JSAI: Journal Scientific and Applied Informatics
Vol. 7, No. 3, November 2024, hal. 531~536
E-ISSN: 2614-3054; P-ISSN: 2614-3062, accredited by Kemenristekdikti, Sinta 4
DOI: 10.36085

Analisis Serangan DDOS Menggunakan *Machine Learning* Pada Arsitektur *Software-Define Network*

[1]Hamid Rahman, [2]Tata Sutabri
[1,2]Universitas Bina Darma, Indonesia
[1]hamidrahman@live.com; [2]tata.sutabri@gmail.com

Article Info

Article history:

Received, 2024-11-06
Revised, 2024-11-14
Accepted, 2024-11-18

Kata Kunci:

DDoS
SDN
MLPC
benign
malicious

ABSTRAK

Arsitektur *Software-Defined Network* (SDN) menjadi solusi utama dalam meningkatkan efisiensi, fleksibilitas, dan skalabilitas dalam pengelolaan jaringan komputer. Dengan pemisahan antara lapisan kontrol dan data, SDN memungkinkan *administrator* jaringan untuk secara terpusat mengelola aturan di seluruh perangkat jaringan. Meskipun memberikan banyak keuntungan, desain ini juga membawa potensi resiko terhadap keamanan jaringan, terutama dari serangan *Distributed Denial of Service* (DDoS). Serangan DDoS dapat membanjiri *controller* SDN dengan trafik yang berlebihan, mengganggu fungsi pengaturan aliran data, dan berpotensi menyebabkan kegagalan jaringan secara keseluruhan. Oleh karena itu, deteksi dini terhadap serangan DDoS menjadi krusial untuk memastikan keberlanjutan dan kinerja optimal dalam jaringan SDN. Penelitian ini bertujuan untuk mengidentifikasi dan mengklasifikasikan lalu lintas data dalam arsitektur SDN, dengan memanfaatkan model *machine learning Multilayer Perceptron Classifier* (MLPC) untuk membedakan antara lalu lintas yang aman (benign) dan berbahaya (malicious). Dataset yang digunakan adalah DDoS *Attack* SDN *Dataset*, yang terdiri dari 23 fitur dengan total 104,345 data. Hasil uji coba menunjukkan bahwa model MLPC mencapai tingkat *accuracy* sebesar 99,05%, dengan *precision* dan *recall* masing-masing mencapai 99% dalam mendeteksi lalu lintas yang aman (*benign*) maupun lalu lintas yang berbahaya (*malicious*).

Keywords:

DDoS
SDN
MLPC
benign
malicious

ABSTRACT

Software-Defined Network (SDN) architecture is becoming a key solution in improving efficiency, flexibility and scalability in computer network management. By separating the control and data layers, SDN allows network administrators to centrally manage rules across network devices. While providing many advantages, this design also brings potential risks to network security, especially from Distributed Denial of Service (DDoS) attacks. DDoS attacks can overwhelm the SDN controller with excessive traffic, disrupt the data flow management function, and potentially lead to overall network failure. Therefore, early detection of DDoS attacks is crucial to ensure sustainability and optimal performance in SDN networks. This research aims to identify and classify data traffic in SDN architecture, by utilizing the Multilayer Perceptron Classifier (MLPC) machine learning model to distinguish between benign and malicious traffic. The dataset used is the DDoS Attack SDN Dataset, which consists of 23 features with a total of 104,345 data. The test results show that the MLPC model achieves an accuracy rate of 99.05%, with precision and recall each reaching 99% in detecting benign and malicious traffic.

Penulis Korespondensi:

Hamid Rahman,
Program Studi Magister Teknik Informatika,
Universitas Bina Darma,
Email: hamidrahman@live.com

JSAI: Journal Scientific and Applied Informatics
Vol. 7, No. 3, November 2024, hal. 531~536
E-ISSN: 2614-3054; P-ISSN: 2614-3062, accredited by Kemenristekdikti, Sinta 4
DOI: 10.36085

1. PENDAHULUAN

Dalam era digital yang semakin berkembang, *Software-Defined Network* (SDN) ditawarkan sebagai solusi inovatif untuk meningkatkan efisiensi, fleksibilitas, dan skalabilitas yang tinggi dalam pengelolaan jaringan komputer. SDN mempunyai sebuah konsep di mana kontrol jaringan komputer dipindahkan dari perangkat fisik (seperti *router* dan *switch*) ke suatu perangkat yang lebih terpusat [1], [2]. Dalam SDN, perangkat jaringan seperti *switch* hanya meneruskan *rule* yang dibuat, sedangkan pengambilan keputusan dan kemampuan logika kontrol dilakukan pada *controller* SDN [3]. Terlepas dari semua inovasi ini, beberapa komponen di lingkungan jaringan berbasis SDN menimbulkan beberapa ancaman keamanan tambahan pada pengontrol SDN. Keamanan dalam sebuah jaringan menjadi sangat penting karena merupakan hal utama agar dapat berbagi berbagai macam informasi serta dapat berkomunikasi [4], [5], [6]. Pada arsitektur SDN, keamanan dari *controller* SDN menjadi hal yang sangat penting dikarenakan *controller* biasanya hanya terdapat satu atau beberapa *controller* yang mengelola jaringan dalam skala besar. Jika *controller* pada arsitektur SDN diserang, maka seluruh jaringan yang dikelola oleh *controller* tersebut dapat terpengaruh, karena *controller* bertanggung jawab untuk mengatur seluruh aliran data di seluruh jaringan. Sehingga keamanan jaringan pada *controller* SDN menjadi tantangan utama dalam pengembangan jaringan berbasis SDN di masa depan. *Distributed Denial of Service* (DDoS) menjadi salah satu tantangan dalam jaringan SDN dikarenakan merupakan perbuatan terkait peretasan dalam suatu jaringan [7].

Serangan DDoS biasanya disebabkan oleh satu atau lebih dari satu bot, yang ditembus oleh perangkat lunak dari kode berbahaya. Serangan DDoS juga berusaha untuk mengganggu ketersediaan sumber daya jaringan dengan membanjiri sistem target dengan lalu lintas yang berlebihan, sehingga mengakibatkan penurunan kinerja atau bahkan kegagalan total dalam sebuah layanan [8], [9]. DDoS menjadi salah satu ancaman paling signifikan bagi infrastruktur jaringan modern. Dalam konteks SDN, serangan ini dapat menargetkan berbagai lapisan, termasuk *controller* yang merupakan pusat pengelolaan jaringan [10]. Ketika *controller* diserang, kapasitasnya untuk memproses permintaan dan mengelola aliran data dapat terganggu, yang pada gilirannya dapat menyebabkan dampak negatif terhadap seluruh jaringan [11]. Serangan DDoS dapat membanjiri *controller* SDN dengan trafik yang berlebihan, mengganggu fungsi pengaturan aliran data, dan berpotensi menyebabkan kegagalan jaringan secara keseluruhan. Oleh karena itu, deteksi dini terhadap serangan DDoS menjadi krusial untuk memastikan keberlanjutan dan kinerja optimal dalam jaringan SDN. Serangan DDoS juga dapat menargetkan berbagai lapisan dalam arsitektur SDN, termasuk perangkat *switch*, *API Northbound*, dan saluran komunikasi antara *controller* dan perangkat. Oleh karena itu, deteksi dan mitigasi serangan DDoS dalam lingkungan SDN menjadi hal yang sangat penting.

Beberapa pendekatan berbasis *Machine Learning* menawarkan solusi yang menjanjikan untuk mendeteksi serangan DDoS dengan lebih efisien. Dengan memanfaatkan teknik analisis data yang canggih, model *machine learning* dapat belajar dari pola lalu lintas jaringan dan mengidentifikasi aktivitas mencurigakan secara real-time. Perez-Diaz J et al. [12] menggunakan algoritma Random Tree, SVM, Random Forest, REP Tree, J48 dan MLP dalam mendeteksi *LR-DDoS Attacks* dengan akurasi yang didapatkan mencapai 95%. Ye J et al. [13], menggunakan metode SVM dalam mendeteksi DDoS *Attack* pada SDN dengan akurasi 95,24%. Sementara Tan L et al. [14], menggunakan metode *hybrid* dengan menggabungkan K-Mean dan K-Nearest Neighbors (KNN) dengan tingkat akurasi mencapai 98,85%. Meskipun hasil yang didapatkan cukup baik dalam mendeteksi serangan *DDoS,* tetapi model tersebut masih belum mampu menghasilkan performa yang maksimal dalam melakukan deteksi serangan *DDoS*.

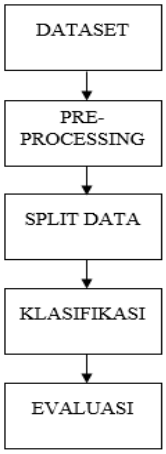
Di antara berbagai metode yang ada, algoritma *Multilayer Perceptron Classifier* (MLPC) dipilih untuk dalam mendeteksi serangan DDoS. MLPC menawarkan kemampuan untuk belajar dari pola yang lebih rumit dalam data melalui struktur jaringan saraf yang dalam. Penelitian ini bertujuan untuk mengeksplorasi efektivitas penggunaan MLPC dalam mendeteksi serangan DDoS pada arsitektur SDN. Dengan menganalisis metode ini, diharapkan dapat ditemukan pendekatan yang lebih efektif untuk meningkatkan keamanan jaringan SDN terhadap ancaman DDoS. Penelitian ini juga menggunakan metrik pengukuran performa seperti *accuracy, precision, recall* dan *F-measure* dalam melihat pendekatan *machine learning* yang efektif dalam melakukan identifikasi serangan DDoS pada arsitektur SDN.

Melalui penelitian ini, diharapkan dapat diperoleh pemahaman yang lebih baik mengenai mekanisme serangan DDoS dalam konteks SDN dan bagaimana pendekatan *machine learning* dapat diterapkan untuk mendeteksi ancaman tersebut secara efektif.

2. METODE PENELITIAN

Tahapan penelitian ini ditunjukkan pada gambar 1. Tahapan yang dilakukan pada penelitian ini terdiri dari mempersiapkan dataset, melakukan *pre-processing* terhadap data yang ada pada dataset, melakukan pembagian data, kemudian membuat model *machine learning* menggunakan algoritma MPLC untuk melakukan klasifikasi, dan terakhir evaluasi model tersebut.

JSAI: Journal Scientific and Applied Informatics
Vol. 7, No. 3, November 2024, hal. 531~536
E-ISSN: 2614-3054; P-ISSN: 2614-3062, accredited by Kemenristekdikti, Sinta 4
DOI: 10.36085



Gambar 1 Tahapan Penelitian

a) Mempersiapkan Dataset

Dataset yang digunakan pada penelitian ini adalah *DDoS Attack SDN Dataset* yang didapat dari *Mendeley Dataset [15].* Dataset ini total terdiri dari 23 kolom dan 104,345 baris dengan rincian 22 kolom *feature* satu kolom *label*. Kolom label pada dataset ini terdiri dari *binary* yaitu *malicious* (1) atau *benign* (0).

	dt	switch	src	dst	pktcount	bytecount	dur	dur_nsec	\
0	11425	1	10.0.0.1	10.0.0.8	45304	48294064	100	716000000	
1	11605	1	10.0.0.1	10.0.0.8	126395	134737070	280	734000000	
2	11425	1	10.0.0.2	10.0.0.8	90333	96294978	200	744000000	
3	11425	1	10.0.0.2	10.0.0.8	90333	96294978	200	744000000	
4	11425	1	10.0.0.2	10.0.0.8	90333	96294978	200	744000000	

	tot_dur	flows	...	pktrate	Pairflow	Protocol	port_no	tx_bytes	\
0	1.010000e+11	3	...	451	0	UDP	3	143928631	
1	2.810000e+11	2	...	451	0	UDP	4	3842	
2	2.010000e+11	3	...	451	0	UDP	1	3795	
3	2.010000e+11	3	...	451	0	UDP	2	3688	
4	2.010000e+11	3	...	451	0	UDP	3	3413	

	rx_bytes	tx_kbps	rx_kbps	tot_kbps	label
0	3917	0	0.0	0.0	0
1	3520	0	0.0	0.0	0
2	1242	0	0.0	0.0	0
3	1492	0	0.0	0.0	0
4	3665	0	0.0	0.0	0

[5 rows x 23 columns]

Gambar 2 Dataset Penelitian

b) Pre-Processing

Tahapan *Pre-Processing* bertujuan untuk menghasilkan data yang terstruktur sehingga dapat dengan mudah dilakukan komputasi [16]. Adapun tahapan *pre-processing* pada dataset ini terdiri dari :

1. Mengganti Kolom yang mempunyai nilai kategorikal menjadi nilai numerikal menggunakan *label encoding*.
2. Pemisahan kolom *feature* dan kolom *label.* Pemisahan kolom dilakukan agar model pembelajaran dapat menjadi lebih jelas dan terstruktur. Selain itu tujuan dilakukan pemisahan kolom *feature* dan kolom *label* dilakukan untuk membangun model *machine learning* yang lebih akurat, efisiensi, dan mudah diinterpretasi.

c) Split Data

Untuk melatih dan menguji model dari *machine learning*. Dibutuhkan pemisahan data menjadi data latih dan data uji. Data latih digunakan model *machine learning* untuk mempelajari pola dan relasi antara kolom *feature* dan kolom *tabel.* Sedangkan, data uji digunakan untuk mengevaluasi kinerja dari model yang telah dilatih. Pemisahan data ini juga bertujuan untuk mendapatkan gambaran tentang kinerja model yang di uji menggunakan metrik evaluasi. Pada penelitian ini dipilih 80% kombinasi data secara acak sebagai data *training* dan sisanya yaitu 20% kombinasi data dipilih sebagai data *testing*.

d) Klasifikasi

Klasifikasi dilakukan dengan menggunakan model *machine learning* yaitu: *MultiLayer Perceptron Classifier* (MLPC). Model MLPC merupakan salah satu jenis dari jaringan saraf tiruan. MLPC memiliki kemampuan untuk melakukan pembelaran dari suatu pola yang kompleks dalam sebuah data, sehingga diharapkan efektif untuk melakukan tugas klasifikasi. Adapun dalam proses klasifikasi ini dilakukan setelah dataset dibagi menjadi data *training* dan *testing*. Selama proses pelatihan, model belajar mengenal pola dari data *training* sehingga dapat menimalkan kesalahan dalam melakukan prediksi. Setelah model melakukan proses pembelajaran, selanjutnya model diuji menggunakan data *testing*. Proses ini menjadi penting untuk melihat seberapa baik model dapat memahami pola yang diperoleh dari data *training* ke data baru yang tidak terlihat sebelumnya.

e) Evaluasi

Confusion matrix digunakan untuk mengevaluasi performa suatu model *machine learning*. Dalam proses ini terdapat dua label data yaitu: positif dan negatif. Klasifikasi dari dua label ini akan menghasilkan empat kondisi yaitu: *true positive* (TP), *true negative* (TN), *false positive* (FP) dan *false negative* (FN). Pada Tabel 2 menggambarkan perbandingan kelas yang sebenarnya dengan kelas prediksi. TP merupakan banyaknya sampel positif yang diklasifikasikan dengan benar. TN merupakan banyaknya sampel negatif yang diklasifiksikan dengan benar. FN merupakan banyaknya sampel positif yang diklasifikasikan dengan salah. FP merupakan banyaknya sampel negatif yang diklasifikasikan dengan salah.

Tabel 1 Confusion Matrix

TP	FP
FN	TN

Nilai-nilai yang didapatkan pada *confusion matrix* digunakan untuk menghitung *performances metrics evaluation* yaitu *accuracy*, *precision*, *recall* dan *F-measure*. Tahapan ini akan menghasilkan kinerja *metrics evaluation* dari model yang telah dibuat.

Accuracy adalah penghitungan keseluruhan dari total data dalam melakukan klasifikasi [17].

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

Presisi didefinisikan sebagai persentase dari kelas positif yang diidentifikasi dengan benar yang dilabeli sebagai positif [18].

$$Presisi = \frac{TP}{FP+TP} \quad (2)$$

Recall adalah pengukuran contoh kelas positif yang teridentifikasi dengan benar dari contoh relevan yang berhasil diambil [19].

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

F-Measure didefinisikan sebagai ukuran di mana presisil dan recall ke dalam satu metrik untuk membuat sebuah penilaian menjadi seimbang [20].

$$F - Measure = \frac{2\ x\ Presisi\ x\ Recall}{Presisi+Recall} \quad (4)$$

3. HASIL DAN ANALISA

Pada penelitian ini dilakukan evaluasi pada model machine learning yang dibuat yaitu: *MultiLayer Perceptron Classifier* (MLPC). Model MLPC di evaluasi untuk melihat keefektifitasan model dalam mendeteksi serangan DDoS pada *Software-Defined Network* (SDN). Metrik performa digunakan dalam mengevaluasi keefektifitasan model ini. Metrik performa yang menjadi acuan ada: *accuracy*, *precision*, *recall*, *F-1 score*, dan *confusion matrix*. Metrik yang menjadi acuan menjadi sangat penting dalam memahami kekuatan dan kelemahan dari model yang dibuat. Tabel 2

menunjukkan ringkasan tentang metrik performa pada model *machine learning* yang dibuat. Tabel 2 juga menjelaskan seberapa baik model tersebut dapat mengklasifikasikan lalu lintas jaringan yang dikenali sebagai *benign* (0) atau *malicious* (1).

Tabel 2 Hasil Evaluasi Metric Performa

Report	Nilai	Kelas	
		0	**1**
Accuracy	0.9905		
Precision	0.9866	0.99	0.99
Recall	0.9892	0.99	0.99
F-1 Score	0.9879	0.99	0.99
Data		12613	8155

Model MLPC mendapatkan *accuracy* sebesar 99,05% dalam menentukan lalu lintas jaringan *benign* dan *malicious.* Selain dari itu, nilai *precision* dan *recall* dapat menunjukkan seberapa baik model MLPC dalam melakukan klasifikasi pada setiap kelas. Model MLPC mendapatkan nilai *precision* dan *recall* sebesar 99% dalam mendeteksi setiap kelas. Hal ini menunjukkan bahwa model MLPC mengidentifikasi dengan benar dari hampir semua contoh dari setiap kelas tetapi juga membuat sangat sedikit *false positive,* dimana trafik yang berbahaya dapat dikategorikan sebagai trafik yang aman. Tabel 3 menunjukkan jumlah benar dan salah dari model MLPC dalam menentukan trafik yang berbahaya ataupun aman.

Tabel 3 Hasil Confusion Matrix

TP	FP
12504	109
FN	TN
88	8067

4. KESIMPULAN

Penelitian ini berhasil mencapai tujuannya untuk mengeksplorasi dan menguji efektivitas penggunaan Multilayer Perceptron Classifier (MLPC) dalam mendeteksi serangan DDoS pada arsitektur Software-Defined Network (SDN), yang merupakan tantangan utama dalam menjaga keamanan controller SDN. Dengan memanfaatkan dataset DDoS Attack SDN Dataset, penelitian ini menunjukkan bahwa model MLPC mampu mendeteksi serangan DDoS dengan tingkat *accuracy* mencapai 99,05%, serta *precision* dan *recall* yang masing-masing mencapai 99%, yang menegaskan kemampuan model ini dalam membedakan lalu lintas yang aman dan berbahaya dengan akurat. Hasil ini membuktikan bahwa solusi berbasis machine learning, khususnya MLPC, efektif dalam meningkatkan keamanan jaringan SDN dengan mendeteksi potensi ancaman DDoS secara real-time, sehingga tujuan penelitian untuk mengidentifikasi metode deteksi yang lebih efisien dan dapat diandalkan telah tercapai. Pendekatan ini tidak hanya menawarkan solusi yang tepat untuk masalah keamanan SDN, tetapi juga membuka jalan bagi pengembangan sistem deteksi ancaman yang lebih adaptif dan berkinerja baik di masa depan.

REFERENSI

[1] Z. Shu, J. Wan, D. Li, J. Lin, A. V. Vasilakos, and M. Imran, "Security in Software-Defined Networking: Threats and Countermeasures," *Mobile Networks and Applications*, vol. 21, no. 5, pp. 764–776, Oct. 2016, doi: 10.1007/S11036-016-0676-X/METRICS.

[2] U. B. Clinton, N. Hoque, and K. Robindro Singh, "Classification of DDoS attack traffic on SDN network environment using deep learning," *Cybersecurity*, vol. 7, no. 1, Dec. 2024, doi: 10.1186/S42400-024-00219-7.

[3] Ö. Tonkal, H. Polat, E. Başaran, Z. Cömert, and R. Kocaoğlu, "Machine Learning Approach Equipped with Neighbourhood Component Analysis for DDoS Attack Detection in Software-Defined Networking," *Electronics 2021, Vol. 10, Page 1227*, vol. 10, no. 11, p. 1227, May 2021, doi: 10.3390/ELECTRONICS10111227.

[4] D. R. Akhiruddin and T. Sutabri, "ANALISIS PENINGKATAN KEAMANAN PADA SIMPLE NETWORK TIME PROTOCOL (SNTP) UNTUK MENDETEKSI CYBERCRIME DALAM AKTIFITAS

JARINGAN MENGGUNAKAN METODE FIREWALL," *Blantika: Multidisciplinary Journal*, vol. 1, no. 2, pp. 21–32, Feb. 2023, doi: 10.57096/BLANTIKA.V1I2.9.

[5] "Konsep Sistem Informasi - Tata Sutabri - Google Buku." Accessed: Nov. 06, 2024. [Online]. Available: https://books.google.co.id/books?id=uI5eDwAAQBAJ&printsec=frontcover&hl=id#v=onepage&q&f=false

[6] T. Sutabri, "Analisis sistem informasi," 2012, Accessed: Nov. 06, 2024. [Online]. Available: https://books.google.com/books/about/Analisis_Sistem_Informasi.html?hl=id&id=ro5eDwAAQBAJ

[7] N. Khasanah and T. Sutabri, "ANALISIS KEJAHATAN CYBERCRIME PADA PERETASAN DAN PENYADAPAN APLIKASI WHATSAPP," *Blantika: Multidisciplinary Journal*, vol. 1, no. 2, pp. 44–55, Feb. 2023, doi: 10.57096/BLANTIKA.V1I2.13.

[8] N. D.G., H. W, and A. K, "A Collaborative Approach to Detecting DDoS Attacks in SDN Using Entropy and Deep Learning," *Journal of Telecommunications and Information Technology*, Sep. 2024, doi: 10.26636/JTIT.2024.3.1609.

[9] M. W. Nadeem, H. G. Goh, V. Ponnusamy, and Y. Aun, "DDoS Detection in SDN using Machine Learning Techniques," *Computers, Materials & Continua*, vol. 71, no. 1, pp. 771–789, Nov. 2021, doi: 10.32604/CMC.2022.021669.

[10] W. Hill *et al.*, "DDoS in SDN: a review of open datasets, attack vectors and mitigation strategies," *Discover Applied Sciences*, vol. 6, no. 9, Sep. 2024, doi: 10.1007/S42452-024-06172-X.

[11] U. B. Clinton, N. Hoque, and K. Robindro Singh, "Classification of DDoS attack traffic on SDN network environment using deep learning," *Cybersecurity*, vol. 7, no. 1, Dec. 2024, doi: 10.1186/S42400-024-00219-7.

[12] J. A. Perez-Diaz, I. A. Valdovinos, K. K. R. Choo, and D. Zhu, "A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning," *IEEE Access*, vol. 8, pp. 155859–155872, 2020, doi: 10.1109/ACCESS.2020.3019330.

[13] J. Ye, X. Cheng, J. Zhu, L. Feng, and L. Song, "A DDoS Attack Detection Method Based on SVM in Software Defined Network," *Security and Communication Networks*, vol. 2018, no. 1, p. 9804061, Jan. 2018, doi: 10.1155/2018/9804061.

[14] L. Tan, Y. Pan, J. Wu, J. Zhou, H. Jiang, and Y. Deng, "A New Framework for DDoS Attack Detection and Defense in SDN Environment," *IEEE Access*, vol. 8, pp. 161908–161919, 2020, doi: 10.1109/ACCESS.2020.3021435.

[15] N. Ahuja, G. Singal, and D. Mukhopadhyay, "DDOS attack SDN Dataset," vol. 1, 2020, doi: 10.17632/JXPFJC64KR.1.

[16] D. Anggraini and T. Sutabri, "Pengembangan Aplikasi Penyaringan Spam e-Mail Menggunakan Teknik Machine Learning dengan Metode Support Vector Machines," *IJM: Indonesian Journal of Multidisciplinary*, vol. 2, no. 3, pp. 106–114, Apr. 2024, Accessed: Nov. 06, 2024. [Online]. Available: https://journal.csspublishing.com/index.php/ijm/article/view/720

[17] 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.

[18] M. Myint Oo, S. Kamolphiwong, T. Kamolphiwong, and S. Vasupongayya, "Advanced Support Vector Machine- (ASVM-) Based Detection for Distributed Denial of Service (DDoS) Attack on Software Defined Networking (SDN)," *Journal of Computer Networks and Communications*, vol. 2019, no. 1, p. 8012568, Jan. 2019, doi: 10.1155/2019/8012568.

[19] N. Ahuja, G. Singal, D. Mukhopadhyay, and N. Kumar, "Automated DDOS attack detection in software defined networking," *Journal of Network and Computer Applications*, vol. 187, p. 103108, Aug. 2021, doi: 10.1016/J.JNCA.2021.103108.

[20] D. Kumar, R. K. Pateriya, R. K. Gupta, V. Dehalwar, and A. Sharma, "DDoS Detection using Deep Learning," *Procedia Comput Sci*, vol. 218, pp. 2420–2429, 2022, doi: 10.1016/j.procs.2023.01.217.