurut APWG *(Anti-Phishing Working Group)* dalam [5] menyebutkan bahwa dari tahun ke tahun, masyarakat sudah semakin sadar terhadap *website phishing.* Namun jumlah *website phishing* yang merugikan pun tumbuh lebih cepat. Hal tersebut dapat mengurangi rasa aman masyarakat dalam melakukan sebuah transaksi *online*, padahal di Indonesia sendiri masyarakat sudah mulai beralih menggunakan transaksi *online.* Maka salah satu upaya yang dapat dilakukan yaitu melakukan penerapan klasifikasi untuk dapat mendeteksi *website phishing.*

Penelitian sebelumnya [5] dengan judul Model Klasifikasi untuk Deteksi Situs *Phishing* di Indonesia, menguji beberapa algoritma seperti SMO *(Sequential Minimal Optimization), Naive Bayes*, *Bagging* dan *Multilayer Perceptron. Multilayer Perceptron* termasuk ke dalam Jaringan Syaraf Tiruan. Algoritme ini meniru struktur dan fungsi otak manusia sebagai model nya. Hasilnya, algoritme *Multilayer Perceptron* memiliki tingkat akurasi terbaik sebesar 91.8%, bahkan unggul dalam aspek lain seperti *precision, recall,* dan *f-measure.*

Penelitian lain [6] melakukan prediksi *website phishing* menggunakan perbandingan algoritme *Suport Vector Machine* (SVM), *Decision Tree,* dan *Naïve Bayes.* Penelitian ini bertujuan untuk memberikan gambaran metode paling efisien dalam memprediksi *website phishing.* Hasilnya algoritme SVM lebih baik dibandingkan algoritme lainnya dengan nilai akurasi 92.34% dan nilai AUC 0.977.

Selain itu, penelitian [7] melakukan optimasi algoritme C4.5 dengan seleksi fitur Genetic Algoritme dalam prediksi *web phishing*. Algoritme C4.5 ini banyak digunakan karena mudah dipahami dimana cabang pohon disimpulkan dalam bentuk klasifikasi berdasarkan kelas atau label. Hasilnya, penggunaan algoritme genetika berhasil meningkatkan akurasi sebesar 3.22% dari yang semula 83.81% menjadi 8.47%.

Pada penelitian ini, dataset merupakan data publik yang menggunakan tiga kategori dalam penentuan *website* yaitu *legitimate, suspicious,* dan *phishing.* Penelitian ini membandingkan empat algoritme klasifikasi yaitu *support vector machine* (SVM), *decision tree, random forest,* dan *multilayer perceptron* untuk membandingkan performa terbaik dalam mendeteksi *website phishing.*

2 Metode Penelitian

Tahapan pada *Cross-Industry Standard Process Model for Data Mining* (CRISP-DM) akan diterapkan pada penelitian ini. Adapun tahapannya terdiri dari:

2.1 Business Understanding

Business understanding melakukan pemahaman tujuan berdasarkan pada perspektif bisnis lalu diubah ke dalam definisi masalah *data mining.* Selanjutnya penentuan solusi yang akan diusulkan untuk menangani permasalahan yang ada. Adapun permasalahan pada penelitian ini adalah bagaimana mendeteksi *website* berpotensi *phishing* berdasarkan beberapa atribut pada data. Solusi yang ditawarkan yaitu perbandingan algoritme SVM, *decision tree, random forest,* dan *Multilayer Perceptron* untuk mengetahui performa terbaik dalam menentukan *website* berpotensi *phishing.*

2.2 Data Understanding

Data understanding berfungsi untuk memahami dan mengidentifikasi kualitas data, setelah itu menemukan pengetahuan awal untuk membentuk hipotesis. Data yang digunakan merupakan data publik yang mengumpulkan arsip data *Phishtank* (www.phishtank.com), yang merupakan situs komunitas gratis di mana pengguna dapat mengirimkan, memverifikasi, melacak, dan berbagi data *phishing.*

Terdapat beberapa karakter atau kriteria sebuah *website* untuk dapat dikatakan

phishing. Karakter *phishing* digolongkan menjadi *Address Bar based Feature*, *Abnormal based Feature,* HTML *and Javascript based Features* dan *Domain based Feature* [8].

2.3 Data Preparation

Tahap ini merupakan tahap persiapan data untuk digunakan pada tahap selanjutnya. Biasanya cenderung dilakukan berulang kali sampai data benar- benar sesuai dengan kebutuhan. *Data preparation* terdiri dari *data cleaning*, *attribute selection,*dan penentuan label pada atribut data.

2.4 Modelling

Tahap selanjutnya yaitu pemilihan teknik pemodelan dengan teknik *data mining.* Untuk penelitian ini, dilakukan perbandingan pada empat algoritme klasifikasi, diantaranya *Support Vector Machine* (SVM), *Decision Tree, Random Forest,* dan *Multilayer Perceptron.*

2.5 Evaluation

Evaluasi digunakan untuk menganalisis hasil penerapan model berdasarkan tujuan penelitian, untuk selanjutnya dilakukan penentuan keputusan terhadap penggunaan hasil *data mining.* Adapun parameter evaluasi pada penelitian ini yaitu tingkat akurasi.

2.6 Deployment

Tahapan terakhir yaitu tahap penyebaran, dilakukan untuk merepresentasikan hasil pengetahuan dan informasi yang didapatkan ke dalam bentuk yang mudah dipahami pengguna.

3 Hasil Dan Pembahasan

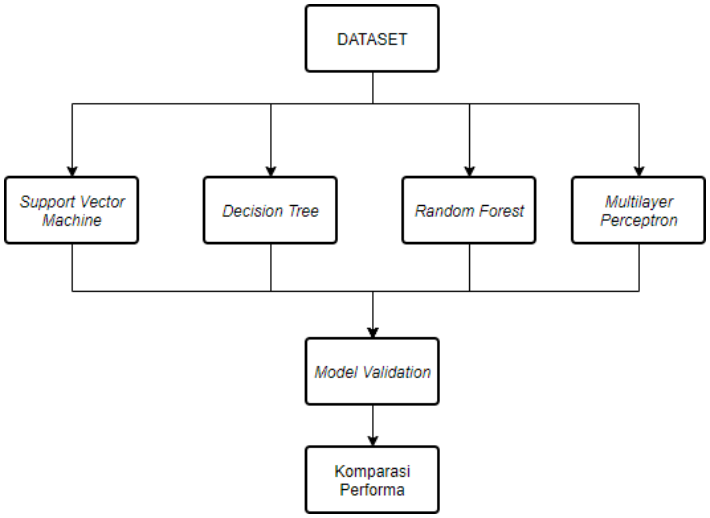
Dengan memanfaatkan sumber data, dapat diterapkan teknik *data mining* yang bertujuan untuk mengetahui performa terbaik dalam klasifikasi *website phishing* dengan membandingkan empat algoritme yaitu SVM, *decision tree, random forest,* dan *Multilayer Perceptron.*

Data yang digunakan diambil dari sumber data publik www.kaggle.com, yang berisi kumpulan data *website phishing.* Dataset berjumlah 1353 data, yang terdiri dari 10 atribut termasuk 1 kelas yang dijadikan label. Terdapat 702 URL *phishing*, 103 URL mencurigakan, dan 548 URL otentik. Adapun keterangan mengenai atribut data terdapat pada tabel 1.

Tabel 1. Atribut Dataset

No.	Nama Atribut	Keterangan	Kategori	Nilai Referensi
1	*SFH (Server Form Handler)*	Memiliki string kosong atau tidak	*Abnormal Based Features*	1 = *Legitimate* (valid), 0 = *Suspicious* (Mencurigakan), -1 = *Phishing*
2	*popUpWindow*	Biasanya *web* asli tidak akan meminta pengguna untuk mengirim informasi pribadi melalui *pop up*	*HTML and JavaScript based Features*	
3	*SSLfinal_State*	Memiliki SSL atau tidak	*Abnormal Based Features*	
4	*Request_URL*	*Request* URL memeriksa apakah objek eksternal yang ada pada halaman web (misal gambar, video, dll)		
5	*URL_of_Anchor*	URL yang terhubung dengan link lain		
6	*web_traffic*	Mengukur popularitas jumlah pengunjung website.	*Domain based Features*	
7	*age_of_domain*	Usia domain dihitung sejak domain diregistrasi		
8	*URL_Length*	Panjang URL, *web phishing* cenderung menggunakan URL yang panjang untuk menyembunyikan link palsu	*Address Bar Based*	
9	*having_IP_Address*	Jika domain menggunakan IP Address, maka merupakan *website phishing*		
10	*Result*	Kategori apakah *legitimate, suspicious,* atau *phishing*		

Penerapan algoritme pada pemodelan ini dibantu dengan pemrograman Python. Terdapat 4 proses yang dilakukan, untuk mengetahui performa terbaik. Parameter pengujian terdiri dari nilai akurasi berdasarkan hasil *data training* dan *data testing*, nilai *recall, precision*, f1-*score,* dan nilai AUC. Alur penelitian ini terdapat pada gambar 2.



Gambar 2 Alur Penelitian

Sebagai parameter tambahan, peneliti menambahkan nilai AUC beserta grafik ROC. Nilai AUC diklasifikasikan ke dalam 5 kategori, seperti pada Tabel 2.

Tabel 2. Klasifikasi Nilai AUC

Nilai AUC	Klasifikasi
0.90 - 1.00	*Excellent Classification*
0.80 - 0.90	*Good Classification*
0.70 - 0.80	*Fair Classification*
0.60 - 0.70	*Poor Classification*
0.50 - 0.60	*Failure*

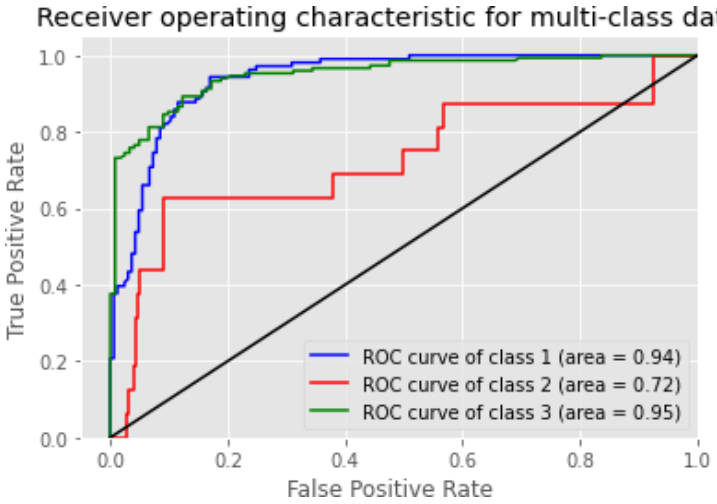
3.1 Penerapan Pada Algoritma *Support Vector Machine* (SVM)

Tabel 3. Performa pada algoritme SVM

Akurasi Data		Rata-Rata			
Training	***Testing***	***Precision***	***Recall***	**F1-*score***	**AUC**
0.844	0.845	0.58	0.63	0.60	0.863

Dari Tabel 3, hasil akurasi pengujian dengan menggunakan algoritme SVM adalah 84.4% untuk data *training*, dan 84.5% untuk data *testing*.

Untuk nilai *precision, recall, f1-score* dan nilai *AUC* diambil hasil rata-rata.



Gambar 3 Kurva ROC Algoritme SVM

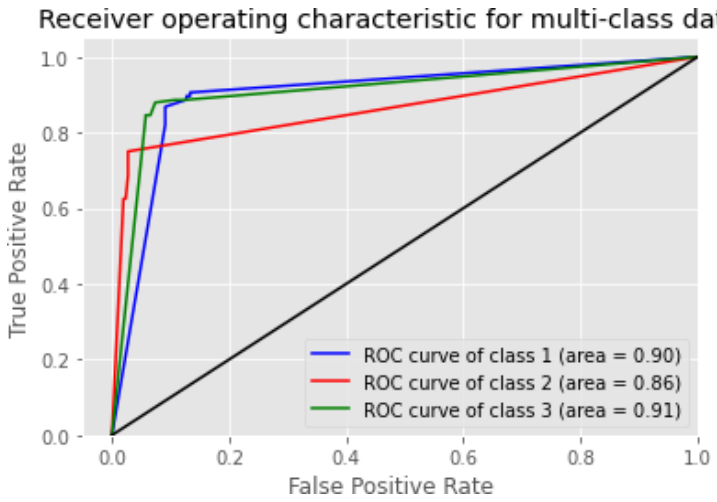
Berdasarkan nilai yang diperoleh dari evaluasi model menggunakan evaluation matrix, maka didapatkan kurva ROC seperti Gambar 4. Rata-rata nilai AUC yang didapatkan adalah 0.863, yang berarti masuk kategori *Good Classification.*

3.2 Penerapan pada Algoritme *Decision Tree*

Tabel 4. Performa pada algoritme *Decision Tree*

Akurasi Data		**Rata-Rata**			
Training	***Testing***	***Precision***	***Recall***	**F1-*score***	**AUC**
0.881	0.823	0.56	0.61	0.59	0.92

Berdasarkan Tabel 4, hasil akurasi pengujian dengan menggunakan algoritme *Decision Tree* adalah 88.1% untuk data *training*, dan 82.3% untuk data *testing*. Nilai rata-rata untuk *precision, recall, dan f1-score* pada algoritme *Decision Tree* lebih kecil dibandingkan dengan algortime *SVM.*



Gambar 4 Kurva ROC Algoritme *Decision Tree*

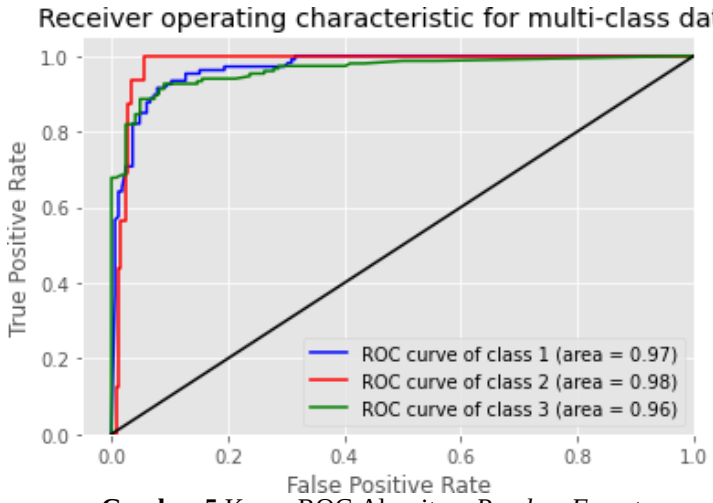
Berdasarkan kurva ROC pada Gambar 4. Rata-rata nilai AUC yang didapatkan adalah 0.92, yang berarti masuk kategori *Excellent Classification.* Artinya, tingkat error pada *Decision Tree* lebih kecil dibandingkan algoritme *SVM.*

3.3 Penerapan pada Algoritme *Random Forest*

Tabel 5. Performa pada algoritme *Random Forest*

Akurasi Data		**Rata-Rata**			
Training	***Testing***	***Precision***	***Recall***	**F1-*score***	**AUC**
0.877	0.823	0.53	0.58	0.56	0.973

Hasil akurasi pengujian dengan menggunakan algoritme *Random Forest* yang dijelaskan pada Tabel 5 adalah 87.7% untuk data *training*, dan 82.3% untuk data *testing*. Nilai AUC yang didapatkan semakin tinggi, yang artinya tingkat error pada penerapan algoritme *Random Forest* semakin kecil dibandingkan algoritme SVM dan *Decision Tree.*



Gambar 5 Kurva ROC Algoritme *Random Forest*

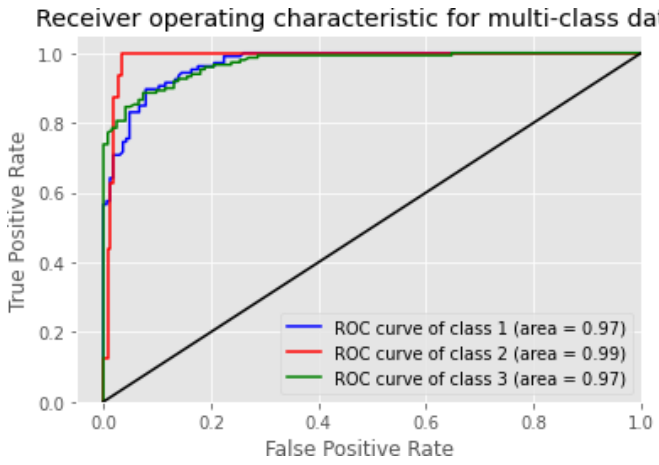
Berdasarkan Gambar 5, hasilnya masuk kategori *Excellent Classification* dengan rata-rata nilai AUC sebesar 0.973.

3.4 Penerapan pada Algoritme *Multilayer Perceptron*

Tabel 6. Performa pada algoritme *Multillayer Perceptron*

Akurasi Data		**Rata-Rata**			
Training	***Testing***	***Precision***	***Recall***	**F1-*score***	**AUC**
0.963	0.900	086	0.84	0.85	0.976

Penerapan algoritme yang terakhir adalah *Multilayer Perceptron* yang hasilnya ditunjukkan pada Tabel 6, yaitu 96.3% untuk data *training*, dan 90% untuk data *testing*. Parameter keseluruhan pada algoritme *Multilayer Perceptron* ini menghasilkan nilai yang tertinggi dibandingkan tiga algoritme lainnya yaitu *SVM*, *Decision Tree* dan *Random Forest.*



Gambar 6 Kurva ROC Algoritme *Multilayer Perceptron*

Begitupun nilai AUC seperti pada Gambar 6, mendapatkan nilai tertinggi sebesar 0.976 yang masuk kategori *Excellent Classification.*

4 Kesimpulan

Hasil penelitian pada klasifikasi *website phishing* menggunakan perbandingan empat algoritme yaitu *Support Vector Machine*, *Decision Tree*, *Random Forest* dan *Multilayer Perceptron* menghasilkan performa yang baik. Performa model algoritme yang mendapatkan nilai paling tinggi adalah algoritme *Multilayer Perceptron*, dengan akurasi sebesar 93.15% dan nilai AUC 0.976.

Kontribusi dari penelitian ini yaitu mengusulkan model klasifikasi untuk mendeteksi *website* apakah termasuk ke dalam kategori *legitimate* (otentik), *suspicious* (meragukan) , atau *phishing.*

Penelitian selanjutnya dapat melakukan penerapan algoritme lain atau peningkatan akurasi dengan tambahan *feature selection.* Selain itu, model klasifikasi yang telah dibuat juga dapat diimplementasikan kedalam sebuah sistem untuk deteksi *website phishing*

5 Referensi

[1] A. S. Gulo, S. Lasmadi, and K. Nawawi, “Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik,” vol. 1, pp. 68–81, 2020.

[2] B. Ludwianto, “Riset: 64% Penduduk Indonesia Sudah Pakai Internet,”

Kumparan, 2020.

[3] M. H. Wibowo and N. Fatimah, "Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime," *JOEICT(jurnal Educ. Inf. Commun. Technol.*, vol. 1, pp. 1–5, 2017.

[4] S. R. Rahayu, "Phishing," 2019.

[5] F. Eka Purwiantono and A. Tjahyanto, "Model Klasifikasi Untuk Deteksi Situs Phising Di Indonesia," Institut Teknologi Sepuluh November, 2017.

[6] Z. Halim, "Prediksi Website Pemancing Informasi Penting Phising Menggunakan Support Vector Machine (SVM)," *Inf. Syst. Educ. Prof.*, vol. 2, no. 1, pp. 71–82, 2017, [Online]. Available: http://download.portalgaruda.org/article.php?article=535068&val=10928&title=Prediksi Website Pemancing Informasi Penting Phising Menggunakan Support Vector Machine (SVM).

[7] A. S. Sunge, "Optimasi Algoritma C4.5 Dalam Prediksi Web Phishing Menggunakan Seleksi Fitur Genetic Algoritma," *Paradigma*, vol. 10, no. 2, pp. 27–32, 2018, doi: 10.31294/p.v%vi%i.4021.

[8] A. Fatkhurohman and E. Pujastuti, "Penerapan Algoritma Naïve Bayes Classifier Untuk Meningkatkan Keamanan Data Dari Website Phising," *J. Teknol. Inf.*, vol. XIV, no. October 2018, pp. 115–124, 2019.