Sistem Deteksi Serangan DDoS menggunakan *Neural Netowrk* Pada Sistem Berbasis IoT

Proposal Tugas Akhir

Kelas TA SMD

Lulus Wahyu Prasetya Adi
NIM: 301150079

Program Studi Sarjana Teknik Informatika

Fakultas Informatika

Universitas Telkom

Bandung

2020

Lembar Persetujuan

Sistem Deteksi Serangan DDoS menggunakan *Neural Netowrk* Pada Sistem Berbasis IoT

DDoS attack detection system using Neural Network on IoT-based systems

Lulus Wahyu Prasetya Adi
NIM: 301150079

Proposal ini diajukan sebagai usulan pembuatan tugas akhir pada
Program Studi Sarjana Teknik Informatika
Fakultas Informatika Universitas Telkom

Bandung, 17 Desember 2020
Menyetujui

Calon Pembimbing 1	Calon Pembimbing 2
Satria Mandala, PhD	Yudhistira Nugraha, D.Phil.
NIP: 16730040	NIP:

Abstrak

Distributed Denial-of-Service (DDoS) adalah sebuah serangan yang bertujuan untuk membuat komputer atau server dengan cara menghabiskan *resource* sehingga mencegah pengguna lain untuk memperoleh layanan mengakses dari komputer yang sedang diserang. Dalam hal ini, ketika target serangan DDoS adalah sebuah sistem yang berbasis IoT, akan menjadi hal yang sangat merugikan bagi orang atau perusahaan yang bergantung dan terbiasa menggunakan perangkat IoT tersebut. Untuk menyelesaikan masalah tersebut, tugas akhir ini mengusulkan merancang *Intrusion Detection System*(IDS) dengan penggunaan algoritma *Neural Network* untuk melakukan *ekstrasion feature* dengan menggunakan perhitungan statistik. Metode yang digunakan dalam tugas akhir ini adalah dengan melakukan klasifikasi dan pengujian terhadap dataset yang didapat dari Koroniotis, Moustafa, Sitnikova and Turnbull (2019). Dengan melakukan pengujian performansi dan analisa. sehingga diharapkan akurasi yang didapatkan dengan menggunakan algoritma yang disarankan lebih dari 92%.

Kata Kunci: DDoS, IoT, IDS, *Neural Network*.

Daftar Isi

Bab I

Pendahuluan

1.1 Latar Belakang

Internet of Things(IoT) adalah sebuah perangkat yang berkembang dijaman sekarang. sebuah perangkat yang dapat mempermudah kehidupan manusia dengan memanfaatkan jaringan pada internet. Meskipun perangkat ini mempunyai *resource* yang terbatas, namun perangkat ini dapat digunakan dalam berbagai bidang, seperti kesehatan, kemanan, maupun pembangkit listrik Cho, Hong and Choi (2011). Dikarenakan IoT adalah perangkat yang menggunakan Internet, maka keamanan jaringan merupakan faktor yang penting dalam pengembangan IoT. Berdasarkan Anstee, Bussiere, Sockrider and Morales (2014), serangan yang umum terjadi pada jaringan adalah *Distributed Denial-of-Service* (DDoS) dengan tujuan untuk membuat komputer atau server dengan cara menghabiskan *resource* sehingga mencegah pengguna lain untuk memperoleh layanan mengakses dari komputer yang sedang diserang. Serangan DDoS adalah salah satu jenis serangan yang cukup populer dikalangan hacker. Serangan DDoS yang biasanya terjadi yaitu dengan *Flooding, Syn Flooding, DNS-Flood, dan UDP-Flood* Aziz, Umar and Ridho (2019).

Dampak yang ditimbulkan dari serangan DDoS cukup besar, jika target dari serangan DDoS adalah *smart house*, maka akan dapat membuat perangkat IoT seperti *smart key*, cctv atau sistem keamanan lain yang berbasis IoT akan mati. Sehingga memungkinkan terjadinya pembobolan pada rumah. Selain itu, jaringan *smart house* juga lebih rentan terhadap ancaman keamanan karena bersifat heterogen dan node dalam jaringan *smart house* biasanya terletak di lingkungan yang heterogen dan dihosting Saxena, Sodhi and Singh (2020).

Sebagai pencegahan terciptalah sebuah sistem deteksi yang bernama *Intrusion Detecting System*(IDS). IDS adalah sebuah sistem yang digunakan untuk mendeteksi serangan DDoS. Seiring berjalannya waktu, IDS harus semakin dikembangkan agar lebih efisien dalam mengatasi serangan *cyber* yang semakin berkembang juga. Hal ini diperlukan karena DDoS menyerang aspek *availabelity* dari sebuah sistem, sehingga dibutuhkan sistem deteksi yang dapat merespon dengan cepat dan akurat ketika terjadi serangan.

Saat ini sudah banyak sistem deteksi DDoS yang menggunakan *Neural Network*. Metode *Neural Network* dipilih karena cakupannya yang cukup luas, selain berguna untuk mendeteksi DDoS, juga dapat digunakan untuk mendeteksi serangan yang lainnya. Seperti yang dibahas sebelumnya oleh Smith, Japkowicz, Dondo and Mason (2008), Berdasarkan dataset DARPA, untuk membentuk suatu alret cluster, menghasilkan kesimpulan bahwa terjadi penurunan dimana pada awalnya berdasarkan dataset DARPA terdapat 21 cluster serangan, ternyata hanya bisa dikelompokkan menjadi 13 cluster serangan, sehingga terdapat kesalahan pemisahan di mana alert dari jenis serangan yang sama dikelompokkan menjadi cluster yang berbeda. Selain itu teknik SVM-RIPPER yang disarankan oleh Bolzoni, Etalle and Hartel (2009) mampu untuk menghasilkan alert cluster dalam deteksi serangan DDoS dengan baik.

Berdasarkan penelitian terdahulu, penggunaan *Neural Network* cukup efektif dalam melakukan deteksi terhadap serangan DDoS, namun pada proposal ini bertujuan menggunakan algoritma *Neural Network* untuk melakukan deteksi pada sistem berbasi IoT. diharapkan hasil analisis dari penelitian ini dapat digunakan untuk mengembangkan keamanan jaringan pada sistem berbasis IoT.

1.2 Perumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah tugas akhir ini adalah sebagia berikut:

1. Bagaimana memodelkan dan mensimulasikan algoritma *Neural Network* untuk melakukan deteksi serangan DDoS pada perangkat IoT?
2. Bagaimana meningkatkan performa deteksi menggunakan *neural network*?
3. Bagaimana melakukan analisis performansi terhadap algoritma yang digunakan?

1.3 Pernyataan Masalah

Berdasarkan latar belakang di atas, dapat disimpulkan terdapat permasalahan pada algoritma*Neural Network* dan deteksi yang sudah ada sebagai berikut ::

1. Algoritma *Neural Network* sudah banyak digunakan untuk deteksi DDoS pada netowrk, namun penelitian terkait untuk sistem berbasis IoT masih jarang dilakukan.
2. Membutuhkan sistem deteksi yang lebih akurat.
3. Perlunya alisis performansi algoritma *Neural Network* pada sistem berbasis IoT

1.4 Tujuan

1. Merancang sistem dengan menggunakan algoritma *Neural Network* untuk melakukan deteksi terhadap serangan DDoS pada sistem berbasis IoT.

2. Meningkatkan performa deteksi menggunakan *neural network*.

3. Melakukan analisis performansi terhadap algoritma yang digunakan

1.5 Batasan Masalah

Berikut adalah ruang lingkup yang ada pada penulisan tugas akhir ini :

1. Jenis serangan yang dideteksi adalah serangan DDoS.

2. Dataset yang digunakan adalah dataset dari Koroniotis et al. (2019).

1.6 Hipotesis

1. Algoritma *Neural Network* yang diusulkan dapat digunakan untuk mendeteksi serangan DDoS pada sistem berbasis IoT secara lebih akurat

2. Dengan menggunakan *neural network* mendapatkan hasil akurasi sesuai atau lebih tinggi dari yang diharapkan.

1.7 Sistematika Penulisan

Tugas Akhir ini disusun dengan sistematika penulisan sebagai berikut :

- **BAB I Pendahuluan**. Bab ini membahas mengenai latar belakang, rumusan masalah, dan tujuan pengerjaan Tugas Akhir ini.

- **Bab II Kajian Pustaka**. Bab ini membahas fakta dan teori yang berkaitan dengan perancangan sistem untuk mendirikan landasan berfikir. Dengan menggunakan fakta dan teori yang dikemukakan pada bab ini penulis menganalisis kebutuhan akan rancangan arsitektur sistem yang dibangun.

- **BAB III Metodologi dan Desain Sistem**. Bab ini menjelaskan metode penelitian, rancangan sistem dan metode pengujian yang dilakukan dalam penelitian.

Bab II

Kajian Pustaka

Bab ini menjelaskan riset terkait tugas akhir dan landasan teori pendukung yang digunakan. Riset Terkait diuraikan di Sub Bab 2.1, sedangkan landasan teori dapat ditemukan pada Sub Bab 2.2 sampai dengan Sub Bab 2.5. Ringkasan disajikan pada bagian terakhir dari Bab 2.

2.1 Penelitian Terkait

Aziz et al. (2019) mengusulkan sebuah algoritma jaringan saraf tiruan untuk melakukan klasifikasi dengan menggunakan perhitungan statistik. Berdasarkan hasil analisis dan pengujian yang dilakukan didapatkan nilai akurasi sebesar 95,23

Muhammad, Riadi and Sunardi (2017) melakukan penelitian menggunakan neural network dengan fungsi *fixed moving average window* (FMAW) sebagai metode deteksi. Data pelatihan dan pengujian diambil dari CAIDA DDoS Attack 2007 dan simulasi mandiri. Pengujian terhadap metode neural network dengan fungsi *fixed moving average window* (FMAW) menghasilkan prosentase rata-rata pengenalan terhadap tiga kondisi jaringan (normal, slow DDoS, Dan DDoS) sebesar 90,52

Di tahun yang sama Ahanger (2017) juga mengusulkan mekanisme pendeteksian DDoS berdasarkan pada prinsip-prinsip Jaringan Saraf Tiruan. Metode ini menganalisis sumber daya sistem dan data jaringan untuk melatih sistem deteksi ANN DDoS untuk mendeteksi lalu lintas normal dan abnormal. Dengan menggunakan sistem yang diusulkan, memperoleh akurasi sebesar 99.67%, sedangkan dengan menggunakan BP methode, diperoleh akurasi sebesar 89,165%.

Li, Liu and Gu (2010) Melalui hasil percobaan dapat diketahui jaringan syaraf tiruan yang digunakan untuk sistem deteksi intrusi berbasis anomali host. Pada jaringan saraf BP mendapat akurasi sebesar 89,9%, sedangkan Jaringan saraf LVQ dapat mencapai tingkat akurasi yang tinggi, dan cukup setabil, yaitu 99.732%,

Roopak, Tian and Chambers (2020) juga mengusulkan IDS yang didirikan pada fusi *Jumping Gene* yang diadaptasi NSGA-II multi- metode optimasi ob-

jektif untuk reduksi dimensi data dan *Convolutional Neural Network* (CNN) mengintegrasikan teknik pembelajaran mendalam Long Short-Term Memory (LSTM) untuk mengklasifikasikan serangan. Eksperimen dilakukan dengan menggunakan Komputer Berkinerja Tinggi (HPC) pada dataset CISIDS2017 terbaru tentang serangan DDoS dan mencapai akurasi 99,03% dengan pengurangan waktu pelatihan 5 kali lipat.

Muhammad, Riadi and Sunardi (2016) melakukan analisis analisis statistik terhadap log jaringan dengan fungsi *neural network* sebagai metode deteksi menghasilkan prosentase rata-rata pengenalan terhadap tiga kondisi jaringan (normal, slow DDoS, dan DDoS) sebesar 90,52

Wehbi, Hong, Al-salah and Bhutta (2019) mencoba menekankan beberapa pendekatan Machine Learning (ML) terbaru yang dikembangkan untuk mendeteksi serangan DDoS di jaringan IoT dengan mengembangkan beberapa pendekatan, menghasilkan akurasi yang hampir 100

Vinayakumar, Soman and Poornachandran (2017) juga melakukan penelitian dengan memodelkan lalu lintas jaringan sebagai rangkaian waktu, terutama paket transmisi kontrolprotocol / internetprotocol (TCP / IP) dalam waktu yang ditentukan dengan metode pembelajaran yang diawasi seperti *multi-layer perceptron* (MLP), CNN, CNN -jaringan saraf berulang (CNN-RNN), memori jangka pendek CNN-panjang (CNNLSTM) dan unit rekuren berpagar CNN (GRU), menggunakan jutaan koneksi jaringan baik dan buruk yang diketahui. hasil tes untuk set fitur minimal KDD Cup '99' dalam pengaturan multi class clasification adalah 81,5%, sedangkan untuk tes KDD Cup '99' dalam mengategori terhadap serangan yang sesuai menghasilkan akurasi 95,75%

Soe, Santosa and Hartanto (2019) melakukan penelitian dengan menggunakan dataset publik untuk mendeteksi serangan menggunakan teknik pembelajaran mesin, arsitektur sederhana dengan *Artificial Neural Network* (ANN). menggunakan dataset serangan botnet modern, Bot-IoT untuk mendeteksi serangan DDoS. Kami menggunakan SMOTE (*Synthetic Minority Over-sampling Technique*) untuk memecahkan masalah ketidakseimbangan data untuk mengimplementasikan sistem deteksi DDoS berbasis pembelajaran mesin. Hasil kami menunjukkan bahwa pendekatan yang diusulkan dapat menghasilkan akurasi hampir 100

Harsono, Khambali and Muhammad (2018) melakukan penelitian untuk membentuk suatu pendekatan baru dalam kaitannya dengan klasifikasi paket jaringan, sehingga bisa menjadi sebuah framework pada pengembangan sistem deteksi serangan *Distributed Denial-of-Service* (DDoS). Berdasarkan pengujian didapatkan bahwa rerata persentase akurasi klasifikasi neural network terhadap paket data jaringan Internet sebesar 92,99%.

Nihri, Pramukantoro and Trisnawan (2018) juga melakukan penelitian menggunakan Algoritma J48 sebagai algoritma machine learning karena memiliki akurasi yang lebih tinggi dibandingkan dengan algoritma lain. Penggunaan

sumber daya, akurasi pembelajaran mesin, kemampuan memberikan peringatan, penebangan dan penanganan serangan adalah faktor sukses dalam IDS. Hasilnya menunjukkan rata-rata akurasi yang dihasilkan mencapai 100%, namun memiliki kelemahan dengan kemampuan penangkapan paket sebesar 73,52%

Silveira, Lima-Filho, Silva, Junior and Silveira (2020) Modul pendeteksian kerja ini untuk pengontrol IoT yang menggunakan Teknik *Machine Learning* (ML) untuk mengklasifikasikan lalu lintas jaringan. Sistem ini dirancang dalam konteks *Software-Defined Networks* (SDN) dan dievaluasi pada platform yang diemulasi menggunakan tiga kumpulan data aktual dan terkenal yang ada dalam literatur. Hasilnya, pada sampling rate (SR) 20% trafik jaringan, menunjukkan presisi tinggi (PR), di atas 93%, false alarm rate (FAR) rendah, dan detection rate (DR) serangan di atas 96%, menggunakan perangkat emulasi profil rendah.

Belej and Halkiv (2020) juga membuat penelitian Jaringan saraf hibrida berdasarkan jaringan Kohonen dan perceptron multilayer digunakan sebagai modul deteksi. Pekerjaan prototipe yang dibuat dari sistem deteksi serangan, metodologi untuk pembentukan sampel pelatihan, kursus eksperimen, dan topologi tempat percobaan dijelaskan. Hasil studi eksperimental prototipe disajikan, selama kesalahan jenis pertama dan kedua, masing-masing. Hasil percobaan menunjukkan bahwa jumlah positif palsu tidak melebihi 0,115% pada kasus terburuk yang disebabkan oleh minimnya ukuran data yang dianalisis dan sampel pelatihan.

Sofa et al. (2019) melakukan sebuah penelitian *Smart Intrusion Detection System* berbasis *Compression Header Analyzer* akan diinvestigasi lebih lanjut dalam menganalisis varian baru model *routing attacks* pada jaringan IoT. *Features selection* berupa *Best First Search* (BFS) dan *Greedy Stepwise* (GS) dengan *Correlation Feature Selection* (CFS) digunakan untuk memilih fitur signifikan yang dapat membedakan antara serangan dan non-serangan. Sedangkan machine learning algorithm (Random Forest, J48, Logistic, MLP, Naïve Bayes dan SMO) digunakan untuk mengklasifikasikan serangan di IoT. Dari enam machine learning algorithm tersebut, kinerja terbaik dalam mendeteksi routing attacks ditunjukkan oleh Random Forest dengan tingkat akurasi sebesar 99,4721

Chen, Sheu, Kuo and Van Cuong (2020) juga melakukan penelitian dengan mengekstrak fitur berdasarkan jenis serangan DDoS. Pemilihan fitur dapat menghasilkan deteksi serangan DDoS dengan akurasi tinggi di lingkungan IoT yang sebenarnya. Hasil percobaan menunjukkan bahwa sistem deteksi DDoS multi-layer kami dapat mendeteksi serangan DDoS secara akurat. Dengan akurasi penelitian 97

Perbandingan hasil penelitian di atas dapat dilihat pada tabel di bawah ini:

Tabel 2.1: Ringkasan riset terkait

No.	Judul	Penulis / Tahun	Hasil Riset	Kelebihan	Kekurangan
1	An Intrusion Detection System Against DDoS Attacks in IoT Networks	Monika Roopak, Prof. Gui Yun Tian, Prof. Jonathon Chambers / 2020	Eksperimen dilakukan dengan menggunakan Komputer Berkinerja Tinggi (HPC) pada dataset CISIDS2017 terbaru tentang serangan DDoS dan mencapai akurasi 99,03% dengan pengurangan waktu pelatihan 5 kali lipat.	metode yang digunakan dapat melampaui metode pendekatan lain yang dibandingkan	Bbutuh komputer yang berkinerja tinggi untuk melakukan uji coba
2	A Survey on Machine Learning Based Detection on DDoS Attacks for IoT Systems	Khadijeh Wehbi, Liang Hong, Tulha Alsalah, Adeel A Bhutta / 2019	deteksi serangan DDoS di jaringan IoT dengan mengembangkan beberapa pendekatan, menghasilkan akurasi yang hampir 100%	-	-
3	An Effective Approach of Detecting DDoS Using Artificial Neural Networks	Tariq Ahamed Ahanger / 2017	Dengan menggunakan sistem yang diusulkan, memperoleh akurasi sebesar 99.67%, sedangkan dengan menggunakan BP methode, diperoleh akurasi sebesar 89,165%.	-	harus mengerti dasar-dasar LVQNN sehingga membutuhkan efort yang lebih dalam proses pengerjaannya.

Tabel 2.1: Ringkasan riset terkait

No	Judul	Penulis / Tahun	Hasil Riset	Kelebihan	Kekurangan
4	Applying Convolutional Neural Network for Network Intrusion Detection	Vinayakumar R, Soman KP, Prabaharan Poornachandran / 2017	hasil tes untuk set fitur minimal KDD Cup '99' dalam pengaturan multi class clasification adalah 81,5%, sedangkan untuk tes KDD Cup '99' dalam mengategori terhadap serangan yang sesuai menghasilkan akurasi 95,75%	dapat mengetahui arsitektur jaringan yang optimal menggunakan CNN	harus mengerti dasar-dasar berbagai arsitektur jaringan
5	DDoS Attack Detection Based On Neural Network	Jin Li, Yong Liu, Lin Gu / 2010	Pada jaringan saraf BP mendapat akurasi sebesar 89,9%, sedangkan Jaringan saraf LVQ dapat mencapai tingkat akurasi yang tinggi, dan cukup setabil, yaitu 99.732%,	memiliki tingkat pengenalan yang tinggi setelah melakukan pelatihan pada jaringan	-
6	DDoS Attack Detection Based on Simple ANN with SMOTE for IoT Environment	Yan Naung Soe, Paulus Insap Santosa, Rudy Hartanto / 2019	Hasil kami menunjukkan bahwa pendekatan yang diusulkan dapat menghasilkan akurasi hampir 100%.	-	harus melakukan training data untuk mendapatkan akurasi yang tinggi
7	Design and Implementation of IoT DDoS Attacks Detection System based on Machine Learning	Yi-Wen Chen, Jang-Ping Sheu, Young-Ching Kuo, Nguyen Van Cuong / 2020	Hasil percobaan menunjukkan bahwa sistem deteksi DDoS multi-layer kami dapat mendeteksi serangan DDoS secara akurat. Dengan akurasi penelitian 97%.	Deteksi DDoS multi-layer dan pengontrol SDN dapat memblokir serangan IoT DDoS	pengerjaan lebih kompleks.

Tabel 2.1: Ringkasan riset terkait

No	Judul	Penulis / Tahun	Hasil Riset	Kelebihan	Kekurangan
8	Smart Detection-IoT: A DDoS Sensor System for Internet of Things	Frederico Augusto Fernandes Silveira, Francisco Lima-Filho, Filipe Sampaio Dantas Silva / 2020	Hasilnya, pada sampling rate (SR) 20% trafik jaringan, menunjukkan presisi tinggi (PR), di atas 93%, false alarm rate (FAR) rendah, dan detection rate (DR) serangan di atas 96%,	-	menggunakan perangkat emulasi profil rendah. .
9	Using Hybrid Neural Networks to Detect DDOS Attacks	Olexander Belej, Liubov Halkiv / 2020	Hasil studi eksperimental prototipe disajikan, selama kesalahan jenis pertama dan kedua, masing-masing. Hasil percobaan menunjukkan bahwa jumlah positif palsu tidak melebihi 0,115% pada kasus terburuk yang disebabkan oleh minimnya ukuran data yang dianalisis dan sampel pelatihan.	-	-
10	ANALISIS STATISTIK LOG JARINGAN UNTUK DETEKSI SERANGAN DDOS BERBASIS NEURAL NETWORK	Arif Wirawan Muhammad, Imam Raidi, Sunardi / 2016	metode deteksi menghasilkan prosentase rata-rata pengenalan terhadap tiga kondisi jaringan (normal, slow DDoS, dan DDoS) sebesar 90,52%.	-	-.

Tabel 2.1: Ringkasan riset terkait

No	Judul	Penulis / Tahun	Hasil Riset	Kelebihan	Kekurangan
11	Deteksi Serangan DDoS Menggunakan Neural Network dengan Fungsi Fixed Moving Average Window	Arif Wirawan Muhammad, Imam Raidi, Sunardi / 2017	Pengujian terhadap metode neural network dengan fungsi fixed moving average window (FMAW) menghasilkan prosentase rata-rata pengenalan terhadap tiga kondisi jaringan (normal, slow DDoS, Dan DDoS) sebesar 90,52%.	-	-
12	Implemetasi Jaringan Saraf Tiruan Untuk Mendeteksi Serangan DDoS Pada Forensik Jaringan	Muhammad Aziz, Rusydi Umar, Faizin Ridho / 2019	Berdasarkan hasil analisis dan pengujian yang dilakukan didapatkan nilai akurasi sebesar 95,23%.	-	-

Tabel 2.1: Ringkasan riset terkait

No.	Judul	Penulis / Tahun	Hasil Riset	Kelebihan	Kekurangan
13	Klasifikasi Paket Jaringan Berbasis Analisis Statistik dan Neural Network	Harsono, Muhammad Chambali, Arif Wirawan Muhammad / 2018	Berdasarkan pengujian didapatkan bahwa rerata persentase akurasi klasifikasi neural network terhadap paket data jaringan Internet sebesar 92,99%.	metode kuantifikasi data secara statistik terhadap aliran paket data jaringan yang digabungkan dengan neural network mampu digunakan untuk mengklasifikasi aktivitas paket data dalam jaringan Internet dan dapat dijadikan sebagai landasan ataupun framework dalam mengambangkan sistem deteksi serangan Distributed Denial-of-Service (DDoS)	-

Tabel 2.1: Ringkasan riset terkait

No	Judul	Penulis / Tahun	Hasil Riset	Kelebihan	Kekurangan
14	Pengembangan IDS Berbasis J48 Untuk Mendeteksi Serangan DoS Pada Perangkat Middleware IoT	Hilman Nahri, Eko Sakti Pramukantoro, Primantara Hari Trisnawan / 2018	Hasilnya menunjukkan rata-rata akurasi yang dihasilkan mencapai 100%, namun memiliki kelemahan dengan kemampuan penangkapan paket sebesar 73,52%	tidak memerlukan komputer berkinerja tinggi untuk melakukan eksekusi sistem	tidak dapat digunakan untuk variasi paket yang sangat banyak.
15	ROUTING ATTACKS PADA PROTOKOL KOMUNIKASI INTERNET OF THINGS MENGGUNAKAN SMART INTRUSION DETECTION SYSTEM	Eka Lailatus Sofa / 2019	Dari enam machine learning algorithm tersebut, kinerja terbaik dalam mendeteksi routing attacks ditunjukkan oleh Random Forest dengan tingkat akurasi sebesar 99,4721%.	-	-

2.2 Internet of Things

Menurut Tan and Wang (2010) Mendefinisakan Internet of Things, sebagai sebuah infrastruktur jaringan global, yang menghubungkan benda-benda fisik dan virtual melalui eksploitasi data capture dan kemampuan komunikasi. Infrastruktur terdiri dari jaringan yang telah ada dan internet berikut pengembangan jaringannya. Semua ini akan menawarkan identifikasi obyek, sensor dan kemampuan koneksi sebagai dasar untuk pengembangan layanan dan aplikasi ko-operatif yang independen. Ia juga ditandai dengan tingkat otonom data capture yang tinggi, event transfer, konektivitas jaringan dan interoperabilitas.

2.3 Intrution Detection System

IDS (Intrusion Detection System) adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan Thatte, Mitra and Heidemann (2010). Menurut Lee, Kim and Kim (2011), sistem IDS pada umumnya hanya memantau dan sebagai alret, sehingga memberikan dampak adanya volume alert yang terlalu besar dengan tingkat rata-rata false-positive yang tinggi. Hal itu disebabkan karena lalu lintas data jaringan merupakan sesuatu yang bersifat non-stasioner

2.4 Distributed Denial-of-Service

Menurut Li et al. (2010), *Distributed Denial-of-Service* (DDoS) merupakan jenis serangan terhadap situs web, atau server, atau layanan online dengan cara membanjiri *traffic* jaringan sehingga layanan tidak dapat diakses oleh pengguna dan juga serangan DDoS ada dua kategori :

1. *DDoS by saturation*, dengan membanjiri mesin dengan permintaan sehingga tidak bisa lagi menanggapi permintaan asli.

2. *DDoS by vulnerability exploitation*, Ini melibatkan mengeksploitasi kelemahan dalam sistem jarak jauh sehingga membuatnya tidak praktis.

2.5 Neural Network

Jaringan saraf tiruan adalah model komputasi yang disusun oleh berbagai elemen pemrosesan (neuron). Neuron terhubung dengan *coefficients* atau bobot yang membangun struktur jaringan saraf. JST memiliki elemen untuk memproses informasi, yaitu fungsi transfer, masukan berbobot, dan output Haykin (2008). Jaringan saraf tiruan memiliki pembelajaran mandiri, pengorganisasian mandiri, toleransi kesalahan dan ketahanan yang lebih baik, paralelisme keunggulan ini Li et al. (2010). Pembangunan beberapa jaringan saraf baru untuk teknologi deteksi intrusi untuk meningkatkan ketahanan, meningkatkan kecerdasan dan adaptasi IDS adalah tren perkembangan teknologi deteksi intrusi. Li et al. (2010).

2.6 Ringkasan

serangan DDoS sangat mudah untuk dilakukan, sementara bagi korban, hal itu sulit untuk disadari. Sebagai contoh adalah serangan SYN-Flood. Secara umum paket tunggal SYN adalah paket yang legal pada aktifitas jaringan, sehingga menyulitan IDS untuk mendeteksinya. Yang kedua adalah adanya masalah alret yang bersifat false-positif yang sering terjadi pada IDS yang berbasis signature.

Berdasarkan penelitian yang sebelumnya, rata-rata akurasi dalam melakukan pemrosesan adalah diatas 90%. Diharapkan pada penelitian kali ini, hasil

yang didapatkan dapat melebihi dari penelitian sebelumnya dengan menggunakan jaringan berbasis IoT.

Bab III

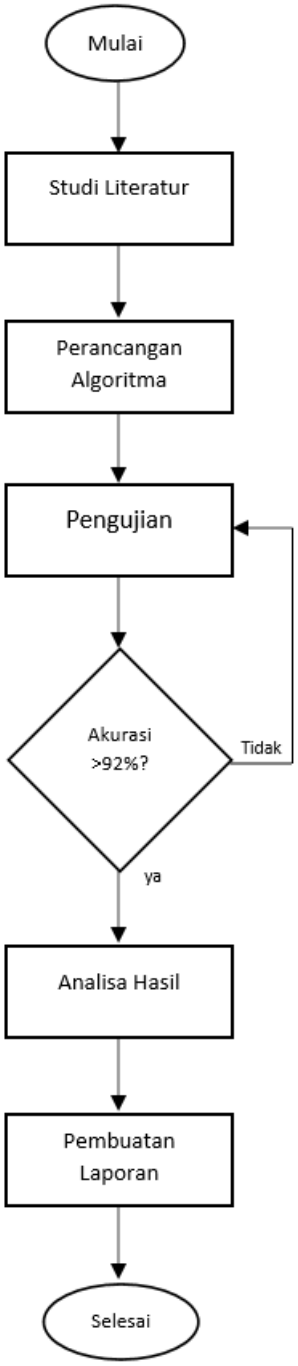
Metodologi dan Desain Sistem

3.1 Metode Penelitian

Seperti yang telah dijelaskan di atas, penelitian ini bertujuan untuk membuat sebuah sistem yang dapat mendeteksi serangan DDoS pada sistem berbasis IoT dengan menggunakan *neural network* dengan pengujian dilakukan menggunakan dataset yang didapat dari Bellekens (2020) .

3.1.1 Framework Penelitian

Metodologi yang dilakukan dalam menyelesaikan penelitian ini ditunjukan pada diagram alir 3.1 dibawah ini :



Gambar 3.1: Diagram Alir Riset *Framework*

Berikut penjelasan dari masing-masing tahapan riset :

1. **Studi Litaratur**

Pada tahap ini dilakukan review terhadap penelitian-penelitian yang telah dilakukan sebelumnya dan merangkum fakta serta teori yang dibutuhkan dalam penelitian. Dilakukan dengan membaca jurnal dan artikel yang berkaitan. Jurnal penelitian didapat dari situs terpercaya seperti IEEE dengan batasan penelitian terakhir 10 tahun lalu. Pada tahap ini juga penulis menganalisis masalah dan membuat alasan mengapa masalah tersebut perlu diselesaikan.

2. **Perancangan Algoritma**
   Pada tahap ini ,dengan data set yang telah tersedia penulis melakukan eksperimen berbagai algoritma dan melakukan perancangan untuk mendapatkan algoritma terbaik yang dapat diusulkan. Hasil dari tahap ini adalah algoritma yang matang untuk mendeteksi serangan DDoS.

3. **Pengujian Algoritma**
   Pada tahap ini dilakukan pengujian algoritma yang diusulkan dengan cara melakukan validasi hasil deteksi algoritma dengan anotasi yang diberikan oleh dataset yang disediakan. Algoritma yang telah diuji akan dianalisa guna memperoleh hasil sesuai yang diharapkan. Pada tahap ini juga dilakukan perhitungan akurasi, spesivisiti dan sensitiviti untuk mengukur performansi algoritma yang diusulkan.

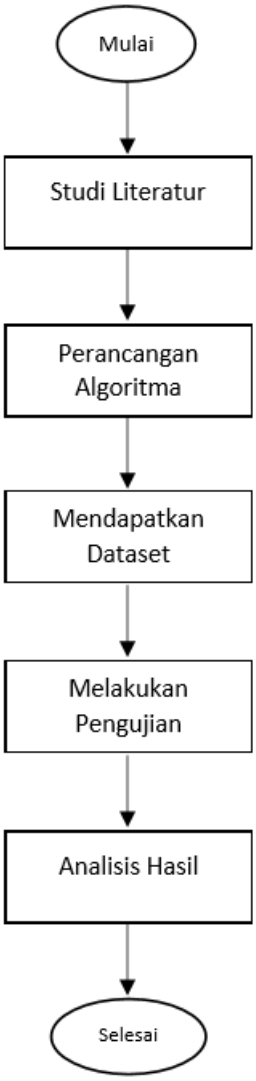
4. **Pengimplementasian Algoritma yang Diusulkan**
   Pada tahap ini penulis melakukan perancangan algoritma yang telah dibuat. Perancangan dilakukan agar sebelum algoritma diterapkan pada sistem berbasis IoT, dapat mengetahui apakah algoritma yang diusulkan dapat mendeteksi serangan DDoS sesuai yang diharapkan.

5. **Pengujian dan Analisis**
   Pada tahap ini penulis melakukan pengujian terhadap performansi algoritma yang dikembangkan dengan menerapkan algoritma pada sistem berbasis IoT. Hasil dari tahap ini adalah nilai-nilai performansi dari algoritma yang diusulkan.

6. **Penulisan Laporan**
   Pada tahap ini penulis menyusun laporan terkait penelitian yang dilakukan mengikuti metode perancangan tata tulis ilmiah. Hasil dari tahapan ini adalah buku tugas akhir.

3.1.2 Metodologi untuk Mencapai Tujuan Penelitian

A) **M**etodologi untuk mencapai objectif pertama
   Metodologi yang dilakukan dalam mencapai objektif pertama adalah sebagai berikut :



Gambar 3.2: Diagram Alir Metodologi Objektif Pertama

Berikut adalah penjelasan untuk setiap tahapan metodologi :

(a) **Studi Litaratur**
Pada tahap ini dilakukan review terhadap penelitian-penelitian yang telah dilakukan sebelumnya dan merangkum fakta serta teori yang dibutuhkan dalam penelitian. Dilakukan dengan membaca jurnal dan artikel yang berkaitan. Jurnal penelitian didapat dari situs terpercaya seperti IEEE dengan batasan penelitian terakhir 10 tahun lalu. Pada tahap ini juga penulis menganalisis masalah dan

membuat alasan mengapa masalah tersebut perlu diselesaikan.

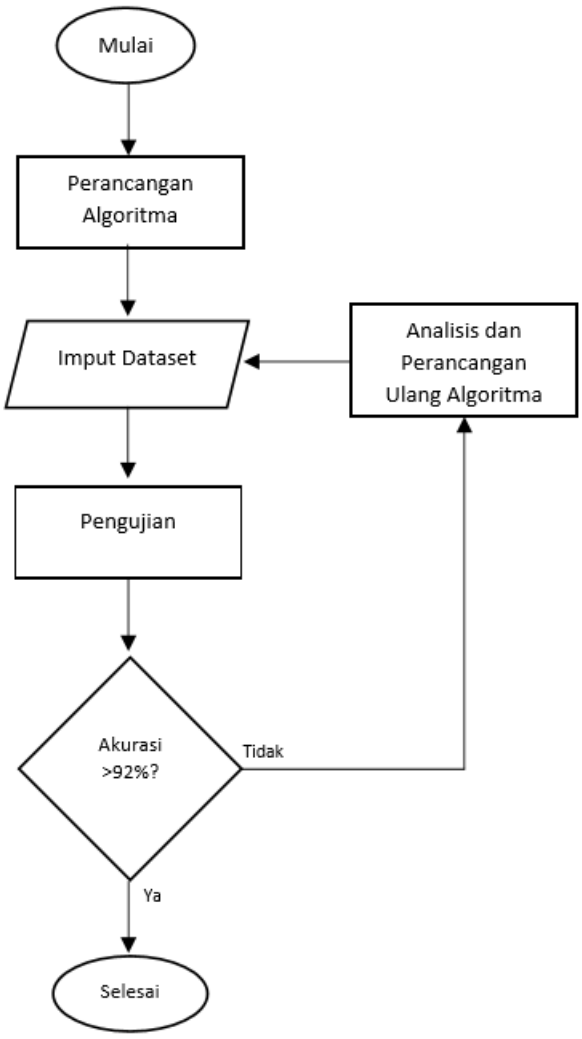
(b) **Perancangan Algoritma**
Pada tahap ini melakukan perancangan dengan menggunakan algoritma *Neural Network* untuk melakukan *ekstrasion feature*. *Output* dari tahap ini adalah algoritma yang siap digunakan.

(c) **Mendaptkan Dataset**
Dataset diambil dari dataset dari Bellekens (2020)

(d) **Melakukan Pengujian**
Pada tahap ini, algoritma yang sudah jadi akan di uji dengan menggunakan dataset yang didapat pada tahap sebelumnya. *Output* dari tahap ini adalah presentase hasil akurasi.

(e) **Analisis Hasil**
Setelah algoritma deteksi diterapkan, dilakukan analisis terhadap algoritma apakah algoritma yang digunakan memiliki hasil yang akurat atau tidak. Apakah algoritma yang diusulkan mencapai akurasi ¿92% atau tidak. Analisis dilakukan dengan cara melihat dataset berdasarkan anotasi apakah sama atau tidak dengan data yang dihasillkan oleh algoritma.

B) **M**etodologi untuk mencapai objectif kedua
Berikut adalah skema *prototype* yang akan dibangun untuk mencapai objektif kedua :



Gambar 3.3: Diagram Alir Metodologi Objektif Kedua

Berikut adalah penjelasan dari masing-masing tahapan :

(a) **Perancangan Algoritma**
Pada tahap ini melakukan perancangan dengan menggunakan algoritma *Neural Network* untuk melakukan *ekstrasion feature*. *Output* dari tahap ini adalah algoritma yang siap digunakan.

(b) **Input Dataset**
Melakukan input dataset yang didapat dari Bellekens (2020)

(c) **Pengujian**
Pada tahap ini, algoritma yang sudah jadi akan di uji dengan meng-

gunakan dataset yang didapat pada tahap sebelumnya. *Output* dari tahap ini adalah presentase hasil akurasi.

(d) **Analisis**
Pada tahap ini dilakukan analisis, apakah algoritma yang digunakan sudah mampu mencapai hasil sesuai yang diharapkan atau tidak, jika tidak, maka akan dilakukan perancangan ulang algoritma untuk mencapai hasil yang diharapkan.

C) **M**etodologi untuk mencapai objektif ketiga Metodologi yang dilakukan dalam mencapai objektif ketiga adalah sebagai berikut :

Gambar 3.4: Diagram Alir Metodologi Objektif Ketiga

Berikut adalah penjelasan untuk setiap tahapan metodologi :

(a) **Studi Literatur**
Pada tahap ini dilakukan review terhadap penelitian-penelitian yang telah dilakukan sebelumnya dan merangkum fakta serta teori yang

dibutuhkan dalam penelitian. Dilakukan dengan membaca jurnal dan artikel yang berkaitan. Jurnal penelitian didapat dari situs terpercaya seperti IEEE dengan batasan penelitian terakhir 10 tahun lalu. Pada tahap ini juga penulis menganalisis masalah dan membuat alasan mengapa masalah tersebut perlu diselesaikan.

(b) **Perancangan Sistem**
Tahap ini merumuskan kebutuhan perangkat kerasa dan lunak yang dibutuhkan untuk membangun sistem serta merancang skema pengambilan data ke dalam sistem yang dibuat.

(c) **Instalasi Perangkat Lunak dan Keras**
Pada tahap ini dilakukan konfigurasi kebutuhan perangkat lunak seperti instalasi python 2.7 dan IDE yang dibutuhkan.

(d) **Melakukan Pengujian**
Pada tahap ini, algoritma yang sudah jadi akan di uji dengan menggunakan dataset yang didapat pada tahap sebelumnya. *Output* dari tahap ini adalah presentase hasil akurasi

(e) **Analisis Akurasi Performansi**
Pada tahap ini dilakukan analisis terhadap sistem yang sudah dilakukan pengujian.

(f) **Pembuatan Kesimpulan**
Setelah hasil analisis, maka akan dilakukan pembuatan kesimpulan untuk menyimpulak sistem yang telah dirancang.

3.1.3 Analisis Kebutuhan Sistem

A) **S**pesifikasi Perangkat Keras

- Laptop Processor AMD Ryzen™ 5-3550H @3.20GHz
- Memory 8GB
- Hard Drive 1TB

B) **S**pesifikasi Perangkat Lunak

- Windows 10 Home
- Python 3.8
- Jupyter Notebook

3.1.4 Data

Data yang digunakan dalam melakukan penelitian ini adalah dataset dari Koroniotis et al. (2019). Dataset dibagi menjadi *data train* dan *data test* sebesar dengan rasio 7 banding 3.

3.1.5 Metrik Uji

Metrik pengujian yang digunakan dalam melakukan pengujian algoritma adalah akurasi, *recall*, *F1-Score*, dan presisi.

Persamaan *Accuracy*

$$accuracy = \frac{TP + TN}{TP + FP + FN + TN} \tag{3.1}$$

Persamaan *Recall*

$$Recall = \frac{TP}{FN + TP} \tag{3.2}$$

Persamaan *Precision*

$$precision = \frac{TP}{TP + FP} \tag{3.3}$$

Persamaan F1-*Score*

$$F1 - Score = 2X\frac{precision * recall}{precision + recall} \tag{3.4}$$

Matriks evaluasi klasifikasi digunakan untuk evaluasi metode yang diusulkan. Dimana TN adalah *True Negatives*, TP adalah *True Positive* , FN adalah *False Negative* dan FP adalah *False Positive*.

3.1.6 Metode Pengujian

Untuk mengetahui keberahasilan seluruh rancangan diperlukan adanya pengujian, baik secara perangkat maupun algoritma. Hal ini ditujukan mengetahui apakah tujuan tugas akhir ini tercapai. Skenario pengujian dilakukan dengan tiga kondisi jaringan.

Skenario Pengujian

1. **Skenario 1 : Klasifikasi Langsung**
   Pada skenario ini, pengujian dilakukan dengan melakukan klasifikasi secara langsung tanpa memilih-milih fitur. Kemudian presentase akan dihitung dengan menggunakan metrik uji.

2. **Skenario 2 : Klasifikasi 8 Fitur**
   Pada skenario ini, pengujian dilakukan dengan menggunakan 8 fitur pilihan yang terdapat pada dataset. Kemudian presentase akan dihitung dengan menggunakan metrik uji.

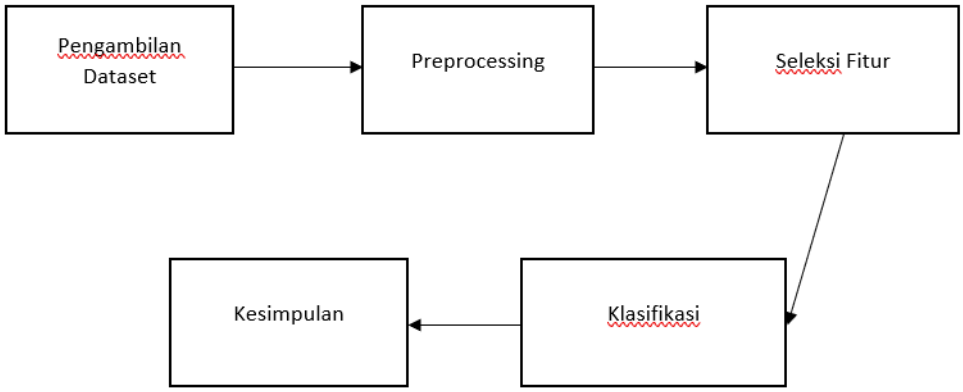
3. **Skenario 3 : Klasifikasi Fitur Tanpa Flow**
   Pada skenario ini, pengujian dilakukan dengan menggunakan fitur-fitur yang ada kecuali flow yang terdapat pada dataset. Kemudian presentase akan dihitung dengan menggunakan metrik uji.

3.1.7 Perbandingan Hasil Penelitian

Tugas Akhir ini melakukan perbandingan hasil yang didapat dengan penelitian serupa yang telah dilakukan oleh Roopak et al. (2020).

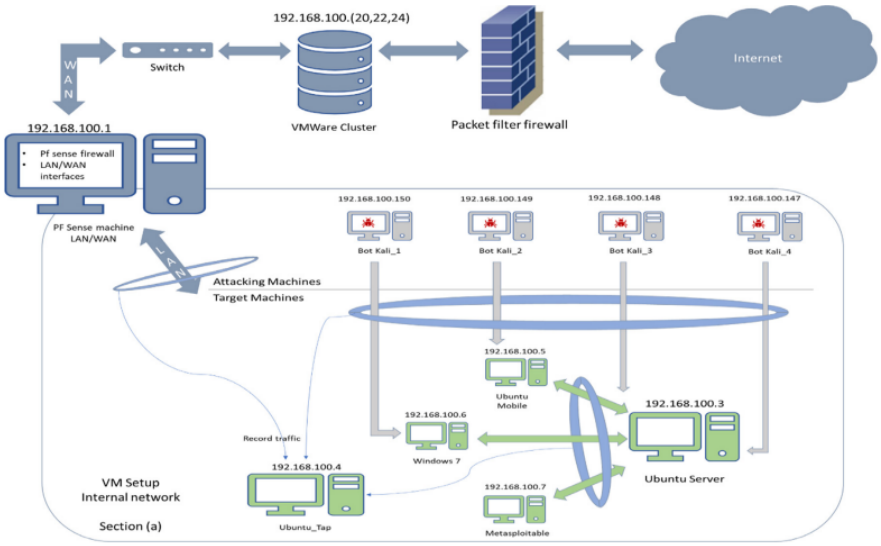
3.2 Desain Sistem

Gambar 3.6 adalah ilustrasi desain dari sistem dari tugas akhir ini.



Gambar 3.5: Desain Sistem yang direncanakan

Seperti terlihat pada Gambar 3.6 dataset dari Koroniotis et al. (2019) kemudian diolah agar bisa dilanjutkan ke tahap ekstraksi fitur, setelah dilakukan deteksi, maka akan diklasifikasikan apakah data tersebut merupakan jenis serangan DDoS atau bukan.



Gambar 3.6: Lingkungan pengujian dari kumpulan data Bot-IoT baru.

3.3 Ringkasan

Ada beberapa hal yang perlu menjadi catatan dari Bab ini sebagai berikut:

1. Penilitian ini menggunakan 3 metodologi sebagai acuan dalam perancangan sistem. Selain itu dengan menggunakan matriks uji, akan terlihat hasil dari penelitian berdasarkan tujuan yang telah terpaparkan.

2. Algoritma yang digunakan dalam penelitian kali ini adalah *neural network*.

3. Dengan penelitian yang dilakukan ini, diharapkan hasil yang didapatkan dapat melebihi dari penelitian sebelumnya yang dijadikan perbandingan.

Bab IV

Hasil dan Pembahasan

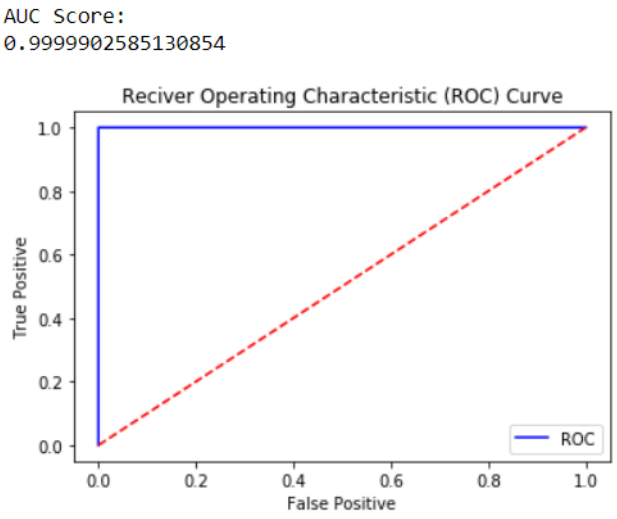
Pada bab ini akan dibahas hasil dari klasifikasi dan hasil pengujian skenario yang dilakukan terhadap data MIT-BIH dan data dari sensor EKG AD8232.

4.1 Hasil Pengujian

Setelah melaksanakan pengujian sistem seperti yang telah dibahas pada bab sebelumnya sub bab ini akan memaparkan hasil dari percobaan.

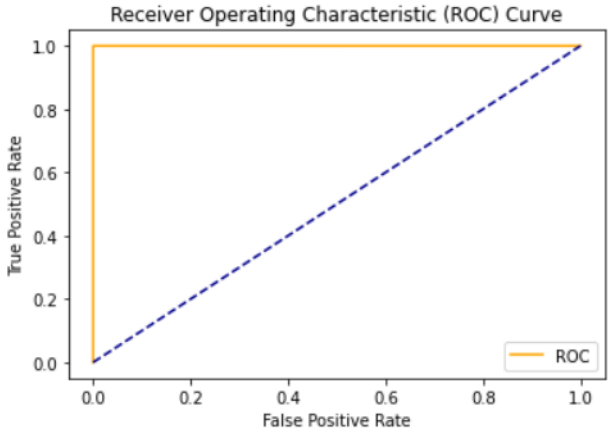
4.1.1 Hasil Klasifikasi Menggunakan Neural Network

Dengan melakukan klasifikasi menggunakan Neural Network, hasil yang didapatkan berdasarkan skenario yaitu berbeda-beda. Skenaria yang dilakukan yaitu melakukan klasifikasi secara langsung, melakukan klasifikasi dengan menggunakan 8 fitur, melakukan klasifikasi dengan semua fitur kecuali flow. Dihasilkan data sebagai berikut:



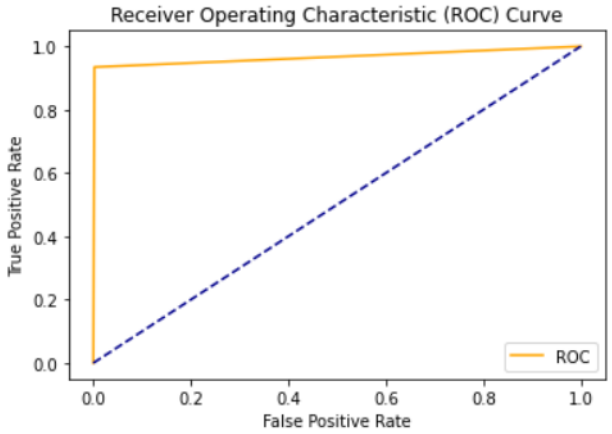
Gambar 4.1: ROC Pada Skenario I

```
AUC Score:
0.9999252980930877
```



Gambar 4.2: ROC Pada Skenario II

```
AUC Score:
0.9662482407112907
```



Gambar 4.3: ROC Pada Skenario III

Selain itu, adapula Fitur-fitur yang dapat diambil dari dataset ada 2 bagian, yaitu fitur standart, dan fitur flow, sebagai berikut:

Features and descriptions.

Feature	Description
pkSeqID	Row Identifier
Stime	Record start time
flgs	Flow state flags seen in transactions
flgs_number	Numerical representation of feature flags
Proto	Textual representation of transaction protocols present in network flow
proto_number	Numerical representation of feature proto
saddr	Source IP address
sport	Source port number
daddr	Destination IP address
dport	Destination port number
pkts	Total count of packets in transaction
bytes	Totan number of bytes in transaction
state	Transaction state
state_number	Numerical representation of feature state
ltime	Record last time
seq	Argus sequence number
dur	Record total duration
mean	Average duration of aggregated records
stddev	Standard deviation of aggregated records
sum	Total duration of aggregated records
min	Minimum duration of aggregated records
max	Maximum duration of aggregated records
spkts	Source-to-destination packet count
dpkts	Destination-to-source packet count
sbytes	Source-to-destination byte count
dbytes	Destination-to-source byte count
rate	Total packets per second in transaction
srate	Source-to-destination packets per second
drate	Destination-to-source packets per second
attack	Class label: 0 for Normal traffic, 1 for Attack Traffic
category	Traffic category
subcategory	Traffic subcategory

Gambar 4.4: Fitur standart

	Feature	Description
1	TnBPSrcIP	Total Number of bytes per source IP
2	TnBPDstIP	Total Number of bytes per Destination IP.
3	TnP_PSrcIP	Total Number of packets per source IP.
4	TnP_PDstIP	Total Number of packets per Destination IP.
5	TnP_PerProto	Total Number of packets per protocol.
6	TnP_Per_Dport	Total Number of packets per dport
7	AR_P_Proto_P_SrcIP	Average rate per protocol per Source IP. (calculated by pkts/dur)
8	AR_P_Proto_P_DstIP	Average rate per protocol per Destination IP.
9	N_IN_Conn_P_SrcIP	Number of inbound connections per source IP.
10	N_IN_Conn_P_DstIP	Number of inbound connections per destination IP.
11	AR_P_Proto_P_Sport	Average rate per protocol per sport
12	AR_P_Proto_P_Dport	Average rate per protocol per dport
13	Pkts_P_State_P_Protocol_P_DestIP	Number of packets grouped by state of flows and protocols per destination IP.
14	Pkts_P_State_P_Protocol_P_SrcIP	Number of packets grouped by state of flows and protocols per source IP.

Gambar 4.5: fitur Flow

4.2 Pembahasan

Berdasarkan hasil analisis pada skenario-skenario di atas, penulis mencoba untuk melakukan perhitungan performansi secara terpisah antara skenario I, II dan III. Dari hasil pengujian klasifikasi fitur Neural Network dapat mendeteksi cukup baik pada skenario I, dan II, namun untuk skenario III hasil yang keluar cukup rendah dibandingkam sekenario sebelumnya. Sebaliknya deteksi menggunakan fitur yang lebih sedikit seperti pada skenario III lebih menghemat waktu. Oleh karena itu penulis mencoba mengukur kembali performansi masing-masing skenario dihitung berdasarkan algoritma yang tepat untuk jenis data tersebut. Hasil dari perhitungan tersebut adalah sebagai berikut :

	precision	recall	f1-score	support
0	1.00	1.00	1.00	771384
1	1.00	1.00	1.00	769903
accuracy			1.00	1541287
macro avg	1.00	1.00	1.00	1541287
weighted avg	1.00	1.00	1.00	1541287

Gambar 4.6: Matrik uji pada skenario I

	precision	recall	f1-score	support
0	1.00	1.00	1.00	771574
1	1.00	1.00	1.00	769726
accuracy			1.00	1541300
macro avg	1.00	1.00	1.00	1541300
weighted avg	1.00	1.00	1.00	1541300

Gambar 4.7: Matrik uji pada skenario II

	precision	recall	f1-score	support
0	0.94	1.00	0.97	771574
1	1.00	0.93	0.97	769726
accuracy			0.97	1541300
macro avg	0.97	0.97	0.97	1541300
weighted avg	0.97	0.97	0.97	1541300

Gambar 4.8: Matrik uji pada skenario III

4.3 Ringkasan

Ada beberapa hal yang perlu menjadi catatan dari Bab ini sebagai berikut:

1. Hasil yang ditunjukkan berdasarkan dataset yang tersedia, belum dilakukan pengujian terhadap dataset lain atau secara langsung.
2. Semakin berbobot fitur-fitur yang dipilih untuk klasifikasi, semakin akurat dan cepat juga hasilnya. .
3. Dengan menggunakan *neural network* sekor yang dihasilkan lebih tinggi daripada algoritma lain, seperti menggunakan KNN ataupun SVM.

Bab V

Kesimpulan dan Saran

5.1 Kesimpulan

Tugas akhir ini telah mencapai semua obyektif yang disebutkan pada Bab I, sebagai berikut:

1. Obyektif Pertama sudah tercapai. Bukti capaian dapat dilihat pada proposal yang dibuat, dihasilkan sebuah sistem dan hasil berupa tulisan untuk menjelaskan keseluruhan sistem yang dibuat

2. Obyektif Kedua sukes dicapai dengan bukti ada pada Bab IV dimana setelah dilakukan pengujian, hasil yang didapatkan kurang sesuai harapan, kemudian dilakukan pengujian ulang

3. Obyektif Ketiga berhasil dicapai. Bukti dari capaian ada pada bab IV dimana setelah melakukan berbagai percobaan sehingga dihasilkan sekor akurasi yang tinggi, yaitu 99,9

5.2 Saran

Berdasarkan proses perancangan dan pengujian sistem, penulis melihat beberapa pengembangan rancangan dan langkah pengujian yang dapat dilakukan, antara lain:

1. Semakin banyak percobaan yang dilakukan dengan berbagai data yang didapatkan akan meningkatkan pengembangan algoritma.

2. Memilih fitur dan klasifikasi lain untuk meningkatkan kehandalan akurasi deteksi

3. Melakukan pengujian terhadap dataset yang didapat secara langsung agar dapat sepenuhnya sistem siap untuk digunakan dan dikembangkan secara umum.

4. Algoritma perlu dikembangkan lagi agar selain dapat mendeteksi, juga dapat mengatasi serangan DDoS.

Daftar Pustaka

Ahanger, T. A. (2017), An effective approach of detecting ddos using artificial neural networks, *in* '2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)', IEEE, pp. 707–711.

Anstee, D., Bussiere, D., Sockrider, G. and Morales, C. (2014), 'Worldwide infrastructure security report', *Arbor Netw., Burlington, MA, USA, Tech. Rep* **9**.

Aziz, M., Umar, R. and Ridho, F. (2019), 'Implemetasi jaringan saraf tiruan untuk mendeteksi serangan ddos pada forensik jaringan', *Query: Journal of Information Systems* **3**(1).

Belej, O. and Halkiv, L. (2020), Using hybrid neural networks to detect ddos attacks, *in* '2020 IEEE Third International Conference on Data Stream Mining & Processing (DSMP)', IEEE, pp. 61–66.

Bellekens, H. H. C. T. R. A. E. B. X. (2020), 'Mqtt-iot-ids2020: Mqtt internet of things intrusion detection dataset'.
URL: *https://dx.doi.org/10.21227/bhxy-ep04*

Bolzoni, D., Etalle, S. and Hartel, P. H. (2009), Panacea: Automating attack classification for anomaly-based network intrusion detection systems, *in* 'International Workshop on Recent Advances in Intrusion Detection', Springer, pp. 1–20.

Chen, Y.-W., Sheu, J.-P., Kuo, Y.-C. and Van Cuong, N. (2020), Design and implementation of iot ddos attacks detection system based on machine learning, *in* '2020 European Conference on Networks and Communications (EuCNC)', IEEE, pp. 122–127.

Cho, E. J., Hong, C. S. and Choi, D. (2011), Distributed ids for efficient resource management in wireless sensor network, *in* '2011 13th Asia-Pacific Network Operations and Management Symposium', IEEE, pp. 1–5.

Harsono, H., Khambali, M. and Muhammad, A. W. (2018), 'Klasifikasi paket jaringan berbasis analisis statistik dan neural network', *Jurnal Informatika: Jurnal Pengembangan IT* **3**(1), 67–70.

Haykin, S. (2008), 'Neural networks and learning machines, hoboken'.

Koroniotis, N., Moustafa, N., Sitnikova, E. and Turnbull, B. (2019), 'Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset', *Future Generation Computer Systems* **100**, 779–796.

Lee, S., Kim, G. and Kim, S. (2011), 'Self-adaptive and dynamic clustering for online anomaly detection', *Expert Systems with Applications* **38**(12), 14891–14898.

Li, J., Liu, Y. and Gu, L. (2010), Ddos attack detection based on neural network, *in* '2010 2nd International Symposium on Aware Computing', IEEE, pp. 196–199.

Muhammad, A. W., Riadi, I. and Sunardi, S. (2016), 'Analisis statistik log jaringan untuk deteksi serangan ddos berbasis neural network', *ILKOM Jurnal Ilmiah* **8**(3), 220–225.

Muhammad, A. W., Riadi, I. and Sunardi, S. (2017), 'Deteksi serangan ddos menggunakan neural network dengan fungsi fixed moving average window', *JISKA (Jurnal Informatika Sunan Kalijaga)* **1**(3), 115–122.

Nihri, H., Pramukantoro, E. S. and Trisnawan, P. H. (2018), 'Pengembangan ids berbasis j48 untuk mendeteksi serangan dos pada perangkat middleware iot', *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN* **2548**, 964X.

Roopak, M., Tian, G. Y. and Chambers, J. (2020), An intrusion detection system against ddos attacks in iot networks, *in* '2020 10th Annual Computing and Communication Workshop and Conference (CCWC)', IEEE, pp. 0562–0567.

Saxena, U., Sodhi, J. and Singh, Y. (2020), An analysis of ddos attacks in a smart home networks, *in* '2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)', IEEE, pp. 272–276.

Silveira, F. A. F., Lima-Filho, F., Silva, F. S. D., Junior, A. d. M. B. and Silveira, L. F. (2020), Smart detection-iot: A ddos sensor system for internet of things, *in* '2020 International Conference on Systems, Signals and Image Processing (IWSSIP)', IEEE, pp. 343–348.

Smith, R., Japkowicz, N., Dondo, M. and Mason, P. (2008), Using unsupervised learning for network alert correlation, *in* 'Conference of the Canadian Society for Computational Studies of Intelligence', Springer, pp. 308–319.

Soe, Y. N., Santosa, P. I. and Hartanto, R. (2019), Ddos attack detection based on simple ann with smote for iot environment, *in* '2019 Fourth International Conference on Informatics and Computing (ICIC)', IEEE, pp. 1–5.

Sofa, E. L. et al. (2019), ROUTING ATTACKS PADA PROTOKOL KOMUNIKASI INTERNET OF THINGS MENGGUNAKAN SMART INTRUSION DETECTION SYSTEM, PhD thesis, UNNES.

Tan, L. and Wang, N. (2010), Future internet: The internet of things, *in* '2010 3rd international conference on advanced computer theory and engineering (ICACTE)', Vol. 5, IEEE, pp. V5–376.

Thatte, G., Mitra, U. and Heidemann, J. (2010), 'Parametric methods for anomaly detection in aggregate traffic', *IEEE/ACM Transactions On Networking* **19**(2), 512–525.

Vinayakumar, R., Soman, K. and Poornachandran, P. (2017), Applying convolutional neural network for network intrusion detection, *in* '2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)', IEEE, pp. 1222–1228.

Wehbi, K., Hong, L., Al-salah, T. and Bhutta, A. A. (2019), A survey on machine learning based detection on ddos attacks for iot systems, *in* '2019 SoutheastCon', IEEE, pp. 1–6.

Lampiran A

Jadwal Kegiatan

The table 5.2 is an example of referenced LaTeXelements. Laporan proposal ini akan dijadwalkan sesuai dengan tabel yang diberikna berikutnya.

Tabel 5.1: Jadwal kegiatan proposal tugas akhir

No	Kegiatan	Bulan ke-																					
		1				2				3				4				5				6			
1	Studi Literatur																						
2	Pengumpulan Data																						
3	Analisis dan Perancangan Sistem																						
4	Implementasi Sistem																						
5	Analisa Hasil Implementasi																						
6	Penulisan Laporan																						

Lampiran B

Jadwal Kegiatan

The table 5.2 is an example of referenced LaTeXelements. Laporan proposal ini akan dijadwalkan sesuai dengan tabel yang diberikna berikutnya.

No	Kegiatan	Bulan ke-																					
		1				2				3				4				5				6			
1	Studi Literatur																						
2	Pengumpulan Data																						
3	Analisis dan Perancangan Sistem																						
4	Implementasi Sistem																						
5	Analisa Hasil Implementasi																						
6	Penulisan Laporan																						

Tabel 5.2: Jadwal kegiatan proposal tugas akhir