BAB I
PENDAHULUAN

1.1 Latar Belakang

Konten web jahat merujuk pada jenis konten online yang meliputi berbagai komponen seperti situs web, halaman web, skrip, dan file yang dapat diunduh, yang sengaja dibuat untuk merugikan atau mengeksploitasi pengguna. Kerentanan semacam itu semakin sulit dideteksi karena terus munculnya teknik baru dalam melakukan serangan. Selain itu, tidak semua pengguna menyadari berbagai jenis eksploitasi yang dapat dimanfaatkan oleh penyerang. Oleh karena itu, ketika pengguna berinteraksi dengan halaman web yang tidak diketahui, sangat penting untuk berhati-hati. Selain itu, jika URL itu sendiri mencurigakan dan menunjukkan tanda-tanda sebagai URL phishing, maka pengguna akan terlindungi dari situs web tersebut. Phishing sering kali dilakukan dengan mengirimkan email yang tampak seperti berasal dari organisasi yang dikenal atau perusahaan tertentu, seperti bank atau toko online, yang meminta pengguna untuk memperbarui informasi akun mereka melalui tautan yang disediakan. Tautan tersebut kemudian mengarahkan pengguna ke situs web palsu yang menyerupai situs web asli, dan jika pengguna memasukkan informasi pribadi mereka, informasi tersebut akan dicuri oleh penipu.

Metode Random Forest merupakan sebuah teknik pembelajaran ansambel yang menggabungkan beberapa pohon keputusan untuk membuat model prediksi yang lebih handal[4]. Dengan melatih pohon keputusan yang berbeda pada subkumpulan data, lalu mengambil rata-rata hasilnya, ini mengurangi overfitting dan meningkatkan kinerja model secara keseluruhan. Teknik ini cocok digunakan dalam tugas klasifikasi dan regresi, dan dianggap sebagai teknik pembelajaran mesin yang kuat[5].

Random Forest mengklasifikasikan atribut dari suatu kelas sehingga dapat digunakan untuk menemukan prediksi pada data yang belum ditemukan. Pohon keputusan sendiri adalah pendekatan " *divide and conquer*" dalam menganalisis masalah dari sekumpulan data independen yang digambarkan dalam bentuk

pohon. Pohon keputusan juga terdiri dari serangkaian pertanyaan yang tersusun secara sistematis, di mana setiap pertanyaan yang ada menentukan percabangan berdasarkan nilai atribut dan berakhir pada daun pohon yang merupakan prediksi dari kelas variabel[7].

KNN adalah algoritma Machine Learning yang digunakan untuk klasifikasi dan regresi. Algoritma ini berfungsi dengan cara mencari K titik terdekat dari data yang telah ada, kemudian memprediksi kelas atau nilai target dari data baru berdasarkan mayoritas kelas atau nilai target dari tetangga terdekat[6].

Dalam tugas klasifikasi, KNN menghitung jarak antara data baru dan titik-titik yang sudah ada, lalu memilih K titik terdekat. Dari K titik tersebut, KNN menentukan kelas data baru berdasarkan mayoritas kelas dari K titik terdekat tersebut.

Malicious adalah sebuah istilah yang digunakan untuk menggambarkan perilaku atau tindakan yang dilakukan dengan sengaja dan bertujuan untuk merusak, mengambil alih, atau mencuri sumber daya atau informasi milik orang atau organisasi lain. Perilaku malicious dapat dilakukan oleh individu, kelompok, atau organisasi dengan berbagai motif, seperti keuntungan finansial, tujuan politik, atau hanya untuk kesenangan semata.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang diuraikan, dapat dirumuskan sebuah permasalahan, yaitu bagaimana melakukan proses klasifikasi menggunakan algoritma berikut:

A. *Random Forest*
B. *K-Nearest Neighbors (KNN)*

1.3 Batasan Masalah

Untuk mempersempit pembahasan pada skripsi ini, maka akan dibuat Batasan Batasan sebagai berikut:

A. Algoritma, penelitian ini akan membandingkan *random forest* dan *K-Nearest Neighbors* (KNN) dalam performa klasifikasi data.
B. Proses pembuatan *source code* menggunakan bahsa pemrograman python dan dibantu oleh library yang dibutuhkan dalam pembuatan *source code*..
C. Datset, dataset yang digunakan merupakan dataset phising yang diperoleh melalui repository Kaggle.
D. Google Colab media yang digunakan untuk penlulisan *source code*.
E. Metode evaluasi, penelitian ini akan menggunakan metode evaluasi seperti akurasi, precision, recall, F1-score, ROC-AUC, dan Confusion matrix untuk mengevaluasi performa dari RF dan KNN.
F. Jenis data, penelitian ini hanya akan fokus pada klasifikasi data numerik dengan target variabel diskrit.
G. Lingkup penelitian, penelitian ini akan dilakukan pada skala kecil, dengan jumlah sampel dan fitur yang terbatas.

1.4 Tujuan Penelitian

Berdasarkan latar belakang dan rumusan masalah yang telah diuraikan, maka tujuan dilakukannya penelitian ini adalah:

A. implementasi *random forest* dan K-Nearest Neighbors (KNN) untuk mendeteksi *malicious web content*.
B. Memberikan hasil implementasi dan Analisa menggunakan *random forest* dan *K-Nearst neighbour* secara relevan dan akurqasi yang tinggi.

1.5 Manfaat Penelitian

Penulisan laporan tugas akhir ini memilki manfaat sebagai pengetahuan untuk menerapkan system kecerdasan buatan terhadap program untuk mendeteksi *malicious web content* berbahaya, dan juga tugas akhir ini diharapkan bermanfaat untuk menambah pengetahuan mengenai sistem pertahanan sebuah program pada computer untuk melindungi computer dari *malicious web content.*