Seminar Nasional Teknologi dan Inovasi (SITASI)
Vol 1, Nomor 1, Juli 2025, hal. 162-171
P-ISSN: XXXX-XXXX | E-ISSN: XXXX- XXXX
Penerbit Institut Bisnis dan Teknologi Indonesia

Analisis dan Evaluasi Model BiLSTM untuk Klasifikasi Serangan Botnet pada Dataset CTU-13

I Nyoman Buda Hartawan[1*], Ni Wayan Suardiati Putri[2], Evi Dwi Krisna [3], Gede Ariel Christian[4]

[1*,2,3,4] *Institut Bisnis dan Teknologi Indonesia, Denpasar, Indonesia*
[1*] *buda.hartawan@instiki.ac.id,* [2]*suardiatiputri@instiki.ac.id,* [2] *evidwikrisna@yahoo.co.id,* [3] *ariel.christian79@gmail.com*

INFO ARTIKEL

Article history:
Received Date Month Year
Accepted Date Month Year
Published Date Month Year

ABSTRAK

Penelitian ini bertujuan untuk mengembangkan dan mengevaluasi model deteksi serangan siber menggunakan arsitektur Bidirectional Long Short-Term Memory (BiLSTM) pada dataset CTU-13, khususnya pada skenario "Neris", yang berfokus pada identifikasi aktivitas botnet dalam lalu lintas jaringan. Dengan meningkatnya kompleksitas serangan siber, metode deteksi yang efektif dan efisien sangat penting untuk melindungi sistem jaringan dari ancaman yang semakin canggih. Model BiLSTM diterapkan untuk mendeteksi pola serangan dalam data jaringan dengan mempertimbangkan rasio pembagian data pelatihan dan validasi yang bervariasi, guna menilai pengaruh pembagian data terhadap kinerja model. Hasil penelitian menunjukkan bahwa rasio 90:10 menghasilkan performa terbaik, dengan tingkat akurasi mencapai 96,68%, recall sebesar 88,63%, dan F1 score 91,02%, yang menandakan keseimbangan optimal antara akurasi dan kemampuan model dalam mendeteksi serangan. Rasio ini juga secara signifikan mengurangi tingkat False Negative, yang penting untuk meningkatkan deteksi serangan yang lebih sensitif terhadap ancaman yang tidak terdeteksi.

Kata Kunci: BiLSTM, CTU-13, Klasifikasi, Machine Learning, Neris

ABSTRACT

This study aims to develop and evaluate a cybersecurity attack detection model using Bidirectional Long Short-Term Memory (BiLSTM) architecture on the CTU-13 dataset, specifically in the "Neris" scenario, focusing on botnet activity identification in network traffic. With the increasing complexity of cyberattacks, effective and efficient detection methods are crucial to protect network systems from more advanced threats. The BiLSTM model is applied to detect attack patterns in network data by considering varying training and validation data splits to assess the impact of data partitioning on model performance. The results show that the 90:10 ratio yields the best performance, with accuracy reaching 96.68%, recall at 88.63%, and an F1 score of 91.02%, indicating an optimal balance between accuracy and the model's ability to detect attacks. This ratio also significantly reduces the False Negative rate, which is important for improving the detection of attacks that may otherwise go undetected.

Keywords: BiLSTM, CTU-13, Classification, Machine Learning, Neris

©2025 Authors. Licensed Under CC-BY-NC-SA 4.0

1. Pendahuluan

Serangan siber saat ini telah menjadi ancaman yang sangat serius di dunia digital. Di tengah kemajuan teknologi yang pesat, ancaman terhadap sistem informasi dan data pribadi semakin kompleks dan beragam. Serangan siber seperti malware (Udiyono et al., 2020), ransomware (Ng et al., 2020), phishing (Y. Chen et al., 2024), dan denial-of-service (DoS)(Alabdulatif et al., 2024) memiliki potensi untuk menyebabkan kerusakan signifikan terhadap berbagai sektor, baik pemerintah, industri, maupun individu. Selain kerugian finansial yang besar, serangan ini juga dapat merusak reputasi perusahaan dan mengganggu operasi yang vital. Oleh karena itu, penting untuk mengembangkan sistem deteksi yang lebih efektif dan cepat dalam mengidentifikasi jenis-jenis serangan ini agar dapat mengurangi dampak yang ditimbulkan.

Dalam menghadapi ancaman siber yang semakin canggih, metode deteksi tradisional sering kali tidak cukup memadai untuk mengatasi volume data yang besar dan kompleksitas serangan yang terus berkembang. Pembelajaran mesin (machine learning) telah menjadi salah satu solusi untuk meningkatkan efektivitas sistem deteksi serangan siber. Penelitian dalam pemanfaatan *artificial intelligence*, *machine learning*, maupun *deep learning* dalam keamanan siber semakin meningkat (Bartwal et al., 2022; M. Chen et al., 2025; Irshad & Basit Siddiqui, 2023; Mishra et al., 2025; Pérez-Gomariz et al., 2025; Rahali & Akhloufi, 2023). Teknologi ini memungkinkan sistem untuk belajar dari data yang ada, mengenali pola-pola serangan, dan memberikan respons yang lebih cepat dan tepat. Salah satu metode pembelajaran mesin yang menunjukkan hasil menjanjikan dalam deteksi serangan siber adalah Bidirectional Long Short-Term Memory (BiLSTM) (Vellela et al., 2025), yang merupakan pengembangan dari Long Short-Term Memory (LSTM) dalam deep learning.

BiLSTM memiliki kemampuan unik dalam memproses data sekuensial dengan mempertimbangkan informasi dari kedua arah, yaitu masa lalu dan masa depan (Zhen & Gao, 2023). Dalam konteks deteksi serangan siber, hal ini sangat penting karena banyak serangan yang memiliki pola yang dapat teridentifikasi tidak hanya dari data sebelumnya, tetapi juga dari data yang terjadi setelahnya (Abu Talib et al., 2022). Dengan kemampuan ini, BiLSTM dapat menangkap informasi yang lebih komprehensif dari data sekuensial, seperti log aktivitas jaringan atau sistem, sehingga meningkatkan akurasi dalam klasifikasi serangan siber. Oleh karena itu, BiLSTM menjadi pilihan yang baik dalam aplikasi deteksi dan klasifikasi serangan yang memerlukan pemahaman pola kompleks dalam data sekuensial.

Untuk mendeteksi serangan botnet, yang merupakan salah satu jenis serangan yang paling merusak, diperlukan dataset yang representatif. CTU-13 adalah salah satu dataset yang banyak digunakan dalam penelitian keamanan siber (Firdaus et al., 2023; Putri et al., 2020), terutama untuk mendeteksi aktivitas botnet. Dataset ini dikumpulkan oleh Czech Technical University (CTU) dan berisi data lalu lintas jaringan yang mencakup berbagai jenis aktivitas, baik yang normal maupun yang terindikasi sebagai serangan botnet (Putra et al., 2022). CTU-13 sangat berharga karena mencakup rekaman data lalu lintas yang bercampur antara aktivitas botnet dan lalu lintas jaringan normal, memberikan tantangan bagi model deteksi untuk membedakan antara keduanya. Dataset ini mencakup file pcap (packet capture) dan file NetFlow yang memberikan informasi lebih detail mengenai koneksi antar perangkat dalam jaringan, yang memungkinkan para peneliti mengembangkan dan menguji algoritma deteksi dengan lebih baik.

Namun, dalam penerapan BiLSTM untuk klasifikasi serangan siber, ada beberapa faktor yang dapat mempengaruhi kinerja model secara signifikan. Salah satunya adalah pembagian data untuk pelatihan dan pengujian. Pembagian data yang tidak tepat dapat menyebabkan model tidak dapat belajar secara optimal, sehingga berisiko mengalami overfitting atau underfitting (Mubarak et al., 2025). Overfitting terjadi ketika model terlalu menyesuaikan diri dengan data pelatihan sehingga tidak dapat menggeneralisasi dengan baik pada data pengujian, sementara underfitting terjadi ketika model tidak cukup belajar dari data pelatihan dan menghasilkan kinerja yang buruk pada data baru. Oleh karena itu, penting untuk menentukan rasio pembagian data pelatihan dan pengujian yang optimal untuk mendapatkan hasil yang maksimal.

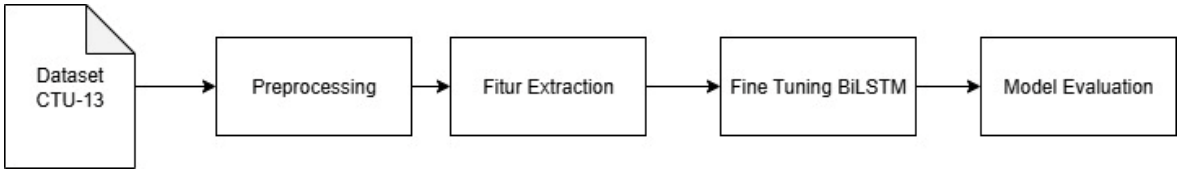
Penelitian ini bertujuan untuk menganalisis dan mengevaluasi kinerja model BiLSTM dalam mengklasifikasikan serangan botnet pada dataset CTU-13, dengan melakukan eksperimen menggunakan berbagai rasio pembagian data pelatihan dan pengujian, seperti 70:30, 80:20, dan 90:10. Dengan melakukan eksperimen ini, diharapkan dapat ditemukan rasio pembagian data yang optimal, yang memberikan keseimbangan terbaik antara akurasi dan kemampuan model untuk menggeneralisasi ke data yang tidak terlihat sebelumnya. Selain itu, penelitian ini juga bertujuan untuk memberikan kontribusi dalam pengembangan sistem deteksi serangan siber berbasis deep learning yang lebih efisien, yang dapat diadaptasi untuk menghadapi ancaman yang semakin canggih dan beragam.

Hasil dari penelitian ini diharapkan dapat memberikan wawasan baru mengenai bagaimana rasio pembagian data mempengaruhi kinerja model BiLSTM dalam deteksi serangan siber. Dengan sistem

deteksi yang lebih akurat, diharapkan ancaman siber dapat dideteksi lebih cepat dan lebih tepat, sehingga dapat mengurangi risiko kerusakan yang ditimbulkan. Penelitian ini juga berpotensi memberikan dampak positif bagi pengembangan teknologi keamanan siber di masa depan, terutama dalam meningkatkan kemampuan sistem untuk menangani volume serangan yang terus berkembang dan semakin kompleks.

2. Metode Penelitian

Pada penelitian ini, framework yang diajukan bertujuan untuk membangun sistem deteksi anomali jaringan menggunakan metode machine learning, khususnya dengan model Bidirectional Long Short-Term Memory (BiLSTM). Framework ini dirancang dengan melalui serangkaian langkah, mulai dari pemilihan dataset, proses preprocessing, ekstraksi fitur, pelatihan model, hingga evaluasi performa model. Penelitian ini berfokus pada penggunaan dataset CTU-13 yang telah banyak digunakan dalam analisis lalu lintas jaringan, baik untuk deteksi serangan maupun identifikasi pola lalu lintas yang normal.



Gambar 1 Alur Penelitian

a) Pemilihan Dataset: CTU-13

Dataset CTU-13 merupakan kumpulan data yang berisi lalu lintas jaringan yang dikumpulkan dari berbagai percobaan yang melibatkan berbagai jenis serangan siber, seperti DoS (Denial of Service), DDoS (Distributed Denial of Service), dan serangan berbasis malware. Keberagaman jenis serangan dalam dataset ini menjadikannya sangat relevan dalam mengembangkan sistem deteksi anomali yang dapat mengidentifikasi berbagai pola serangan pada jaringan secara lebih akurat. Pemilihan dataset yang tepat menjadi langkah awal yang penting dalam membangun model machine learning yang dapat menangani permasalahan deteksi anomali jaringan.

b) Preprocessing Data

Langkah preprocessing merupakan tahapan yang tak kalah penting dalam pipeline machine learning karena dapat menentukan kualitas data yang digunakan dalam pelatihan model. Pada tahap ini, data mentah yang berupa paket-paket jaringan perlu dibersihkan, diolah, dan dipersiapkan dalam format yang lebih terstruktur. Beberapa tahapan dalam preprocessing antara lain:

- Pembersihan Data: Menghilangkan data yang tidak relevan atau memiliki nilai yang hilang. Proses ini penting untuk mencegah model dari pembelajaran yang bias akibat ketidaksesuaian data.
- Normalisasi Data: Menyelaraskan skala antar fitur untuk menghindari dominasi satu fitur atas fitur lainnya dalam proses pelatihan model.
- Pengkodean Data Kategorikal: Mengubah data kategorikal, seperti jenis protokol, menjadi format numerik yang dapat diterima oleh model machine learning.
- Tahap preprocessing yang matang akan menghasilkan data yang lebih bersih, yang akan memungkinkan model untuk belajar dari informasi yang lebih relevan dan berguna.

c) Ekstraksi Fitur

Setelah data diproses, langkah berikutnya adalah ekstraksi fitur. Proses ini berfungsi untuk mengidentifikasi atribut-atribut penting yang relevan dalam membedakan antara lalu lintas jaringan yang normal dan yang mencurigakan. Beberapa fitur yang umumnya diekstraksi dari data jaringan termasuk:

- Ukuran Paket: Ukuran paket data yang dikirimkan dapat memberikan indikasi terkait dengan jenis lalu lintas, baik itu normal ataupun serangan.
- Tipe Protokol: Protokol yang digunakan dalam komunikasi jaringan dapat menjadi indikator dari tipe serangan atau aktivitas yang mencurigakan.
- Jumlah Koeksi: Banyaknya koneksi yang terjadi dalam waktu tertentu dapat menunjukkan adanya pola serangan seperti DDoS.

Ekstraksi fitur yang tepat dapat mengurangi dimensi data dan hanya mempertahankan informasi yang memiliki relevansi tinggi untuk tugas klasifikasi, sehingga memungkinkan model untuk bekerja lebih efisien dan efektif.

d) Pelatihan Model dengan Fine Tuning BiLSTM

Pada tahap ini, model BiLSTM digunakan untuk pelatihan data yang telah diproses. BiLSTM merupakan salah satu jenis jaringan syaraf tiruan berbasis LSTM yang mengolah data secara bidirectional, yaitu mempertimbangkan konteks baik dari urutan data sebelumnya maupun yang akan datang. Hal ini menjadikan BiLSTM sangat efektif untuk menangani data yang bersifat sekuensial, seperti lalu lintas jaringan.

Proses fine-tuning pada BiLSTM dilakukan untuk mengoptimalkan kinerja model. Fine-tuning ini mencakup penyesuaian berbagai hyperparameter, seperti jumlah lapisan LSTM, ukuran batch, laju pembelajaran, dan jumlah epoch, yang dapat memengaruhi kemampuan model dalam mempelajari pola-pola yang ada pada data. Selama pelatihan, model akan berusaha meminimalkan error antara prediksi dan label yang sebenarnya dengan menggunakan algoritma backpropagation dan optimisasi seperti Adam atau SGD.

e) Evaluasi Model

Setelah model dilatih, tahap selanjutnya adalah evaluasi untuk mengukur seberapa baik model dalam melakukan prediksi pada data yang belum pernah dilihat sebelumnya (data uji). Beberapa metrik evaluasi yang digunakan untuk menilai performa model adalah:

- Akurasi: Menunjukkan seberapa banyak prediksi yang benar dibandingkan dengan total prediksi yang dilakukan.
- Presisi dan Recall: Mengukur seberapa baik model dalam mengidentifikasi serangan (positif) dan seberapa sedikit kesalahan dalam mengklasifikasikan data normal sebagai serangan.
- F1-Score: Merupakan rata-rata harmonis antara presisi dan recall, yang memberikan gambaran lebih jelas tentang keseimbangan antara keduanya.
- Confusion Matrix: Menunjukkan jumlah prediksi yang benar dan salah pada masing-masing kategori (benign atau malicious).

Evaluasi yang komprehensif ini memberikan gambaran tentang kekuatan dan kelemahan model dalam mengklasifikasikan jenis lalu lintas jaringan yang berbeda, serta memberikan informasi mengenai area yang perlu diperbaiki untuk meningkatkan kinerja model.

3. Hasil dan Pembahasan

3.1. Hasil Penelitian

Penelitian ini bertujuan untuk mengembangkan dan mengevaluasi model deteksi serangan siber menggunakan dataset CTU-13, khususnya skenario "Neris". Melalui serangkaian tahapan yang meliputi preprocessing data, ekstraksi fitur, fine-tuning model BiLSTM, dan evaluasi model, penelitian ini berfokus pada kemampuan model dalam mendeteksi pola serangan dalam lalu lintas jaringan yang mengandung aktivitas botnet. Setiap tahapan yang dilakukan dalam penelitian ini memiliki peran penting untuk memastikan data yang digunakan berkualitas tinggi dan model yang dikembangkan dapat menghasilkan prediksi yang akurat. Dalam bagian selanjutnya, pembahasan akan dimulai dengan deskripsi mengenai dataset yang digunakan, diikuti dengan tahap-tahap lain yang dilakukan untuk mempersiapkan dan mengevaluasi model deteksi serangan.

a) Dataset CTU-13

Penelitian ini menggunakan dataset CTU-13 yang diambil dari skenario "Neris" yang berisi data lalu lintas jaringan yang mencakup aktivitas botnet dan lalu lintas normal. Dataset ini diambil dari CTU University, Republik Ceko, pada tahun 2011, dan menjadi referensi penting dalam studi keamanan siber. Dataset ini mencakup berbagai jenis data, termasuk file pcap yang merekam jenis lalu lintas (serangan, normal, dan latar belakang) serta file NetFlow yang dihasilkan menggunakan Argus. Data yang tercatat di dalamnya sangat berguna untuk analisis lebih lanjut terhadap perilaku botnet dalam jaringan. Tujuan utama dari penggunaan dataset ini adalah untuk menguji dan mengevaluasi teknik-teknik deteksi botnet dan analisis serangan siber lainnya, yang memungkinkan peneliti untuk mengembangkan dan menguji sistem deteksi botnet yang lebih efektif.

b) Preprocessing

Pada tahap ini, data yang diperoleh dari dataset CTU-13 dipersiapkan untuk digunakan dalam model BiLSTM. Preprocessing dilakukan dengan menggunakan berbagai pustaka Python seperti Pandas dan NumPy untuk memanipulasi data. Proses ini mencakup konversi kolom label menjadi format biner, di mana serangan (Attack) diberi label 1 dan latar belakang (Background) diberi label 0. Selain itu, fitur-fitur yang relevan seperti dur, tot_pkts, tot_bytes, dan src_bytes dipilih untuk digunakan dalam pelatihan model. Langkah-langkah preprocessing ini bertujuan untuk memastikan bahwa data yang digunakan sudah siap dan dapat digunakan secara optimal pada model BiLSTM yang akan dibangun.

Selanjutnya, data dibagi menjadi dua set, yaitu data latih (training) dan data uji (testing), dengan rasio pembagian 80:20 menggunakan fungsi train_test_split. Pembagian data yang tepat ini sangat penting karena memastikan model BiLSTM dapat dilatih pada data yang representatif dan dapat diuji untuk menggeneralisasi data yang belum pernah dilihat sebelumnya. Selain itu, data yang telah dibagi ini diubah menjadi format tiga dimensi (sampel, timesteps, fitur), yang merupakan format yang diperlukan untuk model LSTM.

c) Fitur Ekstraksi

Setelah tahap preprocessing selesai, langkah selanjutnya adalah fitur ekstraksi. Pada tahap ini, fitur-fitur yang relevan seperti durasi koneksi (dur), jumlah paket yang dikirim (tot_pkts), total byte yang dikirim (tot_bytes), dan byte yang diterima dari sumber (src_bytes) dipilih dan diproses lebih lanjut untuk digunakan dalam model pelatihan. Pemilihan fitur yang tepat sangat penting untuk mengurangi kompleksitas model dan meningkatkan kinerja model dalam mendeteksi pola serangan. Fitur-fitur ini dipilih karena diyakini dapat memberikan informasi yang cukup untuk membedakan antara serangan dan latar belakang dalam data jaringan. Dengan pemilihan fitur yang relevan, data yang digunakan akan lebih terfokus dan memiliki kualitas yang lebih baik untuk pelatihan model.

d) Fine Tuning BiLSTM

Pada tahap ini, model BiLSTM (Bidirectional Long Short-Term Memory) dibangun dan dilatih untuk mengklasifikasikan data sebagai serangan atau latar belakang. BiLSTM dipilih karena kemampuannya dalam memproses data sekuensial dalam dua arah, yaitu maju (forward) dan mundur (backward), yang membedakannya dengan LSTM standar. Model BiLSTM ini terdiri dari lapisan input, dua lapisan BiLSTM, dan lapisan output yang menggunakan fungsi aktivasi sigmoid untuk menghasilkan output biner (serangan atau latar belakang). Proses fine-tuning dilakukan untuk mengoptimalkan parameter-parameter model, termasuk jumlah epoch, ukuran batch, dan kecepatan pembelajaran, agar model dapat belajar dengan lebih efektif.

Tabel 1 Perbandingan Performa Model *Epoch* 20

Rasio Data	Akurasi Pelatihan	Loss Pelatihan	Akurasi Validasi	Loss Validasi
60:40	0.9243	0.2099	0.9312	0.1858
70:30	0.9433	0.1376	0.9448	0.1314
80:20	0.9589	0.1043	0.9522	0.1195
90:10	0.9564	0.1089	0.9670	0.0898

Beberapa eksperimen dilakukan dengan menggunakan rasio pembagian data yang berbeda, yaitu 60:40, 70:30, 80:20, dan 90:10. Tujuan dari eksperimen ini adalah untuk menguji bagaimana perubahan rasio pembagian data dapat mempengaruhi kinerja model. Hasil eksperimen menunjukkan bahwa model BiLSTM dapat mengenali pola serangan dengan baik dan stabil meskipun ada perubahan dalam rasio pembagian data. Hal ini menunjukkan bahwa model BiLSTM memiliki kemampuan yang baik dalam mendeteksi serangan pada jaringan.

e) Model Evaluation

Setelah model selesai dilatih, tahap selanjutnya adalah evaluasi model untuk mengukur kinerjanya. Evaluasi dilakukan dengan menggunakan metrik-metrik seperti akurasi, precision, recall, F1-score, dan confusion matrix. Hasil evaluasi menunjukkan bahwa model BiLSTM memberikan kinerja yang sangat baik, dengan akurasi tertinggi mencapai 95,82% pada rasio pembagian data 80:20. Selain itu, precision dan recall juga menunjukkan nilai yang baik, meskipun ada sedikit kekurangan dalam mendeteksi semua jenis serangan (recall).

Evaluasi lebih lanjut dengan menggunakan confusion matrix mengungkapkan bahwa meskipun model dapat membedakan antara serangan dan latar belakang dengan akurasi yang tinggi, masih ada ruang untuk perbaikan dalam hal deteksi serangan. Metrik F1-score yang dihasilkan juga menunjukkan peningkatan yang signifikan pada rasio 70:30 dan 80:20, yang mengindikasikan bahwa model semakin mampu menghasilkan prediksi yang lebih akurat.

Secara keseluruhan, model BiLSTM terbukti efektif dalam mendeteksi serangan siber dalam data lalu lintas jaringan, meskipun masih ada potensi untuk meningkatkan recall agar dapat mendeteksi lebih banyak jenis serangan. Evaluasi yang dilakukan menunjukkan bahwa model ini dapat digunakan sebagai dasar untuk mengembangkan sistem deteksi botnet yang lebih baik, dengan potensi penerapan yang luas dalam keamanan siber

Tabel 2 Perbandingan Performa *Accuracy*, *Precision*, *Recall*, dan *F1 Score*

Rasio Data	*Accuracy*	*Precision*	*Recall*	*F1 Score*
60:40	0.9309	0.8743	0.7387	0.8004
70:30	0.9441	0.8667	0.8359	0.8498
80:20	0.9509	0.9601	0.7727	0.8564
90:10	0.9668	0.9354	0.8863	0.9102

Tabel 3 Perbandingan *Confusion Matrix*

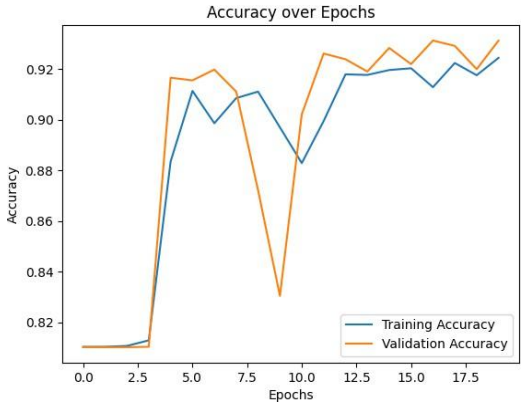
Rasio Data	*True Negative*	*False Positive*	*False Negative*	*True Positive*
60:40	353.946	9.031	22.294	62.821
70:30	264.242	8.162	10.594	53.071
80:20	180.290	1.354	9.636	32.766
90:10	89.463	1.301	2.416	18.843

3.2. Analisis

Penelitian ini bertujuan untuk mengevaluasi kinerja model BiLSTM dalam mendeteksi serangan siber dengan menggunakan dataset CTU-13 yang dibagi berdasarkan berbagai rasio pelatihan dan validasi. Setiap rasio pembagian data memiliki dampak yang signifikan terhadap performa model dalam hal akurasi, precision, recall, dan F1 Score. Dalam bagian analisis ini, akan dibahas secara rinci bagaimana rasio pembagian data mempengaruhi performa model, serta bagaimana nilai metrik evaluasi dan confusion matrix memberikan gambaran mengenai kemampuan model dalam mengklasifikasikan serangan dan latar belakang. Pembahasan ini bertujuan untuk memberikan pemahaman yang lebih dalam tentang pengaruh berbagai rasio pembagian data terhadap efektivitas model BiLSTM dalam tugas deteksi serangan siber.

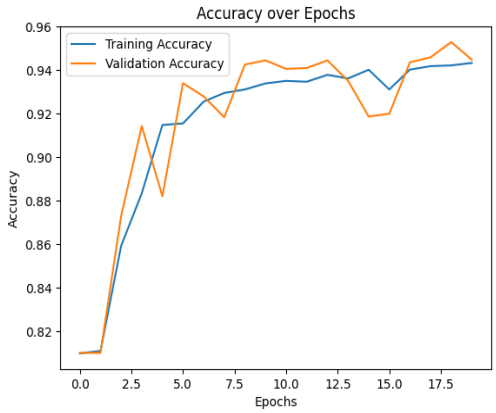
a) Perbandingan performa model pada berbagai rasio

Berdasarkan perbandingan performa model pada berbagai rasio pembagian data pelatihan dan validasi, dapat disimpulkan bahwa rasio pembagian data memiliki pengaruh signifikan terhadap akurasi dan nilai loss model, baik pada tahap pelatihan maupun validasi.



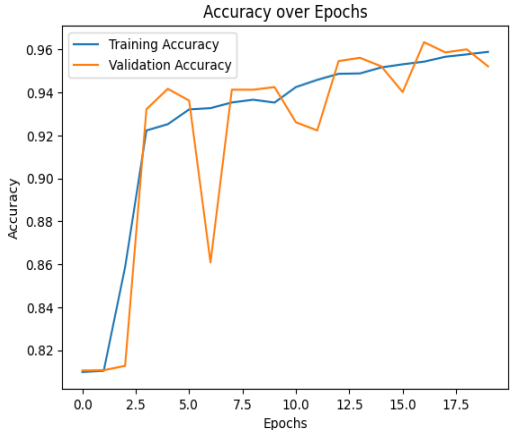
Gambar 2 Accuracy performa model pada perbandingan ratio 60:40

Pada rasio 60:40, akurasi pelatihan mencapai 92,43%, sementara akurasi validasi sedikit lebih tinggi, yaitu 93,12%. Meskipun demikian, nilai loss pelatihan yang sebesar 0,2099 dan loss validasi sebesar 0,1858 menunjukkan bahwa model masih mengalami tingkat kesalahan prediksi yang relatif tinggi jika dibandingkan dengan rasio pembagian data lainnya.



Gambar 3 Accuracy performa model pada perbandingan 70:30

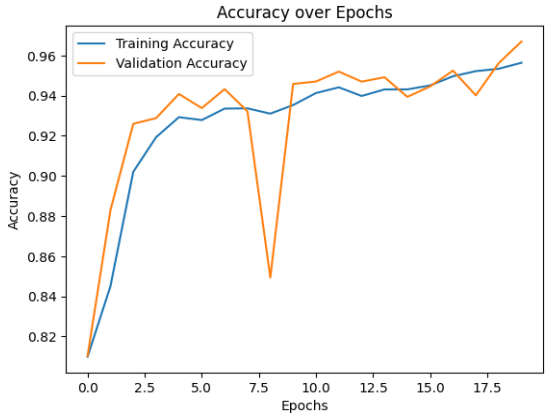
Pada rasio 70:30, terdapat peningkatan signifikan dalam performa model. Akurasi pelatihan mencapai 94,33%, dengan nilai loss pelatihan yang lebih rendah yaitu 0,1376. Akurasi validasi juga meningkat menjadi 94,48%, dengan nilai loss validasi yang menurun menjadi 0,1314. Peningkatan ini mengindikasikan bahwa model semakin efektif dalam mempelajari pola data dan menghasilkan prediksi yang lebih akurat.



Gambar 4 Accuracy performa model pada perbandingan 80:20

Selanjutnya, pada rasio 80:20, akurasi pelatihan terus mengalami peningkatan hingga mencapai 95,89%. Namun, akurasi validasi sedikit menurun menjadi 95,22% jika dibandingkan dengan rasio 70:30. Nilai loss pelatihan dan validasi masing-masing adalah 0,1043 dan 0,1195, yang menunjukkan

bahwa model semakin stabil dan mampu meminimalkan kesalahan prediksi pada data pelatihan maupun validasi.



Gambar 5 Accuracy performa model pada perbandingan 90:10

Rasio 90:10 menunjukkan hasil terbaik pada akurasi validasi, dengan nilai 96,70%, meskipun akurasi pelatihan sedikit lebih rendah (95,64%) dibandingkan dengan rasio 80:20. Namun, nilai loss pelatihan dan validasi masing-masing tercatat pada angka 0,1089 dan 0,0898, yang merupakan nilai terendah dibandingkan dengan rasio pembagian data lainnya. Hal ini menunjukkan bahwa model memiliki kemampuan generalisasi yang baik terhadap data validasi, yang mengindikasikan potensi model untuk diterapkan pada data yang belum pernah dilihat sebelumnya.

Secara keseluruhan, rasio 90:10 memberikan hasil yang paling optimal dalam hal akurasi validasi dan nilai loss. Meskipun rasio 80:20 juga menunjukkan performa yang sangat baik, hasil ini menunjukkan bahwa penggunaan data pelatihan yang lebih besar dapat membantu model dalam belajar lebih efektif, yang pada gilirannya mampu meminimalkan kesalahan dan meningkatkan kualitas prediksi.

b) Perbandingan Performa Model Berdasarkan Metrik Evaluasi

Berdasarkan hasil analisis pada berbagai rasio pembagian data, terlihat bahwa semakin besar proporsi data pelatihan, performa model cenderung meningkat. Pada rasio 60:40, model menghasilkan akurasi sebesar 93,09%, precision 87,43%, recall 73,87%, dan F1 Score 80,04%. Rasio ini menunjukkan performa terendah dibandingkan dengan rasio pembagian lainnya, yang mungkin disebabkan oleh kurangnya jumlah data pelatihan yang digunakan, sehingga kemampuan model untuk mengenali pola serangan terbatas.

Pada rasio 70:30, terjadi peningkatan signifikan dalam kinerja model, dengan akurasi sebesar 94,41%, precision 86,67%, recall 83,59%, dan F1 Score 84,98%. Rasio ini menunjukkan bahwa model mulai seimbang dalam mengidentifikasi kelas positif (serangan) dan kelas negatif (latar belakang), dengan keseimbangan yang lebih baik antara precision dan recall.

Pada rasio 80:20, precision mencapai nilai tertinggi sebesar 96,01%, yang menunjukkan bahwa model sangat efektif dalam mengidentifikasi serangan dengan benar. Namun, recall menurun sedikit menjadi 77,27%, yang mengindikasikan bahwa model masih melewatkan beberapa serangan. F1 Score pada rasio ini meningkat menjadi 85,64%, menunjukkan peningkatan keseimbangan antara precision dan recall.

Terakhir, pada rasio 90:10, performa model mencapai hasil paling optimal, dengan akurasi tertinggi sebesar 96,68%, recall sebesar 88,63%, dan F1 Score sebesar 91,02%. Precision sedikit menurun menjadi 93,54% dibandingkan dengan rasio 80:20, namun secara keseluruhan rasio ini memberikan hasil terbaik dengan keseimbangan yang sangat baik antara akurasi, recall, dan F1 Score.

Dari analisis ini, dapat disimpulkan bahwa rasio 90:10 adalah konfigurasi terbaik untuk model ini, karena menghasilkan performa yang optimal dalam hal akurasi, recall, dan F1 Score. Meskipun rasio 80:20 memiliki precision tertinggi, rasio 90:10 memberikan keseimbangan terbaik antar metrik, yang membuatnya lebih dianjurkan untuk pengembangan model lebih lanjut.

c) Analisis Berdasarkan Confusion Matrix

Tabel berikut menunjukkan perbandingan hasil klasifikasi menggunakan arsitektur BiLSTM untuk berbagai rasio pembagian data (60:40, 70:30, 80:20, dan 90:10). Hasil klasifikasi ini mengungkapkan perbedaan performa yang signifikan pada setiap rasio data yang digunakan.

Pada rasio 60:40, model menunjukkan hasil yang relatif baik, dengan True Negative mencapai 353.946 dan True Positive sebesar 62.821. Namun, False Negative cukup tinggi, yaitu 22.294, yang berarti sejumlah serangan salah diklasifikasikan sebagai latar belakang. Meskipun False Positive relatif rendah (9.031), model masih dapat ditingkatkan dalam hal deteksi serangan yang lebih akurat.

Pada rasio 70:30, meskipun True Negative dan True Positive sedikit menurun dibandingkan rasio 60:40 (264.242 dan 53.071), rasio ini menunjukkan peningkatan signifikan dalam hal False Negative, yang turun menjadi 10.594. Hal ini menunjukkan bahwa model semakin baik dalam mengenali serangan dan mengurangi kesalahan pengklasifikasian. Selain itu, False Positive juga mengalami penurunan menjadi 8.162, yang berarti model lebih tepat dalam membedakan latar belakang dari serangan.

Pada rasio 80:20, model menunjukkan hasil yang semakin baik, dengan False Positive yang sangat rendah, hanya 1.354, dan False Negative yang lebih rendah menjadi 9.636. Meskipun True Positive dan True Negative menurun menjadi 32.766 dan 180.290, rasio ini menunjukkan kemampuan terbaik dalam mengurangi kesalahan klasifikasi pada kedua kategori tersebut. Model ini lebih efektif dalam mengidentifikasi serangan dan latar belakang dengan lebih sedikit kesalahan.

Pada rasio 90:10, meskipun True Negative (89.463) dan True Positive (18.843) tetap tinggi, False Negative sangat rendah (2.416), yang berarti model mampu mengidentifikasi sebagian besar serangan dengan benar. Meskipun False Positive sedikit meningkat menjadi 1.301, model ini tetap menunjukkan performa yang sangat baik, dengan kesalahan pengklasifikasian yang sangat sedikit.

Secara keseluruhan, rasio 80:20 memberikan hasil terbaik dalam hal pengurangan False Positive dan False Negative, menjadikannya rasio yang optimal untuk klasifikasi serangan siber. Rasio ini menunjukkan keseimbangan terbaik antara akurasi dan deteksi serangan. Namun, rasio 90:10 juga menunjukkan kinerja yang sangat baik dalam mengurangi False Negative, meskipun dengan sedikit penurunan pada True Positive dan True Negative. Rasio 70:30 dan 60:40 masih memberikan hasil yang cukup baik, meskipun dengan lebih banyak kesalahan pengklasifikasian serangan.

4. Kesimpulan

Berdasarkan hasil analisis performa model dengan berbagai rasio pembagian data pelatihan dan validasi, dapat disimpulkan bahwa rasio pembagian data berpengaruh signifikan terhadap kinerja model dalam mendeteksi serangan siber. Rasio 90:10 menghasilkan performa terbaik dengan akurasi 96,68%, recall 88,63%, dan F1 Score 91,02%, yang mengindikasikan kemampuan model dalam generalisasi data yang baik. Meskipun rasio 80:20 menunjukkan pengurangan yang signifikan pada False Positive dan False Negative, rasio 90:10 tetap merupakan konfigurasi yang paling optimal, karena memberikan keseimbangan yang sangat baik antara akurasi, recall, dan F1 Score. Berdasarkan temuan ini, disarankan untuk menggunakan rasio 90:10 dalam pengembangan model deteksi serangan siber dengan arsitektur BiLSTM. Model ini dapat diterapkan pada sistem deteksi ancaman real-time, seperti Intrusion Detection Systems (IDS) atau honeypot, untuk meningkatkan akurasi dalam mendeteksi serangan. Meskipun demikian, rasio 80:20 masih dapat dipertimbangkan pada aplikasi yang memerlukan pengurangan False Positive dan False Negative yang lebih baik. Penelitian selanjutnya dapat memperluas pengujian dengan menggunakan teknik preprocessing tambahan, seperti normalisasi atau pengurangan dimensi, serta dataset yang lebih besar dan lebih beragam. Selain itu, eksperimen dengan teknik lain, seperti transfer learning atau ensemble methods, dapat dilakukan untuk meningkatkan akurasi dan kemampuan generalisasi model dalam deteksi serangan siber.

5. Ucapan Terima Kasih

Dengan ini, kami mengucapkan terima kasih yang sebesar-besarnya kepada Institut Bisnis dan Teknologi Indonesia, melalui Direktoran Riset dan Pengabdian Masyarakat (DRPM) yang telah memberikan dukungan dan fasilitasi yang luar biasa dalam penelitian ini. Bantuan yang diberikan, baik berupa sumber daya, fasilitas, maupun bimbingan, sangat berharga dan menjadi faktor penting dalam kelancaran dan kesuksesan penelitian ini.

Daftar Pustaka

Abu Talib, M., Nasir, Q., Bou Nassif, A., Mokhamed, T., Ahmed, N., & Mahfood, B. (2022). APT beaconing detection: A systematic review. *Computers and Security*, *122*. https://doi.org/10.1016/j.cose.2022.102875

Alabdulatif, A., Thilakarathne, N. N., & Aashiq, M. (2024). Machine Learning Enabled Novel Real-Time IoT Targeted DoS/DDoS Cyber Attack Detection System. *Computers, Materials and Continua*, *80*(3), 3655–3683. https://doi.org/10.32604/cmc.2024.054610

Bartwal, U., Mukhopadhyay, S., Negi, R., & Shukla, S. (2022). Security Orchestration, Automation, and Response Engine for Deployment of Behavioural Honeypots. *5th IEEE Conference on Dependable and Secure Computing, DSC 2022 and SECSOC 2022 Workshop, PASS4IoT 2022 Workshop SICSA International Paper/Poster Competition in Cybersecurity*, 1–8. https://doi.org/10.1109/DSC54232.2022.9888808

Chen, M., Zhu, K., Lu, B., Li, D., Yuan, Q., & Zhu, Y. (2025). AECR: Automatic attack technique intelligence extraction based on fine-tuned large language model. *Computers and Security*, *150*. https://doi.org/10.1016/j.cose.2024.104213

Chen, Y., Cui, M., Wang, D., Cao, Y., Yang, P., Jiang, B., Lu, Z., & Liu, B. (2024). A survey of large language models for cyber threat detection. *Computers and Security*, *145*. https://doi.org/10.1016/j.cose.2024.104016

Firdaus, R., Hadiana, A. I., & Kasyidi, F. (2023). Model Deteksi Botnet Menggunakan Algoritma Decision Tree Dengan Untuk Mengidentifikasi Serangan Click Fraud. *Journal of Informatics and Communication Technology (JICT)*, *4*(2), 10–20. https://doi.org/10.52661/j_ict.v4i2.122

Irshad, E., & Basit Siddiqui, A. (2023). Cyber threat attribution using unstructured reports in cyber threat intelligence. *Egyptian Informatics Journal*, *24*(1), 43–59. https://doi.org/10.1016/j.eij.2022.11.001

Mishra, C., Sarma, H., & M., S. (2025). PageLLM: Incremental approach for updating a Security Knowledge Graph by using Page ranking and Large language model. *Information Processing and Management*, *62*(3). https://doi.org/10.1016/j.ipm.2024.104045

Ng, C. K., Rajasegarar, S., Pan, L., & ... (2020). VoterChoice: A ransomware detection honeypot with multiple voting framework. *Concurrency and …*. https://doi.org/10.1002/cpe.5726

Pérez-Gomariz, M., Cerdán-Cartagena, F., & García, J. (2025). LM-Hunter: An NLP-powered graph method for detecting adversary lateral movements in APT cyber-attacks at scale. *Computer Networks*, *262*. https://doi.org/10.1016/j.comnet.2025.111181

Putra, M. A. R., Hostiadi, D. P., & Ahmad, T. (2022). Botnet dataset with simultaneous attack activity. *Data in Brief*, *45*, 108628. https://doi.org/10.1016/j.dib.2022.108628

Putri, V. U., Cahyono, E. B., & Azhar, Y. (2020). Deteksi Botnet Pada Passive DNS Dengan Menggunakan Metode K Nearest Neighbor. *Jurnal Repositor*, *2*(12), 1631. https://doi.org/10.22219/repositor.v2i12.450

Rahali, A., & Akhloufi, M. A. (2023). MalBERTv2: Code Aware BERT-Based Model for Malware Identification. *Big Data and Cognitive Computing*, *7*(2). https://doi.org/10.3390/bdcc7020060

Udiyono, A., Lim, C., & Lukas. (2020). Botnet Detection Using DNS and HTTP Traffic Analysis. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3429789.3429818

Vellela, S. S., D, R., Purimetla, N. M. R., Thalakola, S. R., Vuyyuru, L. R., & Vatambeti, R. (2025). Cyber threat detection in industry 4.0: Leveraging GloVe and self-attention mechanisms in BiLSTM for enhanced intrusion detection. *Computers and Electrical Engineering*, *124*. https://doi.org/10.1016/j.compeleceng.2025.110368

Zhen, Z., & Gao, J. (2023). Chinese Cyber Threat Intelligence Named Entity Recognition via RoBERTa-wwm-RDCNN-CRF. *Computers, Materials and Continua*, *77*(1), 299–321. https://doi.org/10.32604/cmc.2023.042090