FORMAT: Jurnal Ilmiah Teknik Informatika
Akreditasi Sinta 5 RISTEKBRIN No. 164/E/KPT/2021; E-ISSN 2722-7162 | P-ISSN 2089-5615

Vol. 14, No. 2,
July 2025,
125-135, 2025

Penerapan Algoritma SVM pada *Software Define Network* untuk Mendeteksi dan Mitigasi Serangan DDOS pada Server Jaringan

Avrijsto Amandri Achyar[1], Andi Purnomo[2]

[1, 2] *Fakultas Ilmu Komputer, Universitas Ary Ginanjar, Jl. TB. Simatupang Kav 1, Jakarta Selatan, Indonesia.*

[1] a.amandri.a@students.esqbs.ac.id, [2] andri.purnomo@uags.ac.id

Kata kunci:
Support Vector Machine Algoritm, DDoS, SDN, RYU

Abstract

Software Defined Network (SDN) is a network architecture that is very useful in the future where SDN can be used to manage network traffic on server networks. SDN can be implemented using a variety of controllers. In the controller the developer can configure it with various algorithms or other functions. At present, cyber crimes are increasingly numerous and dangerous. One of the most dangerous cyber attacks that is mostly carried out by both novice and professional hackers is the DDoS attack. DDoS attacks are aimed at crippling servers with server administration with multiple streams and packets. SDN as an architect for managing networks can be used to detect and counteract DDoS attacks so that servers are protected from these attacks. In this study researchers used SDN configured using the SVM algorithm to detect and mitigate DDOS attacks. In this study, the researchers obtained results where SDN with the SVM algorithm configuration obtained an accuracy rate of 99.67%. The SDN speed configured with the SVM algorithm does not exceed 0.30ms. Wireshark statistics show that SDN with the SVM algorithm configuration can stabilize and mitigate packets detected as DDOS.

Pendahuluan

Dengan kemanjuan teknologi yang ada saat ini membuat banyak sekali kemudahan karna segala sesuatu hal dapat dikerjakan atau dijalankan dengan menggunakan teknologi yang ada. Dengan seluruh kemudahan yang ditawarkan oleh teknologi saat ini maka banyak masyarakat yang menggantungkan pekerjaan pada teknologi yang ada. Tidak hanya masyarakat namun juga banyak perusahaan yang sudah memanfaatkan teknologi semaksimal mungkin untuk menjalankan bisnis atau pekerjaannya. Salah satu kemajuan teknologi saat ini adalah penggunaan server jaringan di perusahaan. Server adalah sebuah hardware yang memiliki fungsi untuk melayani hubungan antar jaringan yang ada pada suatu workstation (Ardianto 2020). Server jaringan dalam sebuah

perusahaan memiliki peran penting yaitu untuk mengatur seluruh sistem jaringan pada sebuah jaringan computer. Server jaringan juga menjadi pintu masuk dan menjadi pengelola untuk penyebaran jaringan internet yang akan digunakan paka Komputer yang ada dalam suatu perusahaan.

Seluruh kemajuan teknologi terutama dalam hal ini adalah server jaringan membuat perusahaan menjadi lebih mudah dalam menjalankan pekerjaan terutama untuk mendapatkan akses internet. Namun, dari seluruh kemudahan yang ada terdapat juga bahaya yang selalu mengintai yaitu serangan dari hacker. Salah satu serangan dari hacker yang sangat berbahaya dan banyak digunakan pada saat ini adalah DDoS. Menurut indotelko.com pada Q3 tahun 2022 serangan DDoS di dunia meningkat hingga 2 kali lipat yaitu sebanyak 47,87% dibanding tahun sebelumnya dengan periode yang sama. Pada tahun 2018 terjadi serangan DDoS terbesar dalam sejarah internet yang terjadi pada GitHub. Dari seluruh serangan yang terjadi pada banyak perusahaan yang ada di dunia hal ini menjadi sebuah ancaman yang sangat berbahaya bagi perusahaan.

Pada banyak perusahaan saat ini terutama di Indonesia masih banyak yang belum memerhatikan keamanan server jaringan dari perusahaan tersebut. Keamanan jaringan merupakan hal penting yang harus diterapkan pada jaringan suatu perusahaan untuk mengamankan server jaringannya. Salah satu keamanan jaringan yang bisa diterapkan ialah dengan menerapkan Software Defined Network (SDN). SDN merupakan sebuah teknologi pada arsitektur jaringan yang dapat memudahkan dalam hal memanajemen perangkat-perangkat yang ada dalam suatu jaringan. Salah satu perangkan yang bisa diamankan yaitu router. Router merupakan perangkat yang menjadi pintu masuk utama jaringan internet dan juga tempat penyebaran utama untuk menyebarkan internet kepada perangkat yang ada di perusahaan seperti komputer.

SDN memiliki sebuah konsep untuk memanajemen jaringan dimana control plane dengan data plane akan dipisahkan sehingga memiliki jalur tugas sendiri. Pada control plane ada controller yang digunakan untuk mengatur terkait proses apa yang akan dilakukan terhadap suatu paket jaringan yang akan masuk ke dalam router. Sedangkan pada data plane akan melakukan forwarding paket sesuai dengan instrulsi yang diberikan oleh controller. Banyak controller yang bisa digunakan pada SDN seperti POX, RYU, OpenDayLight, dan ONOS. Pemilihan controller yang tepat tentu sangat penting sehingga bisa mendapatkan efektifitas yang tinggi dalam mendeteksi dan memitigasi serangan DDoS yang masuk pada srever jaringan perusahaan. Salah satu controrller yang bagus dan banyak digunakan pada saat ini ialah RYU dimana RYU menggunakan protocol OpenFlow SDN. RYU juga sudah mengalami banyak pengembangan dan bahasa yang digunakan lebih mudah dan sudah banyak digunakan yaitu dengan menggunakan bahasa pemrograman python.

Penggunaan controller dapat digabungkan dengan algoritma machine learning sehingga mendapatkan hasil yang lebih maksimal. Banyak algoritma yang bisa digunakan salah satunya adalah SVM. SVM merupakan sebuah algoritma yang sudah memiliki banyak library pada bahasa pemrograman python. Dengan adanya library seperti numpy, scikit-learn, dan SVC membuat penggunaan algoritma ini menjadi lebih mudah. Pada tahun 2019 Jodi Chris Jordan Sihombing, Dany Primanita Kartikasari, dan Adhitya Bhawiyuga melakukan penelitian untuk membuat sistem deteksi DDoS dengan menggunakan SVM Classifier pada arsitektur SDN. Pada penelitian ini pada peneliti tersebut mendapatkan hasil akurasi rata rata yaitu 96,83% dengan waktu deteksi rata – rata 67.80 milidetik (Chris et al. 2019). Selain itu pada tahun 2023 Khartika P dan Arockiasamy Karmel melakukan penelitian simulasi SDN pada mininet untuk deteksi dan mitigasi serangan DDOS dengan menggunakan machine learning. Dari penelitian ini para peneliti tersebut mendapatkan hasil akurasi yang cukup tinggi yaitu 99,75% (Karthika and Arockiasamy 2023). Lalu pada tahun

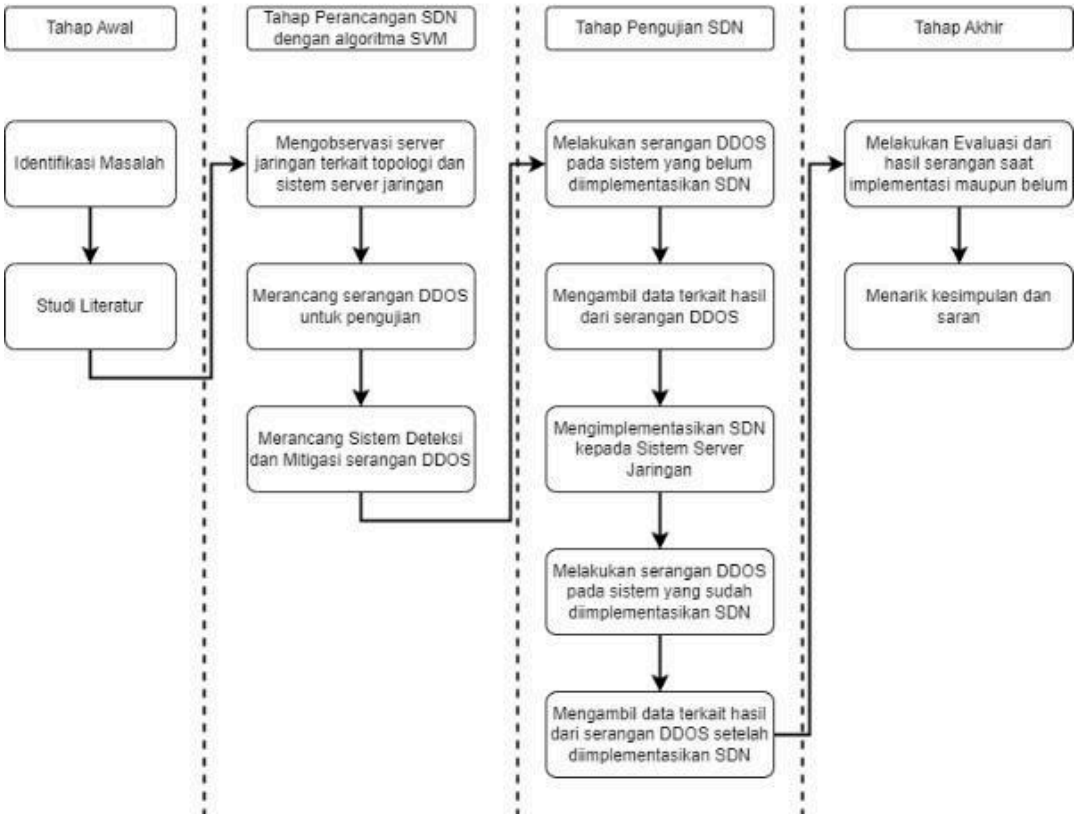
2020 Nan Haymarn Oo, Aris Cahyadi Risdianto, Teck Char Ling, dan Aung Htein Maw elakukan penelitian terkait sistem pendeteksi dan mitigas flooding attack menggunakan adaptive threshold algorithm. Pada penelitian ini para peneliti mendapatkan hasil dalam mengurangi lalu lintas jaringan palsu hingga 17.74% dengan akurasi deteksi yaitu 16,11% (Oo et al. 2020).

Dengan latar belakang dan penelitian terdahulu, peneliti melakukan penelitian yaitu membuat sistem deteksi dan mitigasi serangan DDoS dengan algoritma SVM pada SDN. Judul penelitan ini adalah "Penerapan Algoritma Svm Pada Software Define Network Untuk Mendeteksi Dan Mitigasi Serangan Ddos Pada Server Jaringan". Pada penelitian ini peneliti akan melihat terkait akurasi dan juga durasi deteksi dan mitigasi pada sistem yang peneliti buat.

Metode Penelitian

A. Alur Penelitian

Pada gambar 1 berisikan alur penelitian yang akan peneliti lakukan untuk melakukan penelitian ini.



Gambar 1. Alur Penelitian

Berdasarkan gambar di atas peneliti melakukan penelitian ini dalam 4 tahap yaitu ;

a. Tahap Awal

Pada tahap awal peneliti melakukan identifikasi masalah dimana peneliti akan menemukan masalah yang menjadi landasan peneliti untuk melakukan penelitian ini. Setelah dilakukan identifikasi peneliti melakukan studi literatur yang akan berguna untuk menambah pengetahuan peneliti agar lebih luas terkait masalah yang telah peneliti tentukan.

b. Tahap perancangan SDN dengan algoritma SVM

Pada tahap ini peneliti melakukan observasi terkait server jaringan dimana pada tahap ini didapatkan hasil berupa topologi jaringan yang akan digunakan dalam penelitian. Setelah itu peneliti melakukan perancangan serangan DDOS. Pada tahap ini peneliti menentukan bagaimana serangan DDoS untuk melakukan tes pada sistem dilakukan. Pada tahap ini didapatkan hasil yaitu peneliti menggunakan *tools hping3* untuk melakukan serangan DDoS dan didapatkan skema penyerangan yang akan dilakukan untuk pengujian sistem. Setelah itu peneliti melakukan perancangan sistem deteksi dan mitigasi serangan DDoS dimana peneliti menggunakan *controller* ryu untuk mengkonfigurasi sistem. Pada sistem ini peneliti menggunakan algoritma SVM untuk melakukan deteksi dan mitigasi serangan DDoS.

c. Tahap pengujian SDN

Pada tahap pengujian SDN peneliti melakukan 2 tahap yaitu serangan pada server jaringan yang belum diterapkan sistem SDN dan serangan pada server jaringan yang sudah diterapkan sistem SDN dengan algoritma SVM. Pada tiap – tiap tahap serangan peneliti akan mengumpulkan data dari 2 tahap tersebut untuk melakukan tahapan terakhir pada penelitian ini.

d. Tahap akhir

Pada tahap akhir ini peneliti melakukan evaluasi dari data yang peneliti dapatkan di tahap sebelumnya. Evaluasi atau Analisa ini dilakukan untuk mengetahui perbedaan saat sebelum diterapkannya SDN dan setelah diterapkannya SDN dengan algoritma SVM.

B. Metode Pengumpulan Data

Metode pengumpulan data pada penelitian kali ini dilakukan dengan 2 metode. Metode pertama dilakukan dengan metode observasi. Tujuan dari observasi adalah deskripsi, pada penelitian kualitatif melahirkan teori dan hipotesis, atau pada penelitian kuantitatif digunakan untuk menguji teori dan hipotesis (Hasanah 2017). Peneliti melakukan observasi untuk menemukan bagaimana topologi jaringan dan arsitektur jaringan yang akan digunakan untuk melakukan penelitian ini. Berikutnya peneliti melakukan pengumpulan data dengan metode studi literatur. Studi literatur merupakan sebuah cara yang dapat dipakai untuk menghimpun data ataupun sumber yang berkaitan dengan topik yang akan dibahas dalam penelitian (Habsy 2017). Studi literatur berguna bagi penulis untuk menemukan teori – teori yang berguna dalam penelitian ini.

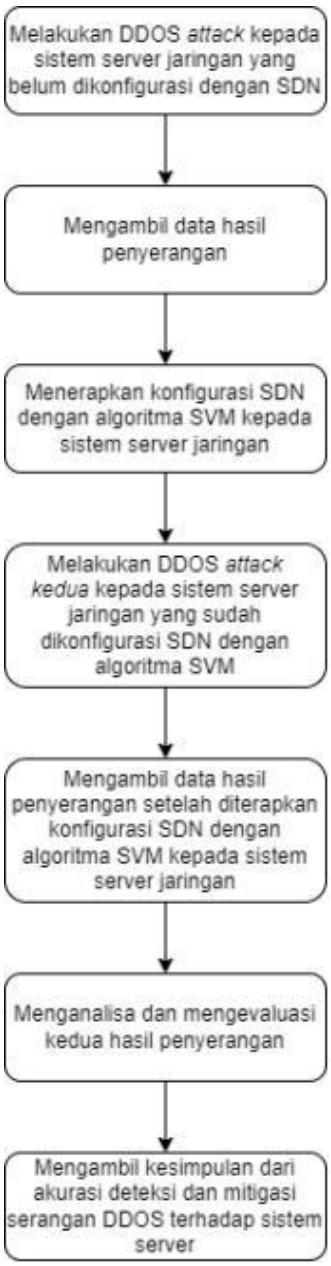
C. Metode Analisis Data

Analisis data yang dilakukan dari data yang didapatkan dari arus lalu lintas jaringan yang masuk pada server jaringan (*router*). Data yang akan diambil ada 6 data yaitu *speed of ip sources, speed of flow entries, flow count, ratio of pair flow, packet count,* dan *byte size.* Data – data ini diambil dari arus lalu lintas pada server jaringan lalu akan digunakan sebagai parameter dalam sistem deteksi dan mitigasi untuk menentukan arus lalu lintas mana yang termasuk dalam serangan DDoS. Data – data tersebut akan dimasukkan ke dalam *database* dan akan dilatih untuk dilakukannnya deteksi dan mitigasi serangan DDoS yang masuk pada server jaringan.

D. Metode Pengujian Data

Metode pengujian data dilakukan dengan beberapa tahap. Pada gambar 2 dapat terlihat tahapan pengujian data yang dilakukan pada penelitian ini. Pengujian data diawali dengan melakukan serangan DDoS pada server jaringan yang belum dikonfigurasi dengan SDN. Dari penyerangan yang dilakukan maka peneliti akan mengambil data dari hasil

pengujian data awal. Berikutnya peneliti akan menerapkan SDN pada server jaringan lalu melakukan uji coba dengan menyerang server jaringan dengan DDoS. Dari serangan yang telah dilakukan maka peneliti akan mengambil data terkait hasil dari pengujian kedua yang telah peneliti lakukan. Dari kedua hasil pengujian yang telah peneliti lakukan maka peneliti akan mengambil kesimpulan dari hasil pengujian tersebut.

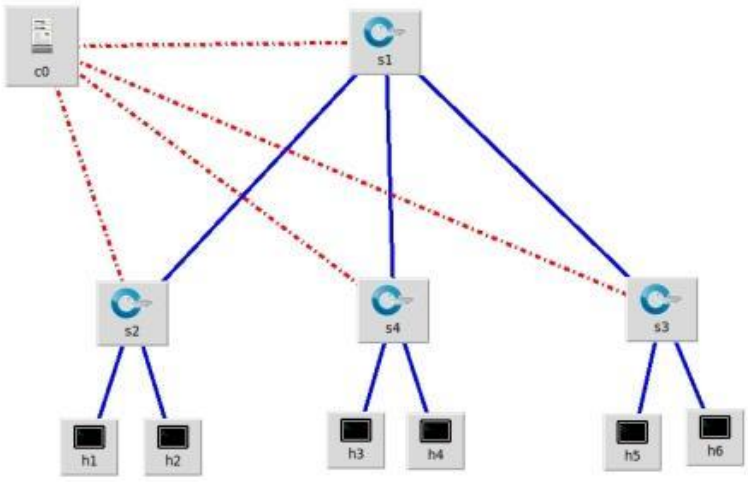


Gambar 2. Tahapan Pengujian Data

Hasil dan Diskusi

A. Topologi Yang Digunakan

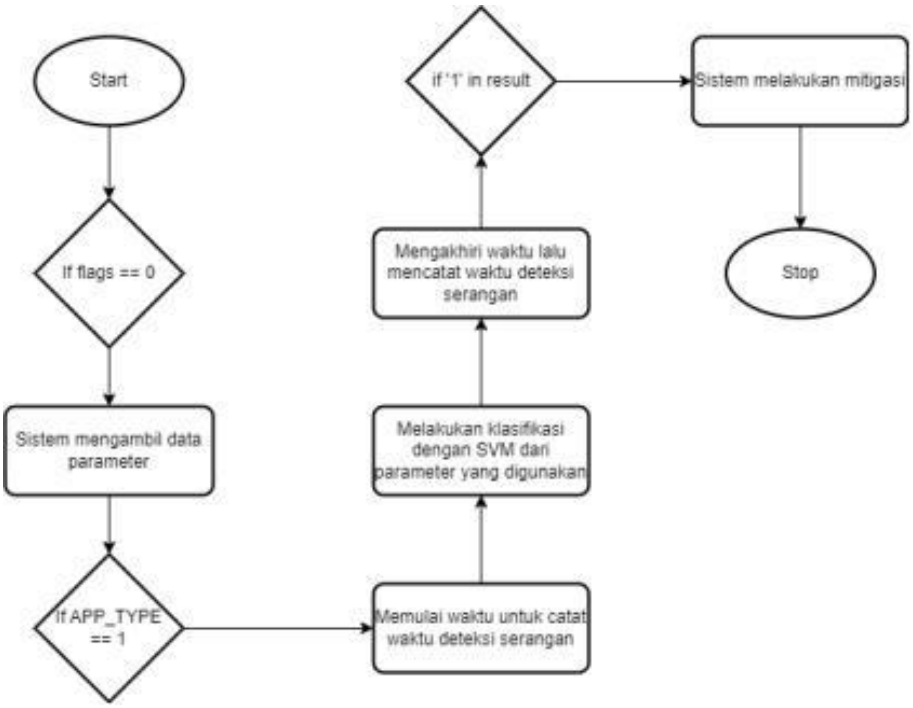
Topologi jaringan yang digunakan pada penelitian ini menggunakan 4 *router* dan 6 *host.* Pada *router* 2, 3, dan 4 masing masing terkoneksi langsung dengan 2 *host*. Pada *router* 1 akan langsung terkoneksi dengan 3 *router* lainnya yaitu *router* 2, 3, dan 4. Seluruh *router* akan terkoneksi dengan konfigurasi SDN yang telah dibuat. Topologi dijalankan pada mininet dengan menggunakan sistem operasi Ubuntu 20.04. Gambar topologi dapan dilihat pada gambar 3.



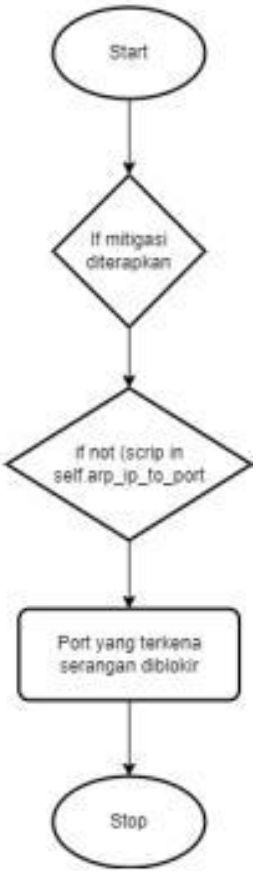
Gambar 3. Topologi Jaringan

B. Rancangan Sistem Deteksi dan Mitigasi Serangan DdoS

Pada sistem yang digunakan pada penelitian kali ini peneliti menggunakan SDN yang dikonfigurasikan dengan algoritma SVM. Sistem akan dibuat dengan bahasa pemrograman *python*. Penelunis menggunakan *python* dikarenakan bahasa tersebut lebih mudah untuk dimengerti dan sudah banyak yang menggunakan bahasa tersebut. *Controller* SDN yang digunakan pada sistem ini ialah RYU. RYU cukup mudah digunakan dan termasuk salah satu *controller* pertama dalam SDN dan sudah memiliki referensi yang banyak. Sistem SDN pada penelitian ini akan memiliki 2 fungsi yaitu mendeteksi serangan DDoS dan juga mitigasi serangan DDoS yang masuk pada server jaringan. Pada gambar 4 merupakan *flowchart* dari sistem deteksi DDoS pada SDN yang dibuat dalam penelitian ini. Sedangkan pada gambar 5 merupakan sistem mitigasi DDoS pada SDN.



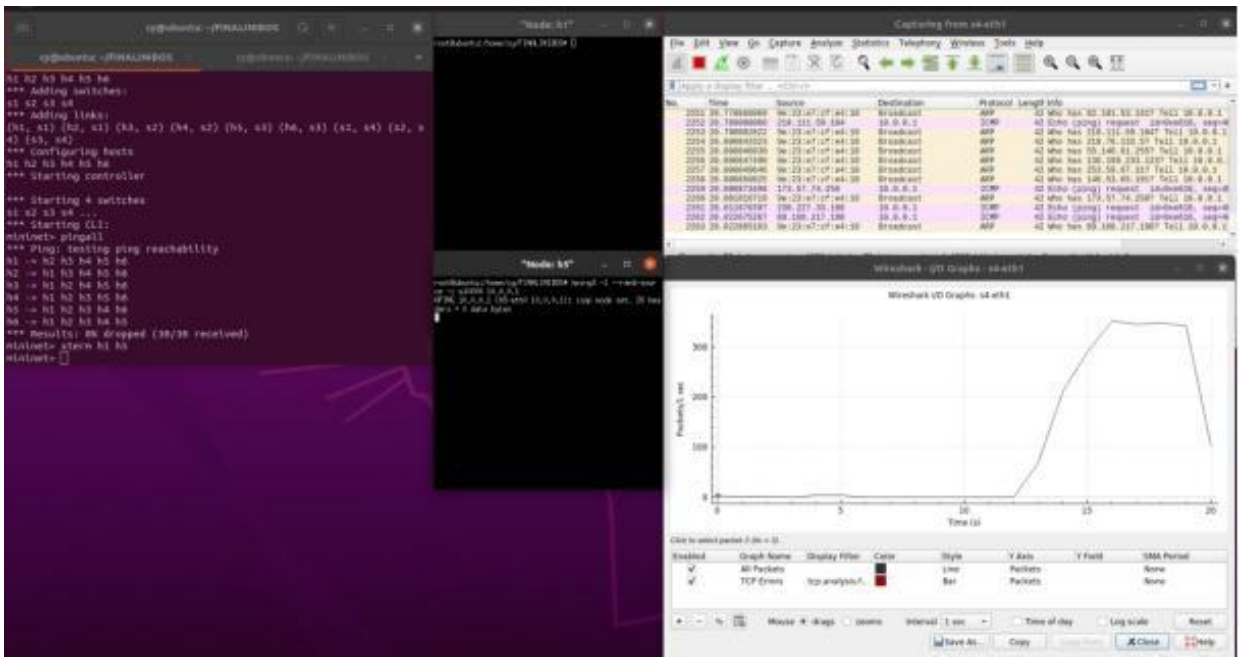
Gambar 4. Flowchart Sistem Deteksi DdoS



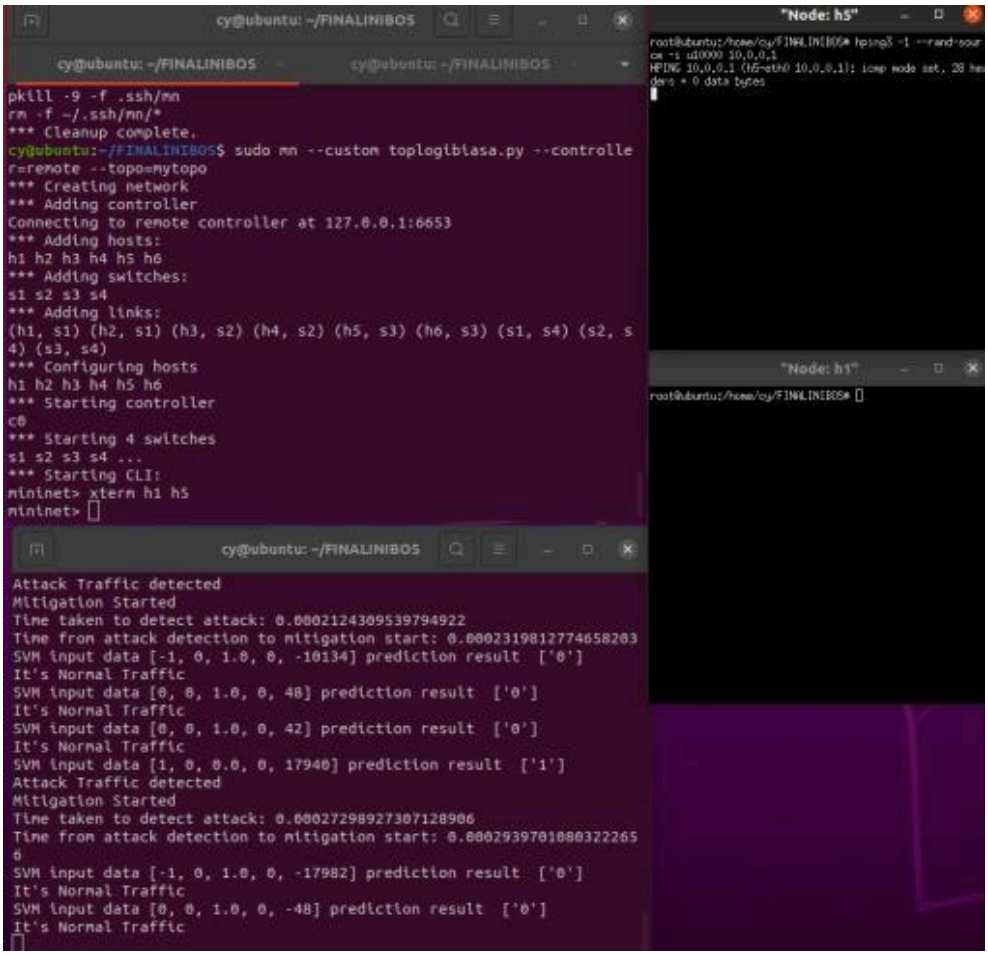
Gambar 5. Flowchart Sistem Mitigasi DDoS

C. Hasil Pengujian Sistem SDN

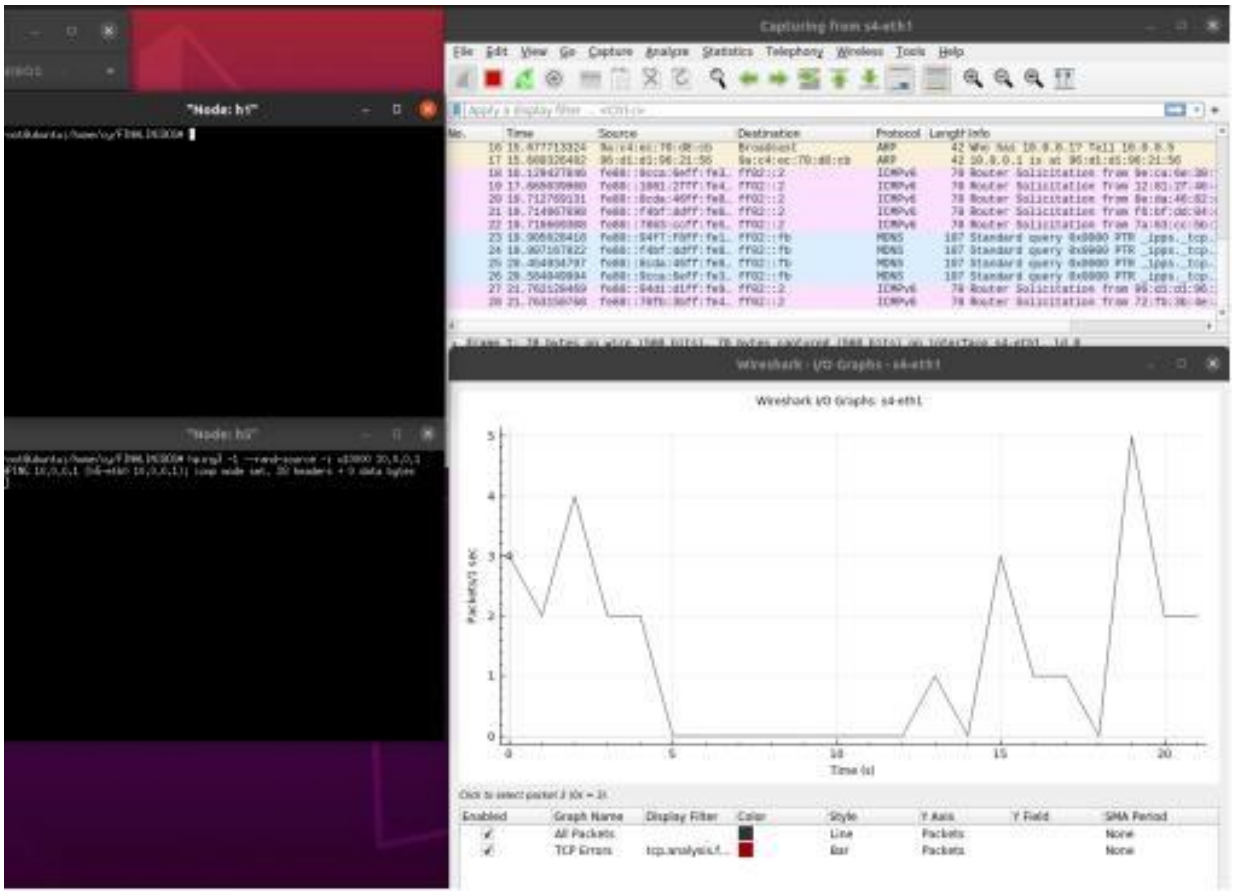
Pengujian sistem SDN dilakukan sesuai dengan metode pengujian yang telah dibuat. Pengujian pertama dilakukan dengan menyerang sistem server jaringan dengan serangan DDoS saat belum dikonfigurasikan dengan SDN. Serangan ini dilakukan dengan menggunakan *tools* DDoS yaitu *hping3*. Perintah yang digunakan untuk pengujian adalah "hping3 -1 –rand-source -I u10000 10.0.0.1" perintah ini akan melancarkan serangan DDoS dengan IP random kepada *host* 1 dengan IP 10.0.0.1. Pada pengujian juga menggunakan *tools* Wireshark untuk memonitor arus lalulintas jaringan. Hasil yang didapatkan dari pengujian ini yaitu paket yang masuk pada server jaringan mencapai 300 paket per detik seperti pada Gambar 6. Setelah melakukan pengujian pertama berikutnya dilanjut dengan pengujian kedua. Pada pengujian kedua server jaringan akan dikonfigurasikan dengan sistem SDN yang telah dibuat. Hal ini dilakukan dengan mengkoneksikan antara SDN yaitu *controller* ryu dengan router yang terdapat pada topologi jaringan. Setelah dilakukan koneksi maka dilancarkan serangan yang sama seperti serangan pada pengujian pertama yaitu menggunakan *tools hping3* dengan perintah "hping3 -l –rand-source -I u10000 10.0.0.1". Dari pengujian kedua didapatkan hasil yaitu paket yang masuk pada server jaringan tidak lebih dari 6 paket per detik seperti pada Gambar 8. Lalu pada Gambar 7 terlihat bahwa sistem SDN telah mendeteksi serangan DDoS yang masuk. Setelah itu dilakukan mitigasi dengan memblokir *port* sumber serangan.



Gambar 6. Hasil Serangan DDoS tanpa SDN dari Terminal dan Wireshark



Gambar 7. Hasil Serangan DDoS saat penerapan SDN melalui Terminal



Gambar 8. Hasil monitorin lalulintas jaringan melalui wireshark saat penerapan SDN

D. Pembahasan Hasil Testing

Dari hasil testing yang telah dilakukan dalam penelitian ini didapatkan hasil yaitu saat server jaringan yang belum dikonfigurasikan dengan sistem SDN diserang maka hal itu sangat berbahaya bagi server jaringan. Terbukti dari paket yang masuk sampai 300 paket per detik. Hal ini dikarenakan tidak adanya tindakan mitigasi maupun deteksi yang dilakukan dalam konfigurasi server jaringan. Namun, dengan diterapkannya sistem SDN ke dalam server jaringan hal ini terbukti dapat mendeteksi dan mitigasi serangan DDoS.

Dalam pengujian saat server jaringan dikonfigurasikan dengan sistem SDN didapatkan hasil yaitu paket yang masuk ke dalam server jaringan tidak sampai 6 paket per detik. Hasil ini tentu sangat signifikan berbeda dengan hasil yang didapatkan saat server jaringan tidak dikonfigurasikan dengan sistem SDN. Waktu deteksi dan mitigasi yang dilakukan saat serangan masuk tidak lebih dari 0.30ms terlihat pada gambar 9. Akurasi yang didapatkan dari sistem SDN ialah sebanyak 99.67%.

```
cy@ubuntu:~/FINALINIBOS/analysis$ python3 accuracy_score.py
Accuracy is  99.67948717948718
cross-validation score 0.9989304812834223
```

Gambar 9. Hasil Akurasi Sistem SDN

Kesimpulan

Kesimpulan dari penelitian ini adalah sistem SDN terbukti mampu untuk melakukan deteksi dan mitigasi serangan DDoS secara optimal. Terbukti dari hasil akurasi yaitu sebanyak 99.67% dan juga waktu yang dibutuhkan untuk deteksi dan mitigasi serangan yang tidak lebih dari 0.30ms. Dari hasil monitoring arus lalulintas jaringan juga terbukti bahwa sistem SDN dapat mendeteksi dan mitigasi serangan DDoS dimana penurunan angka paket masuk ke dalam server jaringan sangat signifikan. Pada hasil pengujian awal sebelum diterapkan SDN didapatkan hasil 300 paket per detik. Namun saat diterapkan SDN maka didapatkan hasil maksimal 5 paket per detik dimana tidak lebih dari 6 paket per detik.

Saran untuk penelitian berikutnya peneliti dapat menambahkan parameter dalam SVM sehingga mendapatkan hasil yang lebih akurat lagi. Penggunaan dataset yang lebih banyak lagi juga bisa dilakukan untuk mendapatkan hasil tingkat akurasi yang lebih tinggi. Topologi yang digunakan juga bisa lebih kompleks lagi seperti topologi data center.

Referensi

[1] Ardianto, Feby. 2020. "Penggunaan Mikrotik Router Sebagai Jaringan Server." *Penggunaan Router Mikrotik* (1): 26–31.

[2] Chris, Jodi, Jordan Sihombing, Dany Primanita Kartikasari, and Adhitya Bhawiyuga. 2019. "Implementasi Sistem Deteksi Dan Mitigasi Serangan Distributed Denial of Service (DDoS) Menggunakan SVM Classifier Pada Arsitektur Software-Defined Network (SDN)." *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer* 3(10): 9608–13. http://j-ptiik.ub.ac.id.

[3] Habsy, Bakhrudin All. 2017. "Seni Memehami Penelitian Kuliatatif Dalam Bimbingan Dan Konseling : Studi Literatur." *JURKAM: Jurnal Konseling Andi Matappa* 1(2): 90.

[4] Hasanah, Hasyim. 2017. "TEKNIK-TEKNIK OBSERVASI (Sebuah Alternatif Metode Pengumpulan Data Kualitatif Ilmu-Ilmu Sosial)." *At-Taqaddum* 8(1): 21. https://doi.org/10.21580/at.v8i1.1163.

[5] Karthika, P., and Karmel Arockiasamy. 2023. "Simulation of SDN in Mininet and Detection of DDoS Attack Using Machine Learning." *Bulletin of Electrical Engineering and Informatics* 12(3): 1797–1805. https://beei.org/index.php/EEI/article/view/5232/3249.

[6] Oo, Nan Haymarn, Aris Cahyadi Risdianto, Teck Chaw Ling, and Aung Htein Maw. 2020. "Flooding Attack Detection and Mitigation in SDN with Modified Adaptive Threshold Algorithm." *International Journal of Computer Networks and Communications* 12(3): 75–95.

Avrijsto Amandri Achyar
Fakultas Ilmu Komputer
Universitas Ary Ginanjar
Jl. TB. Simatupang Kav 1,
Jakarta Selatan, Indonesia

Andi Purnomo
Fakultas Ilmu Komputer
Universitas Ary Ginanjar
Jl. TB. Simatupang Kav 1,
Jakarta Selatan, Indonesia