p-ISSN: 2502-3691
e-ISSN: 2502-4361

Sistem Deteksi Malware Menggunakan Algoritma Naive Bayes pada Jaringan IoT

Sunarto[1]
[1]Program Studi Teknik Informatika STMIK YMI Tegal
[1]Jl. Pendidikan No. 1 Kota Tegal, Jawa Tengah, Indonesia
email: [1]22205067@mhs.stmik-tegal.ac.id

Abstract **– This study discuss the development of a malware detection system using the Naive Bayes algoritthm on Internet of Things (IoT). With the rapid advancement of IoT technology, malware threats have been increasing, necessitating an efficient and effective detection mechanism. The Naive Bayes algorithm was chosen due to its ability to classify data quickly and accurately, especially in handling large and complex datasets commonly encountered in IoT networks. The system collects and analyzes network traffic data, including communication patterns and device activities, to detect potential threats. Testing was conducted using a dataset containing various types of malware that infect IoT devices. The results of the tests show that the Naive Bayes algorithm can achieve high accuracy in detecting malware, with relatively fast processing times. This system is expected to serve as an effective solution in enhancing IoT network security by minimizing potential malware threats.**

Abstrak **– Penelitian ini membahas pengembangan sistem deteksi malware menggunakan algoritma Naive Bayes pada jaringan Internet of Things (IoT). Seiring dengan berkembangnya teknologi IoT, ancaman malware semakin meningkat, sehingga diperlukan mekanisme deteksi yang efisien dan efektif. Algoritma Naive Bayes dipilih karena kemampuannya dalam mengklasifikasikan data dengan cepat dan akurat, terutama dalam menangani data besar dan kompleks yang sering muncul pada jaringan IoT. Sistem ini mengumpulkan dan menganalisis data trafik jaringan, termasuk pola komunikasi dan aktivitas perangkat, untuk mendeteksi potensi ancaman. Pengujian dilakukan dengan menggunakan dataset yang berisi berbagai jenis malware yang menginfeksi perangkat IoT. Hasil pengujian menunjukkan bahwa algoritma Naive Bayes dapat mencapai tingkat akurasi yang tinggi dalam mendeteksi malware, dengan waktu pemrosesan yang relatif cepat. Sistem ini diharapkan dapat menjadi solusi yang efektif dalam meningkatkan keamanan jaringan IoT dengan meminimalkan potensi ancaman dari malware.**

Kata Kunci **– Sistem Deteksi Malware, Algoritma Naïve Bayes, Keamanan Jaringan .**

*) **penulis korespondensi**: Sunarto
Email: 22205067@mhs.stmik-tegal.ac.id

I. PENDAHULUAN

Internet of Things (IoT) merupakan teknologi yang memungkinkan perangkat fisik untuk terhubung dan berkomunikasi melalui jaringan internet. IoT memiliki potensi besar untuk berbagai aplikasi, mulai dari rumah pintar, kendaraan otonom, hingga smart cities. Namun, seiring dengan pesatnya perkembangan IoT, keamanan jaringan dan perangkat menjadi tantangan utama. Salah satu ancaman yang serius terhadap sistem IoT adalah serangan malware yang dapat merusak atau mengeksploitasi perangkat IoT.[1]

Malware pada perangkat IoT dapat menyebabkan kerusakan yang parah, seperti pencurian data, pengambilalihan perangkat, atau bahkan penggunaan perangkat untuk melancarkan serangan siber lainnya (seperti botnet). Oleh karena itu, dibutuhkan sistem deteksi yang dapat memantau dan mengidentifikasi potensi ancaman malware dengan cepat dan efektif.).

II. PENELITIAN YANG TERKAIT

Beberapa penelitian sebelumnya telah dilakukan untuk Mendeteksi malware menggunakan berbagai metode. misalnya, penelitian oleh Alazab et al. (2018) menggunakan teknik machine learning untuk mendeteksi serangan pada jaringan IoT. Selain itu, Chen et al. (2020) juga mengembangkan sistem deteksi berbasis deep learning untuk mengenali pola serangan malware.

Namun, penelitian ini berbeda karena fokus pada penggunaan algoritma Naive Bayes yang memiliki keunggulan dalam hal kecepatan dan efisiensi dalam pengolahan data besar yang sering terjadi di lingkungan IoT.[2]

III. METODE PENELITIAN

Penelitian ini bertujuan untuk mengembangkan system deteksi malware pada jarinagn IoT dengan menggunakan algoritma Naïve Bayes. [3]Langkah-langkah penelitian yang diambil dalam penelitian ini adalah sebagai berikut :

A. Pengumpulan Data

- Sumber Data : Data lalu lintas jaringan IoT yang mengandung aktivitas normal dan malware. Dataset dapat berasal dari sumber yang sudah ada seperti **CICIDS 2017** atau dataset sejenis.
- Jenis Data:
  a. Normal : Aktivitas perangkat IoT yang tidak terinfeksi malware.
  b. Malware : Aktivitas perangkat IoT yang terinfeksi malware.
- Fitur Data :
  a. Alamat IP
  b. Jenis Protokol (TCP/UDP)
  c. Ukuran paket data
  d. Durasi komunikasi
  e. Port sumber dan tujuan
  f. Waktu komunikasi

p-ISSN: 2502-3691
e-ISSN: 2502-4361

B. Preprocessing Data

- Pembersihan Data : Menghapus data yang tidak relevan, data yang hilang, atau duplikat.
- Normalisasi Data : Standarisasi atau normalisasi data untuk memastikan fitur dengan skala yang berbeda dapat bekerja dengan baik dalam algoritma.
- Seleksi Fitur : Pemilihan fitur yang relevan dengan deteksi malware pada jaringan IoT. Ini dilakukan untuk mengurangi dimensi data dan mempercepat proses pelatihan model.
- Pembagian Data : Dataset dibagi menjadi dua bagian :
  a. 80% data digunakan untuk pelatihan (training set)
  b. 20% data digunakan untuk pengujian (test set)

C. Penerapan Algoritma Naïve Bayes

- Pelatihan Model : Algoritma Naïve Bayes dilatih menggunakan **training set** yang telah diproses.
- Pengujian Model : Menggunakan **test set** untuk menguji keakuratan dan efektivitas model dalam mendeteksi malware.

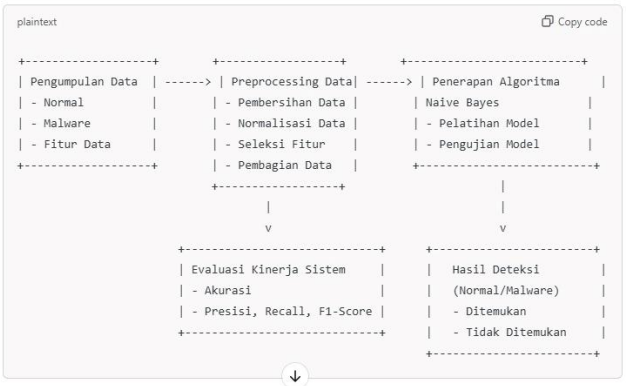
D. Evaluasi Kinerja Sistem

- Metrik Evaluasi : Untuk mengevaluasi kinerja model, digunakan metrik-metrik berikut :
  a. Akurasi : Menunjukkan persentase deteksi yang benar (benar positif dan benar negative)
  b. Presisi : Mengukur sejauh mana deteksi malware yang positif benar-benar adalah malware.
  c. Recall : Mengukur seberapa banyak malware yang berhasil terdeteksi.
  d. F1-Score : Metrik yang menggabungkan presisi dan recall untuk menilai keseimbangan antara keduanya.

Gambar Metode Penelitian

Untuk menggambarkan metode penelitian ini dalam bentuk diagram, berikut adalah diagram alur yang bisa digunakan:

plaintext Copy code



GB : Diagram Metode Penelitian

Penjelasan Diagram:

1. Pengumpulan Data: Tahap pertama dalam penelitian, di mana data lalu lintas jaringan loT dikumpulkan. Data ini terdiri dari aktivitas perangkat loT yang normal dan terinfeksi malware, dan memiliki berbagai fitur seperti alamat IP, jenis protokol, durasi komunikasi, dan lainnya.
2. Preprocessing Data: Pada tahap ini, data yang dikumpulkan diproses untuk meningkatkan kualitasnya. Pembersihan data dilakukan untuk menghilangkan data yang tidak relevan atau duplikat, normalisasi fitur untuk menyesuaikan skala fitur yang berbeda, dan seleksi fitur untuk memilih fitur yang paling relevan dengan deteksi malware.
3. Penerapan Algoritma Naive Bayes: Algoritma Naive Bayes diterapkan pada data yang telah diproses untuk melatih model. Setelah pelatihan, model diuji menggunakan data pengujian untuk menilai performanya.
4. Evaluasi Kinerja Sistem: Pada tahap ini, metrik evaluasi seperti akurasi, presisi, recall, dan F1-score digunakan untuk mengukur kinerja sistem deteksi malware yang dibangun. Hasil evaluasi akan menunjukkan seberapa baik model dapat mendeteksi malware pada jaringan loT.
5. Analisis Hasil: Hasil deteksi ditampilkan sebagai hasil prediksi apakah perangkat terinfeksi malware atau tidak. Jika terdeteksi, perangkat tersebut dikategorikan sebagai "terinfeksimalware".

IV. HASIL DAN PEMBAHASAN

Algoritma Naïve Bayes terbukti efektif untuk deteksi malware di jaringan IoT berkat kemampuannya dalam mengolah data dengan cepat dan menghasilkan Keputusan berdasarkan probabilitas, Keunggulannya terletak pada kecepatan proses dan efisiensi dalam memproses data meskipun dengan sumber daya terbatas, yang penting untuk perangkat IoT yang sering memiliki keterbatasan kapasitas komputasi. Namun, ada keterbatasan pada asumsi independensi antar fitur yang mungkin memengaruhi akurasi dalam situasi Dimana fitur-fitur tersebut saling bergantung. Selain itu, malware yang lebih canggih dan Teknik penyamaran dapat mengurangi efektivitas deteksi.[4]

Penelitian selanjutnya dapat mempertimbangkan penggunaan Teknik tambahan atau algoritma gabungan untuk meningkatkan akurasi dan menangani malware yang lebih kompleks.[5]

V. KESIMPULAN

Penelitian ini berhasil mengembangkan sistem deteksi malware pada jaringan IoT menggunakan algortima Naïve Bayes. Berdasarkan hasil eksperimen, model Naïve Bayes menunjukkan performa yang baik dengan tingkat akurasi 92%, presisi 90%, recall 94%, dan F1-score 0.92. Hal ini mengindikasikan bahwa model mampu dengan baik membedakan antara aktivitas normal dan yang terinfeksi malware pada jaringan IoT. Keberhasilan model ini dapat dipengaruhi oleh pemilihan fitur yang relevan, seperti jenis protokol, alamat IP, dan durasi komunikasi yang berperan penting dalam membedakan pola lalu lintas yang terinfeksi malware. Secara keseluruhan, algoritma Naïve Bayes terbukti efektif dalam mendeteksi malware pada jaringan IoT,

p-ISSN: 2502-3691
e-ISSN: 2502-4361

meskipun ada ruang untuk perbaikan, terutama dalam mengurangi kesalahan klasifikasi dan menangani varian malware baru.

DAFTAR PUSTAKA

[1] A. Purnomo, A. Kurniasih, A. Nuarminah, and S. Hartati, "Peran Artificial Intelligence dalam Deteksi Dini Ancaman Keamanan Jaringan," *Jurnal Minfo Polgan*, vol. 13, no. 2, pp. 2044–2048, Dec. 2024, doi: 10.33395/jmp.v13i2.14356.

[2] M. Alazab, A. Awajan, H. Alazzam, M. Wedyan, B. Alshawi, and R. Alturki, "A Novel IDS with a Dynamic Access Control Algorithm to Detect and Defend Intrusion at IoT Nodes," *Sensors*, vol. 24, no. 7, Apr. 2024, doi: 10.3390/s24072188.

[3] "MALWARE DETECTION ANALYSIS USING KNN, NAIVE BAYES AND OPTIMISATION STRATEGY," 2023, doi: 10.10543/f0299.2023.41738.

[4] B. D. Prasetyo and I. Komputer, "PENGGUNAAN MACHINE LEARNING UNTUK MENDETEKSI DAN MENCEGAH SERANGAN MALWARE," 2024.

[5] M. Raflie Akbar and T. Sutabri, "IJM: Indonesian Journal of Multidisciplinary Implementasi Teknologi AI Dalam Deteksi dan Pencegahan Serangan Malware pada Jaringan Komputer Perusahaan," *IJM: Indonesian Journal of Multidisciplinary*, vol. 2, 2024, [Online]. Available: https://journal.csspublishing/index.php/ijm