Kumpulan jurnaL Ilmu Komputer (KLIK)
Volume 09, No 1 Februari 2022
ISSN: 2406-7857

ANALISIS PENERAPAN DEEP LEARNING UNTUK KLASIFIKASI SERANGAN TERHADAP KEAMANAN JARINGAN

I Made Suartana
Jurusan Teknik Informatika, Universitas Negeri Surabaya
Jalan Lidah Wetan, Surabaya (60213), 031-99421835
madesuartana@unesa.ac.id

Abstract

The growth of the information technology field necessitates newer and better methods for data and information security. Several methods in machine learning are tried to be applied to network security mechanisms. Classical methods in network security use the identification of traffic or network traffic as a critical component in detecting attacks. This mechanism becomes increasingly ineffective as the network scales and data usage increases. One of the solutions to overcome the increase in size and data is deep learning. This type of machine learning method used in security can perform extensive data analysis and is a recent innovation that tries to study information patterns to detect unauthorized entries into computer networks. This study tries to conduct a preliminary study to apply Deep Learning to classify network security attacks originating from attack datasets. Based on the trials conducted, Deep learning can classify attacks with good accuracy according to the Deep learning architectural model used.

Keywords*: Network Security Classification Deep Learning Machine Learning*

Abstrak

Pertumbuhan bidang teknologi informasi mengharuskan perlunya metode yang lebih baru dan lebih baik untuk keamanan data dan informasi. Terdapat beberapa metode dalam pembelajaran mesin yang dicoba diterapkan untuk mekanisme pengaman jaringan. Metode klasik dalam keamanan jaringan menggunakan identifikasi lalu lintas atau trafik jaringan sebagai komponen kunci dalam mendeteksi serangan. Mekanisme ini semakin menjadi tidak efektif karena peningkatan skala jaringan dan penggunaan data. Solusi mengatasi peningkatan ukuran dan data salah satunya dengan Deep learning. Jenis metode pembelajaran mesin ini digunakan dalam keamanan dapat melakukan analisis data dalam ukuran besar dan merupakan inovasi terbaru yang mencoba mempelajari pola informasi dengan tujuan mendeteksi entri yang tidak sah ke dalam jaringan komputer. Penelitian ini mencoba melakukan studi awal untuk menerapkan Deep Learning untuk klasifikasi serangan keamanan jaringan yang berasal dari dataset serangan. Berdasarkan ujicoba yang dilakukan Deep learning dapat melakukan klasifikasi serangan dengan akurasi yang baik sesuai dengan model arsitektur Deep learning yang digunakan.

Kata kunci*: Keamanan Jaringan, Klasifikasi, Deep Learning, Mesin Learning*

1. PENDAHULUAN

Keamanan jaringan merupakan komponen penting dalam bidang teknologi informasi karena memberikan strategi preventif untuk melindungi infrastruktur fisik dan perangkat lunak dari serangan. Dengan masifnya penggunaan Jaringan komputer sampai skala global (internet), mengakibatkan jumlah data yang dihasilkan oleh jaringan terus meningkat. Termasuk juga peningkatan penggunaan komponen teknologi informasi, yang meliputi perangkat-perangkat fisik jaringan, sistem operasi, dan aplikasi. Hal ini juga menimbulkan efek negatif dari segi keamanan.

Salah satu mekanisme keamanan yang bersifaat preventif yaitu *Network Intrusion Detection System* (NIDS). NIDS membantu administrator sistem untuk mendeteksi pelanggaran keamanan yang terjadi dalam jaringan. Namun, banyak tantangan muncul ketika mengembangkan NIDS yang secara fleksibel dan efektif untuk mendeteksi serangan yang tak terduga[1][2]. Mekanisme keamanan jaringan banyak yang menggunakan identifikasi lalu lintas atau trafik jaringan sebagai komponen kunci dalam mendeteksi serangan. Mekanisme ini semakin menjadi tidak efektif karena peningkatan skala jaringan dan penggunaan data dalam tafik jaringan.

Penelitian terkait keamanan jaringan telah mengaplikasikan banyak algoritma pembelajaran mesin dan data mining untuk identifikasi serangan terhadap keamanan jaringan[3]. Seperti : Penggunaan metode Echo State Network (ESN) dan Recurrent Neural Network (RNN) untuk mengklasifikasikan data atau contoh malware[4]. Aplikasi algoritma deep learning untuk deteksi intrusi jaringan dengan skema deteksi intrusi hibrida berbasis anomali dengan menggabungkan DBN dan SVM untuk mengklasifikasikan intrusi jaringan menjadi dua hasil: normal atau serangan[5]. Sistem deteksi anomali semi- supervisi berdasarkan RBM diusulkan[6], [7] di mana classifier dilatih hanya dengan data lalu lintas normal, sehingga pengetahuan tentang perilaku anomali dapat berkembang secara dinamis.

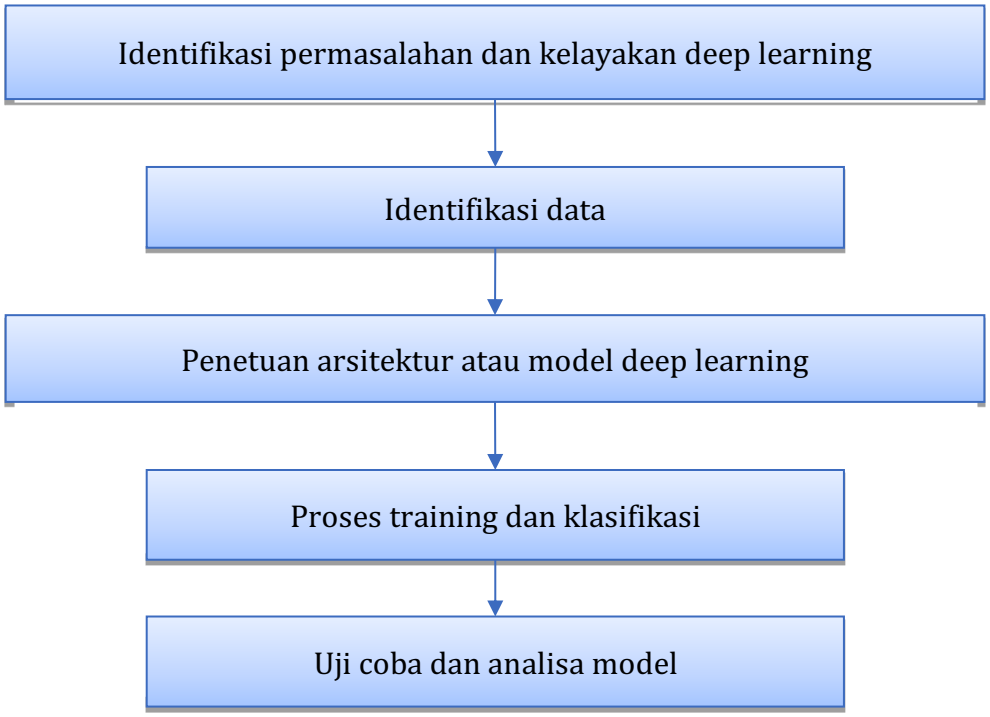
Deep learning belakangan ini menjadi terkenal karena potensinya untuk pembelajaran mesin. Deep learning dapat dijadikan bagian integral dari keamanan jaringan karena memastikan evaluasi yang menyeluruh dan meyakinkan dari sistem keamanan jaringan. Deep learning dapat didefinisikan sebagai penggunaan jaringan syaraf tiruan secara mendalam yang dihubungkan menggunakan beberapa lapisan untuk menghasilkan output[8]. Hasil dari fase sebelumnya dijadikan sebagai input agar dapat menghasilkan suatu luaran. Algoritma Deep Learning (DL) telah membentuk peran kunci dalam memecahkan masalah yang rumit, berkat berbagai keunggulannya dibandingkan dengan teknik Machine Learning (ML) tradisional lainnya. DL didefinisikan sebagai beberapa algoritma ML multi-lapis yang kuat dalam mempelajari abstraksi tingkat tinggi dari data skala besar yang kompleks. Algoritma DL biasanya mempelajari representasi fitur menggunakan banyak lapisan tersembunyi non-linear yang membuat rekayasa fitur otomatis.

Untuk meningkatkan tingkat akurasi dari proses deteksi serangan keamanan jaringan, banyak metode yang digunakan termasuk menggunakan pembelajaran mesin. Pembelajaran mesin banyak digunakan dalam proses kalsifikasi dan deteksi terhadap serangan keamanan jaringan. Penerapan Deep Learning yang merupakan salah satu algoritma pembelajaran mesin sangat diperlukan untuk meningkatkan

akurasi dalam mekanisme deteksi serangan terhadap keamana jaringan. Sehingga kedepannya diharapkan dapat meningkatkan keamanan data dan informasi yang dilewatkan pada jaringan komputer. Penelitian ini menggunakan Deep Learning untuk melakukan klasifikasi terhadap dataset serangan NSL_KDD. Hasil klasifikasi awal diharapkan dapat memberikan analisis penerapan Deep Learning dalam proses klasifikasi serangan terhadap keamanan jaringan. Evaluasi hasil klasifikasi dengan Deep Learning dianalisis berdasarkan pada metrik: akurasi, *precision*, dan *f-measure.*

2. METODOLOGI PENELITIAN

Tahapan penelitian digambarkan pada gambar 1 Pertama, identifikasi masalah yang sebenarnya untuk mendapatkan solusi yang tepat, kelayakan Deep Learning sebagai metode yang diusilkan untuk proses klasifikasi juga harus diperiksa (apakah sesuai atau tidak). Tahap kedua mengidentifikasi data yang relevan yang harus sesuai dengan masalah aktual dan harus disiapkan sesuai dengan kebutuhan. Tahap ketiga penentuam arsitektur dan model Deep Learning yang tepat. Tahap keempat, menggunakan algoritma dalam proses *training* dataset, dan tahap terakhir, pengujian dan analisis hasil.



Gambar 1. Tahapan penelitian

2.1. Dataset

Data yang digunakan untuk proses klasifikasi adalah dataset NSL-KDD. NSL-KDD adalah kumpulan data yang disarankan untuk memecahkan beberapa masalah yang melekat pada kumpulan data KDD'99[9]. KDD merupakan data hasil

pencatatan trafik jaringan nyata yang berfokus pada jaringan kabel. Dalam dataset ini ada 3 grup fitur yaitu: fitur dasar, *content based* dan *time based features*. KDD memiliki 41 fitur yang akan membantu untuk mengimplementasikan berbagai jenis pengklasifikasi. Data terdapat 4 kelas serangan yang berbeda: *Denial of Service* (DoS), *Probe, User to Root* (U2R), dan *Remote to Local* (R2L), seperti pada tabel 1. DoS adalah serangan yang mencoba mematikan arus lalu lintas ke dan dari sistem target. IDS dibanjiri dengan jumlah lalu lintas yang tidak normal, yang tidak dapat ditangani oleh sistem, dan dimatikan untuk melindungi dirinya sendiri. Ini mencegah lalu lintas normal mengunjungi jaringan. Probe atau pengawasan adalah serangan yang mencoba untuk mendapatkan informasi dari sebuah jaringan. Tujuannya di sini adalah untuk bertindak seperti pencuri dan mencuri informasi penting dalam lalu-lintas jaringan. U2R adalah serangan yang dimulai dengan akun pengguna biasa dan mencoba untuk mendapatkan akses ke sistem atau jaringan, sebagai pengguna super (*root*). Penyerang mencoba untuk mengeksploitasi kerentanan dalam sistem untuk mendapatkan hak akses root.

Tabel 1. Karateristik Dasar Dataset KDD

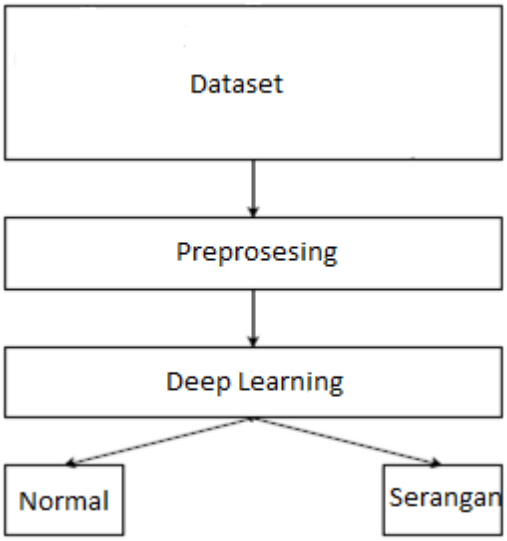
	Anomaly		Misuse		Normal
Dataset	DoS	Probe	U2R	R2L	
10 % KDD	391458	4107	52	1126	97277
Corrected KDD	229853	4166	70	16347	60593
Seluruh KDD	3883370	41102	52	1126	972780

2.2. Proses Training dan Klasifikasi

Proses Training dan klasifikasi serangan ditampilkan pada Gambar 2 klasifikasi data jaringan dilakukan dengan terlebih dahulu mengklasifikasikan data kedalam kelas serangan atau tidak (data serangan atau data normal). Kelas klasifikasi kemudian digunakan sebagai fitur data tambahan saat mengklasifikasikan data ke kategori serangan.
Proses klasifikas dijelaskan sebagai berikut:

a. Preprocessing data.
b. Membagi data untuk proses training(pelatihan) dan proses uji.
c. Proses training data untuk memprediksi label "serangan atau tidak" dengan
d. Prediksi/pengujian kategori serangan dengan data uji
e. Terapkan metrik kinerja untuk mengukur seberapa baik sistem dalam melakukan klassifikasi data

Pada penelitian ini tujuan utamanya adalah menerapkan proses klasifikasi dengan menggunakan teknik Deep Learning, sebagai bahan analisis teknik klasifikasi untuk data serangan pada jaringan[10].



Gambar 2. Langkah-langkah Training dan Klasifikasi

Algoritma Deep Learning dibangun dengan beberapa lapisan (layer) yang terhubung yang terdiri dari:

a. Lapisan pertama disebut *Input* Layer
b. Lapisan terakhir disebut *Output* Layer
c. Semua lapisan di antaranya disebut *Hidden* Layer.

Kata *deep* (mendalam) berarti jaringan bergabung dengan neuron dalam lebih dari dua lapisan. Setiap lapisan tersembunyi terdiri dari neuron, dan neuron terhubung satu sama lain. Neuron akan memproses dan kemudian menyebarkan sinyal input yang diterima lapisan di atasnya. Kekuatan sinyal yang diberikan neuron pada lapisan berikutnya tergantung pada berat, bias dan fungsi aktivasi. Jaringan mengkonsumsi sejumlah besar data input dan mengoperasikannya melalui berbagai lapisan; jaringan dapat mempelajari fitur data yang semakin kompleks pada setiap lapisan.

2.3. Metriks Akurasi

Evaluasi kinerja proses *learning* dan klasifikasi berdasarkan pada metric[11] Akurasi: Didefinisikan sebagai persentase dari data yang terklasifikasi dengan benar terhadap jumlah total data.

a. Precision (P)

Precision (P): Didefinisikan sebagai rasio % dari jumlah data true positive (TP) dibagi dengan jumlah true positive (TP) dan false positive (FP) data yang terklasifikasi.

$$P = \frac{TP}{(TP + FP)} \; x \; 100\%$$

b. Recall (R)

Recall (R): Didefinisikan sebagai rasio % jumlah data true positive (TP) dibagi dengan jumlah true positive (TP)dan false negative (FN) yang diklasifikasikan catatan.

$$P = \frac{TP}{(TP + FN)}\ x\ 100\%$$

c. F-Measure (F)

F-Measure (F): Didefinisikan sebagai rata-rata harmonik dari Precision (P) dan Recall (R) dan mewakili keseimbangan di antara keduanya.

$$F\ \frac{2.P.R}{(\ P + R\ )}\ x\ 100\%$$

3. HASIL DAN PEMBAHASAN

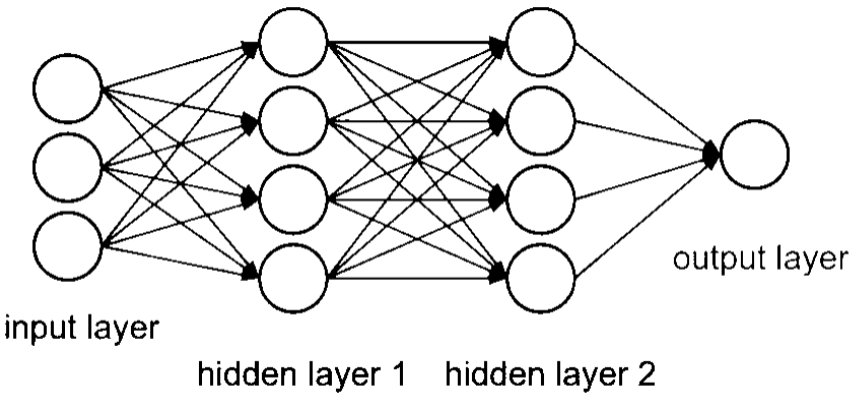
Pada penelitian ini pengujian dilakukan dengan mengekstraksi 125.973 instance dari dua kelompok trafik (Normal dan Anomaly) pada dataset NSL-KDD. Gambar 3 contoh ilustrasi data NSL-KDD yang digunakan pada proses uji coba

No.	1: duration	2: protocol_type	3: service	4: flag	5: src_bytes	6: dst_bytes	7: land	8: wrong_fragment	9: urgent	10: hot	11: num_failed_logins	12: logged_in
	Numeric	Nominal	Nominal	Nominal	Numeric	Numeric	Nominal	Numeric	Numeric	Numeric	Numeric	Nominal
125951	0.0	udp	private	SF	28.0	0.0	0	3.0	0.0	0.0	0.0	0
125952	0.0	tcp	http	SF	254.0	555.0	0	0.0	0.0	0.0	0.0	1
125953	0.0	tcp	smtp	SF	1289.0	408.0	0	0.0	0.0	0.0	0.0	1
125954	0.0	tcp	auth	S0	0.0	0.0	0	0.0	0.0	0.0	0.0	0
125955	0.0	tcp	http	SF	269.0	10939.0	0	0.0	0.0	0.0	0.0	1
125956	0.0	tcp	http	REJ	0.0	0.0	0	0.0	0.0	0.0	0.0	0
125957	0.0	icmp	eco_i	SF	30.0	0.0	0	0.0	0.0	0.0	0.0	0
125958	1.0	tcp	smtp	SF	1247.0	327.0	0	0.0	0.0	0.0	0.0	1
125959	0.0	tcp	private	S0	0.0	0.0	0	0.0	0.0	0.0	0.0	0
125960	0.0	tcp	http	SF	373.0	4777.0	0	0.0	0.0	0.0	0.0	1
125961	0.0	tcp	http	SF	329.0	885.0	0	0.0	0.0	0.0	0.0	1
125962	0.0	tcp	http	SF	236.0	2698.0	0	0.0	0.0	0.0	0.0	1
125963	0.0	udp	domai...	SF	33.0	0.0	0	0.0	0.0	0.0	0.0	0
125964	0.0	tcp	http	SF	334.0	1600.0	0	0.0	0.0	0.0	0.0	1

Gambar 3. Dataset KDD

3.1. Training data

Pada penelitian ini proses klasifikasi dicoba dengan menggunakan kombinasi dua *layer* dan kombinasi jumlah *node* per masing-masing *layer*. Untuk kombinasi jumlah *layer* dengan menggunakan *single* dan *dual layer* dengan kombinasi jumlah node 2-20 per masing-masing layer. Gambar 4 memberikan ilustrasi *layer* dan *node* Deep Neural Network, sedangkan hasil proses klasifikasi disajikan pada tabel 1 untuk *single layer* dan tabel 2 untuk penggunaan *dual layer*.



Gambar 4 Ilustrasi *layer* dan *node* pada Deep Neural Network

Mendefinisikan topologi jaringan saraf harus diselesaikan sebelum pelatihan. Menentukan lapisan input dan output relatif mudah. Untuk percobaan yang dilakukan dalam penelitian ini, delapan belas neuron digunakan untuk lapisan input, satu neuron untuk setiap fitur. Dua neuron digunakan untuk lapisan output, satu neuron untuk setiap klasifikasi yang mungkin. Ketika jumlah neuron meningkat, fungsi hipotesis jaringan saraf menjadi lebih kompleks. Menggunakan lebih dari satu lapisan tersembunyi memungkinkan untuk mengimplementasikan fungsi yang lebih kompleks pada data. Fungsi hipotesis yang terlalu kompleks atau dikenal sebagai overfitting. Menemukan hipotesis dengan kesalahan pelatihan minimum akan menghasilkan hasil yang paling cocok. Sebaliknya, jika fungsi hipotesis kurang kompleks daripada data, kesalahan generalisasi akan tinggi. Ini dikenal sebagai underfitting.

Karena pola dan hubungan dalam data menjadi lebih kompleks, jumlah lapisan tersembunyi yang diperlukan untuk mempelajari peningkatan hubungan nonlinier. Untuk mensimulasikan persamaan nonlinear seperti itu, pengujian beberapa konfigurasi lapisan tersembunyi dilakukan dengan menggunakan dua set data berlabel *split-level*. Jumlah optimal lapisan ditentukan dengan menjalankan tes pada satu lapisan dengan 2 hingga 20 neuron. Jumlah neuron yang menghasilkan akurasi atau skor-f terbesar dengan jumlah waktu pelatihan paling sedikit kemudian dipertahankan konstan sambil memvariasikan lapisan kedua neuron dari 2 hingga 20. Lapisan yang menghasilkan akurasi atau skor-f terbesar dipilih sebagai konfigurasi lapisan tersembunyi paling optimal.

Analisis topologi *single layer* untuk dataset ditunjukkan pada Tabel 2, kombinasi jumlah neuron pada *single hidden layer* menghasilkan akurasi terbaik untuk dataset ini. Penambahan jumlah neuron tidak mempengaruhi hasil klasifikasi.

Tabel 2. *Single Layer*

Node	Accuracy	Precission	Recall	F-Score	Waktu(s)	Epoch
2	91%	0.917	0.910	0.911	0.01	500
4	91%	0.917	0.910	0.911	0.13	500

6	91%	0.917	0.910	0.911	0.14	500
8	91%	0.917	0.910	0.911	0.16	500
10	91%	0.917	0.910	0.911	0.19	500
12	91%	0.917	0.910	0.911	0.2	500
14	91%	0.917	0.910	0.911	0.21	500
16	91%	0.917	0.910	0.911	0.25	500
18	91%	0.917	0.910	0.911	0.28	500
20	91%	0.917	0.910	0.911	0.3	500

Hasil topologi *dual layer* untuk dataset ditunjukkan pada Tabel 3. 6 dan 16 hidden neuron tersembunyi menghasilkan akurasi terbaik untuk dataset ini.

Tabel 3. *Dual Layer*

Hiddel Layer	Accuracy	Precission	Recall	F-Score	Waktu(s)	Epoch
2	84%	0.838	0.840	0.839	0.12	500
4	95%	0.951	0.950	0.950	0.18	500
6	97%	0.970	0.970	0.970	0.32	500
8	96%	0.960	0.960	0.960	0.39	500
10	96%	0.960	0.960	0.960	0.53	500
12	96%	0.960	0.960	96%	0.64	500
14	91%	0.913	0.910	0.911	0.8	500
16	97%	0.970	0.970	0.970	1.02	500
18	95%	0.950	0.950	0.950	1.38	500
20	95%	0.950	0.950	0.950	1.46	500

Hasil klasifikasi dengan dataset yang dingunakan ditunjukkan pada Tabel 4 Kelas 0 berarti bahwa data sampel merupakan data normal atau bukan bukan serangan. Kelas 1 adalah data anomaly atau kemungkinan serangan. Hasil terbaik ditunjukkan pada double layer dengan jumlan neuron 6 dan 16 masing-masing hiden layer

Tabel 4. Hasil spesifik kelas untuk kategorisasi serangan.

Kelas	Precission	Recall	F-Measure
0	0.970	0.985	0.977
1	0.970	0.941	0.955
Rata-rata	0.970	0.970	0.970

Hasilnya menunjukkan bahwa algoritma klasifikasi berfungsi dengan baik dengan data ini. Skor meningkat bahkan lebih setelah pengurangan fitur dengan classifier yang sama. Skor recall sangat baik (0.985 untuk kelas normal dan 0,941 untuk kelas anomally). Presisi untuk kelas 0 dan 1 sama (0.970).

Klasifikasi memiliki masalah dalam membedakan antara kelas serangan dan sebagian besar dapat mengklasifikasikan serangan. Namun, itu dapat secara akurat mengklasifikasikan data jaringan normal. Klasifikasi memiliki banyak masalah

umum dalam pembelajaran mesin. Jumlah data yang besar, kurangnya memori dan ketidakseimbangan antara ukuran kelas adalah masalah yang paling umum.

4. SIMPULAN

Berdasarkan hasil percobaan yang dilakukan dalam penelitian ini menunjukkan bahwa dataset dapat diklasifikasikan dengan dengan algoritma Deep Learning dan dapat mendeteksi aktivitas abnormal. Hasil untuk deteksi data normal dengan nilai 0.985 untuk recall data normal dan 0.941 presisi untuk sampel data Serangan. Algoritma deep learning baik dalam mendeteksi data normal dan data anomaly dengan baik dilihat dari hasil yang tidak berbeda jauh.

DAFTAR PUSTAKA

[1] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 41–50, Feb. 2018, doi: 10.1109/TETCI.2017.2772792.

[2] Bima Putra Firdaus and I Made Suartana, "Implementasi Keamanan Jaringan Intrusion Detection/Prevention System Menggunakan Pfsense," *JMI (Jurnal Manajemen Informasi)*, vol. 11, no. 1, pp. 40–47, 2020.

[3] B. Dong and X. Wang, "Comparison deep learning method to traditional methods using for network intrusion detection," in *2016 8th IEEE International Conference on Communication Software and Networks (ICCSN)*, Jun. 2016, pp. 581–585. doi: 10.1109/ICCSN.2016.7586590.

[4] R. Pascanu, J. W. Stokes, H. Sanossian, M. Marinescu, and A. Thomas, "Malware classification with recurrent networks," in *2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Apr. 2015, pp. 1916–1920. doi: 10.1109/ICASSP.2015.7178304.

[5] M. A. Salama, H. F. Eid, R. A. Ramadan, A. Darwish, and A. E. Hassanien, "Hybrid Intelligent Intrusion Detection Scheme," 2011, pp. 293–303. doi: 10.1007/978-3-642-20505-7_26.

[6] U. Fiore, F. Palmieri, A. Castiglione, and A. de Santis, "Network anomaly detection with the restricted Boltzmann machine," *Neurocomputing*, vol. 122, pp. 13–23, Dec. 2013, doi: 10.1016/j.neucom.2012.11.050.

[7] S. Mahdavifar and A. A. Ghorbani, "Application of deep learning to cybersecurity: A survey," *Neurocomputing*, vol. 347, pp. 149–176, Jun. 2019, doi: 10.1016/j.neucom.2019.02.056.

[8] B. Kolosnjaji, A. Zarras, G. Webster, and C. Eckert, "Deep Learning for Classification of Malware System Call Sequences," 2016, pp. 137–149. doi: 10.1007/978-3-319-50127-7_11.

[9] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, Jul. 2009, pp. 1–6. doi: 10.1109/CISDA.2009.5356528.

[10] K. L. Moore, T. J. Bihl, K. W. Bauer, and T. E. Dube, "Feature extraction and feature selection for classifying cyber traffic threats," *The Journal of Defense*

Modeling and Simulation: Applications, Methodology, Technology, vol. 14, no. 3, pp. 217–231, Jul. 2017, doi: 10.1177/1548512916664032.

[11] T.-T. Wong, "Linear Approximation of F-Measure for the Performance Evaluation of Classification Algorithms on Imbalanced Data Sets," *IEEE Transactions on Knowledge and Data Engineering*, vol. 34, no. 2, pp. 753–763, Feb. 2022, doi: 10.1109/TKDE.2020.2986749.