JITEKH
Jurnal Ilmiah Teknologi Harapan
P-ISSN: 2338-5677 || E-ISSN 2549-6646
Vol. 12, No. 2, September 2024
DOI: https://doi.org/10.35447/jitekh.v12i2.996

Implementasi Recurrent Neural Network Sebagai IDS Terhadap Serangan Jaringan

Fransko Gultom[1], Rosyidah Siregar[2]
[1,2] Teknik Informatika, Universitas Harapan Medan, Indonesia
[1]franskogultom747@gmail.com, [2]rosyidahsiregar@unhar.ac.id

Abstrak-Beberapa tahun terakhir telah muncul istilah baru yang kini banyak diterapkan sebagai IDS (Intrusion Detection System) yaitu Deep Learning. Salah satu jenis Deep-Learning adalah RNN (Recurrent Neural Network) yang belakangan ini telah diterapkan menjadi IDS. Serangan cyber memang tidak bisa dihindarkan, namun dapat diantisipasi dengan membangun suatu sistem yang dapat mendeteksi kinerja aliran data jaringan agar pengguna dapat terhindar dari segala macam bentuk serangan dan usaha-usaha penyusupan dari pihak yang tidak dikenali. Penelitian ini bertujuan untuk menguji dan menganalisis keakuratan dan kecepatan Recurrent Neural Network dalam mendeteksi serangan. Metode yang digunakan untuk penelitian ini yaitu RNN, yang dioperasikan melalui program Phyton dan Google Colab. Berdasarkan hasil uji coba model dilatih dengan jumlah 50 epoch menghasilkan akurasi sebesar 92%. Sedangkan model dengan jumlah 30 epoch menghasilkan akurasi sebesar 99%. Jadi, model dapat bekerja dengan baik terhadap data pelatihan dengan jumlah 30 epoch.

Kata Kunci: *Recurrent neural network; Intrusion detection system; Serangan jaringan*

Abstract-In recent years, a new term has emerged which is now widely applied as IDS (Intrusion Detection System), namely Deep Learing. One type of Deep – Learing is RNN (Recurrent Neural Network) which has recently been applied to IDS. Cyber attacs cannot be avoided, but they can be anticipated by building a system than can detect the performance of network data flows so that users can avoid all kinds of attacks and intrusion attempts from unknown parties. This research aims to test and analyse the accurary and speed of the Recurrent Neural Network in detecting attacks. The method used for this research is RNN, which is operated through the Python and Google Colab programs. Based on the results, the model was trained with 50 epochs resulting in an accurary of 92%. Meanwhile, a model with 30 epochs produces an accurary of 99%. So, the model can work well on training data with a total of 30 epochs.

Keywords: *Recurrent neural network;Intrusion detection system; Network attacks*

1. PENDAHULUAN

Menurut Badan Siber dan Sandi Negara (BSSN) Republik Indonesia serangan cyber terjadi berjumlah 80.837.445 kali sejak Januari hingga Maret 2020[1]. Jenis-jenis serangan yang dilancarkan ialah DDoS, *malware*, *phising*, dan *ransomware* yang melancarkan serangan pada aktifitas pengguna internet, hal ini tentu menarik perhatian para pelaku kejahatan cyber sehingga sudah seharusnya keamanan akan perangkat juga perlu diperhatikan. Serangan cyber memang tidak bisa dihindarkan, namun dapat diantisipasi dengan membangun suatu sistem yang dapat mendeteksi kinerja aliran data jaringan agar pengguna dapat terhindar dari segala macam bentuk serangan dan usaha-usaha penyusupan dari pihak yang tidak dikenali. Salah satu solusi yang paling representatif adalah Instrusion Detection System (IDS). IDS merupakan program atau aplikasi yang dapat mendeteksi aktivitas yang abnormal dalam sebuah sistem atau jaringan. Jika ditemukan kegiatan–kegiatan yang mencurigakan berhubungan dengan traffic jaringan, maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan[3]. IDS adalah salah satu sistem yang dikembangkan untuk mendeteksi serangan berdasarkan informasi yang diperoleh dari merekam trafik pada jaringan[4]. Ada beberapa hal yang bisa dan tidak bisa dilakukan oleh IDS diantaranya, dapat melacak sebuah serangan yang masuk ke dalam jaringan hingga sampai pada akhir berhentinya serangan tersebut. Selain itu, IDS dapat mendeteksi suatu kesalahan dalam konfigurasi yang telah dibuat di dalam sistem. Cabang *IDS* disebut sebagai *Anomaly-based* telah berkembang dan diimplementasikan menjadi beberapa bidang. *Convolutional Neural Network* merupakan implementasi dari *Machine Learning-based*[5].

Beberapa tahun terakhir telah muncul istilah baru yang kini banyak diterapkan sebagai IDS yaitu *deep learning*. *Deep learning* adalah bidang ilmu komputer yang menggunakan teknik statistika untuk memberi kemampuan sistem komputer agar dapat belajar dari data[6][7]. Banyak bidang yang telah menerapkan *deep-learning*, salah satunya diterapkan pada masalah IDS dengan harapan dapat meningkatkan tingkat deteksi dan

JITEKH
Jurnal Ilmiah Teknologi Harapan
P-ISSN: 2338-5677 || E-ISSN 2549-6646
Vol. 12, No. 2, September 2024
DOI: https://doi.org/10.35447/jitekh.v12i2.996

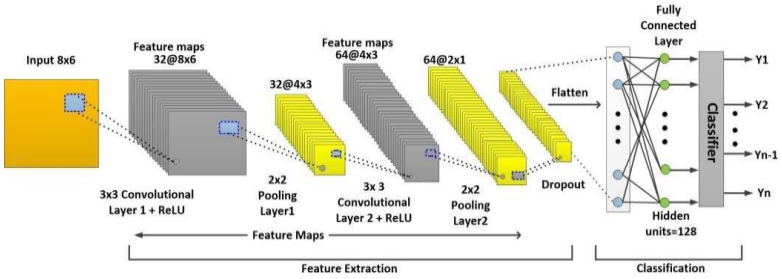
kemampuan klasifikasi. Salah satu jenis *deep learning* adalah RNN (*Recurrent Neural Network*) yang belakangan ini telah diterapkan menjadi IDS. RNN merupakan jaringan saraf berulang atau jaringan saraf tiruan yang pemerosesannya dipanggil secara berulang-ulang untuk memproses masukan yang biasa adalah data sekuensial[8]. Sistem kinerjanya ialah mengubah teks atau angka yang ada pada log jaringan ke dalam bentuk nilai matriks, selanjutnya nilai-nilai tersebut diubah menjadi pixel dan apabila terdapat data berupa string, maka setiap karakter akan diubah bentuknya menjadi nilai ASCII[9]. *Recurrent Neural Network* adalah jenis model pembelajaran mesin yang dirancang khusus untuk mengelola data berurutan atau time series. Permodelan (*modelling*) sesungguhnya digunakan untuk penyederhanaan permasalahan-permasalahan yang kompleks sedemikian rupa sehingga lebih mudah dipelajari dan dipahami[8]. RNN sangat berguna dalam berbagai aplikasi seperti pemrosesan bahasa alami, pengenalan tulisan tangan, dan peramalan waktu. RNN bekerja dengan cara yang unik memiliki simpul yang mengambil masukan dan menyimpan keadaan internal yang berfungsi sebagai memori. Ini memungkinkan RNN untuk mengingat informasi dari langkah-langkah sebelumnya dalam urutan data, yang merupakan aspek penting dalam pemahaman konteks dalam data berurutan[10][11]. Kelebihan dari RNN dapat memahami dan memproses data berurutan karena memiliki struktur berulang yang memungkinkan informasi sebelumnya dipertimbangkan dalam proses berikutnya dan RNN dapat menangani input dengan panjang yang bervariasi[12][13]. Pada suatu penelitian dengan menggunakan tiga parameter pengukuran yaitu akurasi, presisi dan recall menunjukkan performa dari RNN dengan feature extraction (PCA) berhasil dalam mendeteksi serangan pada jaringan kompleks IoT dengan akurasi mencapai 87.55% [10]

Tujuan dari penelitian ini adalah untuk memanfaatkan Intrusion Detection System dengan metode RNN sebagai program yang berkerja dalam mendeteksi serangan dan untuk mengetahui nilai akurasi dalam pendeteksian serangan berdasarkan data latih dan data uji dengan memanfaatkan RNN.

2. METODE PENELITIAN

2.1 Recurrent Neural Network (RNN)

Recurrent Neural Network (RNN) adalah jenis model pembelajaran mesin yang dirancang khusus untuk mengelola data berurutan atau time series. RNN sangat berguna dalam berbagai aplikasi seperti pemrosesan bahasa alami, pengenalan tulisan tangan, dan peramalan waktu. RNN bekerja dengan cara yang unik. Mereka memiliki simpul yang mengambil masukan dan menyimpan keadaan internal yang berfungsi sebagai memori. Ini memungkinkan RNN untuk mengingat informasi dari langkah-langkah sebelumnya dalam urutan data, yang merupakan aspek penting dalam pemahaman konteks dalam data berurutan. Arsitektur RNN terlihat pada Gambar 1



Gambar 1 Arsitektur RNN

Arsitektur dari RNN dibagi menjadi dua bagian besar, yaitu:

2.1.1. Convolution Layer

Memiliki 32 filter, masing – masing dimensi 5x5, maka parameter total yang akan dipelajari sebanyak, 5x5x32=832 parameter. Maksudnya adalah pada 6 convolution layer data dari inputan akan diambil dimensi panjang x tinggi sesuai ukuran dimensi filter dari seluruh total dimensi data inputan. Misalnya, ukuran dimensi filter 3x3 dan ukuran dimensi data input 5x5 maka dimensi dari data input akan diambil sesuai dengan ukuran filter yaitu 3x3, kemudian akan dilakukan proses perkalian sebanyak jumlah filter yang digunakan. Convolution layer dalam arsitektur RNN umumnya menggunakan lebih dari satu filter [14].

JITEKH
Jurnal Ilmiah Teknologi Harapan
P-ISSN: 2338-5677 || E-ISSN 2549-6646
Vol. 12, No. 2, September 2024
DOI: https://doi.org/10.35447/jitekh.v12i2.996

2.1.2 Pooling Layer

Pooling layer berguna untuk pencarian fitur pada citra yang telah didapatkan pada layer sebelumnya. Pooling layer bekerja dengan mengurangi ukuran matriks. Beberapa metode pooling yang dapat digunakan adalah Max Pooling, Average Pooling, Sum Pooling dan sebagainya. Max pooling digunakan dengan mengambil nilai yang paling besar sedangkan untuk average pooling digunakan dengan mengambil nilai rata-rata. Dari kedua cara proses pooling yangpaling sering dijumpai adalah menggunakan max pooling, untuk average pooling sangat jarang digunakan tapi dalam beberapa arsitektur jaringan dapat ditemukan. [15]

2.2 Deep Learning

Deep Learning merupakan metode learning yang memanfaaatkan Artificial Neural Networks yang berlapis – lapis (multilayer). Deep Learning terdiri dari beberapa jaringan saraf tiruan yang saling berhubungan salah satu jenis diantaranya ialah Convolitional Neural Network (RNN). Artificial Neural Networks ini dibuat mirip dengan otak manusia, dimana neuron-neuron terkoneksi satu sama lain sehingga membentuk sebuah jaringan neuron yang sangat rumit[16].

2.3 Arsitektur RNN

Arsitektur RNN (Recurrent Neural Network) adalah model jaringan saraf yang dirancang untuk menangani data berurutan atau data deret waktu. Keunikan utama RNN terletak pada kemampuannya menyimpan dan mengingat informasi dari sebelumnya melalui unitrekurensi, memungkinkan pemrosesan data dengan konteks sepanjang waktu. Pertama, arsitektur RNN terdiri dari beberapa unit atau sel yang diatur dalam serangkaian langkah waktu atau langkah urutan. Setiap unit memiliki dua input: input dari langkah waktu saat ini dan output dari unit pada langkah waktu sebelumnya. Proses ini memungkinkan RNN untuk menyimpan informasi mengenai urutan input sebelumnya dan menggunakan informasi tersebut untuk mempengaruhi pengolahan langkah waktu berikutnya. Arsitektur RNN (Recurrent Neural Network) dapat dijelaskan dengan layer-node yang melibatkan dua jenis layer utama: layer input dan layer rekurensi. [17]

2.4 Jaringan Komputer

Jaringan komputer adalah sebuah sistem yang terdiri dari perangkat komputer dan jaringan yang didesain untuk dapat berbagi sumber daya dan dapat mengakses informasi. Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan (service) [18]. Dalam sebuah jaringan komputer biasanya terdiri dari dua atau lebih komputer yang saling berhubungan satu sama lain dan saling berbagi sumber daya, misalnya CD ROM, printer, scanner, pertukaran file bahkan berkomunikasi secara elektronik. Komputer yang terhubung, dimungkinkan berhubungan dengan media kabel, saluran telepon, gelombang radio, satelit, sinar infra merah, atau tanpa kabel[19].

2.5 Rancangan Sistem Prediksi

Dalam upaya untuk meningkatkan keamanan sistem jaringan dan mengidentifikasi serangan intrusi dengan lebih efektif, penelitian merancang sebuah sistem deteksi IDS (Intrusion Detection System) yang menggunakan pendekatan deep learning dengan algoritma Recurrent Neural Network (RNN)[20]. Rancangan sistem ini bertujuan untuk mengenali serangan-serangan yang tidak sah dalam lalu lintas jaringan dengan tingkat akurasi yang tinggi dan kemampuan adaptasi terhadap serangan baru yang belum pernah terdeteksi sebelumnya. Pada bagian ini akan terdapat tahapan dalam rancangan model seperti berikut: a) Tahap Analisis Sistem b) Pendekatan Deep Learning dengan RNN c) Pengumpulan dan Preprocessing Data d) Pelatihan Model e) Implementasi f) Evaluasi Kinerja.

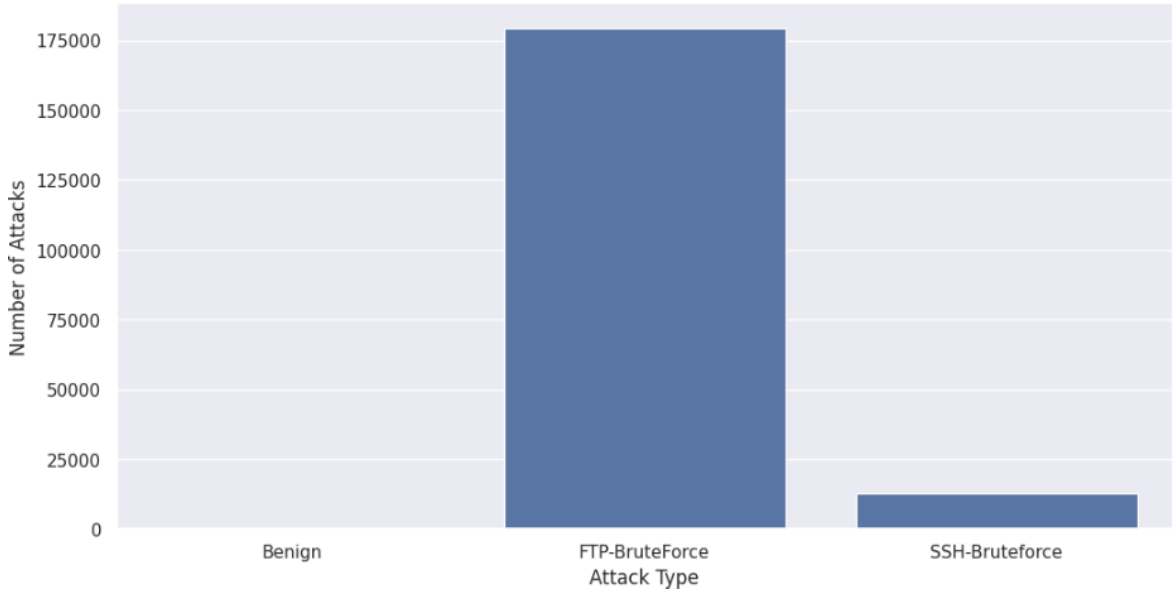
3. HASIL DAN PEMBAHASAN

3.1 Exploratory Data Analysis (EDA)

Exploratory Data Analysis (EDA) adalah mengim por data set kedalam lingkungan analisis. Anda dimulai dengan mengevaluasi struktur dataset, menghitung jumlah baris dan kolom, dan mengidentifikasi jenis variabel yang ada. Tindakan ini berguna untuk memahamiruang lingkup dan format data. Setelah itu, Anda menganalisis variabel-variabel secara terpisah dalam dataset. Anda dapatmelihat statistik deskriptif seperti rata-rata, median,dan quartil

JITEKH
Jurnal Ilmiah Teknologi Harapan
P-ISSN: 2338-5677 || E-ISSN 2549-6646
Vol. 12, No. 2, September 2024
DOI: https://doi.org/10.35447/jitekh.v12i2.996

untuk variabel numerik, sambil mengenali nilai-nilai unik dan frekuensi untuk variabel kategorikal. Ini memberikan pemahaman awal tentang distribusi dan karakteristik variabel tersebut. visualisasi *Exploratory Data Analysis* (EDA) dapat dilihat pada gambar 2.

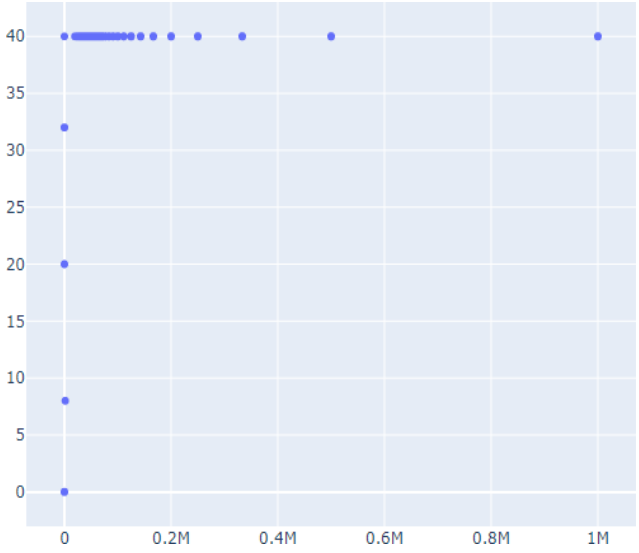


Gambar 2. Visualisasi Data

3.2 Scatter Plot

Scatter plot adalah salah satu jenis grafik atau visualisasi data yang digunakan untuk menunjukkan hubungan antara dua variabel atau lebih dalam bentuk titik-titik yang tersebar di atas bidang kartesian. Dalam scatter plot, masing-masing titik mewakili satu pengamatan atau data, dan letak titik di bidang kartesian mencerminkan nilai dari dua variabel yang berbeda. Tujuan utama dari scatter plot adalah untuk membantu mengidentifikasi pola, tren, atau hubungan antara variabel-variabel tersebut. Scatter plot sangat berguna dalam analisis eksploratori data (Exploratory Data Analysis - EDA). Berikut ini visualisasi scatter plot pada gambar 3.

Gambar 3 adalah representasi visual yang memetakan dua variabel pada koordinat kartesian. Setiap titik dalam scatter plot merepresentasikan satu pengamatan atau data point, dengan sumbu x dan y mewakili dua variabel yang diamati. Misalnya, jika ingin melihat hubungan antara jumlah serangan (sumbu x) dan antisipasi serangan pada IDS (sumbu y), setiap titik pada grafik akan menunjukkan nilai serangan IDS.



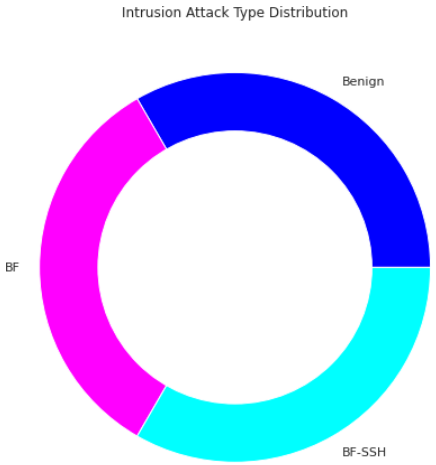
JITEKH
Jurnal Ilmiah Teknologi Harapan
P-ISSN: 2338-5677 || E-ISSN 2549-6646
Vol. 12, No. 2, September 2024
DOI: https://doi.org/10.35447/jitekh.v12i2.996

Gambar 3. Visualisasi Scatter Plot

Scatter plot bisa digunakan untuk menganalisis data keamanan, sehingga bisa mengasumsikan bahwa satu sumbu mewakili waktu (contohnya, timestamp) dan sumbu lainnya mewakili jumlah percobaan login atau serangan brute force. Dalam hal ini, setiap titik pada scatter plot dapat merepresentasikan sebuah peristiwa percobaan login dan waktu ketika itu terjadi. Scatter plot ini dapat membantu analis keamanan untuk melihat pola serangan, tren waktu, atau kejadian berulang yang mungkin menandakan aktivitas mencurigakan.

3.3 Argumentasi Data

Argumentasi data merujuk pada penggunaan data yang ada untuk membangun, melatih, dan menguji model jaringan saraf tiruan (neural network) atau model pembelajaran mendalam lainnya. Ini adalah bagian penting dari proses pengembangan dan evaluasi model *deep learning*. Argumentasi data dalam model *deep learning* melibatkan beberapa aspek, gambar 4 adalah visualisasi dari argumentasi data.



Gambar 4. Visualisasi Argumentasi Data

3.4 Proses Training

Proses pelatihan algoritma RNN (Recurrent Neural Network) dengan 50 epoch merupakan langkah krusial dalam pengembangan model untuk tugas-tugas seperti prediksi time series, analisis teks, atau pemrosesan bahasa alami. Selama pelatihan, model belajar untuk menyesuaikan bobot dan biasanya berdasarkan data latihan untuk mengoptimalkan performa dalam memprediksi data baru. Setiap epoch mengacu pada satu literasi melalui seluruh data set training. Proses training terdapat pada gambar 5.

```
logger = CSVLogger('logs.csv', append=True)
his = model.fit(X_train, y_train, epochs=20, batch_size=32,
          validation_data=(X_test, y_test), callbacks=[logger])

Epoch 1/20
938/938 [==============================] - 44s 44ms/step - loss: 0.0480 - accuracy: 0.9853 - val_loss: 0.1771 - val_accuracy: 0.9583
Epoch 2/20
938/938 [==============================] - 38s 40ms/step - loss: 0.0117 - accuracy: 0.9970 - val_loss: 0.0092 - val_accuracy: 0.9963
Epoch 3/20
938/938 [==============================] - 21s 23ms/step - loss: 0.0073 - accuracy: 0.9986 - val_loss: 0.0431 - val_accuracy: 0.9903
Epoch 4/20
938/938 [==============================] - 24s 25ms/step - loss: 0.0102 - accuracy: 0.9972 - val_loss: 0.0043 - val_accuracy: 0.9993
Epoch 5/20
938/938 [==============================] - 22s 23ms/step - loss: 0.0011 - accuracy: 0.9997 - val_loss: 0.0075 - val_accuracy: 0.9993
Epoch 6/20
938/938 [==============================] - 24s 26ms/step - loss: 0.0052 - accuracy: 0.9986 - val_loss: 0.0053 - val_accuracy: 0.9997
Epoch 7/20
938/938 [==============================] - 22s 23ms/step - loss: 0.0015 - accuracy: 0.9998 - val_loss: 0.0024 - val_accuracy: 0.9997
Epoch 8/20
938/938 [==============================] - 22s 24ms/step - loss: 0.0131 - accuracy: 0.9969 - val_loss: 0.0045 - val_accuracy: 0.9993
Epoch 9/20
938/938 [==============================] - 23s 24ms/step - loss: 0.0013 - accuracy: 0.9997 - val_loss: 0.0066 - val_accuracy: 0.9980
Epoch 10/20
938/938 [==============================] - 22s 23ms/step - loss: 0.0013 - accuracy: 0.9998 - val_loss: 0.0200 - val_accuracy: 0.9943
Epoch 11/20
938/938 [==============================] - 25s 27ms/step - loss: 0.0230 - accuracy: 0.9980 - val_loss: 1.1724 - val_accuracy: 0.8383
Epoch 12/20
938/938 [==============================] - 22s 23ms/step - loss: 0.0024 - accuracy: 0.9993 - val_loss: 0.6718 - val_accuracy: 0.9600
Epoch 13/20
938/938 [==============================] - 26s 28ms/step - loss: 0.0013 - accuracy: 0.9998 - val_loss: 0.4434 - val_accuracy: 0.9630
Epoch 14/20
938/938 [==============================] - 22s 23ms/step - loss: 6.1556e-04 - accuracy: 0.9997 - val_loss: 1.0215e-04 - val_accuracy: 1.0000
Epoch 15/20
```

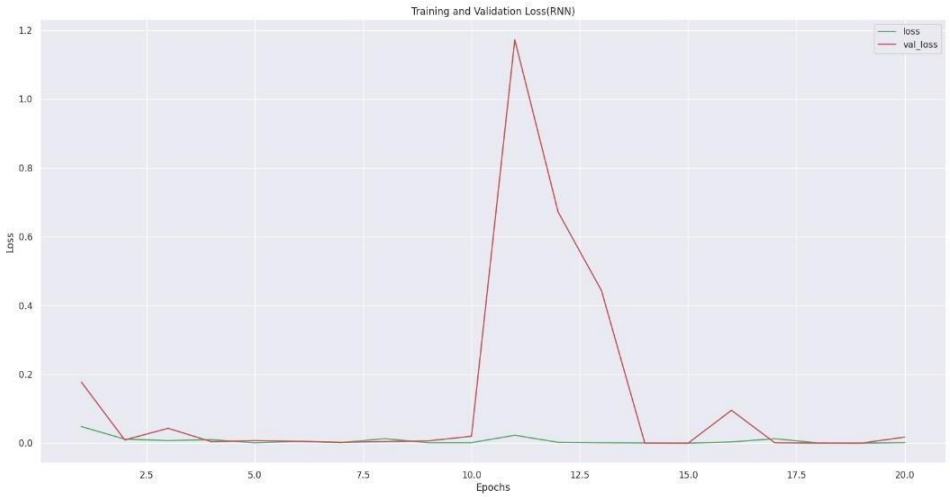
JITEKH
Jurnal Ilmiah Teknologi Harapan
P-ISSN: 2338-5677 || E-ISSN 2549-6646
Vol. 12, No. 2, September 2024
DOI: https://doi.org/10.35447/jitekh.v12i2.996

Gambar 5. Visualisasi Proses Training

3.5 Model Prediksi

Model dari RNN dalam melakukan klasifikasi deteksi serangan IDS. Model ini digunakan untuk memproses data berdimensi tinggi. Pada penerapan validation accuracy merupakan pengembangan model Recurrent Neural Network (RNN) adalah bagian penting dari revolusi teknologi dalam pemrosesan klasifikasi IDS. Saat kita memahami bagaimana model RNN bekerja, penting untuk memerhatikan dua metrik utama yang membantu kita mengukur kinerja model ini: Training Accuracy dan Validation Accuracy. Penelitian ini melatih sebuah model RNN dengan memasukkan data pelatihan yang terdiri dari ribuan atau bahkan jutaan gambar kedalam model. Model RNN ini kemudian belajar untuk mengenali pola data tersebut. Training Accuracy adalah metrik yang mengukur sejauh mana model berhasil dalam mengenali gambar-gambar ini saat melatih. Training Accuracy yang tinggi menunjukkan bahwa model mampu dengan baik dalam menghafal dan mengenali gambar-gambar dari data pelatihan. Hasil training evaluasi terdapat pada gambar 6.

Kemudian terdapat testing validation yang merupakan pemrosesan bahasa alami dan tugas berbasis urutan lainnya, model Recurrent Neural Network (RNN) adalah salah satu alat paling kuat yang digunakan untuk memahami dan menghasilkan urutan data. Dalam menerapkan klasifikasi serangan IDS terdapat metrik kunci yang digunakan untuk mengukur kinerjanya yaitu Testing Accuracy. Saat melatih sebuah model RNN, data pelatihan digunakan untuk mengajarinya bagaimana memahami pola urutan dalam data. Setelah model RNN dianggap memadai berdasarkan Validation Accuracy, langkah selanjutnya adalah menguji model pada data tes yang sepenuhnya baru. Testing Accuracy adalah metrik yang mengukur sejauh mana model mampu melakukan prediksi yang akurat pada datates ini. Ini adalah pengukuran akhir yang menentukan seberapa baik model RNN berkinerja dalam tugas pengujian sebenarnya.



Gambar 6. Model Prediksi

Setelah melatih model RNN mendalam kita pada data pelatihan dan memvalidasinya pada data validasi, dapat diartikan bahwa: Model dilatih pada 50 epoch menghasilkan akurasi sebesar 99% yang dibuktikan dengan evaluasi pada gambar 7.

JITEKH
Jurnal Ilmiah Teknologi Harapan
P-ISSN: 2338-5677 || E-ISSN 2549-6646
Vol. 12, No. 2, September 2024
DOI: https://doi.org/10.35447/jitekh.v12i2.996

	precision	recall	f1-score	support
benign	0.98	1.00	0.99	1007
ftp_bruteforce	1.00	0.98	0.99	996
ssh_bruteforce	1.00	1.00	1.00	997
accuracy			0.99	3000
macro avg	0.99	0.99	0.99	3000
weighted avg	0.99	0.99	0.99	3000

```
94/94 [==============================] - 1s 10ms/step - loss: 0.0176 - accuracy: 0.9937
Test: accuracy = 0.993667  ;  loss = 0.017611
```

Gambar 7. Hasil Akurasi

3.6 Tabel Pengujian

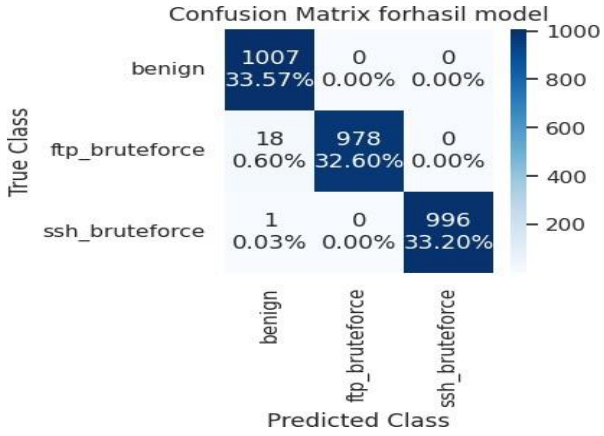
Tabel pengujian digunakan untuk mencatat dan mengorganisir hasil-hasil pengujian yang telah dilakukan dan dapat dilihat pada tabel 1.

Tabel 1. Pengujian

No	Data	Label	Prediksi
1	Data 1	Benign	Benign
2	Data 2	Benign	Benign
3	Data 3	FTP brute force attack	FTP brute force attack
4	Data 4	FTP brute force attack	Benign
5	Data 5	SSH brute force attack	SSH brute force attack
6	Data 6	FTP brute force attack	Benign
7	Data 7	FTP brute force attack	FTP brute force attack
8	Data 8	SSH brute force attack	SSH brute force attack
9	Data 9	SSH brute force attack	SSH brute force attack
10	Data 10	FTP brute force attack	SSH brute force attack

3.7 Confusion Matriks

Teknik yang umum digunakan dalam evaluasi kinerja model klasifikasi, terutama dalam pembelajaran mesin. Ini adalah tabel yang digunakan untuk mengevaluasi kinerja model dengan membandingkan hasil prediksi model dengan nilai sebenarnya dari data yang diamati. Berikut ini hasil confusion matriks yang terdapat pada gambar 8.



Gambar 8. Confusion Matriks

JITEKH
Jurnal Ilmiah Teknologi Harapan
P-ISSN: 2338-5677 || E-ISSN 2549-6646
Vol. 12, No. 2, September 2024
DOI: https://doi.org/10.35447/jitekh.v12i2.996

```
                precision    recall  f1-score   support

        benign       0.98      1.00      0.99      1007
ftp_bruteforce       1.00      0.98      0.99       996
ssh_bruteforce       1.00      1.00      1.00       997

      accuracy                           0.99      3000
     macro avg       0.99      0.99      0.99      3000
  weighted avg       0.99      0.99      0.99      3000

94/94 [==============================] - 1s 10ms/step - loss: 0.0176 - accuracy: 0.9937
Test: accuracy = 0.993667  ;  loss = 0.017611
```

Gambar 9 Evaluasi Kinerja

Berdasarkan gambar 8 terdapat confusion matriks yang akan digunakan untuk evaluasi model prediksi yang menggunakan algoritma RNN, sedangkan pada gambar 9 terdapat akurasi yang dihasilkan oleh model yaitu 0.99%. kemudian pada gambar 9 terdapat presisi, recall dan akurasi. Pada akurasi akan mengukur seberapa sering model memberikan prediksi yang benar secara keseluruhan dibandingkan dengan total jumlah prediksi. Pada Presisi mengukur seberapa banyak dari prediksi positif yang sebenarnya benar dan Recall mengukur seberapa banyak dari kelas positif yang benar terdeteksi oleh model.

4. KESIMPULAN

Implementasi RNN menunjukkan bahwa penelitian ini memanfaatkan teknik kecerdasan buatan dalam bentuk jaringan saraf rekuren untuk meningkatkan kemampuan sistem dalam mendeteksi serangan jaringan. Keamanan jaringan kemungkinan besar berkaitan dengan keamanan jaringan, yang merupakan aspek penting dalam dunia komputasi modern. RNN untuk mendeteksi serangan jaringan, ini bisa mencakup berbagai jenis serangan seperti serangan malware, serangan DDoS, atau upaya peretasan. Berdasarkan hasil uji coba model dilatih dengan jumlah 50 epoch menghasilkan akurasi sebesar 92%. Sedangkan model dengan jumlah 30 epoch menghasilkan akurasi sebesar 99%. Jadi, model dapat bekerja dengan baik terhadap data pelatihan dengan jumlah 30 epoch.

REFERENSI

[1] Muhammad Irfan Hilmy and Rama Halim Nur Azmi, “Konstruksi Pertahanan Dan Keamanan Negara Terhadap Perlindungan Data Dalam Cyberspace Untuk Menghadapi Pola Kebiasaan Baru.,” *Lemhannas RI*, vol. 9, no. 1, pp. 124–124, Mar. 2021.

[2] Rizaldi, A. (2022). *Pengembangan Cyber Security Indonesia Dalam Upaya Menghadapi Ancaman Cyber Crime Melalui Badan Siber Dan Sandi Negara (BSSN)*. Universitas Muhammadiyah Malang.

[3] Sutarti and Alif Alfiyansyah, “Analisis dan Implementasi Sistem Monitoring Koneksi Internet Menggunakan The Dude Di STIKOM Al Khairiyah,” *J. Sist. Inf.*, vol. 4, no. 1, pp. 45–45, Oct. 2017.

[4] J. Jabez and B. Muthukumar, “Instrusion detection System (IDS): Anomaly Detection Using Outlier Detection Approach. Procedia Computer Science ,” *Procedia Comput. Sci.*, vol. 48, no. 1, pp. 346–346, May 2015.

[5] R. Vinayakumar, Mamoun Alazab, K.P. Soman, Prabaharan Poornachandran, Ameer Al-Nemrat, and Sitalakshmi Venkatraman, “Deep Learning Approach For Intelligent Instrusion Detection System,” *IEEE*, vol. 7, no. 1, pp. 41525–41550, Apr. 2019.

[6] Malabay. (2021). Pemanfaatan Flowchart Untuk Kebutuhan Deskripsi Proses Bisnis. *Jurnal Ilmu Komputer*, *12*(1), 21–26. Https://Digilib.Esaunggul.Ac.Id/Pemanfaatan-Flowchart-Untuk-Kebutuhan-Deskripsi-Proses-Bisnis-9347.Html.

[7] Muhammad Rizki, Setio Basuki, and Yufis Azhar, “Implementasi Deep Learning Menggunakan Arsitektur Long Short Term Memory(LSTM) Untuk Prediksi Curah Hujan Kota Malang.,” *J. Rpositor*, vol. 2, no. 3, pp. 338–338, Mar. 2020.

[8] E. D. Tarkus, S. R. U. A. Sompue, dan A. Jacobus, "Implementasi Metode Recurrent Neural Network pada Pengklasifikasian Kualitas Telur Puyuh," *J. Tek. Imform.*, vil. 15, no. 2, hal 137-144,2020, doi: 10.35793/jti.v15i2.29552.

JITEKH
Jurnal Ilmiah Teknologi Harapan
P-ISSN: 2338-5677 || E-ISSN 2549-6646
Vol. 12, No. 2, September 2024
DOI: https://doi.org/10.35447/jitekh.v12i2.996

[9] D. S. Winantio, Eko Arip, Kurniabudi, Sharipuddin, Ibnu Sani Wijaya, "Deteksi Serangan Pada Jaringan Kompleks IoT Menggunakan Recurrent Neural Network," *J. Ris. Komput.*, vol. 9, no. 6, 2022, doi: htpp://dx.doi.org/10.30865/jurikom.v9i6.5298.

[10] Sugiarti, Y., & Sulaeman, O. (2015). Rancang Bangun Knowledge Management System Bahan Ajar Online Dalam Meningkatkan Kompetensi Guru Mts Negeri 2 Pamulang. *Jti (Jurnal Teknik Informatika) Uin Syarif Hidayatullah*, 1–6.

[11] Sugiarti, Y., & Sulaeman, O. (2015). Rancang Bangun Knowledge Management System Bahan Ajar Online Dalam Meningkatkan Kompetensi Guru Mts Negeri 2 Pamulang. *Jti (Jurnal Teknik Informatika) Uin Syarif Hidayatullah*, 1–6.

[12] Mamay Syani, "Implementasi Intrusion Detection System (IDS) Menggunakan Suricata Pada Linux Debian 9 Berbasis Cloud Virtual Private Servers (VPS)," *J. Inkofar*, vol. 1, no. 1, pp. 9–9, Aug. 2020.

[13] I Komang Setia Buana, "Implementasi Aplikasi Speech To Text Untuk Memudahkan Wartawan Mencatat Wawancara Dengan Python," *J. Sist. dan Inform.*, vol. 14, no. 2, pp. 135–142, Aug. 2020.

[14] Suyanto, Ramadhani, K. N., & Mandala, S. (2019). Deep Learning Modernisasi Machine Learning Untuk Big Data. Penerbit INFORMATIKA

[15] Michelucci, U. (2019), Advanced Applied Deep Learning Convolution Neural Networks and Object Detection. SSBM Finence Inc.

[16] Primartha, R. (2018). Belajar Machine Learning Teori Dan Praktik. Penerbit INFORMATIKA.

[17] W. Seok, Y. Kim, and C. Park, "Pattern Recognition Of Human Arm Movement Using Deep Reinforcement Learning Intelligent Information System And Embedded Software Engineering," *Kwangwoon Univ.*, pp. 917–919, 2018.

[18] Noertjahyana, A., & Adipranata, R. (2020). Ipsec Sebagai Salah Satu Solusi Keamanan Data Pada Jaringan Komputer. *Seminar Nasional Aplikasi Teknologi Informasi*, *2005*(Snati).

[19] Rahino, B. G, & Susila A. (2022). Implementasi Jaringan VPN (L2TPIpsec) Mikrotik Untuk *Remote Accsess* Sebagai *Security* Selama *Work From Home*. *Jurnal Ilmu Komputer dan Science*, 1(11), 1911-1918.

[20] Dalia Ezzat, Aboul Ella Hassanien, and Hassan Aboul Ella, "An Optimized Deep Learning Architecture For The Diagnosis Of Covid-19 Disease Based On Gravitational Search Optimization," *Appl. Soft Comput.*, vol. 98, Jan. 2021.