# BAB I
# PENDAHULUAN

## 1.1 LATAR BELAKANG

Teknologi saat ini berkembang dengan cepat dan telah menjawab berbagai tantangan manusia untuk berinteraksi satu sama lain secara *real time* tanpa batas jarak, waktu, atau ruang [1]. Kehidupan manusia sekarang ini sangat bergantung pada teknologi, terutama berkat kemajuan *Internet of Things* (IoT), yang memungkinkan orang berkomunikasi dan berinteraksi dengan berbagai perangkat [2]. *Internet of Things* adalah pemusatan data dari berbagai jenis situasi tertentu ke platform virtual apa pun yang tersedia di internet [3]. *Internet of Things* (IoT) adalah konsep yang memungkinkan perangkat elektronik lokal untuk terhubung ke internet melalui jaringan nirkabel , memungkinkan komunikasi antara perangkat itu sendiri dan juga dengan penggunanya [4].

Kompleksitas dalam jaringan IoT jaringan tidak hanya dipengaruhi oleh perbedaan perangkat , tetapi juga oleh layanan, protokol, saluran komunikasi , tipe data, dan faktor lainnya. Akibat rendahnya hasil daya yang dimilikinya , jaringan *internet of things* ( IoT ) tidak dilengkapi dengan perlindungan yang dapat mencegahnya dari serangan *cyber* termasuk *phishing* , infeksi *malware* , dan *Distributed Denial of Service* ( DDoS) [5]. Sampai saat ini, perangkat *Internet of Things* telah terbukti memiliki masalah keamanan, seperti ketika perangkat IoT terinfeksi *malware Mirai* dan digunakan untuk menyerang *Dyn*, penyedia data

genetik [6].

*Distributed Denial of Service* (DDoS) adalah serangan terdistribusi yang beroperasi dengan cara mengganggu komunikasi beberapa permintaan dikirim ke sumber daya dengan tujuan untuk mencapai kapasitas dan menyebabkan server tidak dapat melibatkan banyak permintaan sehingga membuat server tidak bisa beroperasi secara efektif [7]. Serangan DDoS menggunakan beberapa *server* untuk mengirimkan permintaan informasi ke komputer korban yang mencegah sistem beroperasi secara normal, sehingga mencegah penyediaan layanan normal [6]. Serangan *SYN Flood* adalah serangan DDoS yang bekerja dengan cara memanfaatkan kekurangan pada protokol TCP. *Attacker* mengirim banyak serangan *Syn* ke system. Saat ini sistem menerima serangan, maka *system* akan mengirim balik ke pengirim. Setelah itu, *system* akan menerima serangan kembali untuk mengehentikan komunikasi. Terjadinya beberapa komunikasi mengakibatkan kerja *system* menjadi kurang efektif.[8]

Oleh karena itu, dibutuhkan suatu system yang dapat digunakan untuk melindungi jaringan[6]. *Intrusion Detection System* (IDS) merupakan salah satu sistem yang bertugas menjadi pengawas terhadap lalu lintas data di dalam jaringan komputer serta dapat mengawasi terhadap hal yang mencurigakan didalam jaringan. IDS akan memberitahukan pemberitahuan jika menemukan hal yang buruk di dalam jaringan komputer. Pemberitahuan tersebut bisa berupa pesan kepada sebuah sistem atau administrator jaringan. Namun karena banyaknya kompleksitas pada jaringan IoT, maka dalam membangun IDS yang memiliki kinerja yang tinggi menjadi sebuah tantangan [9] . Salah satu metode yang

ditawarkan adalah *deep learning* [5]. *Deep learning* dianggap sebagai komponen pembelajaran mesin karena memastikan evaluasi menyeluruh dan akurat dari sistem pembelajaran mesin. *Deep learning* didefinisikan sebagai penggunaan jaringan syaraf tiruan transparan yang dihubungkan menggunakan berbagai lapisan untuk menghasilkan output. [10]

Pada penelitian [11] , menunjukkan bahwa hasil pembelajaran mendalam dari IDS dapat mengidentifikasi aktivitas jaringan di antara serangan Dos. Pada pengujian presisi *CNN VGG-19* terhadap informasi dengan menjalankan 5 informasi pengujian diperoleh hasil ketepatan sebesar 99,32% dengan defisiensi tipikal sebesar 4,08%.

Pada penelitian [12] , menunjukan bahwa hasil pengujian RNN dan *Autoencoders* yang mendeteksi serangan tingkat rendah pada jaringan komputer memiliki akurasi tertinggi dibandingkan metode apa pun. Dengan menggunakan dataset *DO-RNN* dengan skor keganjilan paralel dan teknik batas *T(iqr)* dalam membedah asosiasi SMTP dan efektif mengenali hingga 100 persen dan FPR 1%.

Oleh karena itu, penelitian ini menyarankan penggunaan teknik *Convolutional Neural Network* (CNN) untuk mengidentifikasi serangan banjir TCP pada jaringan IoT. CNN merupakan metode *deep learning* yang banyak digunakan dalam *computer vision*, seperti klasifikasi, deteksi, dan segmentasi [13]. CNN cocok untuk pembelajaran visual berbasis komputer dan pengolahan bahasa alami. CNN juga merupakan strategi pembelajaran mendalam yang cocok untuk mengkarakterisasi objek. [14]

Berdasarkan ulasan diatas, maka peneliti mengusulkan Deteksi Serangan *TCP Flood* pada jaringan *Internet of Things (IoT)* menggunakan metode *Convolutional Neural Network (CNN).*

## 1.2 RUMUSAN MASALAH

Berdasarkan latar belakang diatas, maka rumusan masalah dari penelitian ini adalah :

1. Bagaimana cara mendeteksi serangan *TCP Flood* pada jaringan *IoT* menggunakan metode *CNN*?
2. Bagaimana menentukan fitur yang relevan untuk mendeteksi serangan *TCP Flood* pada jaringan *IoT* menggunakan metode *CNN*?
3. Bagaimana performa metode *CNN* dalam mendeteksi serangan TCP *Flood ?*

## 1.3 BATASAN MASALAH

Agar tidak memperluas pembahasan, penting untuk memiliki batasan untuk menyederhanakan masalah ini, yaitu sebagai berikut:

1. Pengujian hanya dilakukan pada serangan *TCP Flood*.
2. Metode yang dipakai untuk mendeteksi serangan *TCP Flood* pada jaringan *IoT* adalah *Convolutional Neural Network* (CNN).
3. Menggunakan dataset *CIC_IOT_Dataset2023.*
4. Menggunakan *tools Google Colaboratory* dengan bahasa pemrograman *Phyton*.

## 1.4 TUJUAN DAN MANFAAT PENELITIAN

### 1.4.1 Tujuan Penelitian

Tujuan penulis melakukan penelitian ini adalah :

1. Mengidentifikasi serangan *TCP Flood DDoS* pada jaringan IoT.
2. Menentukan fitur-fitur yang relevan untuk membedakan paket serangan *TCP Flood DDoS* pada jaringan IoT berbasis *Principal Component Analysis* (PCA).
3. Mengukur kinerja dari *CNN* dalam mendeteksi serangan *TCP Flood.*

### 1.4.2 Manfaat Penelitian

Terdapat beberapa manfaat yang dapat diambil dari hasil penelitian ini yaitu:

1. Mendapatkan rekomendasi informasi mengenai fitur-fitur yang bisa mendeteksi serangan *TCP Flood* dengan baik.
2. Dapat membangun IDS yang lebih baik untuk menangani serangan *TCP Flood*.
3. Sebagai panduan bagi peneliti selanjutnya jika ingin melakukan penelitian tentang serangan jaringan *TCP Flood*.

## 1.5 SISTEMATIKA PENULISAN

Untuk memberikan gambaran umum mengenai keseluruhan penulisan ilmiah, dapat dilihat melalui sistematika penulisan yang meliputi :

- **BAB I : PENDAHULUAN**

  Pada bab ini menjelaskan mengenai latar belakang permasalahan, rumusan permasalahan, batasan permasalahan, tujuan penelitian, manfaat penelitian, serta sistematika penulisan.

- **BAB II : LANDASAN TEORI**

  Pada bab ini menjelaskan mengenai teori dan pendapat para ahli yang berhubungan dengan pembahasan yang dianalisis. teori-teori yang digunakan antar lain mengenai jaringan IoT, *Deep Learning*, DDoS, dan CNN.

- **BAB III : METODOLOGI PENELITIAN**

  Pada bab ini menjelaskan tentang alur kerangka kerja, alur eksperimen, dan alat bantu penelitian yang bertujuan untuk mendukung penelitian.

- **BAB IV : ANALISIS**

  Pada bab ini menjelaskan mengenai profil data, data processing, analisis data, yang digunakan untuk mendeteksi serangan *TCP Flood* pada jaringan IoT.

- **BAB V : PENUTUP**

  Pada bab ini dipaparkan kesimpulan dan saran mengenai hasil dari penelitian yang telah dilakukan.