BAB V PENUTUP 44
5.1 KESIMPULAN 44
5.2 SARAN 45

DAFTAR PUSTAKA 47
LAMPIRAN 50
DAFTAR RIWAYAT HIDUP 50
LAMPIRAN CODING 51

DAFTAR GAMBAR

Gambar 2. 1 Teknik Deep Learning 11
Gambar 2. 2 Arsitektur Convolutional Neural Network 13
Gambar 2. 3 Pooling Layer 14
Gambar 2. 4 Dropout Layer 15
Gambar 3. 1 Kerangka Kerja Penelitian 19
Gambar 3. 2 Alur Eksperimen 22
Gambar 3. 3 Model Convolutional Neural Network 29
Gambar 4. 1 Visualisasi Serangan 34
Gambar 4. 2 Hasil PCA 34
Gambar 4. 3 Membangun Model CNN 35
Gambar 4. 4 Pelatihan Model CNN Epoch 10 36
Gambar 4. 5 Visualisasi Loss dan Akurasi Epoch 10 37
Gambar 4. 6 Confusion Matrix Epoch 10 37
Gambar 4. 7 Pelatihan Model CNN Epoch 50 39
Gambar 4. 8 Visualisasi Loss dan Accuracy Epoch 50 40
Gambar 4. 9 Confusion Matrix Epoch 50 40

DAFTAR TABEL

Tabel 2. 1 Penelitian Sejenis 16
Tabel 3.1 Fitur Dataset CIC 23
Tabel 3. 3 data hasil cleaning 27
Tabel 3. 4 Pseudocode PCA 28
Tabel 3. 5 Pseudocode CNN 29
Tabel 4. 1 Profil Dataset 31
Tabel 4. 2 Data Hasil Cleaning 33
Tabel 4. 3 Hasil Confusion Matrix Seluruh Data (Epoch 10) 38
Tabel 4. 4 Hasil Performa Model CNN (Epoch 10) 38
Tabel 4. 5 Hasil Confusion Matrix Seluruh Data (Epoch 50) 41
Tabel 4. 6 Hasil Performa Model CNN Epoch 50 41
Tabel 4. 7 Perbandingan Performa Setiap Parameter Epoch 42
Tabel 4. 8 Perbandingan Dengan Penelitian Sebelumnya 43

BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Perkembangan teknologi yang pesat telah mengatasi hambatan jarak, waktu, dan ruang, memungkinkan manusia untuk berinteraksi secara langsung [1]. Berdasarkan laporan Gartner, jumlah perangkat IoT diproyeksikan mencapai 25 miliar unit pada tahun 2030. Namun, di tengah pesatnya perkembangan ini, muncul pula ancaman terhadap keamanan IoT, yang dapat menghambat adopsi teknologi ini secara luas [2]. *Internet of Things* (IoT) merupakan sebuah konsep yang menghubungkan perangkat elektronik dengan internet melalui jaringan nirkabel. Konektivitas ini memfasilitasi komunikasi antar perangkat serta antara perangkat dengan penggunanya [3]

Meskipun menjanjikan banyak manfaat, IoT juga dihadapkan pada risiko keamanan siber yang signifikan. Kompleksitas jaringan IoT dan keragaman perangkat yang terhubung meningkatkan kerentanan terhadap serangan siber [4]. Seiring dengan meningkatnya penggunaan perangkat IoT, risiko serangan siber juga turut meningkat. Organisasi di berbagai sektor, termasuk pemerintah, energi, layanan kesehatan, perbankan, dan pusat penelitian, mengalami tantangan dalam hal pemantauan ancaman keamanan jaringan [5].

Serangan *Distributed Denial of Service* (DDoS) bertujuan melumpuhkan server dengan membanjiri sumber daya tersebut menggunakan banyak permintaan yang dikirim secara bersamaan dari berbagai sumber. Akibatnya, server menjadi kewalahan dan tidak mampu menangani lalu lintas yang sah, sehingga

mengakibatkan gangguan layanan [6]. *Advanced Persistent Threats* (APT) yang semakin marak menargetkan sistem IoT**.** APT merupakan serangan siber yang canggih dan berkelanjutan yang dilakukan oleh aktor yang memiliki motivasi dan sumber daya yang besar, seperti kelompok peretas yang disponsori negara.[7]

Convolutional Neural Network (CNN), menawarkan kemampuan untuk mempelajari pola kompleks dan mendeteksi serangan dengan akurasi yang lebih tinggi dibandingkan metode tradisional, termasuk dalam mengidentifikasi aktivitas yang mencurigakan yang berkaitan dengan APT [8]. CNN, sebuah arsitektur *deep learning* yang telah terbukti efektif dalam pengolahan citra dan pola, menunjukkan potensi yang menjanjikan untuk diterapkan dalam deteksi serangan IoT, termasuk APT. CNN mampu mempelajari pola kompleks dari data jaringan dan mengidentifikasi karakteristik serangan dengan akurasi yang tinggi[9].

Pada penelitian [10], Model *deep learning* CNN VGG-19 berhasil mengidentifikasi serangan DDoS dengan akurasi yang sangat tinggi (99,32%) dan tingkat kesalahan yang rendah (4,08%).

Pada penelitian [11] , Hasil pengujian menunjukkan bahwa kombinasi RNN dan Autoencoders sangat efektif dalam mendeteksi serangan siber tingkat rendah pada jaringan komputer. Dengan menggunakan dataset DO-RNN, skor keganjilan paralel, teknik batas T(iqr), dan analisis asosiasi SMTP, model ini mencapai akurasi 100% dan FPR 1%.

Oleh karena itu, penelitian ini mengusulkan penggunaan CNN untuk mendeteksi serangan DDoS pada jaringan IoT. CNN adalah metode *deep learning*

yang efektif dalam mempelajari pola visual dan mengkarakterisasi objek, sehingga cocok untuk diterapkan dalam analisis keamanan jaringan [12]. CNN tidak hanya cocok untuk tugas visual, seperti mengklasifikasikan gambar atau mendeteksi objek, tetapi juga efektif dalam pengolahan bahasa alami, misalnya untuk menerjemahkan Bahasa [13]. Kemampuan CNN dalam mengekstrak fitur dan mengkarakterisasi objek memungkinkan model ini untuk mempelajari pola-pola kompleks dalam data visual maupun teks.

Berdasarkan ulasan diatas, maka peneliti mengusulkan Deteksi Serangan Pada Industrial *Internet Of Things* (Iot) Menggunakan Metode Menggunakan Metode *Convolutional Neural Network* (CNN).

1.2 RUMUSAN MASALAH

Berdasarkan latar belakang yang telah dijelaskan, rumusan masalah dalam penelitian ini adalah:

1. Bagaimana meningkatkan akurasi deteksi serangan *Advanced Persistent Threats* (APT) dan *Distributed Denial of Service* (DDoS) pada jaringan IoT menggunakan metode *Convolutional Neural Network* (CNN) ?
2. Bagaimana model CNN dapat mempelajari pola kompleks pada data jaringan IoT untuk mendeteksi aktivitas mencurigakan yang berkaitan dengan serangan APT dan DDoS secara *real-time* ?

1.3 BATASAN MASALAH

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