Contents lists available at MID Publisher International

Technology Sciences Insights Journal

Journal homepage: https://journal.midpublisher.com/index.php/tsij

KLASIFIKASI DATA URL DENGAN MENGGUNAKAN K- NEAREST NEIGHBOR (KNN) UNTUK DETEKSI PHISHING WEBSITE

Fartiwi Angreini & Adlian Jefiza
Politeknik Negeri Batam, Batam, Indonesia

INFORMASI ARTIKEL

Sejarah Artikel:
Diterima: Juni 2025
Revisi: Juni 2025
Diterima: Juli 2025
Dipublikasi: Juli 2025

Kata Kunci:
Phishing; Klasifikasi URL; K-Nearest Neighbor; Machine Learning; Confusion Matrix

*Penulis Korespondensi:
fartiwiangreini@gmail.com

ABSTRAK

Penelitian ini bertujuan untuk menganalisis deteksi phishing berbasis URL menggunakan metode K-Nearest Neighbor (KNN). Dataset yang digunakan terdiri dari tiga fitur numerik, yaitu panjang URL, panjang hostname, dan panjang path, serta label target berupa kategori phishing (1) atau bukan phishing (0). Data diproses melalui tahapan preprocessing dan normalisasi untuk memastikan kesetaraan skala antar fitur sebelum digunakan sebagai input model.

Hasil penelitian menunjukkan bahwa model KNN menghasilkan akurasi sebesar 59%, dengan kinerja lebih baik pada kelas non-phishing dibandingkan kelas phishing. Kondisi ini mengindikasikan adanya ketidakseimbangan data serta keterbatasan fitur sederhana dalam membedakan karakteristik URL phishing. Temuan ini diharapkan memberikan kontribusi dalam pengembangan metode deteksi phishing berbasis analisis URL dan menjadi referensi untuk penelitian lanjutan.

ABSTRACT

This study aims to analyze phishing detection based on URL characteristics using the K-Nearest Neighbor (KNN) method. The dataset contains three numerical features: URL length, hostname length, and path length, along with a target label representing phishing (1) or non-phishing (0). Preprocessing and normalization were applied to ensure consistent feature scaling before model training.

The results show that the KNN model achieved an accuracy of 59%, performing better on non-phishing URLs than phishing URLs. This indicates class imbalance and the limitations of using simple numerical URL features for classification. These findings are expected to contribute to the development of URL-based phishing detection methods and serve as a reference for future research.

PENDAHULUAN

Perkembangan teknologi informasi yang pesat meningkatkan frekuensi penggunaan layanan digital, yang turut memengaruhi peningkatan ancaman keamanan siber. Salah satu jenis serangan yang paling sering terjadi adalah phishing, yaitu upaya memperoleh data sensitif dengan menggunakan URL palsu yang menyerupai situs resmi. Pengguna sering kali tidak mampu membedakan antara URL asli dan palsu, sehingga menjadi sasaran empuk serangan ini.

Deteksi phishing secara otomatis menjadi penting untuk mengurangi potensi kerugian. Salah satu pendekatan yang umum digunakan adalah klasifikasi URL berdasarkan karakteristik numeriknya. Pemanfaatan algoritma *machine learning* seperti K-Nearest Neighbor (KNN) memungkinkan proses klasifikasi berdasarkan kemiripan pola data.

Beberapa penelitian sebelumnya telah membahas deteksi phishing berbasis *machine learning*, namun sebagian besar masih menghadapi kendala seperti ketidakseimbangan data

serta keterbatasan fitur. Penelitian ini bertujuan untuk mengevaluasi performa algoritma KNN dalam mengklasifikasikan URL phishing menggunakan tiga fitur numerik dasar. Pendekatan ini diharapkan memberikan gambaran mengenai efektivitas metode sederhana untuk deteksi phishing berbasis struktur URL.

LANDASAN TEORI (Optional)

KNN merupakan algoritma non-parametrik yang menentukan kelas suatu data berdasarkan kedekatan jarak dengan sejumlah tetangga terdekat dalam data latih. Algoritma ini sering digunakan dalam klasifikasi karena kesederhanaannya dan efektivitas dalam mengenali pola berbasis jarak. Teori jarak Euclidean biasanya digunakan sebagai dasar perhitungan similaritas antar data.

Penelitian terdahulu menunjukkan bahwa fitur numerik seperti panjang URL, panjang domain, atau jumlah karakter khusus memiliki korelasi dengan kemungkinan phishing. Namun, beberapa penelitian menyoroti bahwa fitur numerik saja tidak cukup untuk mencapai akurasi tinggi, terutama ketika dataset mengalami ketidakseimbangan.

Berdasarkan teori dan penelitian sebelumnya, penelitian ini menggunakan fitur numerik sederhana sebagai dasar klasifikasi, dengan asumsi bahwa pola panjang URL dapat menjadi indikator awal phishing.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif untuk menganalisis performa algoritma KNN dalam mendeteksi phishing. Dataset berisi 5045 data URL dengan empat atribut, yaitu *UrlLength*, *HostnameLength*, *PathLength*, serta *LABEL* sebagai target klasifikasi.
Tahapan penelitian meliputi:

1. **Preprocessing data**
   Dataset diambil dari sumber terbuka dan berjudul AAS.csv, yang memuat 5045 baris data URL dengan 4 atribut, yaitu:
   - UrlLength: Panjang URL
   - HostnameLength: Panjang hostname
   - PathLength: Panjang path URL
   - LABEL: Label klasifikasi (0 untuk bukan phishing, 1 untuk phishing)
   -

   Distribusi label adalah sebagai berikut:
   - Label 0: 3049 sampel
   - Label 1: 1936 sampel

2. **Preprocessing**
   Langkah-langkah preprocessing yang dilakukan:
   - Menghapus duplikat dan nilai kosong
   - Memilih tiga fitur numerik (UrlLength, HostnameLength, PathLength)
   - Melakukan normalisasi data menggunakan StandardScaler untuk menyeimbangkan skala fitur

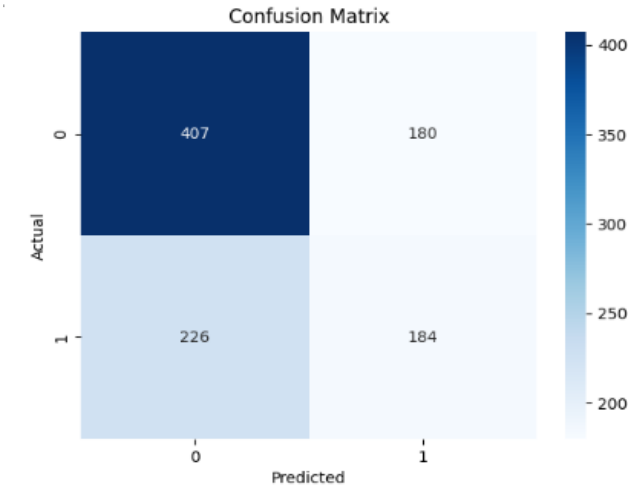
3. **Algoritma Klasifikasi**
   Algoritma K-Nearest Neighbor (KNN) dipilih karena kesederhanaan dan efektivitasnya dalam klasifikasi berbasis kedekatan jarak antar data. Model KNN diimplementasikan dengan parameter n_neighbors = 5.

4. **Pembagian Data**
   - 80% data sebagai data latih
   - 20% data sebagai data uji
     Pembagian dilakukan menggunakan *train_test_split* dengan *random_state = 42*.

5. **Evaluasi Model**
   Evaluasi dilakukan menggunakan *confusion matrix* dan *classification report*, termasuk precision, recall, dan F1-score.

HASIL DAN PEMBAHASAN

Hasil klasifikasi menunjukkan bahwa model KNN menghasilkan akurasi sebesar 59%. Confusion matrix memperlihatkan bahwa model lebih baik mengenali URL non-phishing dibandingkan phishing, yang mengindikasikan ketidakseimbangan kelas dalam dataset.



Classification Report:

	precision	recall	f1-score	support
0	0.64	0.69	0.67	587
1	0.51	0.45	0.48	410
accuracy			0.59	997
macro avg	0.57	0.57	0.57	997
weighted avg	0.59	0.59	0.59	997

Confusion Matrix:
[[407 180]
[226 184]]

Nilai F1-score untuk kelas phishing relatif rendah, yaitu sebesar 0.48, sedangkan kelas non-phishing memiliki nilai yang lebih tinggi. Hal ini menunjukkan bahwa fitur numerik sederhana belum optimal dalam membedakan pola URL phishing yang lebih kompleks.

Penelitian sebelumnya juga mengungkapkan bahwa algoritma dasar seperti KNN sensitif terhadap ketidakseimbangan data dan variasi skala. Oleh karena itu, meskipun model menunjukkan potensi, diperlukan penambahan fitur atau teknik penyeimbangan data seperti SMOTE untuk meningkatkan performa pada kelas phishing.

Secara keseluruhan, hasil penelitian ini mendukung temuan bahwa deteksi phishing berbasis URL membutuhkan kombinasi fitur struktural dan konten untuk mencapai akurasi lebih baik.

KESIMPULAN

Penelitian ini menunjukkan bahwa algoritma K-Nearest Neighbor mampu melakukan klasifikasi terhadap URL phishing dengan akurasi 59%, yang tergolong sedang. Model lebih efektif dalam mendeteksi URL non-phishing dibandingkan phishing, terutama akibat ketidakseimbangan data dan keterbatasan fitur numerik.

Penelitian selanjutnya direkomendasikan untuk menambahkan fitur berbasis analisis konten URL, menerapkan teknik penyeimbangan data, atau menggunakan metode klasifikasi

yang lebih kompleks seperti Random Forest atau XGBoost untuk meningkatkan performa deteksi.

Daftar Pustaka

[1.] UCI Machine Learning Repository. https://archive.ics.uci.edu/
[2.] OpenML. https://www.openml.org/
[3.] Kaggle Datasets. https://www.kaggle.com/datasets
[4.] Pedregosa et al., Scikit-learn: Machine Learning in Python, JMLR 2011