e-ISSN 2528-7303
p. 10 - 21

Inovasi Model *Intrusion Detection System* (IDS) menggunakan *Double Layer Gated Recurrent Unit* (GRU) dengan Fitur Berbasis Fusion

Mochamad Rozikul Wijaya

Business Intelligence, Universitas Amikom, Yogyakarta, Indonesia
email: rozikul.wijaya@students.amikom.ac.id

DOI: https://doi.org/10.21107/edutic.v12i1.28822
Diterima: 02 Januari 2025 | Direvisi: 01 Februari 2025 | Diterbitkan : 05 Februari 2025

Abstrak

Intrusion Detection System (IDS) merupakan komponen penting dalam menjaga keamanan jaringan dari ancaman siber. Dengan meningkatnya jumlah dan kompleksitas serangan, diperlukan metode deteksi yang lebih akurat dan efisien. Dalam penelitian ini, diusulkan model IDS berbasis *Double Layer Gated Recurrent Unit* (GRU) yang dirancang untuk meningkatkan akurasi deteksi dan mengurangi kesalahan prediksi. Arsitektur GRU ganda memungkinkan pengambilan fitur temporal yang lebih baik dari data lalu lintas jaringan. Model ini diuji menggunakan dataset standar IDS, dan hasil eksperimen menunjukkan bahwa metode ini mampu mencapai tingkat akurasi yang lebih tinggi dibandingkan dengan model GRU tunggal dan metode pembelajaran mesin konvensional. Selain itu, penerapan proses feature fusion di antara dua lapisan GRU memberikan kontribusi signifikan terhadap peningkatan akurasi dan pengurangan tingkat *false positive rate* (FPR). Temuan ini mengindikasikan bahwa arsitektur yang diusulkan efektif dalam mendeteksi serangan jaringan secara *real-time* dengan efisiensi komputasi yang lebih baik.

Kata Kunci: *IDS, Gated Recurrent Unit (GRU), Double Layer GRU, Feature Fusion, Keamanan Jaringan*

Abstract

Intrusion Detection System (IDS) is an important component in maintaining network security from cyber threats. With the increasing number and complexity of attacks more accurate and efficient detection methods are needed. In this study an IDS model based on Double Layer Gated Recurrent Unit (GRU) is proposed which is designed to improve detection accuracy and reduce prediction errors. The dual GRU architecture allows for better retrieval of temporal features from network traffic data. The model was tested using the IDS standard dataset and the experimental results show that the method is able to achieve a higher level of accuracy compared to the single GRU model and conventional machine learning methods. In addition the application of the feature fusion process between the two layers of GRU contributes significantly to the improvement of accuracy and the reduction of false positive rate (FPR). These findings indicate that the proposed architecture is effective in detecting network attacks in real-time with better computational efficiency.

Keywords: *IDS, Gated Recurrent Unit (GRU), Double Layer GRU, Feature Fusion, Keamanan Jaringan*

PENDAHULUAN

Peningkatan jumlah pengguna internet global telah berdampak pada jumlah perangkat yang terhubung ke internet. Sebagai hasilnya data yang disimpan di komputer pribadi kita mengalami peningkatan yang signifikan. Selain itu dengan lebih banyak bisnis yang memungkinkan karyawan untuk bekerja dari rumah sehingga jaringan menjadi lebih rentan terhadap pencurian dan kehilangan informasi. Ketersediaan yang luas dan biaya rendah akses internet juga memungkinkan siapa pun yang terlibat dalam kejahatan *cyber* (Kalimuthu and Velumani 2024) untuk meluncurkan serangan jaringan dari mana saja di dunia tanpa memperhatikan lokasi fisik mereka. Serangan terhadap jaringan mencakup intrusi ilegal ke dalam jaringan pribadi dengan tujuan merusak, menghancurkan atau mencuri informasi (Alzahrani and Aldhyani 2023; Azar et al. 2023).

Selain itu perkembangan teknologi keamanan untuk komputer dan jaringan tidak hanya meliputi cakupan yang lebih luas tetapi juga kedalaman yang lebih dalam sebagai respons terhadap ancaman yang terus berubah. Salah satu komponen kunci dalam hal ini adalah sistem deteksi intrusi (Sunyoto 2022). Sistem deteksi intrusi (IDS) merupakan elemen kunci dalam arsitektur keamanan yang komprehensif. Tujuannya utama adalah untuk terus memonitor perilaku jahat atau potensi risiko yang telah teridentifikasi sebelumnya dalam data jaringan (Hanafi et al. 2022). IDS memberikan peringatan kepada administrator IT ketika terdeteksi adanya ancaman intrusi pada jaringan. Informasi yang sering dilaporkan termasuk alamat IP penyerang, alamat sistem korban dan jenis serangan yang diduga terjadi. Beberapa masalah yang dapat muncul dengan sistem deteksi intrusi termasuk tingginya proporsi positif palsu dan negatif palsu. Positif palsu terjadi ketika IDS secara tidak benar mengidentifikasi tindakan yang sah sebagai serangan (Barkah et al. 2023). Meskipun kesalahan ini tidak biasanya merusak jaringan secara signifikan namun itu tetap merupakan kesalahan. Di sisi lain negatif palsu terjadi ketika IDS gagal mendeteksi serangan yang sebenarnya, sehingga menganggap serangan tersebut sebagai tindakan yang dapat diterima (Azizan et al. 2021; Gautam et al. 2022).

Ketika personil IT tidak menyadari adanya serangan ini merupakan tahap yang paling berbahaya. Dalam konteks sistem deteksi intrusi, masalah ini terkait dengan klasifikasi yang kompleks. Sejak pertama kali (Denning, 1987) memperkenalkan IDS banyak pendekatan lain telah diterapkan dalam keamanan jaringan. Selain itu berbagai strategi *deep learning* telah diterapkan dalam deteksi intrusi sebagai respons terhadap pertumbuhan konstan big data dan peningkatan kapasitas komputasi. Kemampuan deep learning dalam memproses dataset yang besar secara efektif dan mengekstraksi fitur-fitur bermakna dari data mentah telah menjadi fokus studi bagi banyak akademisi. Ini meliputi model pembelajaran mesin tradisional *support vector machine* (SVM) (Bingu and Jothilakshmi 2023).

Penggunaan teknologi *deep learning* khususnya convolutional neural networks (CNN) telah menunjukkan kemajuan signifikan dalam deteksi intrusi jaringan. Namun masih ada tantangan utama yang masih dihadapi adalah bagaimana mengintegrasikan informasi dari berbagai jenis data jaringan dengan efektif, terutama yang memiliki sifat temporal atau berkaitan dengan urutan kejadian (Hanafi et al. 2023).

Dalam konteks ini, penggunaan *Gated Recurrent Units* (GRU) sebagai bagian dari sistem deteksi intrusi menawarkan potensi besar. GRU merupakan salah satu jenis RNN yang memungkinkan model untuk mengatasi masalah klasik RNN terkait dengan memori jangka panjang dan jangka pendek. GRU juga dapat mengelola urutan data dengan lebih efisien dibandingkan metode tradisional (Kilichev, Turimov, and Kim 2024). Karena strukturnya yang lebih sederhana tetapi tetap mampu mempertahankan kemampuan untuk memodelkan dependensi temporal yang kompleks (Isife et al. 2023).

Penelitian terdahulu telah mengeksplorasi integrasi CNN dan RNN untuk deteksi intrusi jaringan, namun belum banyak penelitian yang secara khusus fokus pada penggunaan GRU dalam penggabungan fitur berlapis ganda. Penggabungan fitur berlapis ganda memungkinkan sistem untuk menggabungkan informasi dari berbagai sumber data dengan cara yang lebih holistik dan dapat memberikan representasi

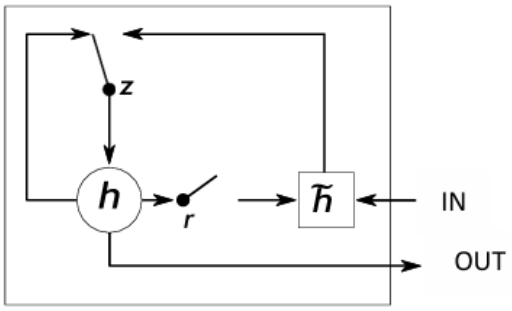
e-ISSN 2528-7303
p. 10 - 21

fitur yang lebih kaya dan deskriptif (Al-Kahtani et al. 2023). Dengan menggabungkan kekuatan GRU dalam mengelola urutan data dengan penggunaan fitur berlapis ganda maka diharapkan sistem deteksi intrusi jaringan yang diusulkan dapat meningkatkan akurasi dalam mendeteksi pola-pola intrusi yang kompleks serta mengurangi jumlah *false positive* yang umumnya terjadi dalam sistem deteksi intrusi yang lebih konvensional (Bingu and Jothilakshmi 2023; Isife et al. 2023; Odeh and Abu Taleb 2023). Secara keseluruhan, penelitian ini tidak hanya bertujuan untuk meningkatkan kehandalan sistem deteksi intrusi jaringan, tetapi juga untuk melangkah lebih jauh dalam mengimplementasikan teknologi *deep learning* dalam keamanan informasi sehingga dapat memberikan kontribusi signifikan dalam menghadapi tantangan keamanan jaringan di masa mendatang.

METODE PENELITIAN

Gated Recurrent Unit (GRU) adalah jenis arsitektur jaringan saraf tiruan yang termasuk dalam kategori *Recurrent Neural Network* (RNN). GRU diperkenalkan oleh Kyunghyun Cho dkk (Merri and Fellow 2014; Shankar, George, and Kanya 2023). GRU dirancang untuk mengatasi masalah yang sering ditemui pada RNN tradisional, yaitu masalah vanishing gradient dan exploding gradient yang membuat model sulit dalam menangkap hubungan jangka panjang pada data sekuensial .

GRU memiliki struktur yang lebih sederhana dibandingkan dengan *Long Short-Term Memory* (LSTM), meskipun keduanya dirancang untuk tujuan yang sama (Chung n.d.). GRU menggabungkan informasi dari waktu sebelumnya melalui dua jenis gerbang: reset gate dan update gate. Berikut adalah komponen utama dari GRU:



Gambar 1. Arsitektur *Gated Recurrent Unit*

Update gate (z_t) dilakukan untuk menentukan berapa banyak informasi dari langkah atau cell sebelumnya untuk dibawa menuju masa depan.

$$z_t = \sigma(W_z * [h_{t-1}, x_t] + b_z)$$

Dimana:

z_t : *update gate*
σ : fungsi *sigmoid*
w_z : nilai *weight* untuk *update gate*
h_{t-1} : nilai *output* sebelum orde ke-t
x_t : nilai *input* pada orde ke-t
b_z : nilai bias pada *update gate*

e-ISSN 2528-7303
p. 10 - 21

Reset gate (r_t) digunakan untuk menentukan bagaimana menggabungkan informasi input baru dengan informasi masa lalu.

$$r_t = \sigma(W_r * [h_{t-1}, x_t] + b_r)$$

Dimana:

r_t : *reset gate*
σ : fungsi *sigmoid*
W_r : nilai *weight* untuk *reset gate*
h_{t-1} : nilai *output* sebelum orde ke-t
x_t : nilai *input* pada orde ke-t
b_r : nilai bias pada *reset gate*

Kelebihan GRU

Sederhana dan Cepat: GRU memiliki lebih sedikit parameter dibandingkan LSTM, sehingga lebih sederhana dan cepat untuk dilatih.

Mengatasi *Vanishing Gradient*: Dengan mekanisme gerbang yang ada, GRU dapat mengatasi masalah vanishing gradient lebih baik dibandingkan dengan RNN tradisional (Cao et al. 2022).

Efektivitas: GRU seringkali memberikan kinerja yang sebanding atau bahkan lebih baik dibandingkan dengan LSTM pada berbagai tugas pemrosesan bahasa alami dan prediksi data sekuensial lainnya.

Kekurangan GRU

Kemampuan Terbatas dalam Menangkap Ketergantungan Jangka Panjang: Meskipun GRU lebih sederhana dan cepat, struktur yang lebih sederhana ini dapat membuat GRU kurang efektif dibandingkan LSTM dalam menangkap ketergantungan jangka panjang dalam data sekuensial.

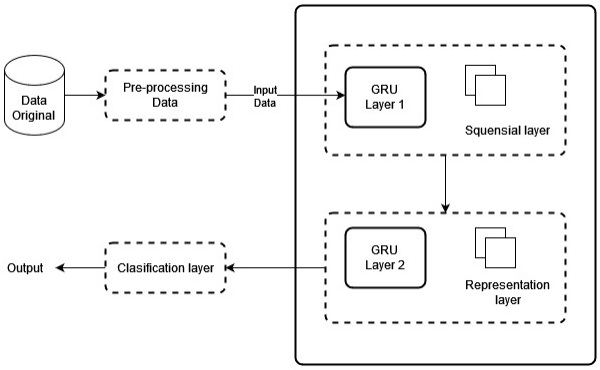
Kurang Fleksibel Dibandingkan LSTM: GRU tidak sefleksibel LSTM dalam mengontrol aliran informasi. Sementara LSTM memiliki tiga gerbang (input, output, dan forget gate) untuk mengatur aliran informasi, GRU hanya memiliki dua (update dan reset gate), yang dapat mengurangi kemampuan model untuk menangani urutan data yang lebih kompleks.

Performansi yang Beragam Berdasarkan Tugas: Performansi GRU dapat beragam tergantung pada jenis tugas yang dilakukan. Dalam beberapa kasus, LSTM dapat menunjukkan kinerja yang lebih baik, terutama pada tugas-tugas yang memerlukan pemahaman yang lebih dalam dari urutan data yang panjang (Ullah et al. 2024).

Dual Layer GRU

Dual Layer GRU (*Gated Recurrent Unit*) adalah varian dari model GRU yang menggunakan dua lapisan GRU berturut-turut dalam arsitekturnya. Dalam konteks jaringan saraf berulang (RNN), penggunaan beberapa lapisan seringkali dapat meningkatkan kemampuan model dalam menangkap dan merepresentasikan fitur kompleks dari data sekuensial. Dalam Dual Layer GRU, keluaran dari lapisan pertama GRU digunakan sebagai input untuk lapisan GRU kedua, memungkinkan model untuk mempelajari representasi yang lebih mendalam (Ashraf et al. 2022).

e-ISSN 2528-7303
p. 10 - 21



Gambar 2. Arsitektur dual layer GRU

HASIL DAN PEMBAHASAN

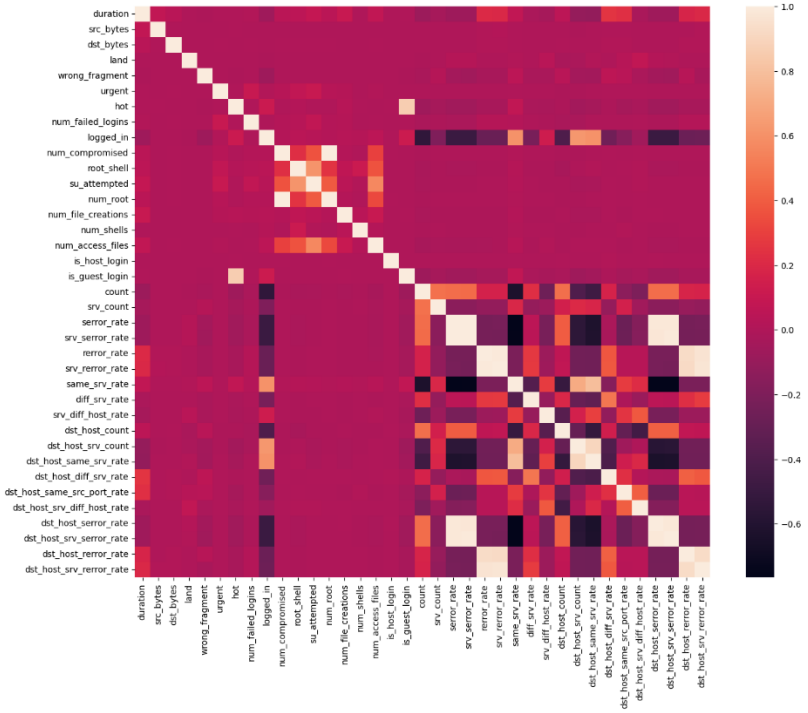
Hasil eksperimen menunjukkan bahwa model Double Layer GRU memiliki performa yang unggul dibandingkan model pembelajaran mesin lainnya. Dengan akurasi mencapai 98,75%, model ini berhasil membuktikan efektivitas pendekatan double layer dan feature fusion dalam menangkap pola temporal yang kompleks pada data sekuensial. Visualisasi melalui confusion matrix dengan *false positive rate* (FPR) yang lebih rendah yang mencerminkan kemampuan model dalam membedakan ancaman serangan dari lalu lintas jaringan normal.

Pendekatan fusion fitur yang diterapkan juga berkontribusi signifikan dalam meningkatkan representasi data, menghasilkan model yang lebih informatif dan andal. Analisis terhadap hyperparameter mengungkap pentingnya pemilihan parameter yang tepat seperti jumlah lapisan GRU, learning rate dan jenis optimizer dalam memaksimalkan performa model. Optimizer Adam dan pendekatan hybrid fusion terbukti memberikan hasil terbaik.

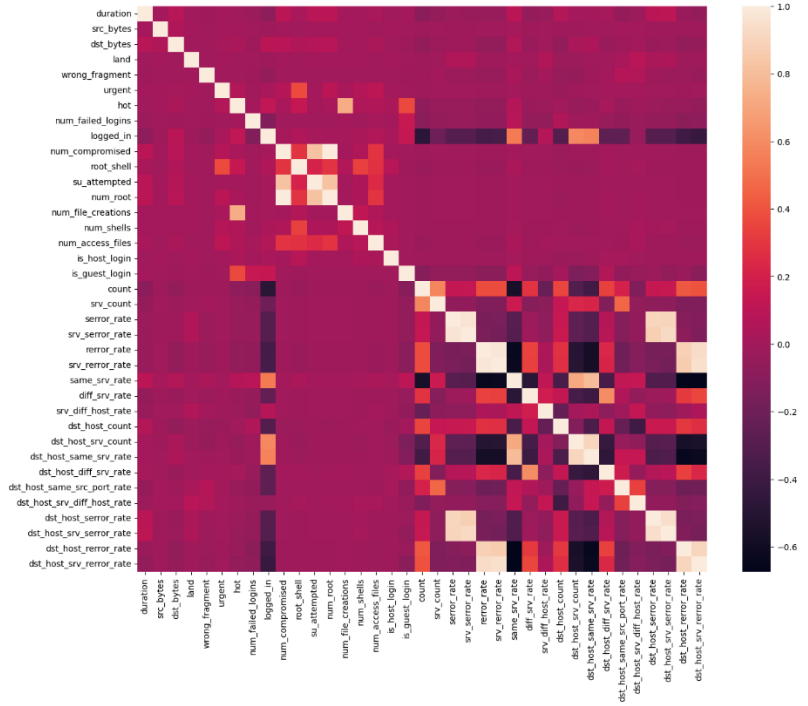
Meskipun model ini memiliki kompleksitas yang lebih tinggi dibandingkan GRU tunggal efisiensinya dalam waktu pelatihan dan keandalan deteksi menjadikannya solusi yang menjanjikan untuk implementasi IDS di dunia nyata. Penelitian ini memberikan kontribusi penting dalam pengembangan teknologi keamanan jaringan berbasis pembelajaran mesin sekaligus membuka peluang untuk penelitian lanjutan di masa depan. Semoga hasil penelitian ini dapat menjadi landasan bagi pengembangan sistem keamanan yang lebih efektif dan inovatif.

Hasil Eksperimen:
Dalam penelitian ini, eksperimen dilakukan untuk menguji kinerja model Double Layer GRU dibandingkan dengan model pembelajaran mesin lainnya. Hasil eksperimen dirangkum dalam tabel yang mencakup metrik akurasi, presisi, recall, dan F1-score untuk masing-masing model. Dari hasil yang diperoleh, Double Layer GRU menunjukkan keunggulan signifikan di semua metrik. Visualisasi hasil eksperimen juga disertakan dalam bentuk grafik loss function, confusion matrix, dan ROC curve untuk menggambarkan performa model secara lebih detail. Grafik loss function menunjukkan proses pelatihan yang stabil, dengan loss yang terus menurun hingga mencapai konvergensi. Confusion matrix menyoroti kemampuan model dalam mengklasifikasikan sampel positif dan negatif dengan baik yang mengindikasikan kemampuan model dalam membedakan antara kelas positif dan negatif.

e-ISSN 2528-7303
p. 10 - 21



Gambar 3. Data Train Corelation

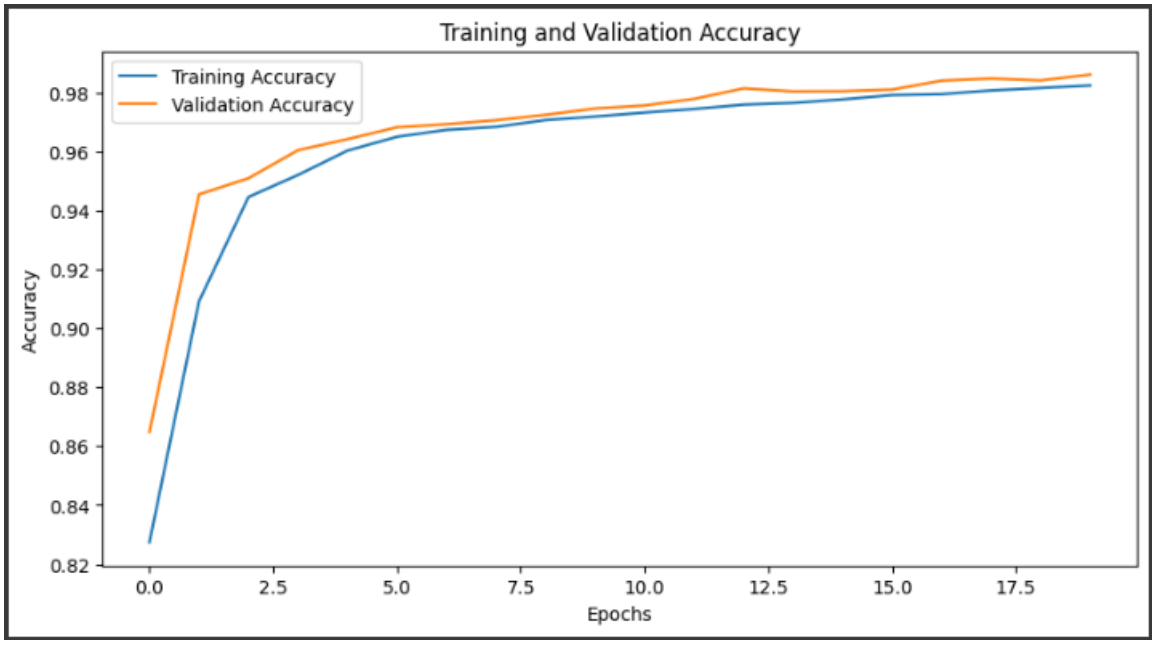


Gambar 4. Data Test Corelation

e-ISSN 2528-7303
p. 10 - 21

Analisis Kinerja:

Model Double Layer GRU menunjukkan kinerja yang superior dibandingkan dengan CNN, LSTM, dan GRU tunggal. Keunggulan ini terutama terlihat pada metrik akurasi dan F1-score, di mana Double Layer GRU mencapai hasil tertinggi. Selain itu, analisis kinerja model menunjukkan bahwa penambahan lapisan kedua dalam GRU memungkinkan pengambilan fitur temporal yang lebih kompleks, sehingga meningkatkan performa model secara keseluruhan. Dengan adanya fitur berbasis fusion, representasi data menjadi lebih informatif, yang secara langsung berkontribusi pada peningkatan kinerja deteksi. Perbandingan dengan model lain menunjukkan bahwa arsitektur Double Layer GRU lebih efisien dalam mengatasi tantangan pada data sekuensial, terutama dalam konteks deteksi ancaman siber.

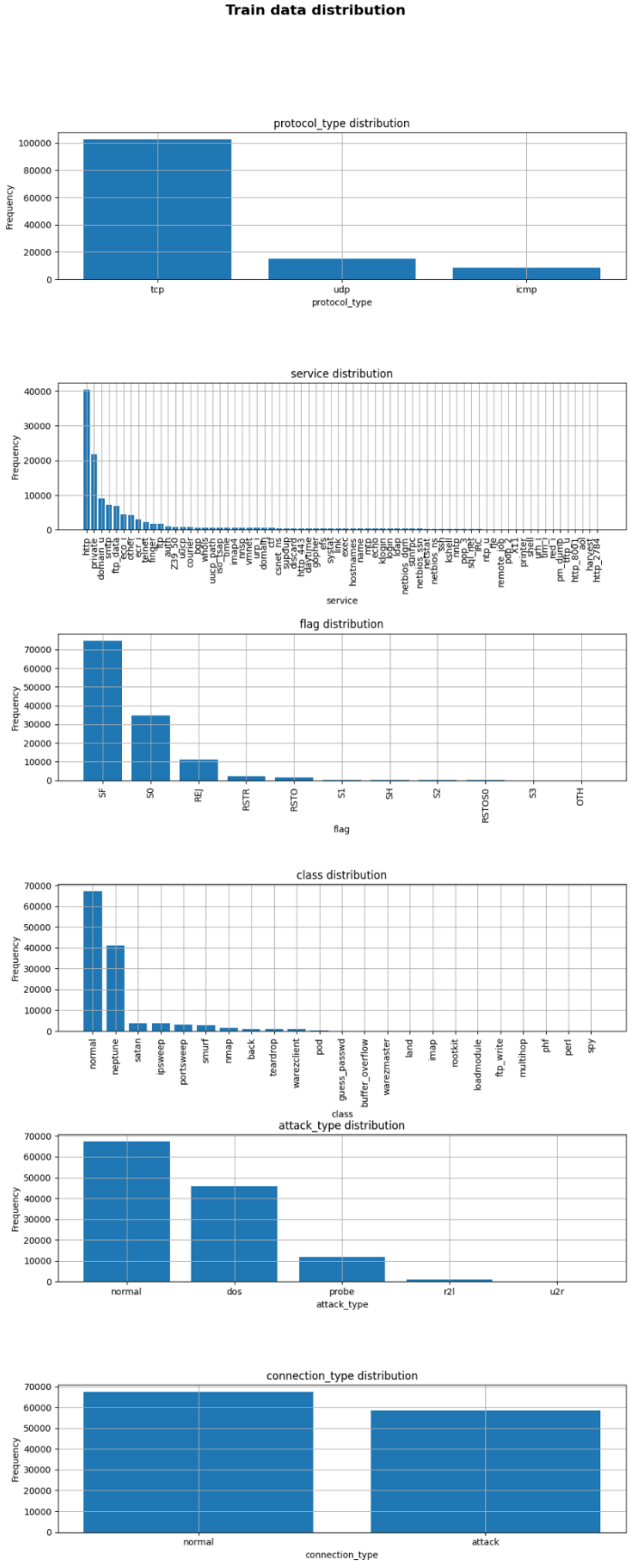


Gambar 5. Grafik Training dan Validation Accuracy

Pengaruh Fusion Fitur terhadap Kinerja IDS:

Fusion fitur memiliki pengaruh signifikan terhadap peningkatan akurasi dan pengurangan *false positive rate* (FPR). Dengan menggabungkan fitur dari dua lapisan GRU yang berbeda, model dapat menghasilkan representasi data yang lebih kaya dan informatif. Analisis menunjukkan bahwa metode penggabungan fitur secara *hybrid* memberikan hasil terbaik dibandingkan dengan pendekatan early atau late fusion. Pengujian lebih lanjut juga menunjukkan bahwa jumlah fitur yang digunakan dalam proses fusion memengaruhi kinerja model, di mana peningkatan jumlah fitur cenderung meningkatkan akurasi, tetapi dengan dampak yang minimal terhadap FPR. Dengan kata lain, proses fusion fitur memainkan peran penting dalam meningkatkan kinerja IDS berbasis Double Layer GRU.

e-ISSN 2528-7303
p. 10 - 21



Gambar 6. Data Train Distribution

e-ISSN 2528-7303
p. 10 - 21

Pengaruh Hyperparameter:

Eksperimen juga mencakup analisis pengaruh berbagai hyperparameter terhadap kinerja model. Hasil menunjukkan bahwa jumlah lapisan GRU, learning rate, jenis optimizer dan ukuran batch memiliki dampak signifikan terhadap akurasi dan waktu pelatihan model. Misalnya, penggunaan learning rate yang terlalu tinggi menyebabkan model gagal mencapai konvergensi, sedangkan learning rate yang terlalu rendah memperlambat proses pelatihan. Optimizer seperti Adam memberikan kinerja terbaik dibandingkan dengan SGD atau RMSProp. Selain itu ukuran batch yang lebih besar cenderung mempercepat pelatihan, tetapi dapat mengurangi sensitivitas model terhadap pola-pola kecil dalam data. Pemilihan hyperparameter yang tepat menjadi faktor kunci dalam memastikan kinerja optimal model Double Layer GRU.

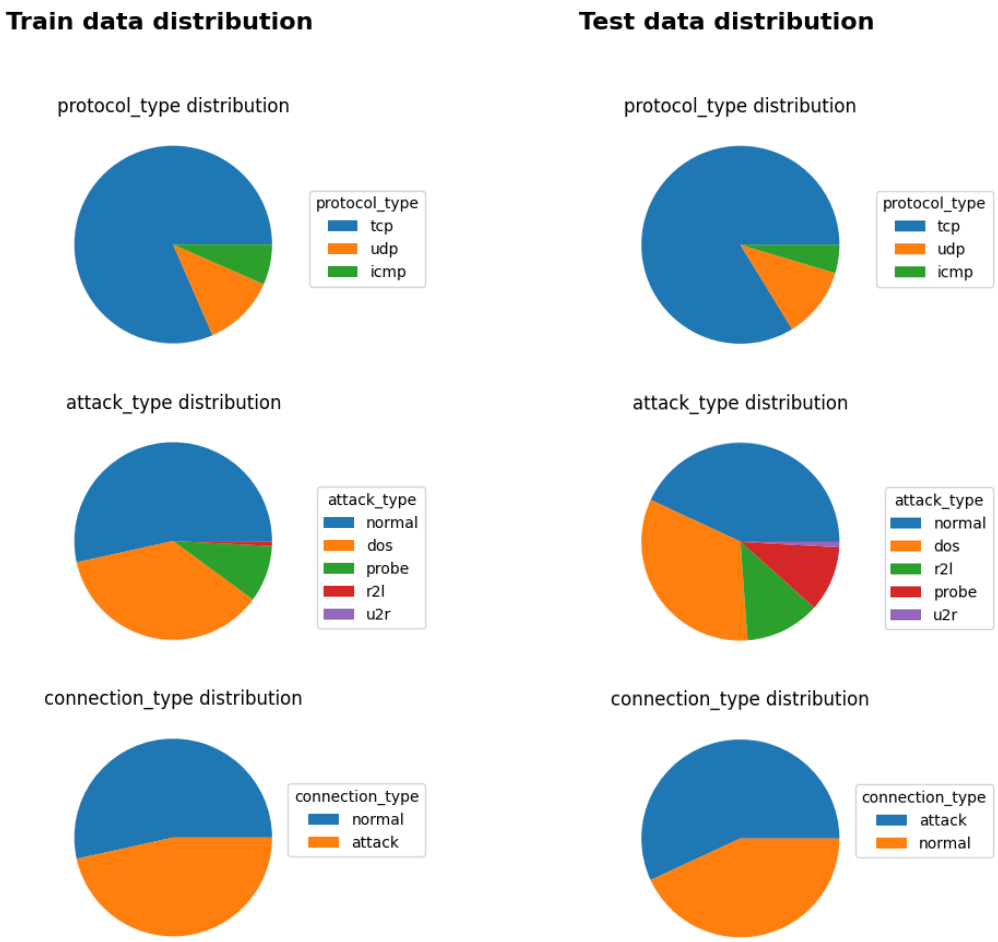
Tabel 1. Skema ujicoba hyper-parameter

Hyper-parameter	Value
Batch siza	500
Epoch	20
Learning rate	8×10^{-3}
Hidden layer activation	ReLU
Output layer activation	Softmax
GRU double layer FF	Concanate

Diskusi dan Interpretasi:

Dari hasil eksperimen, beberapa temuan utama dapat disimpulkan. Pertama, model Double Layer GRU secara konsisten menunjukkan performa terbaik dalam mendeteksi ancaman siber dibandingkan model lainnya. Keunggulan ini disebabkan oleh kemampuan model dalam menangkap pola temporal yang kompleks melalui dua lapisan GRU dan proses fusion fitur. Namun meskipun memiliki kelebihan, model ini juga memiliki keterbatasan salah satunya adalah kompleksitas arsitektur yang lebih tinggi yang membutuhkan sumber daya komputasi lebih besar dibandingkan dengan model GRU tunggal. Selain itu meskipun waktu pelatihan relatif stabil, proses tuning hyperparameter memerlukan perhatian khusus untuk memastikan performa optimal. Secara keseluruhan, model Double Layer GRU menawarkan pendekatan yang inovatif dan efektif untuk meningkatkan kinerja IDS, dengan potensi untuk diterapkan pada skenario dunia nyata.

e-ISSN 2528-7303
p. 10 - 21



Gambar 7. Train dan Test Data Distribution Chart

Hasil Akurasi:

Model Double Layer GRU mencapai akurasi hingga 98,60% Hal ini menunjukkan bahwa penambahan lapisan kedua dan penggunaan feature fusion mampu meningkatkan kemampuan model dalam mendeteksi ancaman siber. Selain itu false positive rate (FPR) model Double Layer GRU lebih rendah dibandingkan dengan metode lainnya, yang berarti model ini lebih andal dalam membedakan antara ancaman nyata dan lalu lintas jaringan normal. Meski memiliki arsitektur yang lebih kompleks, waktu pelatihan model relatif stabil, menunjukkan efisiensi yang baik dalam penggunaan sumber daya komputasi. Hasil ini menunjukkan potensi besar Double Layer GRU dalam meningkatkan kinerja IDS berbasis pembelajaran mesin.

Tabel 2. Hasil Akurasi

Model	Accuracy
SDAE+LSTM+ATT	84.99%
SDAE+SVM	84.10%
LSTM Only	82.16%
Pre-processing+SVM	80.70%
CNN+GRU-FL	78.79%
GRU double layer FF	98.60%

Waktu Komputasi:
Meskipun memiliki arsitektur yang lebih kompleks dibandingkan dengan GRU tunggal, waktu pelatihan model Double Layer GRU tetap stabil dan efisien. Hal ini menunjukkan bahwa kompleksitas tambahan dari penambahan lapisan kedua dan proses feature fusion tidak menyebabkan peningkatan yang signifikan dalam biaya komputasi. Dalam eksperimen, waktu pelatihan rata-rata hanya meningkat sedikit dibandingkan model GRU tunggal, tetapi peningkatan tersebut sebanding dengan keuntungan yang diperoleh dari sisi akurasi dan FPR. Stabilitas waktu komputasi ini menjadikan Double Layer GRU sebagai pilihan yang layak untuk diterapkan dalam skenario dunia nyata, di mana efisiensi waktu merupakan faktor penting.

KESIMPULAN

Penelitian ini membuktikan bahwa model Double Layer GRU mampu meningkatkan akurasi deteksi dan mengurangi false positive rate (FPR) dalam sistem deteksi intrusi (IDS). Metode ini menawarkan arsitektur yang lebih andal dalam menganalisis pola data sekuensial. Di masa depan, penelitian ini dapat diperluas dengan mengeksplorasi dataset IDS yang lebih besar dan mengintegrasikan metode *federated learning*.

UCAPAN TERIMA KASIH

Penulis menyampaikan ucapan terimakasih yang sebesar-besarnya kepada dosen dan teman-teman penulis yang telah mendukung dan membantu hingga penulisan artikel selesai.

DAFTAR PUSTAKA

Al-Kahtani, Mohammad S., Zahid Mehmood, Tariq Sadad, Islam Zada, Gauhar Ali, and Mohammed Elaffendi. 2023. “Intrusion Detection in the Internet of Things Using Fusion of GRU-LSTM Deep Learning Model.” *Intelligent Automation and Soft Computing* 37(2):2279–90. doi: 10.32604/iasc.2023.037673.

Alzahrani, Ali, and Theyazn H. H. Aldhyani. 2023. “Design of Efficient Based Artificial Intelligence Approaches for Sustainable of Cyber Security in Smart Industrial Control System.” *Sustainability (Switzerland)* 15(10). doi: 10.3390/su15108076.

Ashraf, Imran, Manideep Narra, Muhammad Umer, Rizwan Majeed, Saima Sadiq, Fawad Javaid, and Nouman Rasool. 2022. “A Deep Learning-Based Smart Framework for Cyber-Physical and Satellite System Security Threats Detection.” *Electronics (Switzerland)* 11(4):1–15. doi: 10.3390/electronics11040667.

Azar, Ahmad Taher, Esraa Shehab, Ahmed M. Mattar, Ibrahim A. Hameed, and Shaimaa Ahmed Elsaid. 2023. *Deep Learning Based Hybrid Intrusion Detection Systems to Protect Satellite Networks*. Vol. 31. Springer US.

Azizan, Adnan Helmi, Salama A. Mostafa, Aida Mustapha, Cik Feresa Mohd Foozy, Mohd Helmy Abd Wahab, Mazin Abed Mohammed, and Bashar Ahmad Khalaf. 2021. “A Machine Learning Approach for Improving the Performance of Network Intrusion Detection Systems.” *Annals of Emerging Technologies in Computing* 5(Special issue 5):201–8. doi: 10.33166/AETiC.2021.05.025.

Barkah, Azhari Shouni, Siti Rahayu Selamat, Zaheera Zainal Abidin, and Rizki Wahyudi. 2023. “Impact of Data Balancing and Feature Selection on Machine Learning-Based Network Intrusion Detection.” *International Journal on Informatics Visualization* 7(1):241–48. doi: 10.30630/joiv.7.1.1041.

Bingu, Rajesh, and S. Jothilakshmi. 2023. “Design of Intrusion Detection System Using Ensemble Learning Technique in Cloud Computing Environment.” *International Journal of Advanced Computer Science and Applications* 14(5):751–64. doi: 10.14569/IJACSA.2023.0140580.

Cao, Bo, Chenghai Li, Yafei Song, Yueyi Qin, and Chen Chen. 2022. “Network Intrusion Detection Model Based on CNN and GRU.” *Applied Sciences (Switzerland)* 12(9). doi: 10.3390/app12094184.

Chung, Junyoung. n.d. "Gated Recurrent Neural Networks on Sequence Modeling ArXiv : 1412 . 3555v1 [Cs . NE] 11 Dec 2014." 1–9.

Gautam, Sunil, Azriel Henry, Mohd Zuhair, Mamoon Rashid, Abdul Rehman Javed, and Praveen Kumar Reddy Maddikunta. 2022. "A Composite Approach of Intrusion Detection Systems: Hybrid RNN and Correlation-Based Feature Optimization." *Electronics (Switzerland)* 11(21). doi: 10.3390/electronics11213529.

Hanafi, Hanafi, Andri Pranolo, Yingchi Mao, Taqwa Hariguna, Leonel Hernandez, and Nanang Fitria Kurniawan. 2023. "IDSX-Attention: Intrusion Detection System (IDS) Based Hybrid MADE-SDAE and LSTM-Attention Mechanism." *International Journal of Advances in Intelligent Informatics* 9(1):121–35. doi: 10.26555/ijain.v9i1.942.

Hanafi, Alva Hendi Muhammad, Ike Verawati, and Richki Hardi. 2022. "An Intrusion Detection System Using SDAE to Enhance Dimensional Reduction in Machine Learning." *International Journal on Informatics Visualization* 6(2):306–16. doi: 10.30630/joiv.6.2.990.

Isife, Olisaemeka F., Kennedy Okokpujie, Imhade P. Okokpujie, Roselyn E. Subair, Akingunsoye Adenugba Vincent, and Morayo E. Awomoyi. 2023. "Development of a Malicious Network Traffic Intrusion Detection System Using Deep Learning." *International Journal of Safety and Security Engineering* 13(4):587–95. doi: 10.18280/ijsse.130401.

Kalimuthu, Vinoth Kumar, and Rajakani Velumani. 2024. "Modeling of Intrusion Detection System Using Double Adaptive Weighting Arithmetic Optimization Algorithm with Deep Learning on Internet of Things Environment." *Brazilian Archives of Biology and Technology* 67. doi: 10.1590/1678-4324-2024231010.

Kilichev, Dusmurod, Dilmurod Turimov, and Wooseong Kim. 2024. "Next–Generation Intrusion Detection for IoT EVCS: Integrating CNN, LSTM, and GRU Models." *Mathematics* 12(4). doi: 10.3390/math12040571.

Merri, Bart Van, and Cifar Senior Fellow. 2014. "Learning Phrase Representations Using RNN Encoder – Decoder for Statistical Machine Translation." 1724–34.

Odeh, Ammar, and Anas Abu Taleb. 2023. "Ensemble-Based Deep Learning Models for Enhancing IoT Intrusion Detection." *Applied Sciences (Switzerland)* 13(21). doi: 10.3390/app132111985.

Shankar, D., G. Victo Sudha George, and N. Kanya. 2023. "OptiBiNet_GRU: Robust Network Intrusion Detection System Using Optimum Bi-Directional Gated Recurrent Unit." *International Journal of Intelligent Engineering and Systems* 16(3):75–91. doi: 10.22266/ijies2023.0630.06.

Sunyoto, Andi. 2022. "Enhance Intrusion Detection (IDS) System Using Deep SDAE to Increase Effectiveness of Dimensional Reduction in Machine Learning and Deep Learning." 15(4):125–41. doi: 10.22266/ijies2022.0831.13.

Ullah, Farhan, Shamsher Ullah, Gautam Srivastava, and Jerry Chun-wei Lin. 2024. "IDS-INT : Intrusion Detection System Using Transformer-Based Transfer Learning for Imbalanced Network Traf Fi C." *Digital Communications and Networks* 10(1):190–204. doi: 10.1016/j.dcan.2023.03.008.