IMPLEMENTASI *CONVOLUTIONAL NEURAL NETWORK (CNN)* UNTUK DETEKSI SERANGAN DoS PADA *INTERNET OF MEDICAL THINGS* (IOMT)

TUGAS AKHIR

Disusun oleh :

Lara Sagita

8020210135

Untuk Persyaratan Penelitian Dan Penulisan Tugas Akhir

Sebagai Akhir Proses Studi Strata 1

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS DINAMIKA BANGSA

2024

BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Internet of Medical Things (IoMT) merupakan perpaduan antara perangkat medis dengan *Internet of Things* (IoT). IoMT adalah masa depan sistem kesehatan saat ini, di mana setiap alat medis akan terhubung dan diawasi melalui internet oleh tenaga kesehatan yang profesional [1]. *Internet of Medical Things* adalah jaringan yang menghubungkan tidak hanya sejumlah besar perangkat medis individu tetapi juga peralatan dan organisasi yang menawarkan layanan medis, seperti rumah sakit, fasilitas penelitian medis, dan bisnis swasta [2]. *Internet of Medical things* (IoMT) memainkan peran penting dalam industri perawatan kesehatan untuk meningkatkan akurasi, keandalan, dan produktivitas perangkat elektronik [3]. Namun, seiring dengan kemajuan teknologi ini, ancaman terhadap keamanan data juga meningkat, telah ditemukan bahwa IoMT rentan terhadap berbagai jenis serangan, termasuk penolakan layanan (DoS), *malware*, dan serangan penyadapan. Selain itu, IoMT dapat terpapar pada berbagai kerentanan, seperti keamanan, privasi, dan kerahasiaan [4].

Keamanan pada jaringan maupun data dan perangkat-perangkat yang terhubung ke internet dalam sistem IoMT dapat menjadi sasaran serangan siber. Serangan *Denial of Service* (DoS) adalah salah satu ancaman siber yang paling mematikan yang sering disebut dengan DoS *attack*. Dengan mengandalkan serangan ini pelaku menyerang target-target dalam jangkauannya dengan Teknik

membanjiri *packet* atau *request* ke computer target secara terus menerus dan di saat waktu yang bersamaan hingga membuat computer target tidak dapat menanggapi *packet* atau *request* tersebut [5]. Tujuan dari serangan DoS adalah membuat server target kewalahan dalam menangani permintaan yang masuk, yang dapat mengakibatkan penghentian aktivitas atau sistem berhenti beroperasi karena tidak mampu memenuhi permintaan tersebut. Terkadang, metode serangan ini dapat menyebabkan kerusakan atau bahkan mematikan sistem secara keseluruhan. Beberapa tipe serangan *Denial of Service Attack* antara lain : *Ping of Death, SYN Attack, Land Attack, Smurf Attack,* dan *UDP Flood* [6].

Ada beberapa penelitian terkait serangan *Denial of Service* (DoS) antara lain, Menurut laporan yang diterbitkan oleh Securelist dari Kaspersky pada kuartal pertama tahun 2021, rata-rata serangan DoS per hari mencapai 1.500 kali, dengan puncak lalu lintas mencapai 800 GB per detik yang terutama terjadi di sektor swasta. Amerika Serikat tercatat sebagai sumber serangan DoS terbesar, menyumbang 41,98% dari total serangan, lebih tinggi dibandingkan negara-negara lain [7]. Selain itu pada penelitian Mosleh M. Abualhaj, Ahmad Adel Abu-Shareha, Mohammad O. Hiari mengungkapkan deteksi serangan DoS menggunakan pembelajaran mesin dengan model Teknik *Decision Tree* telah menunjukkan kinerja tertinggi. Sedangkan *Accuracy, Recall, Precision*, dan MCC, dari Teknik *Decision Tree* dengan model yang diusulkan adalah 99,891%, 99,904%. masing-masing 99,912%, dan 99,964% [8]. Kemudian penelitian yang di lakukan oleh Meirza Pramana, Endang Setyati, F. X. Ferdinandus melakukan identifikasi serangan DoS menggunakan algoritma C.45 menghasilkan akurasi sebesar 90,68% sedangkan

menggunakan algoritma *Naïve Bayes* menghasilkan akurasi sebesar 86,56% [9]. Dan yang terakhir penelitian yang dilakukan oleh Mohamed Abushwereb dan Mouhammd Al-kasassbeh untuk mempelajari serangan DoS yang menggunakan Teknik *Machine Learning* dengan fitur SNMP-MIB terdeteksi tingkat akurasi 93% [10].

Dari beberapa penelitian sebelumnya yang telah melakukan penelitian tentang serangan DoS Sebagian besar banyak menggunakan *machine learning*, beberapa metode *machine learning* yang telah digunakan seperti *Decision Tree*, Naïve Bayes, dan algoritma lainnya menunjukkan bahwa model-model ini memiliki kemampuan untuk mendeteksi serangan DoS, tetapi masih dibutuhkan tingkat akurasi yang optimal. Algoritma *machine learning* yang di gunakan sebelumnya cukup efektif untuk mendeteksi pola serangan yang kompleks pada IoMT. Selain itu, metode deep learning telah banyak di gunakan untuk mendeteksi serangan DoS, sehingga pada penelitian ini penulis memilih menggunakan algoritma *Convolutional Neural Network* (CNN) untuk mendeteksi serangan DoS di lingkungan IoMT. *Convolutional Neural Network* (CNN) merupakan salah satu arsitektur jaringan dalam bidang *deep learning* yang sangat popular karena CNN sangat efektif dalam mengidentifikasi data berdimensi tinggi. Pemilihan CNN sebagai metode ini didasarkan pada kemampuannya untuk melakukan ekstraksi fitur secara otomatis. Model ini juga mampu menangani data dengan berbagai skala, termasuk gambar, data berurutan, dan jenis data lainnya, serta memiliki tingkat akurasi yang tinggi [11]. CNN dapat diadaptasi untuk mendeteksi serangan DoS pada jaringan IoMT dengan menganalisis pola pada serangan, *convolutional neural network* (CNN) untuk deteksi serangan DoS *de-*

authentication dan *disassociation* dengan akurasi keseluruhan yang lebih baik dibandingkan dengan berbagai solusi saat ini. Kontribusi yang khas mencakup pra-pemrosesan data baru, dan model deteksi serangan *de-authentication/disassociation* disertai dengan pengumpulan dan penguraian data *real-time* yang efektif, analisis, dan visualisasi [12]. CNN merupakan evolusi dari Multilayer Perceptron (MLP) yang dirancang khusus untuk memproses data dua dimensi. CNN termasuk dalam kategori Deep Neural Network karena memiliki struktur jaringan yang dalam dan sering digunakan untuk mengolah data gambar. Dalam kasus klasifikasi gambar, MLP kurang efektif karena tidak mampu mempertahankan informasi spasial [13]. Penelitian sebelumnaya Kim et al. mengusulkan model berdasarkan *Convolutional Neural Network* (CNN) untuk mendeteksi serangan DoS menggunakan dataset KDD-99 dan dataset CICIDS2018 Dalam percobaan mereka, mereka mengubah fitur input menjadi "gambar", model CNN yang diusulkan kemudian menerima gambar skala abu-abu atau RGB sebagai input. Jumlah lapisan yang berbeda dieksplorasi saat mereka melakukan klasifikasi biner (normal vs serangan) dan multikelas [14].

Untuk mendukung penerapan model CNN pada penelitian ini, peneliti menggunakan dataset yang berasal dari *Canadian Institute for Cybersecurity* (CIC) IoMT dataset 2024 di University of New Brunswick, yang dirancang untuk merepresentasikan berbagai ancaman siber, termasuk serangan *Denial of Service* (DoS). Dataset ini memiliki 288.139 baris data dan 46 atribut. Dataset CIC memiliki banyak fitur yang memungkinkan model *Convolutional Neural Network* (CNN) mendeteksi pola serangan dengan akurat dan mengatasi resiko *overfitting*. Dataset

ini mendukung pengembangan solusi deteksi DoS yang tepat dan dapat diandalkan di lingkungan *Internet of Medical Things* (IoMT).

Dari uraian di atas,maka penulis melakukan penelitian yang berfokus pada penerapan algoritma *Convolutional Neural Network* (CNN) untuk deteksi serangan DoS pada lingkungan *Internet Of Medical Things* (IOMT). Dengan judul penelitian "**IMPLEMENTASI *CONVOLUTIONAL NEURAL NETWORK (CNN)* UNTUK DETEKSI SERANGAN DoS PADA *INTERNET IF MEDICAL THINGS* (IOMT)**".

1.2 RUMUSAN MASALAH

Berdasarkan penelitian sebelumnya yang telah menggunakan metode machine learning seperti Decision Tree dan Naïve Bayes masih belum memiliki hasil yang optimal dalam meningkatkan akurasi deteksi serangan [8] [9]. Sehingga di perlukan metode yang lebih efektif dalam mendeteksi pola serangan yang lebih akurat. Oleh karena itu pada penelitian ini, penulis menerapkan metode *deep learning* untuk meningkatkan peforma dalam mendeteksi serangan DoS pada lingkungan iomt.

Berdasarkan latar belakang yang sudah di paparkan diatas, maka terdapat beberapa pertanyaan penelitian sebagai berikut :

1. Bagaimana implementasi algoritma *Convolutional Neural Network* (CNN) untuk mendeteksi serangan DoS pada jaringan *internet of medical things* (IOMT)?
2. Bagaimana peforma CNN dalam mendeteksi serangan DoS pada lingkungan IOMT.

1.3 BATASAN MASALAH

Batasan-batasan dalam penelitian yang diambil oleh peneliti adalah:

1. Pengukuran peforma untuk mencari nilai akurasi, TPR, F1 *score, recall* dan ROC.
2. Penelitian ini menggunakan *Google Colab* sebagai alat bantu analisis data dengan fitur pemrosesan data berbasis *Python*.
3. Dataset yang digunakan pada penelitian ini berasal dari *Canadian Institute for Cybersecurity (CIC)* IoMT dataset 2024. Dengan jumlah data sebanyak 288.138 baris dan 46 atribut.

1.4 TUJUAN PENELITIAN

Berdasarkan latar belakang di atas tujuan penelitian ini adalah:

1. Mengimplementasikan algoritma *Convolutional Neural Network* (CNN) untuk deteksi serangan DoS.
2. Menguji kemampuan model CNN dalam mendeteksi pola serangan DoS pada jaringan *internet of meducal things* (IOMT).

1.5 MANFAAT PENELITIAN

Manfaat dari penelitian ini adalah :

1. Implementasi CNN pada penelitian ini dapat memberikan solusi praktis yang teruji untuk mendeteksi serangan DoS secara cepat dan akurat.
2. Penerapan *deep learning* dalam keamanan jaringan, khususnya penerapan algoritma *Convolutional Neural Network* (CNN) dapat menghasilkan akurasi terbaik.

3. Penelitian ini dapat menjadi acuan untuk mendorong terciptanya inovasi yang lebih luas di bidang keamanan siber berbasis *deep learning*

1.6 SISTEMATIKA PENULISAN

Sistematika penulisan ini dirancang untuk memudahkan pemahaman terhadap laporan penelitian. Oleh karena itu, penulis menyusun sistematika penulisan sebagai berikut.

BAB I : PENDAHULUAN

Pada Bab I yang berjudul Pendahuluan, terdapat penjelasan mengenai latar belakang masalah, perumusan masalah, batasan masalah, tujuan dan manfaat penulisan, serta sistematika penulisan.

BAB II : LANDASAN TEORI

Pada bab ini, penulis menguraikan berbagai definisi dan teori yang relevan dengan topik penelitian, yang bersumber dari buku dan jurnal ilmiah. Tujuannya adalah untuk memperkuat pemahaman penulis serta memberikan dasar teoritis yang solid guna menjawab permasalahan penelitian. Selain itu, landasan teori ini juga membantu penulis dalam membangun kerangka berpikir yang kuat terkait penelitian yang dilakukan.

BAB III : METODOLOGI PENELITIAN

Bab ini menjelaskan metodologi yang diterapkan oleh penulis serta merinci kerangka penelitian, yang mencakup desain penelitian, metode

pengumpulan data, teknik analisis data, dan data yang digunakan dalam penelitian.

BAB IV : ANALISIS DAN HASIL

Pada bab ini, penulis memaparkan analisis data yang diperoleh selama penelitian dan hasil dari analisis tersebut. Bab ini juga mencakup interpretasi hasil serta diskusi mengenai temuan penelitian.

BAB V : PENUTUP

Pada bab ini, penulis memberikan kesimpulan dari hasil penelitian dan menyampaikan saran-saran yang relevan untuk penelitian lebih lanjut atau penerapan praktis dari temuan penilitian.