Deteksi *Serangan DDoS pada Portmap* Menggunakan Metode *Bidirectional Recurrent Neural Networks*

OLEH :

WISNU ADI PUTRA

09012682125021

PROGRAM STUDI MAGISTER ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2025

Deteksi *Serangan DDoS pada Portmap* Menggunakan Metode *Bidirectional Recurrent Neural Networks*

TESIS

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Magister

OLEH :

WISNU ADI PUTRA

09012682125021

PROGRAM STUDI MAGISTER ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2025

LEMBAR PENGESAHAN

Deteksi Serangan DDoS Pada Portmap Menggunakan Metode Bidirectional Recurrent Neural Network

TESIS

Di ajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Magister

Oleh:

WISNU ADI PUTRA
09012682125021

Palembang, Juli 2025
Menyetujui

Pembimbing I	**Pembimbing II**
Prof. Deris Stiawan, S.Kom., M.T., Ph.D.	**M. Qurhanul Rizqie, S.Kom., M.T., Ph.D.**
NIP. 197806172006041002	**NIP. 198712032022031006**

Koordinator Program Studi
Magister Ilmu Komputer

Dr.Firdaus, M.Kom
NIP. 197801212008121003

HALAMAN PERSETUJUAN

Pada hari jumat tanggal 13 Juni 2025 telah dilaksanakan ujian sidang Komprehensif Tesis oleh Magister Ilmu Komputer Fakultas Ilmu Komputer Universitas Sriwijaya

Nama : **Wisnu Adi Putra**
Nim : **09012682125021**
Judul : **Deteksi Serangan DDoS Pada Portmap Menggunakan Metode *Bidirectional Recurrent Neural Networks***

1.Ketua Sidang

Samsuryadi, M.Kom., Ph.D
NIP. 197102041997021003 .....

2.Penguji II

Hadipurnawan Satria, Ph.D.
NIP. 198004182020121001 .....

3.Penguji III

Dr. Ir. Sukemi, M.T.
NIP. 196612032006041001 .....

4.Pembimbing I

Prof. Deris Stiawan, S.Kom., M.T., Ph.D.
NIP. 197806172006041002 .....

5.Pembimbing II

M.Qurhanul Rizqie, S.Kom., M.T., Ph.D.
NIP. 198712032022031006 .....

Mengetahui,
Koordinator Program Studi Magister Ilmu Komputer

Dr. Firdaus, S.T., M.Kom.
NIP. 197801212008121003

LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama	: Wisnu Adi Putra
NIM	: 09012682125021
Program Studi	: Magister Ilmu Komputer
Judul Tesis	: Deteksi Serangan DdoS pada Port PortMap Menggunakan Metode Bidirectional Recurrent Neural Network

Hasil Pengecekan Software iThenticate/Turnitin : 15 %

Menyatakan bahwa laporan tesis saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan tesis ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Palembang, 21 April 2025

Wisnu Adi Putra

NIM. 09012682125021

KATA PENGANTAR

Segala puji dan syukur saya panjatkan kepada **Allah SWT** yang telah memberikan rahmat dan karunianya yang tidak terhingga, sehingga tesis penelitian ini dapat terselesaikan. Judul yang dipilih dalam penelitian ini adalah "***Deteksi Serangan DDoS pada Portmap Menggunakan Metode Bidirectional Recurrent Neural Networks***" Adapun tujuan penulisan dari tesis ini adalah untuk memenuhi syarat memperoleh gelar **Magister Komputer** pada program studi Pasca Sarjana (S2) **Magister Ilmu Komputer Universitas Sriwijaya** , Tahun Akademik 2024/2025. Selain itu, tesis penelitian ini bertujuan untuk memperdalam disiplin keilmuan yang menunjang penempuhan dalam masa studi.

Saya ucapkan terima kasih kepada seluruh Dosen yang telah membantu dan senantiasa memberi semangat yang luar biasa, sehingga tetap semangat menjalankan studi ini dengan baik. Nantinya dalam tesis ini tentunya masih jauh dari kata sempurna, maka dari itu diharapkan kritik dan saran demi perbaikan penulisan ini oleh tim penguji nantinya. Semoga dapat memberikan manfaat, sekian dan Terima Kasih

Palembang, 7 Mei 2025

Wisnu Adi Putra

UCAPAN TERIMA KASIH

Puji syukur kami ucapkan ke hadirat Allah SWT, atas rahmat dan hidayah-Nya telah selesai tesis dengan judul " ***Deteksi Serangan DDoS pada Portmap Menggunakan Metode Bidirectional Recurrent Neural Networks*** ". Rasa syukur tidak terhingga atas kebahagiaan yang tidak ternilai dengan mempersembahkan sebuah karya yang terbaik kepada banyak pihak yang telah mendukung serta memberikan dukungan baik berupa doa, moril dan materil. Ucapan terimakasih kepada:

1. Kedua Orang Tua tercinta Bapak ***Sudarno*** dan Ibu Almh. ***Huda Sarawi***, istri terkasih ***Sefy Emilia, serta anak-anak Gafi Zavier Akhtar*** dan ***Zehan Atharazka*** yang sudah memberikan semangat dan turut mendoakan.
2. Bapak Prof. Dr Taufiq Marwa, S.E., M.Si Selaku Rektor Universitas Sriwijaya
3. Bapak Prof. DR. Erwin, S.Si., M.Si. selaku Dekan Fakultas Ilmu Komputer beserta seluruh staff dan jajarannya.
4. Bapak Dr. Firdaus, S.T., M.Kom Ketua Program Studi Magister Ilmu Komputer Fakultas Ilmu Komputer Universitas Sriwijaya
5. Bapak Prof. Deris Stiawan, S.Kom., M.T., Ph.D. Dosen Pembimbing I
6. Bapak Muhammad Qurhanul Rizqie, S.Kom., M.T., Ph.D.Dosen Pembimbing II
7. Kepada semua dosen khususnya Program Studi Magister Ilmu Komputer Fakultas Ilmu Komputer Universitas Sriwijaya
8. Teman -teman Magister Ilmu Komputer angkatan 2021
9. Semua Pihak yang telah membantu dalam penyelesaian tesis ini

Akhir kata, semoga tesis ini berguna, bermanfaat dan mampu memperkaya khazanah keilmuan khususnya dalam Ilmu Komputer dan Serangan Siber akhir kata saya ucapkan terimakasih.

Deteksi Serangan DDoS pada Portmap Menggunakan Metode Bidirectional *Recurrent Neural Networks*

Wisnu Adi Putra

ABSTRAK

Portmap atau RPC bind adalah protokol yang digunakan dalam sistem operasi Unix dan Linux untuk memetakan nomor port dengan nomor program yang terkait. Pada serangan DDoS terhadap *Portmap*, para penyerang akan memanfaatkan kelemahan dalam protokol ini untuk mengirimkan permintaan yang salah atau manipulatif dalam jumlah besar ke server yang menjalankan Portmap. Karena sifat UDP yang tidak memiliki koneksi dan tidak terotentikasi, server *Portmap* akan mencoba membalas setiap permintaan yang diterimanya. Namun, para penyerang sering kali menyamarinya sehingga alamat IP mereka disembunyikan atau palsu. Akibatnya, server akan mencoba membalas permintaan ke alamat IP palsu atau tidak valid, menghabiskan sumber daya server dan mengakibatkan penolakan layanan untuk klien yang sah. Dampak dari serangan DDoS pada *Portmap* bisa sangat merusak. Layanan yang terkait dengan *Portmap* mungkin menjadi tidak responsif, menyebabkan *downtime* yang signifikan bagi aplikasi atau layanan yang mengandalkan protokol tersebut. Pada penelitian ini digunakan dataset CSE-CIC-IDS 2019 khususnya dataset serangan DDoS pada portmap, Penggunaan Metode *Corelationbased Feature Selection* (CSF) untuk mendapatkan fitur penting pada dataset saat dilakukan deteksi serangan DDoS Menggunakan *Machine Learning Bidirectional* RNN, Metode *Bidirectional* RNN dapat dengan baik mendeteksi serangan DDoS pada *portmap*, dengan menerapkan data latih 70% dan data uji 30% menghasilkan performa nilai akurasi 99.9917%, nilai recall 99.9917%%, nilai spesifitas 99.9942%, nilai presisi 99.994%, nilai F1-Score 99.88%%, dan performa dari nilai BACC 99.92%, serta nilai dari MCC 99.98 %. Kontribusi utama penelitian ini adalah pengembangan pendekatan deteksi serangan DDoS pada Portmap yang lebih akurat dan efisien dengan menggabungkan metode seleksi fitur CFS dan arsitektur Bidirectional RNN. Dengan metode ini, proses deteksi dapat dilakukan dengan lebih cepat dan tepat, mengurangi beban komputasi tanpa mengorbankan performa deteksi.

Kata kunci : *Bidirectional RNN ,DdoS,Correlation-basedfeature selection,Portmap*

DDoS Attack Detection on Portmap Using Bidirectional Recurrent Neural Networks Method

Wisnu Adi Putra

ABSTRACT

Portmap, or RPC bind is a protocol used in Unix and Linux operating systems to map port numbers with their corresponding program numbers. In a DDoS attack against Portmap, attackers would exploit weaknesses in this protocol to send a large number of false or manipulative requests to the server running Portmap. Due to the connectionless and unauthenticated nature of UDP, the Portmap server will attempt to reply to every request it receives. However, attackers often disguise them so that their IP addresses are hidden or fake. As a result, the server will attempt to reply to requests to fake or invalid IP addresses, consuming server resources and resulting in denial of service for legitimate clients. The impact of a DDoS attack on Portmap can be devastating. Services associated with Portmap may become unresponsive, causing significant downtime for applications or services that rely on the protocol. In this research, the CSE-CIC-IDS 2019 dataset is used, especially the DDoS attack dataset on portmaps, using the Correlation-based Feature Selection (CSF) method. The Bidirectional RNN method can well detect DDoS attacks on portmaps by applying 70% training data and 30% test data, resulting in a performance accuracy value of 99.9917%, a recall value of 99.9917%, a specificity value of 99.9942%, a precision value of 99.994%, an F1-score value of 99.88%, a performance of BACC value of 99.92%, and a value of MCC of 99.98%. The main contribution of this research is the development of a more accurate and efficient DDoS attack detection approach on Portmap by combining the CFS feature selection method and bidirectional RNN architecture. With this method, the detection process can be performed more quickly and precisely, reducing the computational burden without sacrificing detection performance.

Keywords: ***Bidirectional RNN, DdoS, Correlation-based feature selection, Portmap***

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I PENDAHULUAN

1.1. Latar Belakang

Berdasarkan data dari Kaspersky menunjukkan peningkatan yang konsisten dalam serangan DDoS pada kuartal ketiga tahun 2022, terutama yang dilakukan oleh profesional. Jumlah serangan cerdas meningkat dua kali lipat dari kuartal sebelumnya. Selain itu, proporsi serangan DDoS yang lebih canggih meningkat.

Serangan Denial of Service terbaru adalah Distributed Denial of Service (DDoS). (Islam and Sabrina, 2009), yang akan menyebabkan lalu lintas tidak normal, baik dari jaringan maupun server. Serangan *DDoS* dan serangan pada layer adalah dua jenis yang berbeda. Serangan DDoS pertama mengganggu konektivitas pengguna yang sah dan mengurangi kemampuan jaringan untuk menggunakan sumber dayanya. Serangan pada lapisan jaringan juga dikenal sebagai (*network layer attack*). Sementara serangan yang merusak sumber daya server (seperti *CPU*, *memori*, dan *soket*) disebut dengan serangan lapisan aplikasi atau serangan (*layer application).*(Toapanta et al., 2019). Pada serangan ini, pelaku mencoba membuat layanan atau sumber daya tidak tersedia bagi pengguna yang sah (Joshi et al., 2018). Karena arsitektur perutean internet dan pengalamatan yang sederhana, serangan *DDoS* berbasis IPv4 masih sangat umum. Penyerang dapat menggunakan celah yang ada untuk meningkatkan beban pada penyedia layanan internet Service Provider (*ISP*) dan operator pusat data (Salopek et al., 2022). Serangan DDoS dapat membuat layanan web server menjadi tidak dapat diakses, namun serangan ini sulit terdeteksi di dalam jaringan karena pola lalu lintas yang dihasilkannya menyerupai aktivitas dari pengguna yang sah.(Hong et al., 2018).

Serangan *DDoS volumetrik* sering kali menggunakan paket dengan alamat sumber yang dimanipulasi (spoofed), yang dikirimkan melalui jaringan host atau penyedia layanan besar dengan kerentanan keamanan. Tantangan utama dalam mendeteksi serangan semacam ini adalah kesulitan mengidentifikasi perbedaan antara lalu lintas jahat dan yang *legitimate*, sebab pelaku sengaja mencampurkan pola serangan dengan aktivitas normal untuk mengelabui sistem. Akibatnya, ancaman DDoS menjadi semakin sulit diatasi dan berpotensi merugikan baik -

pengguna maupun penyedia layanan. (Chonka et al., 2009). Pada kuartal kedua tahun 2022, terjadi peningkatan serangan DDoS pada lapisan jaringan sebesar 109% dibandingkan tahun sebelumnya (*Year on Year/YoY*). Serangan dengan kapasitas 100 Gbps atau lebih mengalami kenaikan sebesar 19% dibandingkan kuartal sebelumnya (*Quarter on Quarter/QoQ*), sementara serangan yang berlangsung lebih dari 3 jam meningkat sebesar 12%. Sektor yang paling banyak mengalami serangan termasuk Telekomunikasi, Permainan/Perjudian, serta Teknologi Informasi dan Layanan. Di antara negara-negara, organisasi di Amerika Serikat menjadi target utama, diikuti oleh Singapura, Jerman, dan China. (https://radar.cloudflare.com/reports/ddos-2022-q2). *Distributed Denial of Service* (DDoS) telah menjadi salah satu metode serangan dalam beberapa dekade terakhir yang mengakibatkan pengguna yang sah tidak bisa mengakses layanan, sementara penyerang berupaya untuk menonaktifkan target atau layanan tersebut. Untuk menjaga keamanan sistem dan jaringan komputer dari berbagai tipe serangan siber, diperlukan penggunaan sistem deteksi intrusi (Intrusion Detection System/IDS). IDS adalah perangkat keras atau perangkat lunak yang dirancang untuk mendeteksi aktivitas kriminal siber di dalam sistem komputer, sehingga keamanan sistem tetap dapat terjaga dari serangan. Tujuan utama IDS adalah untuk mengenali beragam jenis lalu lintas jaringan yang berpotensi berbahaya serta perilaku komputer yang tidak terdeteksi oleh firewall konvensional. (Khraisat et al., 2019) Walaupun *Intrusion Detection System (IDS*) memainkan peran krusial dalam mendeteksi kemungkinan serangan, tingginya volume lalu lintas dapat menimbulkan tantangan teknis dalam hal pemantauan dan identifikasi aktivitas jaringan.(Varghese and Muniyal, 2021).

Ada dua pendekatan utama dalam Intrusion Detection System (IDS). Pendekatan pertama adalah IDS berbasis anomali, yang membandingkan perilaku normal aplikasi yang teramati dengan perilaku yang menyimpang secara signifikan. Pendekatan kedua adalah IDS berbasis signature, yang memantau paket-paket di jaringan dan membandingkannya dengan database yang berisi semua paket malware yang dikenal (Mora-Gimeno et al., 2021). Ada beberapa kelemahan yang

dimiliki oleh IDS. Pertama, sistem ini sering kali tidak mampu menganalisis lalu lintas dengan kecepatan dan volume tinggi, yang dapat menyebabkan deteksi dilakukan secara non-realtime. Selain itu, IDS juga tidak mendukung IP versi 6.0 dan sulit untuk menganalisis lalu lintas yang terenkripsi.(Varghese and Muniyal, 2021). berdasarkan penelitian terkait terdapat tiga teknik yang digunakan berdasarkan pengumpulan informasi dan penyediaan data input. Yang pertama adalah Host-based Intrusion Detection System (HIDS), yang kedua adalah Network-based Intrusion Detection System (NIDS), dan yang ketiga adalah Distributed Intrusion Detection System (DIDS).

Bidirectional Recurrent Neural Networks (BRNN) memanfaatkan konteks dari kedua arah sebelum dan sesudah , sehingga dapat memproses informasi secara lebih menyeluruh untuk menghasilkan output yang lebih akurat. Secara arsitektur, *BRNN* terdiri dari dua jaringan *RNN* yang berjalan dalam arah yang berlawanan, di mana keduanya terhubung ke satu lapisan output yang sama untuk menggabungkan informasi dari kedua arah tersebut.(Wei et al., 2022). Bidirectional Recurrent Neural Networks terdiri dari komponen LSTM dan GRU. Unit-unit di lapisan pertama dua arah terdiri dari LSTM yang merambat maju (propagation forward) dan GRU yang merambat mundur (propagation back), sehingga komposisi di lapisan kedua berlawanan (Xianlun Tang, 2019). Dalam proses pelatihan Bidirectional Recurrent Neural Networks (BRNN), setiap arah dipelajari secara terpisah. Setelah itu, jalur maju dan jalur mundur digabungkan untuk mengintegrasikan informasi dari kedua urutan fitur tersebut secara lebih efektif. (Xu et al., 2021).

Pada penelitian sebelumnya (Yi-Wen Chen, 2020), Implementasi dari sistem deteksi serangan DDOS IoT menggunakan Machine learning dengan metode *Decesion Tree*. Dalam penelitian tersebut terdapat empat jenis serangan DDoS, yaitu sensor data Flood, ICMP Flood, SYN Flood, dan UDP Flood. Berdasarkan hasil dari percobaan penelitian tersebut didapatkan nilai dari Akurasi sebesar 97.39%, Presisi sebesar 97.38%, Recall sebesar 97.39%, dan F1-Score sebesar 97.33% dari segi kemampuan dalam melakukan deteksi serangan DDoS.

Penelitian sebelumnya yang dilakukan pada tahun 2017(Xiaoyong Yuan et al., 2017), Dalam penelitian ini, identifikasi serangan DDoS dilakukan menggunakan berbagai metode deep learning. Beberapa metode yang diuji mencakup Random Forest, yang memberikan akurasi 96.627%, presisi 95.532%, recall 94.893%, dan F1-Score 93.698%. Metode berikutnya adalah CNN-LSTM, yang mencatat akurasi 95.896%, presisi 97.534%, recall 94.208%, dan F1-Score 95.831%. Sementara itu, LSTM menunjukkan hasil terbaik dengan akurasi 97.606%, presisi 97.832%, recall 97.387%, dan F1-Score 97.601%. Berdasarkan hasil tersebut, penelitian ini memilih metode Bidirectional Recurrent Neural Networks (BRNN) untuk melakukan pengujian terhadap file fitur serangan yang berasal dari dataset DDoS, khususnya pada protokol portmap yang dirilis oleh CIC-IDS-2019.

1.2. Rumusan Masalah

Berikut adalah rumusan masalah yang akan dibahas dalam implementasi tesis ini:

1. Bagaimana penerapan seleksi fitur untuk mendapatkan fitur penting dalam deteksi serangan DDoS pada Portmap? Rumusan ini akan membahas metode dan teknik yang digunakan untuk memilih fitur-fitur yang relevan dan signifikan dalam mendeteksi serangan DDoS khususnya pada protokol Portmap.

2. Bagaimana cara mendeteksi serangan DDoS pada Portmap dengan penerapan metode Bidirectional RNN? Di sini akan dijelaskan pendekatan yang diterapkan dalam deteksi serangan DDoS menggunakan model Bidirectional Recurrent Neural Networks, termasuk langkah-langkah dan strategi yang digunakan dalam proses deteksi

3. Bagaimana kinerja hasil deteksi dengan metode Bidirectional RNN dalam hal nilai akurasi, presisi, sensitivitas, spesifisitas, F1-Score, BAAC, dan MMC? Rumusan ini akan mengevaluasi dan menganalisis

kinerja model Bidirectional RNN berdasarkan berbagai metrik evaluasi untuk mengukur efektivitas deteksi serangan DDoS.

1.3. Batasan Masalah

Dari rumusan masalah di atas, berikut adalah batasan masalah yang ditetapkan dalam penelitian ini:

1. Konsentrasi pada Protokol Portmap: Penelitian ini akan difokuskan pada identifikasi serangan DDoS yang terjadi pada protokol Portmap, sehingga analisis dan pengujian akan terbatas pada jenis serangan yang terkait dengan protokol ini.

2. Penggunaan Metode Bidirectional RNN: Penelitian ini akan melaksanakan analisis dengan menggunakan metode *Bidirectional Recurrent Neural Networks (BRNN)* dan tidak akan menyertakan metode lain dalam proses deteksi serangan DDoS.

3. Teknik Seleksi Fitur Tertentu: Penelitian ini akan menerapkan metode seleksi fitur khusus untuk menentukan fitur-fitur penting dalam dataset. Hanya fitur-fitur yang relevan yang akan diambil untuk analisis selanjutnya.

4. Dataset dari CIC-IDS-2019: Penelitian ini akan mengandalkan dataset serangan DDoS yang dipublikasikan oleh *CIC-IDS-2019* sebagai sumber data utama untuk pengujian dan analisis.

5. Evaluasi dengan Metrik Tertentu: Kinerja model akan dinilai berdasarkan metrik tertentu seperti akurasi, presisi, sensitivitas, spesifisitas, F1-Score, BAAC, dan MMC. Penelitian ini tidak akan membahas metrik evaluasi lainnya.

1.4. Tujuan Penelitian

Tujuan dari penelitian tesis ini adalah sebagai berikut:

1. Menentukan Fitur Penting: Penelitian ini bertujuan untuk mengidentifikasi dan mengekstrak fitur-fitur penting yang berkontribusi dalam deteksi serangan DDoS pada protokol Portmap, sehingga dapat mencapai hasil yang lebih akurat dalam analisis.
2. Menerapkan Metode BRNN: Penelitian ini bertujuan untuk menerapkan metode *Bidirectional Recurrent Neural Networks (BRNN)* dalam upaya mendeteksi serangan *DDoS* pada Portmap dan mengevaluasi efektivitasnya dalam mengidentifikasi serangan.
3. Mengevaluasi Kinerja Deteksi: Penelitian ini bertujuan untuk mengukur kinerja model deteksi yang menggunakan BRNN dengan menganalisis metrik-metrik seperti akurasi, presisi, sensitivitas, spesifisitas, F1-Score, BAAC, dan MMC, untuk menentukan seberapa baik model tersebut dalam mengidentifikasi serangan DDoS.

1.5. Manfaat Penelitian

Mamfaat dari penelitian tesis ini adalah sebagai berikut:

1. Peningkatan Keamanan Jaringan: Hasil penelitian ini dapat membantu dalam mengembangkan metode yang lebih efektif untuk mendeteksi dan mengatasi serangan DDoS pada protokol Portmap, yang berkontribusi terhadap peningkatan keamanan sistem jaringan.
2. Pengembangan Metode Deteksi yang Efisien: Dengan menerapkan metode Bidirectional RNN, penelitian ini bertujuan untuk menciptakan model deteksi yang lebih akurat dan efisien, sehingga dapat mengurangi jumlah false positives dan false negatives dalam identifikasi serangan.
3. Peningkatan Pemahaman tentang Serangan DDoS: Penelitian ini juga dapat memperdalam pemahaman akademis dan praktis mengenai karakteristik serangan DDoS, serta strategi yang efektif untuk mendeteksinya.

1.6. Metode Penelitian

Beberapa tahapan metode yang akan dilakukan pada penelitian ini adalah sebagai berikut:

1. Metode Literatur dan Metode Studi Pustaka

Pada tahap ini, penulis akan mencari informasi terkait sistem deteksi serangan dengan menggunakan metode Bidirectional Recurrent Neural Networks. Pencarian informasi ini akan dilakukan melalui berbagai sumber, seperti artikel, jurnal ilmiah, situs internet, dan membaca buku yang relevan untuk menuliskan tesis

2. Metode Konsultasi

Metode ini melibatkan pakar yang memiliki pengetahuan dan pengalaman yang mendalam dalam mengatasi masalah terkait penulisan tugas akhir. Diskusi ini bertujuan untuk mendapatkan wawasan dan saran yang berharga

3. Metode Pengumpulan Data

Penulis akan mengumpulkan data yang berkaitan dengan serangan Distributed Denial of Service (DDoS). Data ini akan menjadi dasar bagi analisis dan pengujian yang dilakukan dalam penelitian..

4. Metode Pengujian

Penulis akan merancang sistem yang akan digunakan untuk melatih model dalam deteksi serangan DDoS. Ini termasuk pengembangan algoritma yang diperlukan untuk membangun model yang efektif.

5. Metode Analisa dan Penarikan Kesimpulan

Setelah pengujian dilakukan, hasil yang diperoleh akan dianalisis untuk mengevaluasi proses deteksi serangan. Dari analisis ini, penulis akan menarik kesimpulan yang berdasarkan temuan penelitian tesis ini.

1.7. Sistematika Penulisan

Sitematika pada penulisan penelitian tesis adalah sebagai berikut:

BAB I. PENDAHULUAN

Pada bab I, penelitian terdiri dari latar belakang, rumusan masalah, Batasan masalah, tujuan, mamfaat peneltian, metodologi penelitian dan sistematika penulisan

BAB II. TINJAUAN PUSTAKA

Pada bab II, Mejelaskan teori yang berkaitan serangan cyber khususnya DDoS dan teori *Bidirectional Recurrent Neural Networks (BRNN)*

BAB III. METODOLOGI PENELITIAN

Metodologi penelitian ini akan terdiri dari proses penelitian yang dilakukan, pembuatan rancangan dari Deteksi serangan, serta penerapan dari proyek penelitian tesis ini.

BAB IV. HASIL DAN ANALISIS PENELITIAN

Hasil dan analisis penelitian akan terdiri dari proses penelitian, dan analisa terhadap hasil dataset serangan DDos pada *portmap* menggunakan metode *Bidirectional Recurrent Neural Networks* .

BAB V. KESEIMPULAN DAN SARAN

Pada bab ini akan dilakukan penarikan beberapa kesimpulan dari penjelasan yang ada di bab sebelumnya serta diberikan saran yang dapat membangun guna penelitian selanjutnya

DAFTAR PUSTAKA

Alda Cendekia Siregar, Barry Ceasar Octariadi. 2019. *Feature Selection For Sambas Traditional Fabric "Kain Lunggi" Using Correlation-Based Featured Selection (CFS)*. Vol. (ICoDSE).

Bach, M, A Werner, J Żywiec, and W Pluskiewicz. 2017. The study of under- and over-sampling methods' utility in analysis of highly imbalanced data on osteoporosis . Information Sciences 384, 174–90.

Chonka, A, J Singh, and W Zhou. 2009. Chaos theory based detection against network mimicking DDoS attacks . IEEE Communications Letters 13(9), 717–19.

Chormunge, Smita, and Sudarson Jena. 2018. Correlation based feature selection with clustering for high dimensional data . Journal of Electrical Systems and Information Technology 5(3), 542–49.

Chou, TS, KK Yen, J Luo, N Pissinou, and K Makki. 2007. Correlation-Based Feature Selection for Intrusion Detection Design , MILCOM 2007 - IEEE Military Communications Conference, pp. 1–7.

Deif, Mohanad A, Ahmed AA Solyman, Mehrdad Ahmadi Kamarposhti, Shahab S Band, and Rania E Hammam. 2021. A deep bidirectional recurrent neural network for identification of SARS-CoV-2 from viral genome sequences . Mathematical Biosciences and Engineering 18(6), 8933–50.

Hassib, Eslam, Ali El-Desouky, Mohanad Labib, and El-Sayed El-kenawy. 2020. WOA + BRNN: An imbalanced big data classification framework using Whale optimization and deep neural network . Soft Computing 24.

Hong, K, Y Kim, H Choi, and J Park. 2018. SDN-Assisted Slow HTTP DDoS Attack Defense Method . IEEE Communications Letters 22(4), 688–91.

Iman Sharafaldin, Arash Habibi Lashkari, Saqib Hakak and Ali A Ghorbani. 2019. *Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy*. Ed. Arash Habibi Lashkari, Saqib Hakak and Ali A. Ghorbani Iman Sharafaldin.

Islam, ABMAA, and T Sabrina. 2009. Detection of various denial of service and Distributed Denial of Service attacks using RNN ensemble , 2009 12th International Conference on Computers and Information Technology, pp. 603–8.

Joshi, B Kumar, N Joshi, and M Chandra Joshi. 2018. Early Detection of Distributed Denial of Service Attack in Era of Software-Defined Network , 2018 Eleventh International Conference on Contemporary Computing (IC3), pp. 1–3.

Kabir, Muhammad, Saeed Ahmad, Muhammad Iqbal, Zar Nawab Khan Swati, Zi Liu, and Dong Jun Yu. 2018. Improving prediction of extracellular matrix proteins using evolutionary information via a grey system model and asymmetric under-sampling technique . Chemometrics and Intelligent Laboratory Systems 174, 22–32.

Khraisat, Ansam, Iqbal Gondal, Peter Vamplew, and Joarder Kamruzzaman. 2019. Survey of intrusion detection systems: techniques, datasets and challenges . Cybersecurity 2(1).

Moon, Seung Hyun, and Yong Hyuk Kim. 2020. An improved forecast of precipitation type using correlation-based feature selection and multinomial logistic regression . Atmospheric Research 240, 104928.

Mora-Gimeno, FJ, H Mora-Mora, B Volckaert, and A Atrey. 2021. Intrusion Detection System Based on Integrated System Calls Graph and Neural Networks . IEEE Access 9, 9822–33.

Pristyanto, Y, S Adi, and A Sunyoto. 2019. The Effect of Feature Selection on Classification Algorithms in Credit Approval , 2019 International Conference on Information and Communications Technology (ICOIACT), pp. 451–56.

Ruiz-Bañobre, Juan, Raju Kandimalla, and Ajay Goel. 2019. Predictive Biomarkers in Metastatic Colorectal Cancer: A Systematic Review.

Salopek, Denis, Marko Zec, Miljenko Mikuc, and Valter Vasic. 2022. Surgical DDoS Filtering with Fast LPM . IEEE Access 10, 4200–4208.

Schuster, M, and KK Paliwal. 1997. Bidirectional recurrent neural networks . IEEE Transactions on Signal Processing 45(11), 2673–81.

Su, Shen, Yanbin Sun, Xiangsong Gao, Jing Qiu, and Zhihong Tian. 2019. A Correlation-Change Based Feature Selection Method for IoT Equipment Anomaly Detection . Applied Sciences 9, 437.

Toapanta, Segundo Moisés T, Dhilan Torres Tapia, and Luis Enrique Mafla Gallegos. 2019. An approach of cyberattacks with the use of social networks and communication media for public organizations of the ecuador , ACM International Conference Proceeding Series. Association for Computing Machinery, pp. 67–72.

Varghese, Josy Elsa, and Balachandra Muniyal. 2021a. An Efficient IDS Framework for DDoS Attacks in SDN Environment . IEEE Access 9, 69680–99.

------. 2021b. An Efficient IDS Framework for DDoS Attacks in SDN Environment . IEEE Access 9, 69680–99.

Wei, Y, J Jang-Jaccard, F Sabrina, A Singh, W Xu, and S Camtepe. 2021. AE-MLP: A Hybrid Deep Learning Approach for DDoS Detection and Classification . IEEE Access 9, 146810–21.

Wei, Z, Q Zhu, C Min, Y Chen, and G Wang. 2022. Bidirectional Hybrid LSTM Based Recurrent Neural Network for Multi-view Stereo . IEEE Transactions on Visualization and Computer Graphics, 1.

Xianlun Tang, YUYAN DAI , QING LIU, XIAOYUAN DANG, AND JIN XU. 2019. Application of Bidirectional Recurrent Neural Network Combined With Deep Belief Network in Short-Term Load Forecasting . IEEE.

Xiaoyong Yuan, Chuanhuang L, and Xiaolin Li. 2017. *2017 IEEE International Conference on Smart Computing (SMARTCOMP) Hong Kong, China, 29-31 May 2017*.

Xu, Y, X Yan, Y Wu, Y Hu, W Liang, and J Zhang. 2021. Hierarchical Bidirectional RNN for Safety-Enhanced B5G Heterogeneous Networks . IEEE Transactions on Network Science and Engineering 8(4), 2946–57.

Yi-Wen Chen, Jang-Ping Sheu, Yung-Ching Kuo, and Nguyen Van Cuong. 2020. *Design and Implementation of IoTDDoS Attacks Detection System based on Machine Learning*.

Zy, AT, Amali, AM Rifa'i, AZ Kamalia, and AA Sulaeman. 2024. Detecting DDoS Attacks Through Decision Tree Analysis: An EDA Approach with the CIC DDoS 2019 Dataset , 2024 8th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), pp. 202–7.