BAB I

PENDAHULUAN

1.1. LATAR BELAKANG MASALAH

Internet of Things (IoT) adalah jaringan perangkat fisik yang saling terhubung melalui internet untuk mengumpulkan dan bertukar data. Teknologi ini mencakup perangkat rumah tangga, kendaraan, mesin industri, hingga perangkat kesehatan yang dilengkapi sensor dan perangkat lunak untuk meningkatkan efisiensi dan kenyamanan pengguna [1].

Perangkat *IoT* rentan untuk diambil alih dan digunakan dalam serangan berskala besar tanpa sepengetahuan pemilik perangkat, yang dapat menyebabkan pembentukan *botnet* Kerentanan ini disebabkan oleh kata sandi yang lemah dan kurangnya standar keamanan yang kuat dari produsen Contohnya adalah *botnet* Mirai pada tahun 2016, yang meluncurkan serangan *DDoS* besar-besaran dari jutaan perangkat yang terkompromi, menunjukkan potensi ancaman dari IoT. Contoh lainnya adalah Mozi, varian tipe Mirai yang muncul pada tahun 2019, mengendalikan sekitar 438.000 *host*, dan pada tahun 2020 menyumbang 89% dari total serangan *IoT* yang terdeteksi oleh *IBM* [2].

Serangan *Distributed Denial of Service (DDoS)* adalah salah satu ancaman utama terhadap sistem jaringan, yang memengaruhi aplikasi dan perangkat yang bergantung padanya. Serangan *DDoS* dilakukan dengan mengelompokkan banyak perangkat untuk menyerang satu target, sehingga pengguna yang sah tidak dapat mengakses layanan seperti email dan situs web. Serangan ini merupakan jenis

serangan paling umum dan kritis pada perangkat *Internet of Things (IoT),* komputasi awan, dan jaringan komunikasi generasi kelima (*5G*) [3]

Serangan *DDoS* dapat dikategorikan ke dalam dua jenis utama berdasarkan ukuran lalu lintas yang dihasilkannya: serangan tingkat tinggi (*high-rate*) dan serangan tingkat rendah (*low-rate*)**.** Serangan tingkat rendah sangat sulit terdeteksi karena pola lalu lintasnya mirip dengan lalu lintas normal, dan dapat mencakup sekitar 10–20% dari total lalu lintas jaringan normal Serangan ini dengan cepat menguras sumber daya jaringan dan kapasitasnya, membuat korban tidak responsif dalam waktu singkat [4].

Meskipun rata-rata lalu lintasnya kecil, serangan ini dapat secara signifikan mengurangi kualitas layanan, bahkan menghentikannya sepenuhnya, dengan mengirimkan data dalam pola pulsa periodik, bukan aliran kontinu. Sebaliknya, serangan tingkat tinggi menggunakan transmisi paket dengan kecepatan tinggi, sehingga perubahan statistik dalam pola lalu lintasnya dapat digunakan untuk membedakan dari aliran data normal [5].

Untuk mengatasi serangan *DDOS* telah dilakukan berbagai penelitian sebelumnya misalnya, Sicari et al. [6] membahas pendekatan keamanan untuk meningkatkan keandalan perangkat *IoT* dengan model berbasis privasi dan kontrol akses. Penelitian lain oleh Moustafa et al. [7] memanfaatkan dataset *TON_IoT* untuk mengembangkan algoritma deteksi serangan siber yang lebih efektif, dengan fokus pada pola trafik anomali. Selain itu, Al-Hadhrami dan Hussain [8] menerapkan machine learning pada dataset *IoT* untuk mendeteksi serangan *DDoS*

secara real-time, menunjukkan hasil yang menjanjikan pada beberapa algoritma seperti *Random Forest* dan *SVM* [8].

Meskipun banyak pendekatan telah diusulkan, ada beberapa kesenjangan utama. Pertama, sebagian besar penelitian kurang memperhatikan distribusi data yang tidak seimbang, yang sering terjadi dalam dataset serangan siber, sehingga model menjadi bias terhadap kelas mayoritas [7]. Kedua, banyak metode seperti *SVM* dan *Random Forest* membutuhkan waktu komputasi yang tinggi untuk dataset besar, yang kurang ideal untuk aplikasi real-time pada infrastruktur *IoT* [9]. Selain itu, studi sebelumnya sering kali hanya berfokus pada akurasi, tanpa mengevaluasi efisiensi waktu atau skalabilitas algoritma pada data *IoT* yang terus berkembang.

Berbagai metode telah digunakan dalam deteksi serangan *DDoS*. Pendekatan tradisional seperti signature-based detection sering kali digunakan karena sederhana dan efektif untuk pola serangan yang dikenal. Namun, metode ini tidak dapat mendeteksi serangan baru atau yang bervariasi [6]. Sebaliknya, metode berbasis machine learning, seperti *Decision Tree, Naïve Bayes, dan Support Vector Machine (SVM),* menunjukkan kemampuan lebih baik dalam mendeteksi pola anomali, terutama pada dataset yang kompleks. *Random Forest* sering digunakan karena kemampuannya menangani dataset yang besar, sementara metode ensemble learning lainnya, seperti *Gradient Boosting* dan *AdaBoost*, memberikan hasil yang lebih akurat dalam mendeteksi serangan *DdoS* [8].

Metode *XGBoost* dipilih karena memiliki keunggulan signifikan dibandingkan metode lain. Pertama, algoritma ini dapat menangani data tidak seimbang dengan baik melalui pengaturan scale_pos_weight. Kedua, *XGBoost*

dirancang untuk efisiensi tinggi, dengan kemampuan paralelisasi yang memungkinkan pelatihan lebih cepat dibandingkan metode seperti *Random Forest* atau *SVM.* Selain itu, fleksibilitas parameter tuning pada *XGBoost* memungkinkan penyesuaian model sesuai kebutuhan dataset spesifik, yang sangat penting dalam menangani pola trafik *IoT* yang heterogen. Kombinasi efisiensi, akurasi tinggi, dan skalabilitas menjadikan *XGBoos*t pilihan ideal untuk deteksi serangan *DDoS* pada *IoT* [9].

XGBoost (Extreme Gradient Boosting) menjadi solusi yang menjanjikan untuk mengatasi kesenjangan tersebut. Dengan kemampuannya untuk menangani dataset besar dan tidak seimbang, *XGBoost* mampu mendeteksi pola serangan secara lebih efektif dan efisien dibandingkan metode lain [9]. Algoritma ini juga mendukung paralelisasi selama pelatihan, yang mempercepat proses komputasi bahkan untuk dataset *IoT* yang kompleks. Penelitian menunjukkan bahwa *XGBoost* memberikan akurasi tinggi hingga 99% pada berbagai dataset serangan *DDoS,* termasuk *dataset TON_IoT dan CIC-DdoS* [7].

Berdasarkan uraian latar belakang di atas maka penulis akan melakukan penelitian dengan judul "**DETEKSI SERANGAN DDOS PADA INFRASTRUKTUR IOT MENGGUNAKAN METODE XGBOOST**"

1.2. RUMUSAN MASALAH

Perangkat *IoT* rentan terhadap serangan *DDoS*, sementara metode deteksi tradisional dan beberapa algoritma *machine learning* kurang optimal dalam mengatasi data tidak seimbang dan kebutuhan. Dalam hal ini, perlu dieksplorasi

sejauh mana algoritma *XGBoost* dapat meningkatkan efisiensi, dan skalabilitas deteksi serangan *DDoS* pada lingkungan *IoT* yang kompleks.

Berdasarkan pernyataan diatas maka rumusan masalah penelitian adalah:

1. Bagaimana mengimplementasikan metode *xgboost* untuk mendeteksi serangan *ddos* attack pada *iot*?
2. Bagaimana performa metode *xgboost* dalam mendeteksi serangan *ddos* pada infrastruktur *iot*?

1.3. BATASAN MASALAH

Dalam penelitian yang dilakukan oleh penulis agar dapat selalu fokus pada pokok permasalahan yang ada, maka penulis membatasi hal- hal sebagai berikut:

1. Fokus penelitian ini adalah pada deteksi serangan *DDoS* berbasis protokol jaringan pada perangkat *IoT.*
2. Dataset yang digunakan adalah datasets *CIC-IOT 2023* dengan jumlah data 385931 dengan 40 atribut.
3. Pengukuran performa menggunakan *F1-Score.*
4. *Software* analisis yang digunakan adalah *google colab*.

1.4. TUJUAN PENELITIAN

Berdasarkan rumusan masalah diatas, penelitian yang akan dilakukan oleh penulis memiliki tujuan sebagai berikut:

1. Mengembangkan model deteksi serangan *DDoS* berbasis *XGBoost* yang dioptimalkan untuk infrastruktur *IoT*.

2. Menganalisis performa *xgboost* dalam mendeteksi serangan *DDoS.*

1.5. MANFAAT PENELITIAN

Dengan adanya penelitian ini diharapkan dapat memberikan manfaat antara lain:

1. Memberikan solusi praktis berupa model deteksi serangan *DDoS* yang lebih akurat dan cepat, khususnya untuk infrastruktur *IoT*. Dengan mengoptimalkan *XGBoost*, model ini dapat membantu mengatasi tantangan spesifik seperti data yang tidak seimbang dan kebutuhan *real-time* dalam pengelolaan serangan *DDoS.* Hal ini dapat mendorong pengembangan sistem *IoT* yang lebih aman dan andal.
2. Agar memudahkan pada pemahaman lebih dalam tentang efektivitas *XGBoost* dalam mendeteksi serangan *DDoS.* Analisis performa ini juga memberikan wawasan yang dapat membantu praktisi dan peneliti memilih algoritma machine learning terbaik untuk keamanan *IoT,* sehingga meningkatkan efisiensi dan kualitas sistem deteksi serangan di dunia nyata.

1.6. SISTEMATIKA PENULISAN

Sistematika penulisan menggambarkan secara umum tentang apa yang akan dibahas secara umum tentang apa yang akan dibahas penulis dalam setiap Bab dari laporan tugas akhir yang terdiri dari 5 (lima) Bab. Adapun susunannya adalah sebagai berikut:

BAB I : PENDAHULUAN

Bab ini akan memberikan gambaran umum tentang topik penelitian, latar belakang, rumusan masalah, batasan masalah, manfaat penelitian, dan sistematika penulisan.

BAB II : LANDASAN TEORI

Bab ini akan menjelaskan teori - teori yang relevan untuk penelitian ini, dan memberikan pemahaman yang mendalam tentang konsep-konsep yang terkait.

BAB III : METODOLOGI PENELITIAN

Bab ini menjelaskan tentang metodologi penelitian yang digunakan, termasuk langkah-langkah dalam melatih dan mengimplementasikan metode *XGBoost*, pengumpulan dan pra proses data, pelatihan model *XGBoost*, serta perangkat lunak yang digunakan.

BAB IV : ANALISIS DAN HASIL

Bab ini akan dipresentasikan analisis mengenai implementasi *XGBoost* dalam penelitian ini. Penulis akan membahas data yang digunakan, hasil eksperimen, dan perhitungan yang relevan dengan penggunaan metode *XGBoost.*

BAB V : KESIMPULAN DAN SARAN

Bab ini merangkum temuan-temuan utama yang dihasilkan dari penelitian ini dan memberikan saran-saran yang relevan. Kesimpulan ini mencakup penilaian terhadap sejauh mana

tujuan penelitian telah tercapai, sementara saran memberikan rekomendasi mengenai pengembangan lebih lanjut dari penelitian ini dan potensi penelitian lanjutan.