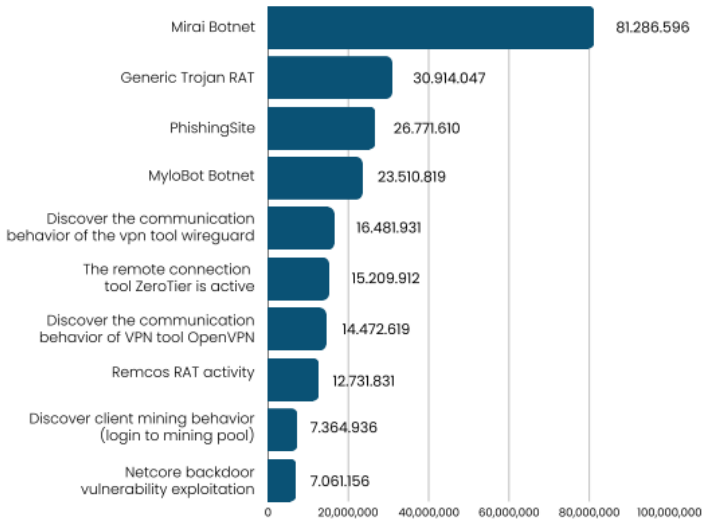
BAB I
PENDAHULUAN

1.1 Latar belakang

Bertambahnya ketergantungan pada teknologi digital dan peningkatan penggunaan konektivitas jaringan komputer telah menyebabkan peningkatan frekuensi ancaman siber. Indonesia merupakan negara yang masih menghadapi kerentanan dalam keamanan sibernya, sehingga kolaborasi berbagai pihak sangat penting untuk meningkatkan keamanan siber di Indonesia[1]. Jaringan komputer telah digunakan oleh berbagai pihak termasuk pemerintah, akademisi, industri, lembaga, dan individu untuk mencari, memperoleh, mengelola, dan mengirim informasi [2]. Di indonesia pengguna internet sudah mencapai 221.563.479 jiwa atau 79,5% pada tahun 2024 naik 1,4% dari tahun 2023[3]. Semakin bertambahnya pengguna jaringan komputer menyebabkan munculnya berbagai kejahatan dan kepadatan lalu lintas jaringan, serta variasi dan pengenalan jenis intrusi baru yang menjadi tantangan bagi deteksi intrusi, sehingga isu Keamanan Siber menjadi sangat penting untuk mendukung aktivitas jaringan internet di Indonesia[2], [4]. Pada tahun 2024 Badan Sandi dan Siber Negara (BSSN) mencatat terjadi 330.527.636 anomali atau gangguan pada trafik jaringan di indonesia.



Gambar 1. 1 Top 10 Trafik Anomali di Indonesia tahun 2024[5]

Grafik di atas menunjukkan jumlah aktivitas dari berbagai jenis ancaman *cyber*, dengan *Mirai Botnet* menempati posisi teratas dengan 81.286.596 kejadian. Di bawahnya, *Generic Trojan* RAT dan *PhishingSite* juga menunjukkan angka signifikan, masing-masing dengan 30.914.047 dan 26.771.610 kejadian. Mirai Botnet adalah salah satu jenis botnet yang menargetkan perangkat *Internet of Things* (IoT). Botnet ini dibuat untuk melakukan serangan *Distributed Denial of Service* (DDoS) pada situs web atau layanan online, sehingga mengakibatkan adanya gangguan atau *downtime*.

Dalam asistensi yang dilaksanakan oleh BSSN secara menyeluruh, disusun *lesson learned* untuk 5 (lima) jenis kasus terbanyak berdasarkan asistensi tanggap insiden siber, yaitu Kebocoran Data. Pada tahun 2024, tercatat 56,1 juta data exposure di Darknet, termasuk informasi pribadi, kredensial akses, dan data keuangan [6]. Akses ilegal adalah tindakan memasuki atau meretas sistem komputer atau jaringan tanpa izin dari pemiliknya. Dari 593 dugaan insiden siber yang dicatat oleh *Cyber Threat Intelligence* (CTI), sejumlah besar kasus melibatkan peretasan sistem dengan memanfaatkan celah keamanan. *Web defacement* adalah tindakan merusak atau mengubah wajah sebuah situs web tanpa izin, biasanya oleh individu atau kelompok dengan niat jahat. Dalam kasus *defacement web*, terdeteksi sebanyak 5.780 insiden yang menargetkan beragam domain, serta 4.071 *defacement web* yang berkaitan dengan perjudian online yang menyasar situs pemerintahan. Kasus terbanyak terjadi di domain GO.ID dengan 1.240 serangan, AC.ID dengan 2.362 serangan, dan SCH.ID dengan 1.706 serangan. *Ransomware* adalah serangan siber yang disebabkan oleh malware yang menginfeksi perangkat dan mengenkripsi data yang ada di dalamnya. Setelah menginfeksi perangkat, ransomware akan mengacak file-file penting sehingga tidak bisa diakses lagi. Pada tahun 2024 tercatat 514.508 aktivitas *ransomware*, meningkat 40% kasus *ransomware* dibanding tahun lalu. *Distributed Denial of Service* (DDoS) adalah serangan siber di mana aktor ancaman berusaha membuat layanan atau situs web tidak dapat diakses oleh pengguna yang sah dengan membanjiri sistem target dengan volume lalu lintas jaringan yang sangat besar. Serangan ini telah cukup mengganggu layanan dengan angka mencapai 1 Tbps dalam kasus serangan terhadap layanan finansial pada tahun 2023 yang menimpa bank BSI[5].

Beberapa insiden *Cyber* yang di sebabkan DDoS adalah lumpuhnya sistem Sirekap KPU dalam pemilihan umum 2024 pada tanggal 14 februari 2024, serangan terjadi pukul 13:00-21.00 sehingga mengakibatkan server KPU sempat lumpuh dengan trafik sangat tinggi yang mengakses ke server[7]. Selain itu pada jaringan *Cloudflare* memitigasi adanya 4,5 juta serangan DDoS Q1, 4 juta serangan pada Q2[8], 6 juta seranganpada Q3[9], 6,9 juta serangan pada Q4 selama tahun 2024menunjukkan peningkatan sebesar 16% dari *Quarter on Quarter* (QoQ) dan 83% dari *Year on Year* (YoY)[10]. Laporan Keamanan Microsoft pada 2024 mengungkapkan tren dan kemajuan terbaru terkait serangan DDoS, dengan peningkatan signifikan mencapai 4.500 serangan harian pada bulan Juni yang menargetkan aplikasi berukuran sedang. Berbeda dari serangan jaringan konvensional, serangan pada lapisan aplikasi lebih tersembunyi, rumit, dan sulit untuk ditangani. Serangan ini, yang berkisar antara 100.000 sampai 1 juta paket per detik, ditujukan langsung pada aplikasi web tertentu, menunjukkan sifat penyerang yang tekun dalam usahanya untuk menghindari strategi perlindungan DDoS volumetrik. Perbedaan dalam teknologi, pendekatan, dan taktik serangan memengaruhi keberhasilan dalam mengenali serangan, sedangkan deteksi tanda-tanda juga tergantung pada adanya perangkat lunak dan perangkat keras yang dipakai oleh server. Tanpa adanya teknologi deteksi yang terpercaya, usaha mitigasi menjadi sulit, sehingga diperlukan kolaborasi antara keduanya untuk menciptakan sistem keamanan siber yang kuat dan stabil. Tanpa jaminan yang cukup, aplikasi ini akan menghadapi masalah ketersediaan yang serius[11]. Perbedaan dalam teknologi, teknik, dan taktik serangan memengaruhi efisiensi dalam mendeteksi serangan, sedangkan identifikasi gejala juga tergantung pada perangkat lunak dan perangkat keras yang digunakan oleh server. Tanpa adanya dukungan teknologi deteksi yang efektif, usaha mitigasi menjadi sulit, sehingga diperlukan kolaborasi antara keduanya untuk menciptakan sistem keamanan siber yang kuat dan stabil[12].

Serangan *Distributed Denial of Service* (DDoS) adalah salah satu risiko bagi sistem jaringan, yang berdampak pada aplikasi dan perangkat yang bergantung padanya[13]. *Distributed Denial of Service* (DDoS) merupakan tipe serangan siber yang berupaya menghabiskan sumber daya yang dimiliki sebuah sistem, sehingga

sistem tersebut tidak dapat berfungsi dengan baik dan secara tidak langsung menghalangi pengguna lain untuk mendapatkan akses layanan dari sistem yang diserang. Serangan DDoS memanfaatkan celah dalam sistem yang terkait dengan keterbatasan sumber daya, seperti bandwidth, kapasitas memori, server, dan kelemahan lainnya [14]. Dalam mengidentifikasi serangan ini ternyata tidak mudah, akibat pertumbuhannya yang pesat dan kerumitan yang terlibat dalam proses deteksinya. Dengan beragam atribut yang digunakan dalam analisis pengguna jaringan untuk mengidentifikasi pola serangan yang diterapkan, semakin banyak atribut yang digunakan, maka proses pengolahan dan penentuan pola serangan akan semakin lama dalam komputasi deteksinya. Agar terlindungi dari berbagai jenis serangan DDoS, sangat krusial untuk menciptakan sistem yang tangguh. Ada dua tipe utama serangan DDoS: serangan *volumetrik* [15] dan *Application-layer attacks* [16]. Serangan volumetrik atau serangan banjir mengisi dan menguras bandwidth infrastruktur jaringan. Ini biasanya memanfaatkan protokol lapisan 3 atau 4 untuk menghasilkan jumlah lalu lintas yang besar, dengan jenis yang umum meliputi banjir ICMP, UDP, dan TCP-SYN. Serangan lapisan aplikasi lebih kompleks dan dalam banyak situasi memanfaatkan bandwidth yang lebih sedikit untuk dilakukan. Serangan lapisan aplikasi memanfaatkan celah pada perangkat lunak, sehingga memerlukan lebih sedikit sumber daya dari pihak penyerang, sukar untuk terdeteksi, dan perangkat keras yang lebih tangguh di pihak korban tidak menjamin kegagalan serangan tersebut. Hal ini menargetkan aplikasi atau layanan spesifik dan secara bertahap menguras sumber daya jaringan. Penyerang bisa mempertahankan koneksi terbuka lebih lama dengan mengirim data yang diminta menggunakan jendela paket yang sangat kecil. Contohnya meliputi serangan DNS dan HTTP[17]. *Application-layer attacks* adalah jenis serangan siber di mana sekelompok mesin yang telah terinfeksi (dikenal sebagai *zombie machines*) menyerang server target dengan mengirimkan paket-paket yang tampak sepenuhnya sah. Paket-paket ini memiliki format yang benar dan dikirim melalui koneksi TCP yang normal, sehingga sistem deteksi intrusi (IDS) maupun server target tidak dapat membedakannya dari lalu lintas pengguna biasa. Serangan ini pada dasarnya membanjiri server dengan permintaan yang sah, seperti permintaan HTTP, hingga sumber daya server habis dan tidak dapat melayani pengguna lain.

Karena setiap mesin penyerang harus membangun koneksi TCP yang valid, mereka harus menggunakan alamat IP asli, bukan alamat IP palsu (IP spoofing)[18]. Pemanfaatkan algoritma *Mechine learning* untuk deteksi serangan DDoS menjadi solusi yang menarik karena kemampuannya untuk mendeteksi pola anomali pada lalu lintas jaringan komputer.

Mechine learning merupakan teknologi yang saat ini menjadi perhatian berbagai bidang, karena kemampuannya dalam menciptakan sistem yang lebih cerdas dan mampu beradaptasi dengan lingkungannya secara terus-menerus. *Mechine learning* memiliki kemampuan untuk mengekstrak fitur mentah dari data tanpa campur tangan manusia. *Mechine learning* dapat memenuhi tingkat kinerja tinggi dengan menemukan korelasi pada data mentah secara otomatis. Teknologi ini dapat di manfaatkan dalam keamanan cyber terutama DDoS karena dapat menganalisis pola yang kompleks, beradaptasi dengan ancaman baru, dan menangani pemrosesan data skala besar.

Pada tinjauan komprehensif[19] Penggunaan strategis metode *Machine Learning dan Deep Learning* untuk identifikasi serangan *Distributed Denial of Service* (DDoS) di dalam ekosistem komputasi awan telah menjadi bidang penelitian dan pengembangan yang signifikan. Pendekatan teknologi maju ini tidak hanya memperlihatkan peningkatan luar biasa dalam ketepatan dan keseluruhan efektivitas mekanisme deteksi DDoS, tetapi juga menekankan peran penting yang dijalankan algoritma canggih ini dalam melindungi data sensitif dan menjamin pengiriman layanan tanpa hambatan. Selain itu, penggabungan sinergis metode pembelajaran mesin kuantum dengan sistem respons otomatis menciptakan kerangka kerja yang tangguh, sangat efisien, dan mudah beradaptasi untuk mendeteksi DDoS, yang dapat memperkuat infrastruktur cloud modern terhadap berbagai ancaman cyber yang semakin canggih dan berbahaya. Pada akhirnya, inovasi yang berkembang dari teknologi canggih ini memberikan solusi yang menjanjikan untuk tantangan mendesak yang dihadapi akibat musuh cyber modern, sehingga secara signifikan memajukan bidang keamanan siber dalam konteks komputasi awan. Menurut penelitain [20] menujukan bahwa penggunaan teknologi *mechine learning* dapat meminimalkan resiko serangn dengan melakulakukan deteksi instruksi pada serangan DDoS. *Machine Learning* memiliki dampak

signifikan dalam keamanan siber. *Machine learning* belajar pada dataset untuk membuat prediksi berdasarkan pengetahuan yang mereka peroleh saat belajar. Dalam penelitian lainya yang dilakukan [21]dengan peningkatan penggunaan teknologi sehingga menghadirkan tantangan dalam sistem deteksi instruksi. Penggunaan *Mechine learning* merupakan salah satu cara yang efektif dalam penanganan masalah tersebut. Dengan efektifitas penanganan untuk kasus internet dengan delapan algoritma pembelajaran mesin dengan skor f1 rata-rata 0,95, area rata-rata di bawah kurva ROC 0.98, dan overhead rata-rata 1.4% CPU dan 3.6% RAM pada ruang pengguna di komputer papan tunggal.

Pembelajaran mesin bergantung pada data berkualitas tinggi untuk secara tepat mendeteksi anomali. Proses klasifikasi atau clustering sangat memerlukan fitur. Fitur itu harus mampu membedakan satu contoh dengan contoh lainnya. Sering kali untuk membedakan satu *instance* dari yang lainnya memerlukan fitur vektor dengan dimensi yang besar. Sayangnya, data dengan dimensi yang sangat besar menghadirkan beberapa masalah dalam *machine learning*, di mana *machine learning* sulit untuk mencapai kinerja optimal pada data berdimensi tinggi. Semakin banyak fitur yang digunakan, semakin rumit sebuah model *machine learning* harus memecahkan permasalahannya. Hal ini mengakibatkan terjadinya overfitting dikarenakan banyaknya konfigurasi fitur. Dengan ukuran yang besar sulit untuk menjalankan komputasi (biaya komputasi tinggi), baik dari sisi waktu maupun memori [22]. Untuk itu dilakukan proses pemilihan fitur (*feature selection*) di mana dalam proses ini dipilih subset dari fitur-fitur yang relevan atau representatif dari keseluruhan dataset agar digunakan dalam model [23]. Penggunaan metode pemilihan fitur dalam proses seleksi fitur bertujuan untuk mereduksi dimensi fitur dataset[24]. Pengurangan dimensi fitur pada dasarnya meningkatkan efisiensi komputasi, menyusutkan kompleksitas, serta menekan biaya sistem pelatihan model *machine learning* yang lebih efektif dan tepat. Metode seleksi fitur juga berperan penting dalam menurunkan dimensi dataset[25].

Kumpulan data dikumpulkan dari *Canadian Institute for Cyber security*, pada dataset tersebut menyajikan pendekatan untuk menghasilkan kumpulan data DDoS baru yang disebut CICDDoS2019. Kumpulan data CICDDoS2019 berisi serangan DDoS waktu nyata dari lalu lintas jaringan. Kumpulan data berisi berbagai macam

serangan DDoS. Ada 12 jenis serangan yang tersedia dalam kumpulan data, termasuk 'DNS', 'SNMP', 'NTP', 'WebDDoS', 'MSSQL', 'UDP', 'LDAP', 'NetBIOS', 'SSDP', 'PortScan', 'UDP-Lag', dan 'SYN'. Dengan 88 atribut/fitur yang di dapat dari penelitian tersebut. Mengingat kumpulan data yang luas yang lazim dalam keamanan siber, secara akurat mengkarakterisasi pola lalu lintas jaringan yang rumit yang penuh dengan fitur dan nilai yang kompleks menghadirkan tantangan yang sulit[17]. Untuk mengatasi masalah tersebut makan dilakukan *feature Selection* guna mengambil data-data dan fitur terpenting dan berpengaruh dalam model clasifikasi.

Banyak peneliti menggunakan dataset ini dalam penelitian mereka untuk menemukan fitur terbaik dan model terbaik untuk mendeteksi serangan DDoS dengan waktu dan biaya eksekusi minimum. Pengguna harus selalu memperoleh pengetahuan dari data yang ada dan data yang tidak perlu harus dihilangkan menggunakan prosedur rekayasa atribut[26]. salah satu teknik yang dapat di gunakan dalam mengektraksi dan mereduksi atribut atau fitur berbasis neural network. Pada penelitian kali ini menggunakan *Learning Vector Quantization* (LVQ), dan *Autoencoder* sebagai perangkat extraction fitur guna mengoptimalkan kinerja algoritma klasifikasi. *Learning Vector Quantization* (LVQ) sendiri merupakan salah satu metode dalam JST untuk melakukan pembelajaran pada lapisan kompetitif yang terawasi. LVQ merupakan jenis jaringan saraf tiruan (neural network) yang bekerja dengan cara mempelajari representasi dari data input dan mengelompokkannya ke dalam kelas-kelas tertentu. Algoritma ini sering digunakan untuk tugas-tugas seperti pengenalan pola, kompresi data, dan ekstraksi fitur. LVQ adalah algoritma *supervised learning*, artinya ia memerlukan data yang sudah dilabeli untuk proses pelatihan. Tujuan utama LVQ adalah untuk menemukan vektor-vektor *representatif* (*codebook vectors* atau *prototypes)* yang mewakili setiap kelas dalam data. Vektor-vektor ini kemudian digunakan untuk mengklasifikasikan data baru. Sedangkan *Autoencoder* itu sendiri adalah jenis arsitektur jaringan saraf yang dirancang untuk secara efisien mengompresi (*encode*) data input hingga ke fitur-fitur esensialnya, kemudian merekonstruksi (*decode*) input asli dari representasi yang dikompresi ini[27]. *Autoencoder* merujuk pada subset spesifik arsitektur *encoder-decoder* yang dilatih melalui pembelajaran yang

tidak diawasi untuk merekonstruksi data input sendiri. penyandi otomatis dilatih untuk menemukan pola tersembunyi dalam data yang tidak berlabel, daripada memprediksi pola yang diketahui yang ditunjukkan dalam data pelatihan berlabel. menurut LVQ dan *Autoencoder* sangant efektif dalam mengurangi dimensi data tanpa kehilangan informasi penting, sehingga dapat meningkatkan efisiensi proses analisis. Dalam konteks deteksi DDoS, LVQ dan *Autoencoder* membantu mengidentifikasi fitur-fitur utama yang paling relevan untuk membedakan lalu lintas normal dan anomali.

Fitur yang sudah diseleksi akan dilakukan klasifikasi melalui machine learning dengan memanfaatkan algoritma *Recurrent Neural Network* (RNN). Berdasarkan dataset yang berupa data tipe time series, Serangan DDoS sering menunjukkan pola temporal, seperti lonjakan *volume traffic* yang mendadak atau pola paket yang aneh dalam jangka waktu tertentu. RNN memperhitungkan hasil sebelumnya bersama dengan peristiwa sekarang di setiap langkah input[27]. Melatih model menggunakan metode tersebut dapat menyimpan seluruh informasi data dengan kehilangan yang sangat sedikit. Kami memakai RNN konvensional karena kami tidak mengedepankan pembelajaran ketergantungan temporal yang berlangsung lama. RNN standar yang sederhana memerlukan waktu pelatihan lebih sedikit saat dibandingkan dengan metode RNN lainnya. Beberapa studi menunjukkan bahwa penerapan algoritma itu memiliki tingkat akurasi yang tinggi. Penelitian yang dilakukan [25] melakukan penelitian serangan DDOS terhadap *cloud computing*. Dalam penelitian ini peneliti mengusulkan sistem deteksi menggunakan sistem *fiture selection* dan kalasifikasi jenis serangan. Serangan diklasifikasikan menggunakan teknik pembelajaran mesin NB, SVM dan DT dengan metode pemilihan fitur seperti LVQ dan PCA. Kinerja algoritma ini dianalisis untuk mengklasifikasikan serangan DDoS. 20 fitur dari 42 fitur dipilih oleh LVQ dan 21 fitur dipilih oleh PCA. Hasil menunjukkan bahwa pemilihan fitur berbasis LVQ dalam model DT mengidentifikasi serangan lebih akurat daripada metode lain yang dipertimbangkan dengan presentasi akurasi mencapai 98,74%. Penelitian yang di lakukan [28] mendapati penggunaan seleksi fitur sangat membantu dalam meningkatkat akurasi pada penggunaan algoritma clasifikasi yang di usulkan. Teknik ini dapat meningkatkan kinerja secara drastis. Skor F1

untuk SNMP meningkat dari 75,0% menjadi 88,2% dengan menerapkan *Auto Encoder*. Untuk UDP, perbedaannya lebih menonjol. Sebelum menggunakan *Auto Encoder*, skor F1 adalah 0,3%, yang berarti model salah mengklasifikasikan hampir semua serangan menjadi jinak. Setelah menerapkan *Auto Encoder*, skor F1 ditingkatkan menjadi 98,6%. pendekatan ketiga, yang mengintegrasikan profil panda, skor F1 meningkat secara signifikan menjadi 93,3%. Penelitian lainya menyebutkan bahwa dalam pekerjaan yang diusulkan[29], model RNN, LSTM, dan GRU dievaluasi menggunakan 20 fitur teratas dari kumpulan data CICDDOS2019. Model RNN mencapai akurasi 99,99% untuk klasifikasi biner dan 99,54% untuk klasifikasi multi-kelas, menunjukkan bahwa model RNN mengidentifikasi dan mengklasifikasikan dengan benar 99% dari semua contoh positif yang sebenarnya. Temuan pada penelitain ini menunjukkan bahwa model RNN lebih tangguh dan berhasil dalam klasifikasi biner daripada model LSTM dan GRU, karena mencapai akurasi yang lebih tinggi, tingkat positif palsu dan negatif palsu yang lebih rendah, dan memiliki risiko *overfitting* yang lebih rendah. Hasil eksperimen menunjukkan bahwa model berkinerja sama baiknya pada kumpulan data CICDDoS2019 dengan skor akurasi 0,99, tetapi ada perbedaan dalam waktu eksekusi, dengan GRU menunjukkan waktu eksekusi yang lebih sedikit daripada RNN dan LSTM.

Berdasarkan hal tersebut penelitian ini bertujuan untuk mengembangkan metode deteksi serangan DDoS yang cepat dan akurat menggunakan algoritma Recurent neural network (RNN) yang mampu mendeteksi serangan dengan cepat dan akurat dibandingkan metode deteksi konvensional dengan memanfaatkan memanfaatkan *feature Selection* dengan mengunakan CIC-DDoS2019 sebagai dataset. Penelitian ini mengekplorasi pengaruh *embedded model* yeng berupa seleksi fitur dan pengklasifikasian untuk meningkatkan akurasi deteksi, mengurangi *overfiting* dan *nois* serta mempercepat dalam proses deteksi. Dengan demikian, penelitian ini diharapkan dapat memberikan meminimalkan alaram palsu dan memberikan akurasi deteksi yang tinggi terhadap serangan DDoS Attack.

1.2 Rumusan masalah

Berdasarkan uraian latar belakang di atas dapat di ambil rumusan masalah sebagai berikut:

1. Bagaimana pengaruh penerapan teknik seleksi fitur *dengan Learning Vector Quantization* (LVQ) dan *Autoencoder* dalam meningkatkan efisiensi dan akurasi deteksi serangan DDoS?
2. Bagaimana performa model Recurrent Neural Network (RNN) dalam mendeteksi serangan DDoS setelah dilakukan optimasi fitur menggunakan LVQ dan *Autoencoder*?

1.3 Batasan penelitian

Adapun batasan masalah yang dapat di ambil dalam penelitian ini adalah sebagai berikut:

1. Penelitian ini akan menggunakan dataset CIC-DDoS2019 sebagai sumber data utama untuk melatih dan menguji model deteksi serangan DDoS.
2. Fokus utama penelitian ini adalah pada penerapan algoritma *Recurrent Neural Network* (RNN) sebagai metode klasifikasi untuk mengidentifikasi dan membedakan serangan DDoS dari lalu lintas jaringan normal.
3. Penelitian ini akan mengeksplorasi efektivitas metode *Learning Vector Quantization* (LVQ) dan *Autoencoder* dalam melakukan feature selection pada dataset CIC-DDoS2019, dengan tujuan untuk memilih fitur-fitur yang paling relevan untuk meningkatkan kinerja model.
4. Penelitian ini hanya berfokus pada deteksi serangan DDoS, bukan pada mitigasi atau respons terhadap serangan.
5. Tidak mencakup aspek implementasi keamanan jaringan secara luas seperti *firewall*, IPS (*Intrusion Prevention System*), atau teknik mitigasi berbasis cloud.

1.4 Tujuan penelitian

Berdasarkan uraian di atas tujuan dari penelitian ini adalah sebagai berikut.

1. Mengembangkan model RNN dengan kombinasi ekstrasi fitur menggunakan LVQ dan *Autoencoder*.
2. Melihat faktor apa saja yang mempengaruhi proses deteksi serangan DDOS.
3. Mengevaluasi dan mengukur peforma model RNN dengan *fitur selection*

(LVQ dan Autoencoder)

4. Menganalisa hasil klasifikasi dari serangan-serangan DDOS

1.5 Manfaat penelitian

Berdasarkan dari apa yang telah diurain latar belakang, manfaat dari penelitian ini sebagai berikut.

1. Penelitian ini diharapkan dapat meningkatkan akurasi dan efisiensi deteksi serangan DDoS dengan menerapkan teknik *fitur selection Learning Vector Quantization* (LVQ) dan Autoencoder.
2. Metode yang dikembangkan dapat mengurangi *false alarm* pada deteksi serangan DDoS, sehingga meningkatkan keandalan sistem keamanan jaringan.
3. Penerapan teknik fitur seleksi dalam penelitian ini dapat mengoptimalkan pemrosesan data dan mengurangi kompleksitas komputasi, sehingga mempercepat proses deteksi serangan.
4. Dengan adanya teknologi deteksi yang lebih efisien, di harapkan tingkat ancaman serangan DDoS dapat dikurangi dan bahkan dihilangkan melalui deteksi dini dan penanganan lebih cepat.

1.6 Sistematika penulisan

Sistematika penulisan tesis ini di bagi menjadi beberapa bab dan sub bab. Berikut penjelasan dari masing-masing bab.

BAB I Pendahuluan

Bab ini mencakup aspek-aspek seperti latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan struktur laporan.

BAB II Tinjauan Pustaka

Bab ini menyajikan teori, konsep, prinsip, pengetahuan teoritis terkini tentang masalah yang diteliti, dan temuan-temuan yang relevan dari penelitian sebelumnya. Secara garis besar, bab ini mencakup keamanan jaringan, serangan DDoS, dan Python.

BAB III Metodologi Penelitian

Bagian ini menjelaskan metode pendekatan pemecahan masalah, termasuk metode klasifikasi dan metode deteksi serangan.

BAB IV Hasil Penelitian dan Pembahasan

Bab ini akan membahas temuan penelitian, seperti analisis dan interpretasi data yang diuji. Bab ini akan menjelaskan secara rinci proses klasifikasi data serangan DDoS dan kemampuannya untuk memprediksi serangan tersebut dengan menggunakan metode tertentu, dengan melihat perbandingan penggunaan seleksi fitur yang paling berpengaruh. Pengujian akan melibatkan klasifikasi paket yang masuk dalam jumlah tertentu, memperoleh data akurasi dan presisi algoritma untuk klasifikasi paket.

BAB V Simpulan dan Saran

Bagian ini memberikan gambaran umum dari pembahasan, termasuk perumusan masalah, tujuan penelitian, respon terhadap klasifikasi berdasarkan ekstraksi fitur serangan DDoS. Bab ini juga menyajikan kesimpulan dari eksperimen yang dilakukan dan tantangan yang dihadapi selama pengerjaan tugas akhir. Selanjutnya, rekomendasi untuk penelitian selanjutnya yang muncul dari pembahasan penelitian atas keterbatasan penelitian yang dilakukan akan diberikan.

Daftar Pustaka

Bagian ini memuat sumber-sumber yang digunakan atau dikutip dalam penelitian, seperti buku, artikel jurnal baik dalam bentuk fisik maupun elektronik/online.

Lampiran

Bagian ini berisi dokumen pendukung penelitian berupa tabel, gambar, grafik, diagram alir, dan materi lain yang relevan.