Journal of Science and Social Research ISSN 2615 – 4307 (Print)
Nov 2024, VII (4): 1866 – 1874 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

INTRUSION DETECTION SYSTEM BERBASIS DEEP LEARNING UNTUK PENINGKATAN MITIGASI SQL INJECTION DAN SYN FLOOD ATTACK

Sahren[1], Adi Prijuna Lubis[2]
Universitas Royal
e-mail: sahren.one@gmail.com

Abstract: *Intrusion Detection Systems (IDS) are often unable to keep up with the speed of attack development, leaving gaps that can be exploited by attackers. This research aims to protect network infrastructure from increasingly complex security threats. In this research, the author proposes the use of the VGG-16 CNN architecture Deep Learning model in the Intrusion Detection System to mitigate SqL Injection and Syn Flood attacks with a more in-depth process, namely by applying initial data normalization and augmentation techniques as a way to increase training data variation and reduce overfitting. Public dataset used CICDDoS2019 and CSE-CIC-IDS2018. By utilizing the power of Deep Learning models in recognizing complex and changing attack patterns, as well as data augmentation techniques to provide a better level of accuracy. Experimental results show that CNN with VGG 16 architecture has an accuracy of 99.9261%, a loss of 0.018590 for Syn Flood attack and accuracy 99.9983%, loss 0.001294 for Sql Injection. Resnet 50 with accuracy 99.9263%, loss 0.024910 for syn flood, accuracy 99.9962%, loss 0.001749 for Sql Injection. InceptionV3 with an accuracy of 99.7784%, a loss of 0.015571 for the syn flood attack, while for SQL injection an accuracy value of 99.9872% and a loss of 0.000392.*

Keywords: *Augmentation; CNN_VGG-16; Deep_Learning; IDS; InceptionV3; ResNet50.*

Abstrak: Intrusion Detection System (IDS) tradisional seringkali tidak mampu mengikuti kecepatan perkembangan serangan, sehingga meninggalkan celah yang dapat dimanfaatkan oleh penyerang. Penelitian ini bertujuan untuk melindungi infrastruktur jaringan dari ancaman keamanan yang semakin kompleks. Dalam penelitian ini, penulis mengusulkan penggunaan model Deep Learning arsitektur CNN VGG-16 pada Intrusion Detection System untuk mitigasi serangan SqL Injection dan Syn Flood dengan proses yang lebih mendalam yaitu dengan penerapan normalisasi data diawal dan teknik augmentation sebagai cara meningkatkan variasi data pelatihan dan mengurangi overfitting. Public dataset yang digunakan CICDDoS2019 dan CSE-CIC-IDS2018. Dengan memanfaatkan kekuatan model Deep Learning dalam mengenali pola serangan yang kompleks dan berubah-ubah, serta teknik augmentation data untuk dapat memberikan tingakat Accuracy yang lebih baik. Hasil Percobaan menujukkan hasil CNN dengan Arsitektur VGG 16 memiliki Accuracy 99.9261%, loss 0,018590 untuk serangan Syn Flood dan Accuracy 99.9983%, loss 0.001294 untuk Sql Injection. Resnet 50 dengan Accuracy 99.9263%, loss 0.024910 untuk syn flood, Accuracy 99.9962%, loss 0.001749 untuk Sql Injection. InceptionV3 dengan Accuracy 99.7784%, loss 0.015571 untuk serangan syn flood, sedangkan untuk sql injection dengan nilai Accuracy 99.9872% dan loss 0.000392.

Kata kunci: Augmentation; CNN_VGG-16; Deep_Learning; IDS; InceptionV3; ResNet50

Journal of Science and Social Research ISSN 2615 – 4307 (Print)
Nov 2024, VII (4): 1866 – 1874 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

PENDAHULUAN

Dalam konteks perkembangan teknologi informasi yang pesat (Faizin et al., 2024), keamanan jaringan menjadi semakin penting bagi organisasi tak terkecuali dunia Pendidikan tingg (Sahren, 2021). Ancaman terhadap keamanan jaringan, seperti serangan Sql Injection dan Syn Flood (Sbai & Elboukhari, 2022), terus berkembang dalam kompleksitas dan kerusakan yang mungkin ditimbulkan (Dalimunthe & Sahren, 2020). Serangan Sql Injection melibatkan penyusupan kode berbahaya ke dalam query Sql untuk mengakses atau memanipulasi basis data (Hassan et al., 2021), sementara Syn Flood adalah jenis serangan DDoS yang bertujuan untuk menghabiskan sumber daya jaringan dengan mengirimkan sejumlah besar permintaan koneksi palsu (Sahren et al., 2023) (Faiz et al., 2022). Ancaman-ancaman ini tidak hanya dapat menyebabkan kebocoran data sensitif, tetapi juga dapat mengganggu operasi bisnis/akademik yang penting (Wahyudi & Utomo, 2021) (Sahren et al., 2024). Meningkatnya frekuensi dan kompleksitas serangan cyber menunjukkan urgensi mendesak untuk mengembangkan solusi keamanan yang lebih efektif (Alimi et al., 2022) (Azmi et al., 2021).

Pentingnya penelitian ini terletak pada kebutuhan mendesak untuk mengembangkan solusi keamanan yang lebih adaptif dan responsif terhadap ancaman cyber yang berkembang pesat (Ashiku & Dagli, 2021) (Faizin et al., 2024). Penelitian ini bertujuan untuk melindungi infrastruktur jaringan dari ancaman keamanan yang semakin kompleks dengan memanfaatkan perkembangan Artificial Intelegence khususnya Deep Learning. Berdasarkan tinjauan penelitian sebelumnya Dimana dalam mitigasi serangan sql injection, syn flood serta bentuk serangan cyber lainnya dengan menggunakan Intrusion Detection System (IDS) tradisional seringkali tidak mampu mengikuti kecepatan perkembangan serangan, sehingga meninggalkan celah yang dapat dimanfaatkan oleh penyerang (Sahren et al., 2023).

Penelitian terkait Intrusion Detection System yang telah dilakukan oleh penulis dan penelitian sebelumnya atara lain: Penelitian oleh (Sahren et al., 2023) dengan judul IDPS Performance Analysis For Mitigating Sql Injections And Syn Flood Attacks, dimana pada penelitian ini melakukan Analisa performa dari Intrusion Detection System dengan mengukur Tingkat Accuracy, kecepatan deteksi dan penggunaan resource dari Intrusion Detection System dalam mitigasi Sql Injections dan Syn Flood Attacks. Akan tetapi pada penelitian ini masih menggunakan Intrusion Detection System tradisional atau belum menggunakan model berbasis Deep Learnig. Penelitian (Ashiku & Dagli, 2021) dengan judul Network Intrusion Detection System Using Deep Learning. Pada penelitian ini mengusulkan Intrusion Detection System dengan Deep Neural Network (DNN) menggunakan public dataset UNSW-NB15 menunjukkan kinerja yang lebih baik dibandingkan dengan metode tradisional seperti signature-based dan anomaly-based, adapun Accuracy keseluruhan sebesar 95,4% dan 95,6% untuk klasifikasi multikelas dalam mendeteksi serangan siber. Penelitian (I Made Suartana, 2022) dengan judul Analisis Penerapan Deep Learning Untuk Klasifikasi serangan Terhadap Keamanan Jaringan, penelitian ini menggunakan Deep Learning untuk klasifikasi serangan keamanan jaringan, pada dataset NSL-KDD dan analisis data KDD CUP 99 dengan nilai Recall normal 0.985 dan presisi serangan 0.941. Akan tetapi pada penelitian ini proses normalisasi data belum terlihat dan penggunaan pemodelan arsitektur dari Deep Learning belum secara spesifik dipaparkan dalam jurnal. Penelitian (Cao et al., 2022) dengan judul Network Intrusion Detection Model Based on CNN and GRU. Mengusulkan model Network Intrusion Detektion System (NIDS) yang menggabungkan

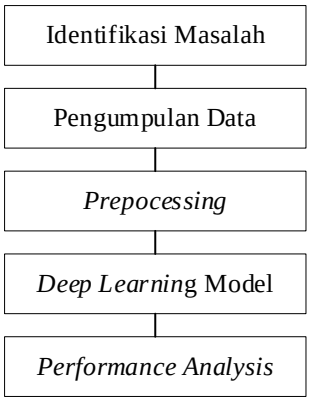
Journal of Science and Social Research ISSN 2615 – 4307 (Print)
Nov 2024, VII (4): 1866 – 1874 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

Convolutional Neural Network (CNN) dan Gated Recurrent Unit (GRU) untuk meningkatkan Accuracy deteksi serangan siber. CNN dan GRU mencapai tingkat Accuracy deteksi yang tinggi, yaitu 99,86% pada dataset NSL-KDD, 99,69% pada dataset UNSW-NB15, dan 99,65% pada dataset CIC-IDS2017. Pada penelitian ini terfokus pada penggunaan metode CNN dan GRU yang merupakan salah satu arsitektur Recurent Neural Network (RNN). Disini penelitian pada jurnal ini belum terlalu khusus membahas arsitektur pada CNN yang dapat juga gunakan untuk meningkatkan Accuracy dari deteksi NIDS.

Pada penelitian ini penulis mengusulkan Intrusion Detection System (IDS) sebagai sistem pencegahan serangan cyber, khususnya dalam mengatasi serangan Sql Injection dan Syn Flood dengan pendekatan yang mengintegrasikan teknologi Deep Learning dengan menggunakan data log yang ditangkap dengan wireshark sebagai dataset. Adapun dataset yang digunakan adalah public dataset CICDDoS2019 dan CSE-CIC-IDS2018 (Aldhaheri et al., 2024) (Gaber et al., 2023), pada penilitian ini penggunaan model arsitektur CNN VGG-16 ini dipilih karena miliki Tingkat Accuracy yang tinggi (Weny Indah Kusumawati & Adisaputra Zidha Noorizki, 2023). Namun nantinya akan dilakukan perbandingan Accuracy dengan arsitektur CNN lainnya seperti ResNet50 dan InceptionV3. Kami juga akan mambahkan teknik Augmentation sebagai cara meningkatkan Accuracy dan mengurangi overfitting (Fadillah et al., 2021) (Shorten et al., 2021).

METODE

Pendekatan pemecahan masalah untuk mengatasi tantangan dalam penelitian ini dapat melibatkan serangkaian langkah yang terstruktur dan terintegrasi. Adapun tahapan penelitian yang dilakukan dapat dilihat pada gambar 1 berikut ini:



Gambar 1. Tahapan Penelitian

Identifikasi Masalah

Permasalahan yang sering terjadi dengan semangkin pesatnya pertukaran data melalui aktifitas jaringan computer menimbulkan masalah terkait keamanan dari gangguan seperti *Syn Flood Attack* dan *Sql injection* dimana penggunaan system keamanan pada umumnya perlu untuk ditingkatkan dengan memanfaatkan *Artificial Intelegence* khususnya pada *Deep Learning*. Disini akan diuji beberapa model untuk mengetahui Tingkat Accuracy didalam mendeteksi serangan yang terjadi.

Pengumpulan Data

Pada tahapan ini melibatkan pengambilan Kumpulan data dimana dataset yang digunakan yaitu CICDDoS2019 untuk *dataset* serangan *Syn Flood* dan CSE-CIC-IDS2018 untuk *dataset* serangan *Sql Injection*. Dataset untuk *Syn Flood Attack* terdiri dari 5416 *training* data dan 1354 testing data. Sedangkan untuk *Sql Injection Attack* terdiri dari 3160 *training* data dan 790 *testing* data.

Preprocessing

Pada tahapan ini melakukan dua operasi untuk membersihkan data yaitu konversi dan normalisasi data. Langkah konversi merubah atribut katagorikal menjadi atribut numerik. Sedangkan proses normalisasi bertujuan membawa nilai-nilai atribut dalam bentuk yang lebih mudah keolah. Secara umum penelitian

Journal of Science and Social Research ISSN 2615 – 4307 (Print)
Nov 2024, VII (4): 1866 – 1874 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

ini menggunakan Teknik penskalaan minimum maksimum dan dapat dilihat dalam bentuk rumus berikut ini:

$$Y_{norm} = \frac{Y - min(Y)}{max(Y) - min(Y)} \quad (1)$$

Selanjutnya akan digunakan Teknik *augmentation* data untuk meningkatkan variasi data pelatihan, sehingga meningkatkan kinerja model dan mengurangi risiko *overfitting*. Ini bisa mencakup teknik seperti rotasi, pergeseran, atau flipping data.

Model *Deep Learning*

Model *Deep Learning* yang digunakan adalah arsitektur CNN VGG-16. Model VGG-16 memiliki 16 lapisan konvolusi. VGG menekankan pentingnya kedalaman dalam ekstraksi fitur dan memberikan hasil yang sangat baik dalam berbagai tugas. Pada tahap ini, lapisan konvolusi digunakan untuk melatih peta fitur pada lapisan yang lebih tinggi. Teknik ini menghasilkan peta fitur baru yang memiliki beberapa peta fungsi sebagai input ke inti konvolusi, dan untuk setiap peta fungsi *output*, lapisan *output* baru dibuat dengan menghubungkan beberapa peta fitur. Proses perhitungan lapisan konvolusi dijelaskan dalam persamaan berikut.

$$X_j^l = f\left(\sum_{i \in M_j} X_i^{l-1} x K_{ij}^l + b_j^l\right) \quad (2)$$

Pada penelitian yang dilakukan nantinya tidak hanya terfokus pada metode CNN dengan Arsitektur VGG-16 saja, namun akan dilakukan perbandingan dengan model CNN arsitektur lainnya seperti *ResNet50* dan *InceptionV3*.

Performance Analysis

Pada penelitian ini kami menggunakan berbagai matrik kinerja untuk menilai hasil dari model yang diusulkan dan membandingkan antara model *Deep Learning* CNN arsitektur VGG 16, *ResNet50* dan *InceptionV3*. Adapun matrik umum yang digunakan dalam *Deep Learning Intrusion Detection System* meliputi *Accurancy, Precision, Recall, F1-Score, True Positive Rate* (TPR), dan *True Negative Rate* (TNR). Adapun bentuk rumus adalah sebagai berikut

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (3)$$

$$Precision = \frac{TP}{TP+FP} \quad (4)$$

$$Recall = \frac{TP}{TP+FN} \quad (5)$$

$$F1 - Score = \frac{2*Precision*Recall}{Precision+Recall} \quad (6)$$

HASIL DAN PEMBAHASAN

Dalam percobaan yang kami lakukan menggabungkan berbagai nilai *hyper parameters* yang kami sajikan pada tabel 1 untuk mendapatkan hasil *Accuracy* yang optimal dan sesuai untuk mendeteksi *Syn Flood Attack* dan *Sql Injection Attack.* Penulis membuat dataset pelatihan dan dataset pengujian dari dua dataset utama yaitu CICDDoS2019 untuk *Syn Flood Attack* dan CSE-CIC-IDS2018 untuk *Sql Injection Attack*. Pada Tabel 1 menjelaskan rincian dataset yang digunakan.

Tabel 1. Clasifikasi *Dataset*

Jenis Serangan	Jumlah Data *Trainig*	Jumlah Data Testing
Syn Flood	5416	1354
Sql Injection	3160	790

Pada proses preprocessing data penulis menggunakan teknik augmentasi untuk meningkatkan Accuracy dan menghindari overfitting pada saat melakukan training dan uji dataset.

Journal of Science and Social Research ISSN 2615 – 4307 (Print)
Nov 2024, VII (4): 1866 – 1874 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

```
SQL Injection Dataset:
**Original SQL Injection Dataset**
          Sentence  Label
0                a      1
1              a'       1
2           a' --       1
3  a' or 1 = 1; --      1
4                @      1
Shape: (4200, 2)
Columns: Index(['Sentence', 'Label'], dtype='object')
```

Gambar 2. Original Dataset Sql Injections

Gambar 2 menunjukkan Dataset asli memiliki dua kolom "Sentence", yang berisi input teks yang berpotensi sebagai SQL injection, dan "Label", dengan nilai 1, yang menandakan bahwa parameter tersebut dikategorikan sebagai serangan *Sql injection*. *Dataset* ini berukuran 4.200 baris dan hanya fokus pada mendeteksi serangan *Sql injection* dari kalimat-kalimat tertentu. Pada gambar 3 ini akan diperlihatkan hasil dari proses

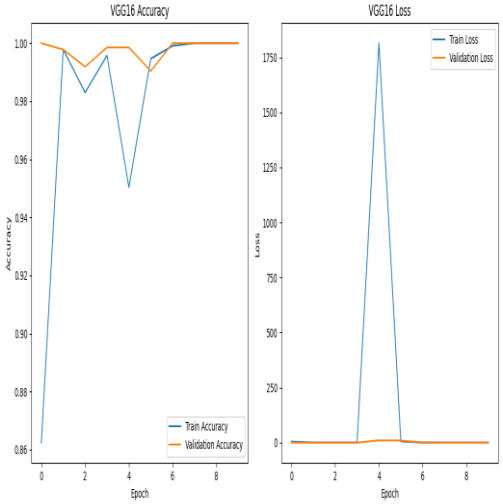
```
Augmented SQL Injection Dataset:
**Augmented SQL Injection Dataset**
          Sentence  Label     0     1
0                a      1  False  True
1              a'       1  False  True
2           a' --       1  False  True
3  a' or 1 = 1; --      1  False  True
4                @      1  False  True
Shape: (3950, 4)
Columns: Index(['Sentence', 'Label', 0, 1], dtype='object')
```

augmentasinya.

Gambar 3. Dataset *Augmented Sql Injection*

Pada gambar 3 adalah versi yang telah ditingkatkan, dengan tambahan dua kolom (0 dan 1) yang berisi nilai *boolean* (*False* dan *True*). Kolom tambahan ini merepresentasikan hasil dari fitur atau karakteristik baru yang diperoleh melalui proses augmentasi. *Dataset augmented* ini memiliki 3.950 baris, lebih sedikit dari dataset asli, karena adanya pembersihan atau pengurangan data selama proses augmentasi. Dengan penambahan informasi dari kolom baru, dataset *augmented* berpotensi membantu meningkatkan kemampuan model dalam mendeteksi pola serangan yang lebih kompleks. Teknik augmentasi ini juga dilakukan pada dataset untuk serangan *syn flood.*

Model deteksi serangan *Syn Flood* yang menggunakan *Deep Learning* metode *Convolution Neural Network* (CNN) dengan arsitektur VGG16, ResNet50, dan InceptionV3 menunjukkan hasil yang cukup baik, meskipun ada beberapa perbedaan antara masing-masing model. Model VGG16 memiliki



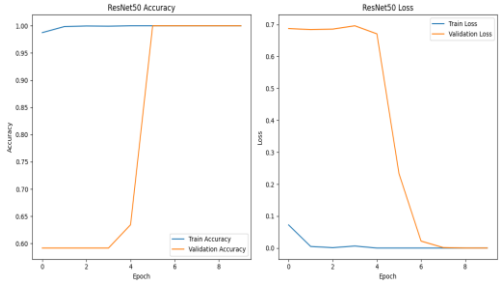
Gambar 4. Grafik Train Accuracy dan Train Loss VGG 16 Pada Syn Flood Attack

nilai *Loss* 0,018590 dan *Accuracy* yang sangat tinggi, yaitu 99.9261%. Dapat dilihat pada gambar 4

Model CNN VGG 16 memiliki *precision* dan *Recall* masing-masing sebesar 99.9262% dan 99.9261% serta *F1-Score* 99.9261%. Dengan demikian, model ini menunjukkan keseimbangan yang hampir sempurna antara *Precision* dan *Recall.*

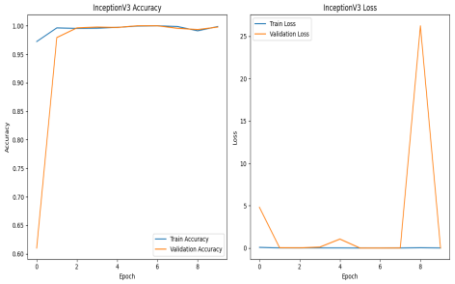
Meskipun CNN ResNet50 mengalami kehilangan yang lebih besar, yaitu 0.024910, *Accuracy, Precision*, dan *Recall* ResNet50 sama dengan VGG16 pada 99.9261% untuk *Accuracy*, 99.9263% terlihat pada gambar 5 untuk *Precision*, dan 99.9261% untuk *Recall* dan 99.9261% untuk *F1-Score.* Ini menunjukkan bahwa, dengan perbedaan yang sangat kecil dalam hal *Precision*, performa ResNet50 hampir sama dengan VGG16.

Journal of Science and Social Research ISSN 2615 – 4307 (Print)
Nov 2024, VII (4): 1866 – 1874 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR



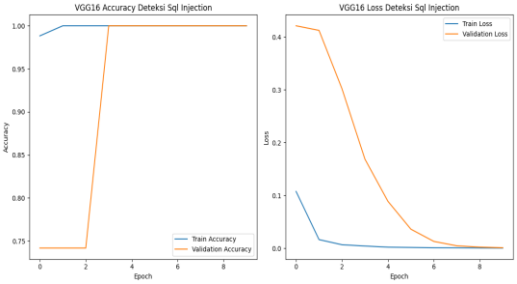
Gambar 5. Grafik *Train Accuracy* dan *Train Loss* Resnet 50 Pada *Syn Flood Attack*

Meskipun mengalami penurunan yang lebih kecil di antara ketiga model, yaitu 0,015571, InceptionV3 menunjukkan *Accuracy* yang lebih rendah di 99.7784% seperti pada gambar 6. *Accuracy* dan Recall-nya juga lebih rendah, masing-masing 99.7796% dan 99.7784%, menunjukkan bahwa model ini cenderung menghasilkan kesalahan yang lebih besar baik dalam mendeteksi positif palsu maupun negatif palsu dibandingkan VGG16 dan ResNet50. *F1-Score* InceptionV3 juga lebih rendah, yaitu 99.7785%.



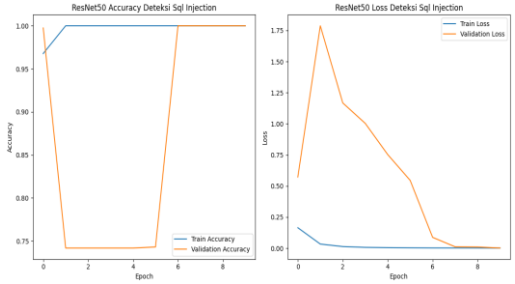
Gambar 6. Grafik *Train Accuracy* dan *Train Loss* InceptionsV3 Pada *Syn Flood Attack*

Hasil model deteksi Sql injection yang menggunakan CNN VGG16, ResNet50, dan InceptionV3 menunjukkan perbedaan yang signifikan dalam performa. Model VGG16 memiliki nilai *Loss* sebesar 0.001294 dengan *Accuracy* yang sangat tinggi, yaitu 99.9983% dalam 10 epoch seperti terlihat pada gambar 7. Selain itu, *Accuracy* dan Recall-nya masing-masing mencapai 99.9881% dan 99.9681%, menunjukkan bahwa model ini sangat baik dalam mendeteksi serangan *Sql injection* dengan sedikit kesalahan dalam mendeteksi positif palsu (*false positives*). VGG16 menunjukkan kinerja yang sangat seimbang, seperti yang ditunjukkan oleh *F1-Score*-nya yang 99,9781%.



Gambar 7. Grafik *Train Accuracy* dan *Train Loss* VGG 16 Pada *Sql Injection Attack*

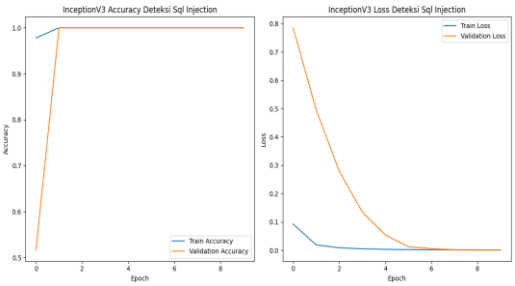
Meskipun kehilangan sedikit lebih besar, CNN ResNet50 masih memberikan *Accuracy* tinggi sebesar 99.9962% yang diperoleh dalam 10 *epoch* seperti pada gambar 7, dengan *precision* sebesar 99.9872% dan Recall sebesar 99.9861%, yang menunjukkan bahwa ResNet50 sedikit lebih baik dalam mendeteksi serangan sebenarnya dengan Recall yang lebih tinggi. Namun, secara keseluruhan, hasilnya hampir sama dengan VGG16.



Gambar 8. Grafik *Train Accuracy dan Train Loss* Resnet50 *Pada Sql Injection Attack*

Sementara, CNN InceptionV3 menunjukkan *Accuracy* yang lebih rendah (99.9872%) pada gambar 9 dibandingkan kedua model lainnya, meskipun nilai loss yang jauh lebih rendah (0.000392). Dengan precision dan Recall masing-masing 99.7796% dan 99.7784%, model

ini lebih sering melakukan kesalahan dalam mendeteksi serangan *Sql injection*, baik dalam mendeteksi positif palsu maupun negatif palsu. *F1-Score* InceptionV3, yang hanya mencapai 99.7663%, menunjukkan bahwa model ini kurang optimal dibandingkan dengan VGG16 dan ResNet50, sementara InceptionV3 mencapai skor 99.7663%.



Gambar 9. Grafik *Train Accuracy dan Train Loss* InceptionsV3 *Pada Sql Injection Attack*

Pada kesemuan model dilatih dengan jumlah *epoch* yang sama yaitu 10 *epoch* alasan penulis berhenti pada 10 *epoch* karena sudah mendapatkan nilai *Accuracy* yang tinggi dan nilai *Loos* yang rendah. Penggunaan teknik augmentasi pada saat *processing* data sangat berperan penting dalam meningkatkan *Accuracy.*

SIMPULAN

Berdasarkan hasil deteksi serangan SYN flood dan SQL injection menggunakan model Arsitektur CNN seperti VGG16, ResNet50, dan InceptionV3, VGG16 menunjukkan performa yang paling konsisten dan kuat. Dengan Accuracy yang sangat tinggi pada kedua jenis serangan, yaitu 99.9983% untuk Sql injection dan 99.9261% untuk Syn flood, serta nilai precision dan Recall yang hampir sempurna, VGG16 terbukti mampu mendeteksi serangan dengan sangat sedikit kesalahan, baik positif palsu maupun negatif palsu. ResNet50 memberikan hasil yang hampir identik dengan VGG16, terutama dalam mendeteksi serangan Syn flood, dengan Accuracy, Precision, dan Recall yang hampir sama. Namun, ResNet50 sedikit tertinggal dari VGG16 dalam hal precision pada deteksi Sql injection. Sementara itu, InceptionV3, meskipun memiliki nilai Loss yang lebih rendah, menunjukkan performa yang kurang optimal dibandingkan kedua model lainnya, terutama dalam hal Accuracy, Precision, dan Recall untuk kedua jenis serangan. InceptionV3 menghasilkan lebih banyak kesalahan dalam mendeteksi serangan dibandingkan VGG16 dan ResNet50. Secara keseluruhan, VGG16 direkomendasikan sebagai model yang paling andal dan seimbang untuk mendeteksi serangan Syn flood dan Sql injection, diikuti oleh ResNet50, sementara InceptionV3 berada di posisi terakhir dalam hal performa.

UCAPAN TERIMA KASIH

Terimakasih yang sebesar besarnya kami sampaikan kepada Direktorat Riset dan Teknologi. Kementrian Pendidikan, Kebudayaan, Riset, dan Teknologi yang telah memberikan dukungan Pendanaan Penelitian melalui skema Penelitian Dosen Pemula (PDP) Tahun Anggaran 2024.

DAFTAR PUSTAKA

Aldhaheri, A., Alwahedi, F., Ferrag, M. A., & Battah, A. (2024). Deep learning for cyber threat detection in IoT networks: A review. *Internet of Things and Cyber-Physical Systems*, *4*(October 2023), 110–128. https://doi.org/10.1016/j.iotcps.2023.09.003

Alimi, K. O. A., Ouahada, K., Abu-Mahfouz, A. M., Rimer, S., & Alimi, O. A. (2022). Refined LSTM Based Intrusion Detection for Denial-of-Service Attack in Internet of Things. *Journal of Sensor and Actuator Networks*, *11*(3). https://doi.org/10.3390/jsan11030032

Ashiku, L., & Dagli, C. (2021). Network Intrusion Detection System using Deep Learning. *Procedia Computer Science*, *185*, 239–247. https://doi.org/10.1016/j.procs.2021.05.025

Azmi, M. A. H., Foozy, C. F. M., Sukri, K. A. M., Abdullah, N. A., Hamid, I. R. A., & Amnur, H. (2021). Feature Selection Approach to Detect DDoS Attack Using Machine Learning Algorithms. *International Journal on Informatics Visualization*, *5*(4), 395–401. https://doi.org/10.30630/JOIV.5.4.734

Cao, B., Li, C., Song, Y., Qin, Y., & Chen, C. (2022). Network Intrusion Detection Model Based on CNN and GRU. *Applied Sciences (Switzerland)*, *12*(9). https://doi.org/10.3390/app12094184

Dalimunthe, R. A., & Sahren, S. (2020). Intrusion Detection System and Modsecurity for Handling Sql Injection Attacks. *... Social, Sciences and Information ...*, *4509*, 187–194. https://doi.org/10.33330/icossit.v1i1.711

Fadillah, R. Z., Irawan, A., Susanty, M., & Artikel, I. (2021). Data Augmentasi Untuk Mengatasi Keterbatasan Data Pada Model Penerjemah Bahasa Isyarat Indonesia (BISINDO). *Jurnal Informatika*, *8*(2), 208–214. https://ejournal.bsi.ac.id/ejurnal/index.php/ji/article/view/10768

Faiz, M. N., Somantri, O., & Muhammad, A. W. (2022). Rekayasa Fitur Berbasis Machine Learning untuk Mendeteksi Serangan DDoS. In *Jurnal Nasional Teknik Elektro dan Teknologi Informasi* | (Vol. 11, Issue 3).

Faizin, M. A., Kurniasari, D. T., Elqolby, N., Putra, M. A. R., & Ahmad, T. (2024). Optimizing Feature Selection Method in Intrusion Detection System Using Thresholding. *International Journal of Intelligent Engineering and Systems*, *17*(3), 214–226. https://doi.org/10.22266/ijies2024.0630.18

Gaber, T., Awotunde, J. B., Torky, M., Ajagbe, S. A., Hammoudeh, M., & Li, W. (2023). Metaverse-IDS: Deep learning-based intrusion detection system for Metaverse-IoT networks. *Internet of Things (Netherlands)*, *24*(October), 100977. https://doi.org/10.1016/j.iot.2023.100977

Hassan, M. M., Ahmad, R. B., & Ghosh, T. (2021). Sql injection vulnerability detection using deep learning: A feature-based approach. *Indonesian Journal of Electrical Engineering and Informatics*, *9*(3), 702–718. https://doi.org/10.52549/.v9i3.3131

I Made Suartana. (2022). Analisis Penerapan Deep Learning untuk Klasifikasi Serangan Terhadap Keamanan Jaringan. *Klik-Kumpulan Jurnal Ilmu Komputer*, *9*(1), 100–109.

Sahren, S. (2021). IMPLEMENTASI TEKNOLOGI FIREWALL SEBAGAI KEAMANAN SERVER DARI SYN FLOOD ATTACK. *JURTEKSI (Jurnal Teknologi Dan Sistem Informasi)*, *7*(2), 159–164. https://doi.org/10.33330/jurteksi.v7i2.933

Sahren, S., Dalimunthe, R. A., Saputra, H., & Kurnia Sirni, D. Y. (2023). Idps Performance Analysis for Mitigating Sql Injections and Syn Flood Attacks. *JURTEKSI (Jurnal Teknologi Dan Sistem Informasi)*, *10*(1), 171–178. https://doi.org/10.33330/jurteksi.v10i1.2880

Sahren, S., Saputra, H., Siddik, M., Dalimunthe, R. A., & Hasibuan, H. E. (2024). *Analysis of Intelligent Load Balancing on Software Defined Network Architecture*. 1–23.

Sbai, O., & Elboukhari, M. (2022). Deep learning intrusion detection system for mobile ad hoc networks against flooding attacks. *IAES International Journal of Artificial Intelligence*,

11(3), 878–885. https://doi.org/10.11591/ijai.v11.i3.pp878-885

Shorten, C., Khoshgoftaar, T. M., & Furht, B. (2021). Text Data Augmentation for Deep Learning. In *Journal of Big Data* (Vol. 8, Issue 1). Springer International Publishing. https://doi.org/10.1186/s40537-021-00492-0

Wahyudi, F., & Utomo, L. T. (2021). Perancangan Security Network Intrusion Prevention System Pada PDTI Universitas Islam Raden Rahmat Malang. *Edumatic: Jurnal Pendidikan Informatika*, *5*(1), 60–69. https://doi.org/10.29408/edumatic.v5i1.3278

Weny Indah Kusumawati, & Adisaputra Zidha Noorizki. (2023). Perbandingan Performa Algoritma VGG16 Dan VGG19 Melalui Metode CNN Untuk Klasifikasi Varietas Beras. *Journal of Computer, Electronic, and Telecommunication*, *4*(2). https://doi.org/10.52435/complete.v4i2.387