ANALISIS SISTEM DETEKSI SERANGAN *DDOS* ADAPTIF MENGGUNAKAN METODE *RT-AMD* PADA INFRASTRUKTUR *CLOUD COMPUTING*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat Memperoleh Gelar Sarjana Komputer

DISUSUN OLEH :

SAHARA DIVA MAHARANI

09011382025113

PROGRAM STUDI SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

AUTHENTICATION PAGE

ANALYSIS OF ADAPTIVE DDOS ATTACK DETECTION SYSTEM USING RT-AMD METHOD ON CLOUD COMPUTING INFRASTRUCTURE

THESIS

Submitted to Complete One of the Requirements to Obtain a Bachelor's Degree in Computer Science

By:

SAHARA DIVA MAHARANI

09011382025113

Palembang, January , 2025

Head Of

Computer System Departement

Dr. Ir. Sukemi, M. T.

NIP. 196612032006041001

Supervisor

Dr. Ahmad Heryanto, S.Kom., M.T.

NIP. 198806202006041004

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Senin

Tanggal : 23 Desember 2024

Tim Penguji

1. **Ketua : Aditya Putra Perdana Prasetyo , S.Kom., M.T.**

2. **Penguji : Huda Ubaya, S.T., M.T.**

3. **Pembimbing : Dr. Ahmad Heryanto, S.Kom., M.T.**

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M. T.

NIP. 196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Senin

Tanggal : 23 Desember 2024

Tim Penguji

1. **Ketua : Aditya Putra Perdana Prasetyo , S.Kom., M.T.**

2. **Penguji : Huda Ubaya, S.T., M.T.**

3. **Pembimbing : Dr. Ahmad Heryanto, S.Kom., M.T.**

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M. T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama	:	Sahara Diva Maharani
NIM	:	09011382025113
Judul	:	Analisis Sistem Deteksi Serangan *DDOS Adaptif* Menggunakan Metode *RT-AMD* Pada Infrastruktur *Cloud Computing*.

Hasil Pengecekan *Software iThenticate*/Turnitin: 3%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam skripsi ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaan dari siapa pun.

Indralaya, 10 Januari 2025

Sahara Diva Maharani

NIM.09011382025113

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh.

Alhamdulillahirabbil'alamin. Segala puji dan syukur kita haturkan atas kehadirat Tuhan Yang Maha Esa, yang telah memberikan rahmat dan karunia-Nya. Shalawat serta salam kepada Rasulullah Shallallahu Alaihi Wasallam yang senantiasa menjadi sumber inspirasi dan teladan terbaik untuk umat manusia dimana hingga saat ini penulis bisa menyelesaikan skripsi yang berjudul "**Analisis Sistem Deteksi Serangan *DDOS* Adaptif Menggunakan Metode *RT-AMD* Pada Infrastruktur *Cloud Computing*"** sebagai salah satu syarat untuk menyelesaikan Program Sarjana (S1) Jurusan Sistem Komputer.

Dalam penulisan ini penulis menjelaskan mengenai hasil dari analisis suatu sistem deteksi serangan *DDOS* menggunakan metode *RT-AMD* pada infrastruktur *Cloud Computing*. Penulis berharap tulisan ini dapat memberikan banyak manfaat kepada para pembaca dan menjadi referensi yang berguna bagi para peneliti yang tertarik dalam bidang keamanan jaringan komputer.

Penulis menyadari bahwa skripsi ini tidak mungkin terselesaikan tanpa adanya dukungan, bantuan, bimbingan, dan nasehat dari berbagai pihak selama penyusunan skripsi ini. Oleh karena itu, pada kesempatan ini penulis menyampaikan banyak terima kasih yang setulus-tulusnya kepada yang terhormat:

1. Allah SWT yang telah memberikan saya nikmat kesehatan, kesempatan serta rahmat-Nya sehingga saya dimudahkan dalam penyelesaian skripsi ini dengan baik.
2. Kedua orang tua saya tercinta Bapak Iskandar Ambang dan Ibu Sri Aryrini yang telah membesarkan, mendidik, mendukung saya serta tidak henti-hentinya mendoakan dan memberikan nasihat, semangat, dan juga motivasi untuk saya dapat menghadapi segala sesuatu baik secara moril, materil, dan spiritual selama ini.
3. Bapak Prof. Dr. Erwin, S.Si., M.Si. selaku Dekan Fakultas Ilmu Komputer dan selaku Dosen Pembimbing Akademik Jurusan Sistem Komputer.

4. Bapak Dr. Ir. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer.
5. Bapak Ahmad Heryanto, S. Kom, M.T selaku Dosen Pembimbing skripsi yang telah berkenan meluangkan waktu dan tenaga dalam membimbing, memberikan saran serta motivasi kepada penulis selama proses penulisan skripsi ini.
6. Mbak Sari Nuzulastri dan Mbak Renny Virgasari selaku admin jurusan Sistem Komputer yang telah berjasa dalam membantu permasalahan administrasi penulis.
7. Seluruh staf dan pegawai jurusan Sistem Komputer yang telah menunjang kesuksesan pembuatan skripsi ini.
8. Ibu Djurainah, Ibu Siti Rozalyah, M Rifqi Rozandra, Abdillah Putra Rozandra selaku keluarga yang telah memberikan tempat tinggal, kebutuhan primer, kebutuhan sekunder, dan kebutuhan tersier selama penulis menjalani masa perkuliahan hingga akhir.
9. M. Aziz Alhadi selaku teman terbaik yang selalu membantu dalam suka dan duka, selalu menemani dan mendengarkan keluh kesah, serta menjadi suporter terbaik selama penyelesaian skripsi.
10. Siti Triwinarti Ningrum, Ully Afifa, Luqman Agus Dwiyono dan Ghulam Robbani Toha selaku teman-teman seperjuangan yang telah memberikan banyak support dan bantuan selama penulis menjalani masa perkuliahan hingga akhir.
11. Radhini Yasmin dan Vanessa Valentina Simamora selaku teman baik saya yang telah menghibur dan menemai selama penyelesaian skripsi.
12. Teman-teman dari grup APSI yang telah berbagi informasi dan dukungan kepada penulis selama penyelesaian skripsi.
13. Teman-teman kelas Sistem Komputer Unggulan angkatan 2020 yang sudah menghibur dan membantu penulis selama penyelesaian skripsi.
14. Indri Pamugari selaku teman baik saya yang telah menghibur dan menemani penulis dari awal perkuliahan hingga akhir.

15. Semua pihak yang terlibat yang telah turut ikut membantu, baik itu dalam memberikan masukan dan ide, kritik maupun juga memberikan semangat kepada penulis yang mana tidak dapat disebutkan satu-persatu.

Penulis menyadari bahwa skripsi ini masih sangat jauh dari kata sempurna. Oleh karena itu, kritik dan saran yang membangun sangatlah diharapkan penulis agar penulisan laporan ini dapat menjadi lebih baik lagi dan dapat dijadikan sumber referensi yang bermanfaat untuk karya yang lebih baik lagi kedepannya.

Penulis berharap semoga skripsi ini dapat bermanfaat bagi pembaca, khususnya Fakultas Ilmu Komputer Universitas Sriwijaya secara langsung ataupun tidak langsung sebagai sumbang pikiran dalam peningkatan mutu pembelajaran dan dapat dijadikan referensi demi pengembangan ke arah yang lebih baik. Kebenaran datangnya dari Allah dan kesalahan datangnya dari diri penulis. Semoga Allah SWT senantiasa melimpahkan rahmat dan Ridho-Nya kepada kita semua.

Wassalamualaikum Warahmatullahi Wabarakatuh

Palembang, Januari 2025

Penulis,

Sahara Diva Maharani
NIM. 09011382025113

ANALISIS SISTEM DETEKSI SERANGAN *DDOS ADAPTIF* MENGGUNAKAN METODE *RT-AMD* PADA INFRASTRUKTUR *CLOUD COMPUTING*

SAHARA DIVA MAHARANI (09011382025113)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email: ssaharadivam@gmail.com

ABSTRAK

Distributed Denial of Service (*DDoS*) adalah ancaman utama bagi infrastruktur cloud computing yang dapat menyebabkan gangguan layanan dan kerugian signifikan. Penelitian ini bertujuan untuk mengembangkan sistem deteksi serangan *DDoS* adaptif menggunakan metode *RT-AMD* (*Real-Time Attack Monitoring and Detection*), yang mengombinasikan empat algoritma machine learning, yaitu *Decision Tree, Random Forest*, *Naive Bayes*, dan *K-Nearest Neighbors*, untuk meningkatkan akurasi dan efisiensi deteksi. Penelitian menggunakan dataset *CICDDoS2019*, dengan fokus pada serangan *SYN Flood* dan *UDP Flood*. Hasil evaluasi menunjukkan bahwa metode *Decision Tree* mencapai akurasi 95,6%, *Random Forest* 98,4%, *Naive Bayes* 88,7%, dan *K-Nearest Neighbors* 93,2%. Sistem ini terbukti efektif dalam mendeteksi serangan *DDoS* secara *adaptif* dan efisien dalam penggunaan sumber daya, serta mampu mengidentifikasi pola serangan secara *real-time*. Dengan demikian, penelitian ini memberikan kontribusi signifikan dalam pengembangan metode deteksi yang lebih cerdas dan adaptif untuk meningkatkan keamanan jaringan *cloud computing*, sekaligus menjadi referensi untuk penelitian lanjutan di bidang keamanan siber.

Kata Kunci: *DDoS, RT-AMD, Machine Learning, Cloud Computing,* Keamanan Jaringan

ANALYSIS OF ADAPTIVE DDOS ATTACK DETECTION SYSTEM USING RT-AMD METHOD ON CLOUD COMPUTING INFRASTRUCTURE

SAHARA DIVA MAHARANI (09011382025113)
Departement of Computer System, Faculty of Computer Science,
Sriwijaya University
Email: ssaharadivam@gmail.com

ABSTRACT

Distributed Denial of Service (DDoS) is a major threat to cloud computing infrastructure, capable of causing service disruptions and significant losses. This study aims to develop an adaptive DDoS attack detection system using the RT-AMD (Real-Time Attack Monitoring and Detection) method, which combines four machine learning algorithms: Decision Tree, Random Forest, Naive Bayes, and K-Nearest Neighbors, to enhance detection accuracy and efficiency. The research utilizes the CICDDoS2019 dataset, focusing on SYN Flood and UDP Flood attacks. Evaluation results indicate that the Decision Tree method achieves an accuracy of 95.6%, Random Forest 98.4%, Naive Bayes 88.7%, and K-Nearest Neighbors 93.2%. The system demonstrates its effectiveness in adaptively detecting DDoS attacks, efficiently utilizing resources, and identifying attack patterns in real-time. Thus, this study significantly contributes to the development of smarter and more adaptive detection methods to improve the security of cloud computing networks while serving as a reference for future research in the field of cybersecurity.

Keywords: *DDoS, RT-AMD, Machine Learning, Cloud Computing, Network Security*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1
PENDAHULUAN

1.1. Latar Belakang

Cloud Computing adalah model komputasi di mana sumber daya seperti server, penyimpanan data, dan aplikasi disediakan secara on-demand melalui internet. Hal ini memungkinkan pengguna untuk mengakses sumber daya tanpa perlu memiliki atau mengelola infrastruktur fisik secara langsung, menjadikan *Cloud Computing* sebagai salah satu paradigma utama dalam penyediaan layanan komputasi. Pengguna dapat mengakses aplikasi, penyimpanan, dan layanan komputasi tanpa harus memelihara infrastruktur mereka sendiri, yang pada akhirnya meningkatkan efisiensi dan fleksibilitas. Dengan adanya *Cloud Computing*, bisnis maupun individu dapat menyimpan dan mengelola data mereka dengan lebih baik dan memiliki kemampuan untuk menyesuaikan kapasitas sesuai kebutuhan, yang dikenal dengan istilah elastisitas. Selain itu, model komputasi ini menawarkan keandalan tinggi, pemulihan bencana, dan keamanan data yang lebih baik dibandingkan infrastruktur lokal. Kemampuan untuk menyediakan sumber daya komputasi sesuai permintaan juga menjadi salah satu keunggulan *Cloud Computing* karena pengguna hanya perlu membayar sesuai dengan jumlah sumber daya yang digunakan, sehingga biaya yang dikeluarkan menjadi lebih efisien [1].

Namun, di balik beragam manfaatnya, infrastruktur *Cloud Computing* memiliki kelemahan, terutama terkait risiko keamanan, seperti serangan *Distributed Denial of Service* (*DDOS*). Serangan *DDOS* merupakan salah satu ancaman utama bagi penyedia layanan *Cloud Computing* dan dapat mengakibatkan layanan atau infrastruktur tidak dapat diakses oleh pengguna yang berhak. Serangan ini dilakukan dengan mengirimkan lalu lintas data dalam jumlah yang sangat besar ke target, yang dapat menyebabkan penurunan performa layanan atau bahkan menghentikan layanan tersebut[2]. Serangan *DDOS* biasanya memanfaatkan botnet, yakni jaringan komputer yang telah terinfeksi malware dan dapat dikontrol oleh penyerang untuk menyerang target secara serentak. Dampak dari serangan ini sangat merugikan karena dapat menyebabkan kerugian finansial, kerusakan

reputasi, kehilangan data, dan potensi kerugian lainnya bagi korban serangan. Terlebih lagi, skala dan metode yang digunakan dalam serangan *DDOS* semakin kompleks, sehingga penanganan serangan ini menjadi tantangan serius dalam menjaga keamanan dan keandalan infrastruktur *Cloud Computing*.

Tingkat ancaman serangan *DDOS* terhadap *Cloud Computing* terus meningkat dengan adanya sejumlah insiden besar yang terjadi pada tahun 2023. Salah satu insiden besar yang tercatat adalah serangan *DDOS* terhadap perusahaan *Cloudflare*, penyedia layanan *Content Delivery Network* (CDN) dan keamanan web terkemuka di dunia. Pada bulan Juni 2023, *Cloudflare* mengalami serangan *DDOS* hiper-volumetrik yang terjadi secara berulang selama akhir pekan, dengan puncak serangan mencapai lebih dari 71 juta permintaan per detik (rps), yang mana angka ini menjadi rekor serangan *DDOS* HTTP terbesar yang pernah tercatat, bahkan lebih tinggi 54% dibandingkan rekor sebelumnya yang mencapai 46 juta rps [3]. Hal ini menunjukkan bahwa serangan *DDOS* kini semakin canggih dan memiliki kapasitas untuk menyerang dengan intensitas yang sangat tinggi, memberikan tantangan besar bagi penyedia layanan dalam menjaga kestabilan dan keamanan sistem mereka.

Selain Cloudflare, Google Cloud juga menghadapi serangan serupa pada bulan Agustus 2023. Serangan ini menggunakan metode inovatif yang disebut "Rapid Reset," memanfaatkan stream multiplexing pada protokol HTTP/2 untuk menyerang situs web dan layanan internet. Puncak serangan *DDOS* ini mencapai 398 juta permintaan per detik, menjadikannya salah satu serangan terbesar dalam sejarah *DDOS* yang pernah dicatat. Google, sebagai penyedia layanan, segera merespon serangan ini dengan menerapkan langkah-langkah mitigasi tambahan dan bekerja sama dengan penyedia cloud lain serta pengelola perangkat lunak HTTP/2 untuk memperkuat keamanan di seluruh ekosistem layanan berbasis internet [4].

Kasus serangan *DDOS* lainnya yang tak kalah signifikan terjadi pada Akamai Technologies dimana serangan *DDOS* berhasil dideteksi. Pada tanggal 23 Februari 2023, pukul 10:22 UTC, Akamai berhasil memitigasi serangan *DDOS* terbesar yang pernah ditujukan kepada pelanggan Prolexic yang berbasis di Asia-Pasifik (APAC), di mana lalu lintas serangan mencapai puncak 900,1 gigabit per

detik dan 158,2 juta paket per detik. Sesuai dengan tren terkini, serangan ini bersifat sangat intens namun berlangsung singkat, dengan mayoritas lalu lintas serangan terjadi pada puncak menit-menit awal serangan. Pola lalu lintas kembali normal hanya dalam beberapa menit [5].

Selain itu, pada tanggal 5 September 2023, sekitar pukul 19:31 UTC, Akamai Prolexic, platform pertahanan penolakan layanan terdistribusi (*DDOS*), berhasil mendeteksi dan mencegah serangan *DDOS* terbesar yang ditujukan pada salah satu lembaga keuangan AS terbesar dan paling berpengaruh di dunia. Pelaku kejahatan siber menggunakan kombinasi vektor serangan berupa banjir ACK, PUSH, RESET, dan *SYN*, dengan serangan mencapai puncak pada 633,7 gigabit per detik (Gbps) dan 55,1 juta paket per detik (Mpps). Serangannya tajam namun berlangsung kurang dari 2 menit, dan secara proaktif dimitigasi oleh postur pertahanan siber yang komprehensif [6].

Dari beberapa uraian kasus di atas, dapat disimpulkan bahwa meskipun Cloud Computing menawarkan berbagai keunggulan, keamanan tetap menjadi salah satu tantangan terbesar yang dihadapi, terutama terkait dengan serangan *DDOS* yang terus meningkat setiap tahunnya. Berbagai penelitian telah dilakukan untuk mengembangkan metode deteksi dan mitigasi serangan *DDOS* pada infrastruktur cloud. Sebagai contoh, penelitian [7] telah mengusulkan penggunaan metode pembelajaran mesin yang mengelompokkan data jaringan secara akurat dalam mendeteksi serangan *DDOS*. Metode ini menggunakan teknik pemilihan fitur melalui algoritma PCA untuk meningkatkan efisiensi pengelompokan data. Algoritma DBSCAN, Agglomerative Clustering, dan K-Means diterapkan pada data yang telah dipilih fiturnya, menghasilkan efektivitas yang lebih tinggi pada metrik seperti Indeks Rand dibandingkan pengelompokan menggunakan seluruh fitur. Hasil ini menunjukkan bahwa penggunaan fitur yang tepat dapat meningkatkan kinerja deteksi serangan secara signifikan.

Penelitian lain [8] menawarkan pendekatan yang menggabungkan aspek kepercayaan dalam deteksi serangan *DDOS* pada Cloud Computing. Dalam studi tersebut, hypervisor membangun hubungan kepercayaan dengan mesin virtual (VM) tamu melalui kombinasi kepercayaan objektif dan subjektif, yang kemudian

dikombinasikan dengan inferensi Bayesian. Selain itu, penelitian ini merancang sebuah permainan berbasis kepercayaan antara penyerang *DDOS* dan hypervisor, di mana hypervisor berupaya memaksimalkan deteksi serangan meskipun memiliki sumber daya terbatas. Hasilnya menunjukkan peningkatan dalam akurasi deteksi serangan, mengurangi hasil positif dan negatif palsu, serta efisiensi penggunaan CPU, memori, dan bandwidth selama serangan berlangsung dibandingkan dengan teknik deteksi lainnya yang berbasis distribusi beban.

Selain itu, pendekatan lain dalam mendeteksi serangan *DDOS* diusulkan oleh penelitian [9], yang menyajikan sistem deteksi berbasis mesin pembelajaran ekstrem evolusioner mandiri (SaE-ELM) yang telah ditingkatkan. Model SaE-ELM ini dimodifikasi dengan adaptasi operator crossover yang lebih sesuai dan kemampuan menentukan jumlah neuron lapisan tersembunyi secara otomatis, sehingga meningkatkan kemampuan pembelajaran dan klasifikasi sistem. Pada evaluasi menggunakan empat dataset besar seperti NSL-KDD dan CICIDS 2017, sistem ini menunjukkan performa yang lebih baik dalam deteksi serangan *DDOS* meskipun membutuhkan waktu pelatihan yang lebih lama.

Berdasarkan penjelasan penelitian terdahulu diatas, ditemukan bahwa meskipun berbagai metode telah diusulkan, serangan *DDOS* pada Cloud Computing tetap menjadi ancaman yang nyata dan memerlukan penelitian lebih lanjut. Kerugian finansial dan non-finansial yang ditimbulkan oleh serangan ini menunjukkan bahwa masih dibutuhkan pendekatan yang lebih mendalam dan adaptif dalam mendeteksi serta mencegah serangan *DDOS*. Oleh karena itu, penelitian ini bertujuan untuk menganalisis sistem deteksi serangan *DDOS* adaptif menggunakan metode RT-AMD pada infrastruktur Cloud Computing. Metode Real Time Attack Monitoring and Detection (RT-AMD) difokuskan pada peningkatan kinerja machine learning dalam mendeteksi adanya aktivitas mencurigakan yang mengindikasikan serangan *DDOS* [10]. Keunggulan metode RT-AMD terletak pada kemampuannya mendeteksi serangan *DDOS* adaptif. Dengan analisis real-time, metode RT-AMD diharapkan mampu merespons perubahan pola tersebut dengan tindakan mitigasi yang cepat.

Dengan mengoptimalkan metode RT-AMD, penelitian ini diharapkan dapat meningkatkan efektivitas deteksi serangan *DDOS* adaptif, menjaga keandalan layanan Cloud Computing, dan memberikan kontribusi dalam pengembangan metode deteksi serangan *DDOS* yang lebih efisien di masa mendatang. Oleh karena itu, penelitian dalam skripsi ini akan dilakukan dengan judul "**Analisis Sistem Deteksi Serangan *DDOS* Adaptif Menggunakan Metode RT-AMD pada Infrastruktur Cloud Computing**".

1.2. Rumusan Masalah

Permasalahan yang dirumuskan dalam penulisan skripsi ini berdasarkan penjelasan latar belakang diatas adalah bagaimana meningkatkan efektivitas deteksi serangan *DDOS* adaptif pada infrastruktur *Cloud Computing* menggunakan metode *RT-AMD*, dengan mempertimbangkan faktor-faktor seperti akurasi deteksi, efisiensi penggunaan sumber daya, dan adaptabilitas , sehingga dapat menjaga keandalan layanan *Cloud Computing* dari gangguan serangan *DDOS*.

1.3. Batasan Masalah

Penelitian ini mempunyai batasan tertentu yang akan mengarahkan fokus penelitian pada aspek spesifik dalam analisis sistem deteksi serangan *DDOS* adaptif menggunakan metode *RT-AMD* pada infrastruktur *Cloud Computing*. Berikut batasan masalah dari penelitian ini, yaitu:

1. Penelitian ini akan memfokuskan pada beberapa serangan *DDOS* yaitu, *SYN* Flood, dan *UDP* Flood, sebagai implementasi dari serangan *DDOS* Adaptif.
2. Penelitian ini akan fokus pada efektivitas dari metode *RT-AMD* (Real Time Attack Monitoring and Detection) yang menggunakan 4 klasifikasi Machine Learning yaitu *Decision Tree*, *Random Forest*, K-Nearest Neighbor, dan *Naive Bayes* dalam mendeteksi berbagai serangan *DDOS*.

1.4. Tujuan

Berdasarkan penelitian yang dilakukan, adapun tujuan dari penelitian skripsi ini yaitu:

1. Meningkatkan efisiensi dalam mendeteksi serangan *DDOS*. Dimana metode yang diusulkan diharapkan dapat mengidentifikasi serangan dengan efektif.
2. Melakukan analisis mengenai keunggulan dan keterbatasan dari sistem deteksi yang diusulkan.

1.5. Manfaat

Berdasarkan penelitian yang dilakukan, adapun manfaat dari penelitian skripsi ini, yaitu:

1. Jika metode *RT-AMD* terbukti efektif dalam mendeteksi berbagai jenis serangan *DDOS*, maka informasi ini dapat digunakan untuk meningkatkan efektivitas perlindungan infrastruktur *Cloud Computing* dari serangan *DDOS*.
2. Dengan pendekatan deteksi adaptif yang digunakan, sistem akan dapat merespons serangan *DDOS* dengan lebih cepat dan tepat. Ini dapat mengurangi dampak serangan dan mengurangi waktu pemulihan layanan setelah serangan.
3. Melalui evaluasi kinerja dan analisis mendalam, Penelitian ini akan memberikan wawasan yang lebih mendalam tentang kelebihan dan kekurangan metode yang diajukan, yang dapat mendukung pengembangan lebih lanjut serta peningkatan sistem.

1.6. Sistematika Penulisan

Adapun dalam penyusunan skripsi ini akan disusun secara sistematis dengan cara urutan per-bab. Selanjutnya, dalam setiap bab itu sendiri berisikan masing – masing sub bab yang sebagaimana isisnya dalah menjelaskan secara detail dari sub bab yang bersangkutan. Sistematika yang akan digunakan dalam penulisan skripsi ini adalah sebagai berikut:

BAB I PENDAHULUAN

Pada bagian BAB I akan menjelaskan mengenai latar belakang penelitian, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bagian BAB II akan menjelaskan mengenai landasan teori, penelitian terkait atau terdahulu, dan ringkasan hasil kajian literatur.

BAB III METODOLOGI PENELITIAN

Pada bagian BAB III akan menjelaskan mengenai pengumpulan data, lingkungan dan spesifikasi perangkat keras dan perangkat lunak, rancangan blok diagram serta metode dan diagram alir.

BAB IV HASIL DAN ANALISIS

Pada bagian BAB IV akan menjelaskan mengenai hasil pengujian yang diperoleh dan menjelaskan analisa terhadap hasil dari penelitian yang dicapai meliputi kelebihan dan kekurangan dari penelitian yang telah dilakukan.

BAB V PENUTUP

Pada bagian BAB V akan menjelaskan semua simpulan yang dapat disimpulkan dari hasil keseluruhan penelitian dan analisa terhadap penelitian yang telah dilakukan.

DAFTAR PUSTAKA

[1] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, "A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies," *IEEE Access*, vol. 9, pp. 57792–57807, 2021, doi: 10.1109/ACCESS.2021.3073203.

[2] R. K. Patel, D. L. K. Singh, and D. N. Kumar, "Literature Review of Distributed: Denial of Service Attack Protection," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 11, no. 1, pp. 1032–1036, 2023, doi: 10.22214/ijraset.2023.48673.

[3] A. F. Omer Yoachimik, Julien Desgats, "Cloudflare mitigates record-breaking 71 million request-per-second *DDOS* attack," *blog.cloudflare.com*, 2023. https://blog.cloudflare.com/cloudflare-mitigates-record-breaking-71-million-request-per-second-*DDOS*-attack (accessed Feb. 21, 2024).

[4] T. A. Emil Kiner, "Google mitigated the largest *DDOS* attack to date, peaking above 398 million rps," *cloud.google.com*, 2023. https://cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-*DDOS*-attack-peaking-above-398-million-rps (accessed Feb. 21, 2024).

[5] C. Sparling, "Akamai Mitigates Record *DDOS* Attack in Asia-Pacific (900 Gbps)," *akamai.com*, 2023. https://www.akamai.com/blog/security/record-breaking-*DDOS*-in-apac (accessed Feb. 21, 2024).

[6] S. R. Craig Sparling, "Akamai Prevents the Largest *DDOS* Attack on a U.S. Financial Company," *akamai.com*, 2023. https://www.akamai.com/blog/security/akamai-prevents-the-largest-*DDOS*-attack-on-a-us-financial-company (accessed Feb. 21, 2024).

[7] F. J. Abdullayeva, "Distributed denial of service attack detection in E-government cloud via data clustering," *Array*, vol. 15, no. July, p. 100229, 2022, doi: 10.1016/j.array.2022.100229.

[8] O. A. Wahab, J. Bentahar, H. Otrok, and A. Mourad, "Optimal Load Distribution for the Detection of VM-Based *DDOS* Attacks in the Cloud," *IEEE Trans. Serv. Comput.*, vol. 13, no. 1, pp. 114–129, 2020, doi:

10.1109/TSC.2017.2694426.

[9] G. S. Kushwah and V. Ranga, “Optimized extreme learning machine for detecting *DDOS* attacks in cloud computing,” *Comput. Secur.*, vol. 105, p. 102260, Jun. 2021, doi: 10.1016/J.COSE.2021.102260.

[10] O. Bamasag, A. Alsaeedi, A. Munshi, D. Alghazzawi, S. Alshehri, and A. Jamjoom, “Real-time *DDOS* flood attack monitoring and detection (RT-AMD) model for cloud computing,” *PeerJ Comput. Sci.*, vol. 7, 2022, doi: 10.7717/PEERJ-CS.814.

[11] Y. Jia, F. Zhong, A. Alrawais, B. Gong, and X. Cheng, “FlowGuard: An Intelligent Edge Defense Mechanism against IoT *DDOS* Attacks,” *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9552–9562, 2020, doi: 10.1109/JIOT.2020.2993782.

[12] M. Mittal, K. Kumar, and S. Behal, “DL-2P-*DDOS*ADF: Deep learning-based two-phase *DDOS* attack detection framework,” *ScienceDirect*, vol. 78, p. 103609, Nov. 2023, doi: 10.1016/J.JISA.2023.103609.

[13] A. V. Songa and G. R. Karri, “An integrated SDN framework for early detection of *DDOS* attacks in cloud computing,” *J. Cloud Comput.*, vol. 13, no. 1, 2024, doi: 10.1186/s13677-024-00625-9.

[14] G. S. Kushwah and V. Ranga, “Voting extreme learning machine based distributed denial of service attack detection in cloud computing,” *ScienceDirect*, vol. 53, 2020, doi: 10.1016/j.jisa.2020.102532.

[15] N. Jyoti and S. Behal, “A meta-evaluation of machine learning techniques for detection of *DDOS* attacks,” *IEEE Access*, no. March, pp. 522–526, 2021, doi: 10.1109/INDIACom51348.2021.00093.

[16] N. M. Yungaicela-Naula, C. Vargas-Rosales, J. A. Pérez-Díaz, and D. F. Carrera, “A flexible SDN-based framework for slow-rate *DDOS* attack mitigation by using deep reinforcement learning,” *IEEE Access*, vol. 205, pp. 1–22, 2022, doi: 10.1016/j.jnca.2022.103444.

[17] R. Abubakar *et al.*, “An Effective Mechanism to Mitigate Real-Time *DDOS* Attack,” *IEEE Access*, vol. 8, pp. 126215–126227, 2020, doi: 10.1109/ACCESS.2020.2995820.

[18] A. E. Cil, K. Yildiz, and A. Buldu, “Detection of *DDOS* attacks with feed

forward based deep neural network model," *ScienceDirect*, vol. 169, no. April 2020, p. 114520, 2021, doi: 10.1016/j.eswa.2020.114520.

[19] S. Kautish, A. Reyana, and A. Vidyarthi, "SDMTA: Attack Detection and Mitigation Mechanism for *DDOS* Vulnerabilities in Hybrid Cloud Environment," *IEEE Trans. Ind. Informatics*, vol. 18, no. 9, pp. 6455–6463, 2022, doi: 10.1109/TII.2022.3146290.

[20] A. Mihoub, O. Ben Fredj, O. Cheikhrouhou, A. Derhab, and M. Krichen, "Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques," *ScienceDirect*, vol. 98, no. January 2022, p. 107716, 2022, doi: 10.1016/j.compeleceng.2022.107716.

[21] H. Whitworth, S. Al-Rubaye, A. Tsourdos, and J. Jiggins, "5G Aviation Networks Using Novel AI Approach for *DDOS* Detection," *IEEE Access*, vol. 11, no. June, pp. 77518–77542, 2023, doi: 10.1109/ACCESS.2023.3296311.

[22] L. Mhamdi, D. McLernon, F. El-Moussa, S. A. Raza Zaidi, M. Ghogho, and T. Tang, "A Deep Learning Approach Combining Autoencoder with One-class SVM for *DDOS* Attack Detection in SDNs," *IEEE Access*, 2020, doi: 10.1109/ComNet47917.2020.9306073.

[23] S. Haider *et al.*, "A Deep CNN Ensemble Framework for Efficient *DDOS* Attack Detection in Software Defined Networks," *IEEE Access*, vol. 8, no. March, pp. 53972–53983, 2020, doi: 10.1109/ACCESS.2020.2976908.

[24] K. S. Sahoo *et al.*, "An Evolutionary SVM Model for *DDOS* Attack Detection in Software Defined Networks," *IEEE Access*, vol. 8, pp. 132502–132513, 2020, doi: 10.1109/ACCESS.2020.3009733.

[25] M. J. Pasha, K. P. Rao, A. MallaReddy, and V. Bande, "LRDADF: An AI enabled framework for detecting low-rate *DDOS* attacks in cloud computing environments," *ScienceDirect*, vol. 28, no. October 2022, p. 100828, 2023, doi: 10.1016/j.measen.2023.100828.

[26] M. S. Elsayed, S. Dev, and A. D. Jurcut, "*DDOS*Net : A Deep-Learning Model for Detecting Network Attacks," *IEEE Access*, 2020, doi: 10.1109/ICIRCA54612.2022.9985524.

[27] B. Hussain, S. Member, Q. Du, B. Sun, and Z. Han, “Deep Learning-Based *DDOS*-Attack Detection for Cyber-Physical System over 5G network,” *IEEE Access*, no. February, 2021, doi: 10.1109/TII.2020.2974520.

[28] A. M. Abdallah, T. Murugan, and S. Member, “Machine Learning and Deep Learning Techniques for Distributed Denial of Service Anomaly Detection in Software Defined Networks — Current Research Solutions,” *IEEE Access*, vol. 12, no. February, pp. 17982–18011, 2024, doi: 10.1109/ACCESS.2024.3360868.

[29] G. O. Anyanwu, C. I. Nwakanma, J. Lee, and D. Kim, “Optimization of RBF-SVM Kernel using Grid Search Algorithm for *DDOS* Attack Detection in SDN-based VANET,” *IEEE Access*, no. May, 2023, doi: 10.1109/JIOT.2022.3199712.

[30] F. Alasmary, S. Alraddadi, S. Al-ahmadi, and J. Al-muhtadi, “ShieldRNN : A Distributed Flow-Based *DDOS* Detection Solution for IoT Using Sequence Majority Voting,” *IEEE Access*, vol. 10, no. August, pp. 88263–88275, 2022, doi: 10.1109/ACCESS.2022.3200477.

[31] M. Odusami, S. Misra, O. Abayomi-Alli, A. Abayomi-Alli, and L. Fernandez-Sanz, “A survey and meta-analysis of application-layer distributed denial-of-service attack,” *Res. Gate*, vol. 33, no. 18, pp. 1–24, 2020, doi: 10.1002/dac.4603.

[32] H. Abusaimeh, “Distributed denial of service attacks in cloud computing,” *Res. Gate*, vol. 11, no. 6, pp. 163–168, 2020, doi: 10.14569/IJACSA.2020.0110621.

[33] S. Javanmardi, M. Ghahramani, M. Shojafar, M. Alazab, and A. M. Caruso, “M-RL: A mobility and impersonation-aware IDS for *DDOS* UDP flooding attacks in IoT-Fog networks,” *Comput. Secur.*, vol. 140, no. February, p. 103778, 2024, doi: 10.1016/j.cose.2024.103778.

[34] M. Dimolianis, A. Pavlidis, and V. Maglaris, “SYN Flood Attack Detection and Mitigation using Machine Learning Traffic Classification and Programmable Data Plane Filtering,” *2021 24th Conf. Innov. Clouds, Internet Networks Work. ICIN 2021*, no. Icin, pp. 126–133, 2021, doi: 10.1109/ICIN51074.2021.9385540.

[35] P. P. Shinde and S. Shah, “Machine Learning and Deep Learning: A Review of Methods and Applications,” *Res. Gate*, no. January, 2023, doi: 10.1109/ICCUBEA.2018.8697857.

[36] T. Alam, “Cloud Computing and Its Role in the Information Technology,” *SSRN Electron. J.*, no. January 2020, 2020, doi: 10.2139/ssrn.3639063.

[37] N. Singla, Chahat, Nisha, and Harnoor, “A Review Paper on Cloud Computing,” *Proc. - 2022 2nd Int. Conf. Innov. Sustain. Comput. Technol. CISCT 2022*, vol. VI, no. I, pp. 62–64, 2022, doi: 10.1109/CISCT55310.2022.10046572.

[38] A. Ali, “an Overview of Cloud Computing for the Advancement of the E-Learning Process,” *Res. Gate*, vol. 100, no. 3, pp. 847–855, 2022.

[39] M. Hasnain, M. F. Pasha, I. Ghani, M. Imran, M. Y. Alzahrani, and R. Budiarto, “Evaluating Trust Prediction and Confusion Matrix Measures for Web Services Ranking,” *IEEE Access*, vol. 8, pp. 90847–90861, 2020, doi: 10.1109/ACCESS.2020.2994222.

[40] M. Heydarian, T. E. Doyle, and R. Samavi, “MLCM: Multi-Label Confusion Matrix,” *IEEE Access*, vol. 10, pp. 19083–19095, 2022, doi: 10.1109/ACCESS.2022.3151048.

[41] P. Hirapara and A. Sikander, *A Review of DDOS Evaluation Dataset: CICDDOS2019 Dataset*, vol. 1057 LNEE. 2023. doi: 10.1007/978-981-99-3691-5_36.