p-ISSN: 2963-7856| e-ISSN: 2961-9890
Available online at jerkin.org/index.php/jerkin
Jurnal Pengabdian Masyarakat dan Riset Pendidikan
Volume 4 No. 3 Januari-Maret 2026, pp 16587-16591

Analisa Komparasi Kinerja Algoritma *K-Nearest Neighbor* (K-NN) dan *Decision Tree* dalam Klasifikasi Situs Web Phising

Fajar Dwi Prasetyo[1*], Muhammad Maulana[2], Faris Ramadhan[3], Ananda Lutfi Setiabudi[4], Imam Budiawan[5], Desmulyati[6]

[1-5]Sistem Informasi, [6]Informatika, Universitas Bina Sarana Informatika, Jl. Kramat Raya No.98, RT.2/RW.9, Kwitang, Kec. Senen, Kota Jakarta Pusat
E-mail: 17230450@bsi.ac.id
* Corresponding Author

https://doi.org/10.31004/jerkin.v4i3.4965

ARTICLE INFO

Article history
Received: 23 Nov 2025
Revised: 05 Dec 2025
Accepted: 30 Dec 2025

Kata Kunci:
Machine Learning, *Phishing Detection*, *K-Nearest Neighbor*, Decision Tree, Cybersecurity, Klasifikasi URL.

Keywords:
Machine Learning, Phishing Detection, K-Nearest Neighbor, Decision Tree, Cybersecurity, URL Classification.

ABSTRACT

Serangan phishing merupakan salah satu ancaman keamanan siber terbesar yang bertujuan mencuri informasi sensitif pengguna melalui manipulasi psikologis menggunakan situs web tiruan. Metode deteksi konvensional yang mengandalkan daftar hitam (blacklist) dinilai kurang efektif dalam mengenali serangan zero-day atau situs phishing yang baru dipublikasikan. Penelitian ini bertujuan untuk mengembangkan model deteksi otomatis menggunakan pendekatan Machine Learning dengan membandingkan kinerja dua algoritma Supervised Learning, yaitu K-Nearest Neighbor (K-NN) dan Decision Tree. Dataset yang digunakan bersumber dari UCI Machine Learning Repository yang terdiri dari 11.055 data dengan 30 fitur karakteristik URL. Evaluasi kinerja dilakukan menggunakan metrik Accuracy dan analisis Confusion Matrix. Hasil eksperimen menunjukkan bahwa algoritma Decision Tree mengungguli K-NN secara signifikan dengan akurasi mencapai 95,21%, sedangkan K-NN hanya memperoleh akurasi sebesar 60,11%. Selain itu, Decision Tree menunjukkan tingkat kesalahan prediksi (False Negative) yang sangat rendah, menjadikannya model yang lebih direkomendasikan untuk implementasi sistem keamanan siber waktu nyata.

Phishing attacks represent a significant cybersecurity threat aimed at stealing sensitive user information through psychological manipulation using fake websites. Conventional detection methods relying on blacklists are considered ineffective in recognizing zero-day attacks or newly published phishing sites. This study aims to develop an automated detection model using a Machine Learning approach by comparing the performance of two Supervised Learning algorithms: K-Nearest Neighbor (K-NN) and Decision Tree. The dataset used is sourced from the UCI Machine Learning Repository, consisting of 11,055 records with 30 URL characteristic features. Performance evaluation was conducted using Accuracy metrics and Confusion Matrix analysis. Experimental results indicate that the Decision Tree algorithm significantly outperforms K-NN with an accuracy of 95.21%, while K-NN achieved an accuracy of only 60.11%. Furthermore, Decision Tree demonstrated a very low False Negative rate, making it a more recommended model for real-time cybersecurity system implementation.

How to Cite: Fajar Dwi Prasetyo, et al (2025). Analisa Komparasi Kinerja Algoritma K-Nearest Neighbor (K-NN) dan Decision Tree dalam Klasifikasi Situs Web Phising, 4(3) 16587-16591. https://doi.org/10.31004/jerkin.v4i3.4965

PENDAHULUAN

Pesatnya pertumbuhan teknologi internet telah mentransformasi cara manusia berinteraksi dan bertransaksi. Namun, kemajuan ini diiringi dengan meningkatnya kejahatan siber (cybercrime). Salah satu vektor serangan yang paling dominan adalah phishing. Phishing didefinisikan sebagai upaya kriminal untuk mendapatkan informasi sensitif seperti username, kata sandi, dan detail kartu kredit

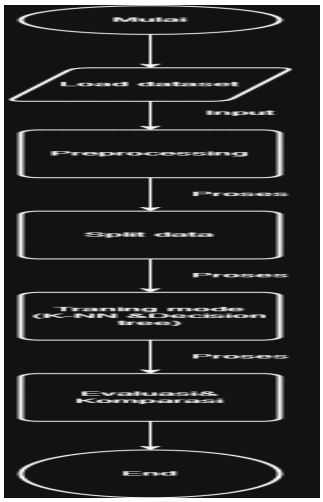
dengan menyamar sebagai entitas terpercaya dalam komunikasi elektronik [1].

Mekanisme pertahanan tradisional terhadap phishing umumnya menggunakan pendekatan berbasis daftar hitam (blacklist), di mana URL berbahaya disimpan dalam basis data terpusat. Kelemahan utama metode ini adalah ketidakmampuannya mendeteksi situs phishing baru yang belum dilaporkan atau situs yang menggunakan teknik pengaburan (obfuscation) pada URL [2]. Oleh karena itu, diperlukan pendekatan heuristik berbasis kecerdasan buatan (Artificial Intelligence) yang mampu mempelajari pola karakteristik URL berbahaya secara otomatis.

Penelitian ini berfokus pada penerapan teknik Machine Learning untuk mengklasifikasikan situs web. Penulis memilih untuk membandingkan dua algoritma populer: K-Nearest Neighbor (K-NN) sebagai representasi metode instance-based learning yang sederhana, dan Decision Tree sebagai representasi metode model-based yang menghasilkan aturan logika (rules). Penelitian ini diharapkan dapat memberikan kontribusi berupa analisis komparatif yang mendalam mengenai kelebihan dan kekurangan kedua algoritma tersebut dalam konteks keamanan siber.

METODE

Penelitian ini dilakukan menggunakan pendekatan kuantitatif eksperimental untuk mengukur kinerja algoritma *Machine Learning*. Secara umum, tahapan penelitian disusun secara sistematis yang meliputi: pengumpulan *dataset*, pra-pemrosesan data (*preprocessing*), pembagian data (*data splitting*), pelatihan model (*model training*), dan evaluasi hasil. Alur kerja penelitian ini dirancang untuk memastikan bahwa perbandingan antara algoritma *K-Nearest Neighbor* dan *Decision Tree* dilakukan secara adil (*fair*) dan valid.



Pengumpulan Data

Data yang digunakan adalah "*Phishing Websites Dataset*" dari *UCI Machine Learning Repository* [4]. Dataset ini memiliki 11.055 sampel data. Setiap sampel memiliki 30 fitur ekstraksi dari *URL*, antara lain:

1. URL Length: Panjang karakter URL.
2. Having @ Symbol: Keberadaan simbol '@'.
3. Prefix/Suffix: Penggunaan tanda hubung (-) pada domain.
4. SSL State: Status keamanan sertifikat HTTPS.

Pra-Pemrosesan Data

Tahap pra-pemrosesan meliputi:Pemisahan Fitur dan Label:

1. Pemisahan Fitur dan Label: (x) dan target kelas (y), di mana kelas -1 merepresentasikan *Phishing* dan -1 merepresentasikan *Legitimate* (Aman).
2. Pembagian Data (*Splitting*): *Dataset* dibagi menggunakan rasio 80:20. Sebanyak 80% data digunakan untuk pelatihan (*training*) dan 20% sisanya digunakan untuk pengujian (*testing*) guna menghindari *overfitting*.

ISSN 2963-7856 (print), ISSN 2961-9890 (online)

Algoritma Klasifikasi

A. *K*-Nearest *Neighbor (K-NN)* Pada penelitian ini, K-NN dikonfigurasi dengan parameter $k = 5$. Klasifikasi dilakukan berdasarkan jarak terdekat dengan tetangga menggunakan rumus *Euclidean Distance*:

$$d(x,y) = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2}$$

Keterangan: $d(x,y)$ adalah jarak, x dan y adalah data uji dan latih.

B. *Decision Tree* (C4.5/CART) Algoritma ini membangun model prediksi berbentuk struktur pohon. Pembagian simpul (*node splitting*) dilakukan berdasarkan kriteria *Gini Impurity* atau *Information Gain* untuk memisahkan kelas *phishing* dan aman seoptimal mungkin.

Metrik Evaluasi Kinerja model diukur menggunakan akurasi (Persamaan 2):

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \times 100\backslash\%$$

Lingkungan Eksperimen

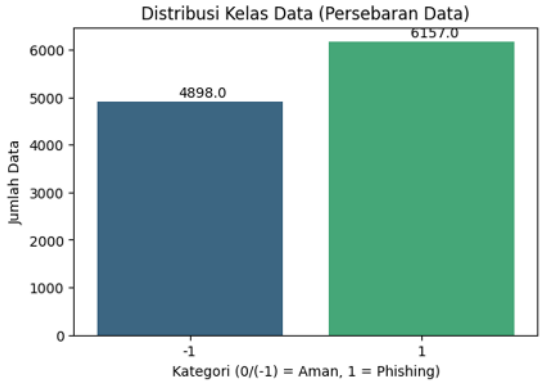
Implementasi kode dan pengujian model dilakukan menggunakan platform berbasis *cloud Google Colaboratory*. Spesifikasi lingkungan eksperimen yang digunakan adalah sebagai berikut:

1. Bahasa Pemrograman: *Python* 3.10.
2. Pustaka (Library): *Scikit-Learn* (pemodelan), *Pandas* (manipulasi data), *Matplotlib & Seaborn* (visualisasi data).
3. Perangkat Keras: Google Compute Engine Backend (CPU Intel Xeon, RAM ~12GB).
4. Format Data: CSV (Comma Separated Values) yang diproses menggunakan struktur Dataframe *Pandas*.

HASIL DAN PEMBAHASAN

Analisis Persebaran Data

Sebelum pelatihan model, dilakukan analisis distribusi kelas pada dataset untuk memastikan keseimbangan data.



Gambar 2. Distribusi Kelas pada Dataset

Berdasarkan Gambar 2 dan hasil perhitungan statistik, diketahui bahwa dataset terdiri dari 6.157 data situs phishing (Label 1) dan 4.898 data situs aman (Label -1). Meskipun jumlah data phishing sedikit lebih mendominasi, distribusi ini masih tergolong cukup seimbang, sehingga model dapat mempelajari karakteristik kedua kelas dengan baik tanpa mengalami bias mayoritas yang signifikan.

Hasil Evaluasi Kinerja

Setelah proses pelatihan dan pengujian pada data uji (20%), diperoleh hasil akurasi sebagai berikut:

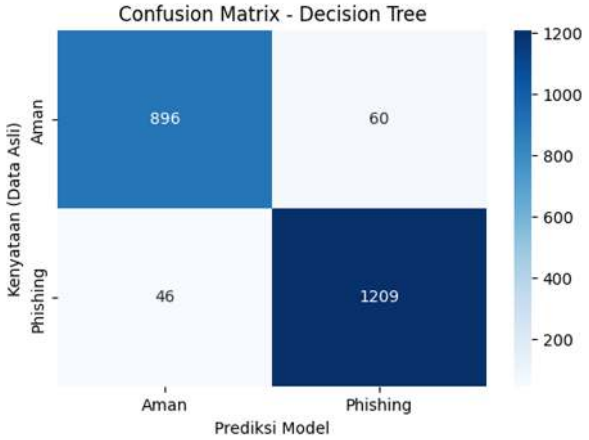
Jumlah baris: 11055, Jumlah kolom: 32

Sedang melatih model K-NN...
Sedang melatih model Decision Tree...
==========
Hasil Komparasi Akurasi
==========
1. Akurasi K-Nearest Neighbor (K-NN) : 60.11%
2. Akurasi Decision Tree : 95.21%
==========

Tabel 1 memperlihatkan bahwa algoritma Decision Tree mengungguli K-NN dengan selisih akurasi yang sangat signifikan, yaitu sebesar 35,10%.

Analisis Confusion Matrix

Akurasi saja tidak cukup untuk menggambarkan kinerja deteksi. Analisis Confusion Matrix pada model terbaik (Decision Tree) ditampilkan pada Gambar 3.



Gambar 3. Confusion Matrix Model Decision Tree

True Positive (TP): 1.209 (Situs Phishing berhasil dideteksi dengan benar).
True Negative (TN): 896 (Situs Aman berhasil dikenali dengan benar).
False Positive (FP): 60 (Kesalahan: Situs aman dianggap phishing).
False Negative (FN): 46 (Kesalahan Vital: Situs phishing lolos terdeteksi sebagai aman).

Model *Decision Tree* memiliki jumlah *False Negative* yang sangat rendah (hanya 46 dari ribuan data). Dalam konteks keamanan siber, menekan angka False Negative sangat krusial agar tidak ada serangan phishing yang lolos menyerang pengguna.

Pembahasan

Keunggulan performa Decision Tree (95,21%) dibandingkan K-NN (60,11%) dalam eksperimen ini disebabkan oleh karakteristik data. Fitur-fitur pada dataset Phishing Websites mayoritas bersifat kategorikal dan biner (nilai -1, 0, 1). Decision Tree bekerja sangat efektif pada tipe data ini karena dapat membuat aturan keputusan (if-then rules) yang tegas (misalnya: "JIKA URL memiliki @ MAKA Phishing").

Sebaliknya, K-NN bekerja berdasarkan perhitungan jarak geometris (Euclidean). Pada data dengan dimensi tinggi (30 fitur) dan nilai diskrit biner, konsep "jarak" menjadi kurang representatif (curse of dimensionality), yang menyebabkan akurasi K-NN turun drastis dalam percobaan ini.

SIMPULAN

Berdasarkan hasil penelitian dan analisis yang telah dilakukan, dapat disimpulkan bahwa: 1) Penerapan Machine Learning efektif mendeteksi phishing pada dataset berjumlah 11.055 baris. 2) Algoritma Decision Tree terbukti jauh lebih unggul dengan tingkat akurasi mencapai 95,21%,

ISSN 2963-7856 (print), ISSN 2961-9890 (online)

mengalahkan K-NN yang hanya mencapai 60,11%. 3) Analisis Confusion Matrix menunjukkan bahwa Decision Tree mampu meminimalkan risiko serangan lolos dengan tingkat kesalahan False Negative yang rendah.

Untuk penelitian selanjutnya, disarankan untuk: 1) Menerapkan teknik seleksi fitur (Feature Selection) untuk melihat fitur mana yang paling berpengaruh. 2) Mengeksplorasi algoritma Ensemble Learning seperti Random Forest untuk melihat apakah akurasi bisa ditingkatkan hingga mendekati 98-99%.

UCAPAN TERIMA KASIH

Peneliti menyampaikan ucapan terima kasih kepada pihak yang sudah berkontribusi dalam pelaksanaan penelitian dan penyusunan artikel ini.

REFERENSI

A. P. Author, "Understanding Phishing Attacks: A Comprehensive Review," Journal of Cyber Security, vol. 12, no. 4, pp. 45-50, 2023.

B. Santoso, "Kelemahan Metode Blacklist pada Sistem Keamanan Web," Jurnal Informatika Indonesia, vol. 8, no. 1, 2022.

R. Ramianto and D. Kusuma, "Analisis Komparasi Algoritma SVM dan Naive Bayes untuk Deteksi Phishing," Jurnal Teknologi Informasi, vol. 5, no. 2, pp. 100-112, 2022.

D. Dua and C. Graff, "UCI Machine Learning Repository: Phishing Websites Data Set," University of California, Irvine, School of Information and Computer Sciences, 2019. [Online]. Available: http://archive.ics.uci.edu/ml/datasets/Phishing+Websites.

Scikit-learn Developers, "Scikit-learn: Machine Learning in Python," Journal of Machine Learning Research, vol. 12, pp. 2825-2830, 2011.

B. Srivastava and P. K. Singh, "Optimal Detection of Phishing Attack using SCA based K-NN," Procedia Computer Science, vol. 218, pp. 2450-2459, 2023. [Online]. Available: https://doi.org/10.1016/j.procs.2023.01.220

A. K. Jain and B. B. Gupta, "Comparative evaluation of machine learning algorithms for phishing detection," PeerJ Computer Science, vol. 9, p. e1373, 2023. [Online]. Available: https://doi.org/10.7717/peerj-cs.1373

M. A. Al-Shareeda, M. A. Alazzawi, S. Manickam, and A. H. H. Al-naji, "Improved Phishing Attack Detection with Machine Learning," Applied Sciences, vol. 13, no. 13, p. 7822, 2023. [Online]. Available: https://doi.org/10.3390/app13137822

B. Srinivas, K. V. Swamy, and B. E. Reddy, "Improving the phishing website detection using empirical analysis of FT and its variants," Heliyon, vol. 9, no. 8, p. e18676, 2023. [Online]. Available: https://doi.org/10.1016/j.heliyon.2023.e18676

S. Alhumoud, "Machine Learning Approach for Email Phishing Detection," Procedia Computer Science, vol. 220, pp. 793-798, 2023. [Online]. Available: https://doi.org/10.1016/j.procs.2023.03.106