

BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Di era digital yang berkembang pesat ini, keamanan siber menjadi salah satu aspek yang sangat penting untuk diperhatikan. Perkembangan teknologi informasi dan komunikasi telah memberikan banyak manfaat bagi kehidupan kita, juga menghadirkan risiko serius terkait keamanan data[1]. Salah satu bentuk penerapan teknologi digital yang tengah berkembang pesat adalah *Internet of Things* (IoT). *Internet of Things* (IoT) merupakan konsep yang memungkinkan berbagai objek atau perangkat saling terhubung dan berkomunikasi melalui jaringan digital. Teknologi ini merupakan perluasan dari konsep internet sebelumnya yang hanya terbatas pada koneksi antar komputer[2].

Internet of Things (IoT) telah menjadi bagian tak terpisahkan dari kehidupan modern. *Internet of Things* (IoT) merupakan teknologi yang terkait dengan teknologi jaringan sensor nirkabel yang di dalamnya terdapat sensor, aktuator, perangkat *GPS* dan seluler, tetapi juga merambah ke sektor transportasi, khususnya pada kendaraan[3]. Kombinasi antara teknologi *Internet of Things* (IoT) dan kendaraan melahirkan konsep yang dikenal dengan istilah *Internet of Vehicles* (IoV). *Internet of Vehicles* IoV merupakan bentuk implementasi IoT di sektor transportasi yang bertujuan untuk meningkatkan konektivitas antar kendaraan dan infrastruktur pendukung. Konsep ini merupakan hasil integrasi dari berbagai bidang, seperti teknologi internet, industri elektronik, otomotif, serta sektor industri lainnya, sebagai mewujudkan sistem transportasi yang ramah lingkungan dan efisien [4].

Meskipun jaringan IoT, termasuk dalam implementasinya pada IoV menawarkan berbagai kemudahan dan efisiensi, aspek keamanannya masih menjadi titik lemah yang rentan terhadap serangan siber. Ancaman ini berpotensi membahayakan privasi data serta keselamatan pengguna, terutama dalam konteks sistem transportasi cerdas yang sangat bergantung pada konektivitas dan integritas data. [5]. Pelaku kejahatan siber umumnya berupaya memperoleh sebanyak mungkin informasi dari sistem target melalui berbagai metode. Salah satu teknik serangan yang sering digunakan adalah *Distributed Denial of Service* (DDoS), yang bertujuan untuk melumpuhkan sistem atau layanan dengan membanjirinya menggunakan lalu lintas data secara berlebihan dari berbagai sumber [6].

Serangan *DOS* (*Denial Of Service*) dan *DDoS* (*Distributed Denial Of Service*) adalah serangan yang mungkin sering dijumpai diantara serangan serangan lainnya[7]. Serangan *Distributed Denial-of-Service* (*DDoS*) merupakan jenis serangan yang bertujuan untuk menyebabkan gangguan atau kerusakan (crash) pada server maupun sistem jaringan dengan cara membanjiri jaringan tersebut menggunakan sejumlah besar paket data atau permintaan secara simultan. [8]. Untuk mencegah serangan *DDoS*, *Intrusion Detection System* (*IDS*) digunakan sebagai solusi dalam mendeteksi dan memperkuat keamanan jaringan..

Intrusion Detection System (*IDS*) merupakan sistem yang berfungsi memantau lalu lintas dan aktivitas dalam jaringan untuk mendeteksi adanya perilaku mencurigakan. Jika ditemukan ancaman, *IDS* akan memberikan peringatan kepada sistem atau administrator jaringan[9]. Dalam mendeteksi terjadinya anomali pada lalu lintas jaringan, sistem deteksi intrusi (*Intrusion Detection System* atau *IDS*) memerlukan metode yang tepat dan andal. Salah satu pendekatan yang dapat digunakan adalah penerapan teknik *Deep Learning*. *Deep Learning* merupakan cabang dari *Artificial Neural Network* yang termasuk ke dalam metode *machine learning* dengan arsitektur yang lebih kompleks, karena terdiri atas banyak lapisan (*layers*). Kompleksitas arsitektur ini memungkinkan *Deep Learning* untuk menangani permasalahan yang bersifat non-linear dan kompleks, serta mampu mengolah data dalam jumlah besar secara lebih efisien.[10].

Pada penelitian [11], menguraikan suatu pola untuk mendeteksi serangan *brute-force* pada protokol *SSH* dan *FTP* dengan memanfaatkan pendekatan *Machine Learning*, khususnya menggunakan algoritma *Long Short-Term Memory* (*LSTM*). Dalam implementasinya, penelitian ini menggunakan dataset *CIC-IDS-2017* sebagai sumber data pelatihan dan pengujian. Hasil pengujian menunjukkan bahwa deteksi serangan *brute-force* mencapai tingkat akurasi tertinggi, yaitu sebesar 99,88%, ketika model dilatih menggunakan fungsi aktivasi *tangent hyperbolic* (*TANH*) dan fungsi optimasi *categorical crossentropy*.

Dan pada penelitian [12], membahas penerapan pendekatan *Deep Learning* dalam mendeteksi serangan *SSH Brute-Force* dengan menggunakan dataset *CIC-IDS 2018*. Berdasarkan hasil eksperimen yang dilakukan, *Convolutional Neural Network* (*CNN*) menunjukkan kinerja yang lebih unggul dibandingkan dengan beberapa metode *Deep Learning* lainnya, seperti *Naïve Bayes*, *Logistic*

Regression, Decision Tree, k-Nearest Neighbor, dan Support Vector Machine. Model CNN berhasil mencapai tingkat akurasi sebesar 94,3%, presisi sebesar 92,5%, *recall* sebesar 97,8%, serta *F1-score* sebesar 91,8% dalam mengidentifikasi serangan SSH *Brute-Force*.

Pada penelitian [13], menunjukkan bahwa pembelajaran mendalam (*Deep Learning*) yang diterapkan pada *Intrusion Detection System* (IDS) mampu mengidentifikasi aktivitas jaringan, khususnya dalam mendeteksi serangan *Denial of Service* (DoS). Pada pengujian yang dilakukan terhadap model CNN VGG-19, dengan lima kali uji data, diperoleh tingkat presisi sebesar 99,32% dan standar deviasi sebesar 4,08%, yang mengindikasikan kinerja model yang sangat baik dalam mendeteksi serangan tersebut.

Berdasarkan permasalahan yang telah diuraikan diatas maka penelitian ini mengusulkan “Deteksi serangan *DDoS* pada jaringan *IoV* menggunakan *Convolutional Neural Network*”.

1.2. RUMUSAN MASALAH

Berdasarkan pada uraian latar belakang yang telah disampaikan, maka rumusan masalah dalam penelitian ini dapat dinyatakan sebagai berikut:

1. Bagaimana menerapkan model deteksi serangan *DDoS* pada jaringan *Internet of Vehicles* (IoV) menggunakan metode *Convolutional Neural Network* (CNN)?
2. Seberapa akurat model CNN dalam mengklasifikasikan serangan *DDoS* pada jaringan IoV?

1.3. BATASAN MASALAH

Berikut merupakan beberapa batasan masalah yang dapat diuraikan pada penelitian ini, antara lain:

1. Penelitian ini hanya berfokus pada pendeteksian jenis serangan *DDoS* dalam jaringan *Internet of Vehicles* (IoV).
2. Dataset yang digunakan dalam penelitian ini yaitu *CICIoT2023*.
3. Model *deep learning* yang digunakan dalam penelitian ini adalah *Convolutional Neural Network* (CNN) tanpa membandingkan dengan metode lain.

4. Menggunakan *tools Google Colaboratory* dengan Bahasa pemrograman *Phyton*.

1.4 TUJUAN DAN MANFAAT PENELITIAN

Adapun tujuan dan manfaat dari penelitian ini akan dijelaskan sebagai berikut:

1.4.1. Tujuan Peneltian

1. Mengidentifikasi fitur-fitur penting yang mempengaruhi deteksi serangan *DDoS* pada jaringan IoV.
2. Mengembangkan model deteksi serangan *DDoS* pada jaringan IoV menggunakan metode *Convolutional Neural Network (CNN)*.
3. Menganalisis kinerja model CNN dalam mengklasifikasikan lalu lintas jaringan IoV antara serangan *DDoS* dan lalu lintas normal.

1.4.2 Manfaat Penelitian

1. Mengembangkan model deteksi serangan *DDoS* pada jaringan IoV menggunakan metode *Convolutional Neural Network (CNN)*.
2. Menganalisis kinerja model CNN dalam mengklasifikasikan lalu lintas jaringan IoV antara serangan *DDoS* dan lalu lintas normal.
3. Mengidentifikasi fitur-fitur penting yang mempengaruhi deteksi serangan *DDoS* pada jaringan IoV.

1.5 SISTEMATIKA PENULISAN

Untuk memberikan gambaran secara menyeluruh mengenai isi dari penulisan ilmiah ini, disajikan sistematika penulisan yang mencakup bagian-bagian sebagai berikut:

BAB I : PENDAHULUAN

Bab ini menyajikan bagian pendahuluan yang mencakup pembahasan latar belakang masalah, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, serta sistematika penulisan.

BAB II : LANDASAN TEORI

Bab ini memberikan landasan teori untuk menjadi dasar untuk membahas laporan tertentu, dan memberikan definisi yang mendasari penelitian yang dilakukan melalui tinjauan literatur sebagai dasar untuk melakukan analisis.

BAB III : METODOLOGI PENELITIAN

Bab ini membahas kerangka penelitian, metode atau pendekatan yang diterapkan, serta alat yang digunakan untuk menjawab pertanyaan penelitian guna mencapai tujuan yang telah ditetapkan.

BAB IV : ANALISIS DAN HASIL

Bab ini menjelaskan gambaran umum objek penelitian, serta menganalisis data. Hasil analisis disajikan dalam bentuk visualisasi dari tools yang digunakan yaitu *google collaboration*.

BAB V : KESIMPULAN

Kesimpulan dan pedoman yang disajikan dalam bab ini berasal dari hasil analisis yang mencakup semua informasi yang diperoleh.