**Prosiding Seminar Nasional Ilmu Teknik**
**Volume 2 Nomor 2 Desember 2025**
e-ISSN: 3063-5713; p-ISSN: 3063-4709, Hal 812-821
DOI: https://doi.org/10.61132/prosemnasproit.v2i2.104
Tersedia: https://prosiding.aritekin.or.id/index.php/PROSEMNASPROIT/

# Deteksi Serangan *Mirai* Pada IoT Menggunakan *Recurrent Neural Network* (RNN) dengan Optimasi *Hyperparameter* Berbasis *Bayesian Optimization*

**Muhammad Ilham Mansis[1], Riza Pahlevi[2*], Ronald Naibaho[3], Eko Arip Winanto[4]**
[1,2*]Fakultas Ilmu Komputer, Program Studi Teknik Informatika, Universitas Dinamika Bangsa, Jambi, Indonesia
[3]Fakultas Ilmu Komputer, Program Studi Sistem Informasi, Universitas Dinamika Bangsa, Jambi, Indonesia
[4]Fakultas Ilmu Komputer, Program Studi Sistem Komputer, Universitas Dinamika Bangsa, Jambi, Indonesia
*Email: mansisilham88@gmail.com[1], rizapahlevi@unama.ac.id[2*], rhodes8083@yahoo.co.id[3], ekoaripwinanto@gmail.com[4]*

Alamat: Jl. Jend. Sudirman, The Hok, Kec. Jambi Selatan, Kota Jambi, Jambi 36138
**Penulis Korespondensi: rizapahlevi@unama.ac.id*

***Abstract.*** *The massive adoption of Internet of Things (IoT) devices is expanding the cyberattacks surface, particularly by the Mirai botnet, which exploits the dynamic characteristics of data traffic. This research proposes a Mirai detection approach based on a Recurrent Neural Network (RNN) optimized using Bayesian Optimization to improve prediction accuracy on sequential data. Unlike previous studies, this research utilizes the latest CIC IoT-DIAD 2024 dataset and applies probabilistic optimization to the hyperparameter space, including RNN units, dropout, and learning rate. The experiment was conducted on 201,021 valid data points, with dimensionality reduction using PCA as the optimal point to represent essential features without redundancy. The results show a significant increase in accuracy from 97.95% to 99.69%, accompanied by an 84% decrease in False Negatives, an 86% decrease in False Positives, and an AUC value of 0.9999. These findings confirm that integrating RNN and Bayesian Optimization not only improves numerical performance but also strengthens the reliability of the intrusion detection system for modern IoT ecosystems with controlled computational loads.*

***Keywords****: Bayesian Optimization; Intrusion Detection; Internet of Things; Mirai; Recurrent Neural Network.*

**Abstrak**. Masifnya adopsi perangkat Internet of Things (IoT) memperluas permukaan serangan siber, khususnya oleh botnet Mirai yang mengeksploitasi karakteristik lalu lintas data yang dinamis. Penelitian ini mengusulkan pendekatan deteksi Mirai berbasis Recurrent Neural Network (RNN) yang dioptimasi menggunakan Bayesian Optimization untuk meningkatkan ketepatan prediksi pada data sekuensial. Berbeda dari studi terdahulu, penelitian ini memanfaatkan dataset terbaru CIC IoT-DIAD 2024 serta menerapkan optimasi probabilistik pada ruang hyperparameter yang mencakup RNN units, dropout, dan learning rate. Eksperimen dilakukan pada 201.021 data valid dengan reduksi dimensi menggunakan PCA sebagai titik optimal untuk merepresentasikan fitur esensial tanpa redundansi. Hasil menunjukkan peningkatan akurasi signifikan dari 97,95% menjadi 99,69%, disertai penurunan False Negative sebesar 84%, False Positive 86% dan nilai AUC mencapai 0,9999. Temuan ini menegaskan bahwa integrasi RNN dan Bayesian Optimization tidak hanya meningkatkan performa numerik, tetapi juga memperkuat reliabilitas sistem deteksi intrusi untuk ekosistem IoT modern dengan beban komputasi yang terkontrol.

**Kata kunci**: Bayesian Optimization; Deteksi Intrusi; Internet of Things; Mirai; Recurrent Neural Network.

## 1. LATAR BELAKANG

Peningkatan penggunaan perangkat *Internet of Things* (IoT) yang diproyeksikan mencapai 55,7 miliar unit pada tahun 2025 telah memperluas permukaan serangan siber secara signifikan (Bikila & Čapek, 2025). Keterbatasan sumber daya komputasi serta minimnya mekanisme keamanan bawaan menjadikan perangkat IoT rentan terhadap eksploitasi *botnet* (Dahiya & Bhattacharya, 2024). Kondisi ini tercermin dalam laporan Badan Siber dan Sandi

*Naskah Masuk: 10 Oktober 2025; Revisi: 27 Oktober 2025; Diterima: 28 November 2025; Terbit: 30 Desember 2025;*

Negara (BSSN) pada Juli 2025 yang mencatat 567.717.476 anomali trafik, dengan 301.028.940 kejadian didominasi oleh serangan *Mirai* (BSSN, 2025). Meskipun telah muncul sejak 2016, *Mirai* terus berevolusi melalui eksploitasi kredensial lemah dan serangan *Distributed Denial of Service* (DDoS) yang semakin kompleks, sehingga menuntut mekanisme deteksi yang akurat dan adaptif terhadap dinamika trafik jaringan modern (Jin et al., 2024; Palla & Tayeb, 2021).

Dalam merespons ancaman tersebut, *Intrusion Detection System* (IDS) berbasis *deep learning* berkembang sebagai pendekatan utama dalam lingkungan IoT (Suwaryo et al., 2021). Dibandingkan arsitektur *Multilayer Perceptron* (MLP) yang bersifat statis atau *Convolutional Neural Network* (CNN) yang berfokus pada fitur spasial, *Recurrent Neural Network* (RNN) unggul dalam memodelkan ketergantungan temporal dari data trafik sekuensial (Borisenko et al., 2021; Rahman et al., 2024). Sejumlah penelitian melaporkan akurasi deteksi di atas 97% menggunakan RNN (Alsadhan et al., 2024; Azarudeen et al., 2024). Namun, performa RNN sangat bergantung pada konfigurasi *hyperparameter*, sementara pendekatan konvensional seperti manual *tuning* kurang efisien dalam menghadapi karakteristik trafik IoT yang heterogen dan dinamis (Shahira et al., 2025).

Kesenjangan penelitian terletak pada dominasi penggunaan *dataset* konvensional, seperti NSL-KDD atau UNSW-NB15, yang tidak lagi merepresentasikan pola serangan pada infrastruktur IoT kontemporer (Kasongo, 2023). Selain itu, penerapan *Bayesian Optimization* untuk optimasi *hyperparameter* pada deteksi *Mirai* berbasis RNN masih relatif terbatas, meskipun pendekatan probabilistik ini terbukti efisien dalam ruang pencarian parameter yang kompleks (Isa & Junedi, 2022; Simamora et al., 2025). Berdasarkan kesenjangan tersebut, penelitian ini mengusulkan model deteksi serangan *Mirai* berbasis *Recurrent Neural Network* (RNN) yang dioptimasi menggunakan *Bayesian Optimization*. Kebaruan penelitian terletak pada pemanfaatan *dataset* mutakhir CIC IoT-DIAD 2024 serta integrasi optimasi sistematis untuk meningkatkan akurasi, stabilitas, dan relevansi model terhadap kondisi aktual ekosistem IoT.

## 2. KAJIAN TEORITIS

Deteksi intrusi pada lingkungan *Internet of Things* (IoT) menghadapi tantangan utama akibat karakteristik lalu lintas jaringan yang bersifat sekuensial dan dinamis, terutama pada serangan *Mirai* yang mengeksploitasi pola komunikasi berulang dalam rentang waktu tertentu (Jin et al., 2024). Berbeda dengan jaringan konvensional, ekosistem IoT didominasi oleh

perangkat heterogen dengan keterbatasan sumber daya dan mekanisme keamanan bawaan yang minimal, sehingga menghasilkan pola trafik temporal yang kompleks dan tidak statis (Dahiya & Bhattacharya, 2024). Kondisi ini menuntut pendekatan deteksi intrusi yang mampu memodelkan ketergantungan waktu secara eksplisit, bukan sekadar mengandalkan representasi fitur statistik.

Dalam konteks pemodelan data sekuensial, *Recurrent Neural Network* (RNN) banyak digunakan karena kemampuannya menangkap dependensi temporal pada data berurutan, termasuk lalu lintas jaringan IoT yang berubah secara kontinu (Sharma et al., 2024). Sejumlah studi menunjukkan bahwa RNN mampu mencapai tingkat akurasi tinggi dalam mendeteksi serangan jaringan IoT (Alsadhan et al., 2024; Azarudeen et al., 2024). Namun, performa RNN sangat bergantung pada konfigurasi *hyperparameter*, seperti jumlah unit tersembunyi, *dropout*, dan *learning rate*. Penentuan *hyperparameter* secara manual atau melalui metode pencarian sederhana sering kali kurang optimal dalam menghadapi kompleksitas trafik IoT yang heterogen, sehingga berpotensi membatasi stabilitas dan kemampuan generalisasi model (Shahira et al., 2025).

Di sisi lain, mayoritas penelitian terdahulu masih mengevaluasi sistem deteksi intrusi menggunakan *dataset* konvensional, seperti NSL-KDD dan UNSW-NB15, yang dirancang untuk jaringan umum dan kurang merepresentasikan karakteristik lalu lintas IoT kontemporer (Ali et al., 2023; Saravanan et al., 2023). Selain itu, pemanfaatan optimasi *hyperparameter* secara sistematis, khususnya menggunakan *Bayesian* masih relatif terbatas dalam kajian deteksi *Mirai* berbasis RNN, meskipun pendekatan ini terbukti efisien dalam ruang pencarian parameter yang kompleks (Isa & Junedi, 2022). Oleh karena itu, penggabungan kedua pendekatan tersebut menjadi dasar konseptual perancangan model deteksi *Mirai* yang adaptif terhadap lalu lintas data yang dinamis.

## 3. METODE PENELITIAN

Bagian ini memaparkan rancangan eksperimen mulai dari pengolahan data hingga evaluasi kinerja model.

### Rancangan Eksperimen

Penelitian ini menggunakan rancangan eksperimen sebagai acuan pelaksanaan uji coba, sebagaimana ditunjukkan pada gambar 1.

**Gambar 1.** Rancangan Eksperimen

Alur rancang eksperimen deteksi serangan *Mirai* pada lingkungan *Internet of Things* (IoT) disajikan pada gambar 1, dengan evaluasi dilakukan menggunakan *dataset* CIC IoT-DIAD 2024. Tahapan eksperimen mencakup data *preprocessing* berupa pembersihan data, konversi label ke format numerik, dan reduksi dimensi menggunakan *Principal Component Analysis* (PCA) dengan 20 komponen utama untuk menekan kompleksitas dan risiko *overfitting* (Rabbani et al., 2024). *Dataset* kemudian dibagi menjadi data pelatihan, validasi, dan pengujian dengan rasio 70:15:15. Pemodelan dilakukan menggunakan *Recurrent Neural Network* (RNN) dalam dua skenario, yaitu model *baseline* dan model teroptimasi. Konfigurasi *baseline* serta penerapan *early stopping* mengacu pada penelitian terdahulu (Andika Surya et al., 2025), sedangkan peningkatan performa dicapai melalui optimasi *Bayesian Optimization* dengan ruang parameter yang disusun berdasarkan studi terkait. Evaluasi kinerja dilakukan pada data pengujian menggunakan metrik *accuracy*, *precision*, *recall*, dan *f1-score*.

### *Dataset* CIC IoT-DIAD 2024

Penelitian ini menggunakan *dataset* CIC IoT-DIAD 2024 yang dikembangkan oleh *Canadian Institute for Cybersecurity*, dengan fokus pada trafik *Benign* dan serangan *Mirai*. *Dataset* ini menyediakan 84 fitur lalu lintas jaringan yang merepresentasikan karakteristik komunikasi IoT secara komprehensif dan relevan dengan kondisi jaringan kontemporer (Rabbani et al., 2024).

**Algoritma *Recurrent Neural Network* (RNN)**

*Recurrent Neural Network* (RNN) merupakan model *deep learning* untuk memproses data sekuensial dengan memanfaatkan koneksi berulang guna menangkap ketergantungan temporal (Holubenko et al., 2025). Secara matematis, mekanisme RNN dirumuskan melalui perhitungan *hidden state* pada waktu ke-*t* sebagai berikut (Vajrobol et al., 2024):

$$h_t = \sigma_h(W_{xh}x_t + W_{hh}h_{t-1} + b_h) \quad (1)$$

Dimana $h_t$merupakan *hidden state* saat ini, $x_t$adalah input pada waktu ke-*t*, $h_{t-1}$adalah *hidden state* sebelumnya, $W_{xh}$dan $W_{hh}$adalah bobot jaringan, serta $b_h$merupakan bias. Selanjutnya, keluaran jaringan dihitung menggunakan persamaan:

$$y_t = \sigma_y(W_{hy}h_t + b_y) \quad (2)$$

Dengan $y_t$sebagai output prediksi dan $W_{hy}$sebagai bobot antara *hidden layer* dan *output layer*.

**Optimasi Model RNN**

*Bayesian Optimization* diterapkan untuk mengoptimalkan *hyperparameter* RNN melalui 20 iterasi pencarian guna mencapai konvergensi optimal pada ruang parameter yang mencakup jumlah unit, *dropout*, dan *learning rate* agar meningkatkan kinerja deteksi serangan *Mirai* (Muhammad Dzaki Arkaan Nasir, 2024).

**Tabel 1.** Ruang Pencarian *Hyperparameter* RNN

| Hiperparameter | Rentang |
|---|---|
| RNN *Units* | 16 - 128 |
| *Dropout* | 0.0 – 0.5 |
| *Learning rate* | 0.01, 0.001, 0.0005, 0.0001 |

**Pengukuran Kinerja**

Evaluasi model dilakukan menggunakan metrik klasifikasi utama yang mencakup *accuracy*, *precision*, *recall*, dan *f1-score* berdasarkan komponen *Confusion Matrix*: *True Positive* (TP), *False Positive* (FP), *False Negative* (FN), dan *True Negative* (TN). Perumusan metrik tersebut didefinisikan sebagai berikut (Azmi & Voutama, 2024):

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

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

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

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

Penekanan khusus diberikan pada nilai *Recall* dan FN untuk meminimalkan risiko serangan *Mirai* yang tidak terdeteksi, serta FP guna menjamin efisiensi operasional sistem.

## 4. HASIL DAN PEMBAHASAN

Bagian ini menyajikan analisis hasil eksperimen yang diawali dengan pemaparan data penelitian, hasil prapengolahan data, pembagian data dan evaluasi hasil.

### Data Penelitian

*Dataset* yang digunakan adalah CIC IoT-DIAD 2024 yang merekam lalu lintas jaringan perangkat *Internet of Things* (IoT) dengan dua kelas, yaitu *Benign* dan *Mirai*. *Dataset* ini memiliki 84 fitur yang merepresentasikan karakteristik aliran jaringan. Tabel 2 menyajikan sepuluh fitur representatif yang dipilih berdasarkan kontribusinya terhadap komponen utama hasil PCA untuk menggambarkan karakteristik data dominan, sementara daftar lengkap fitur mengacu pada spesifikasi resmi CIC IoT-DIAD 2024.

**Tabel 2.** Contoh Fitur Pada *Dataset* CIC IoT-DIAD 2024

| No | Nama Fitur | Tipe Data | Contoh Data |
|---|---|---|---|
| 1 | *Total Length of Bwd Packet* | *Float64* | 3838.0 |
| 2 | *Dst Port* | *Int64* | 8443 |
| 3 | *Src Port* | *Int64* | 35863 |
| 4 | *ECE Flag Count* | *Int64* | 0 |
| 5 | *Bwd IAT Min* | *Float64* | 1218.0 |
| 6 | *CWR Flag Count* | *Int64* | 0 |
| 7 | *Subflow Fwd Packets* | *Int64* | 0 |
| 8 | *Total Fwd Packet* | *Int64* | 11 |
| 9 | *Fwd IAT Min* | *Float64* | 675.0 |
| 10 | *Bwd IAT Total* | *Float64* | 627386.0 |

### Hasil Tahapan Data *Preprocessing*

Tahap *preprocessing* data dilakukan untuk memastikan kualitas dan konsistensi *dataset*. Sebelum digunakan dalam proses pelatihan dan pengujian model. Proses pembersihan data menghapus 17 nilai hilang, 68 data duplikat, dan 58 nilai tak hingga, sehingga jumlah data berkurang dari 201.164 menjadi 201.021 baris data valid. Label kelas *Benign* dan *Mirai* dikonversi ke dalam format numerik [0, 1] agar dapat diproses oleh model pembelajaran mesin. Selanjutnya, PCA digunakan untuk mereduksi 83 atribut menjadi 20 komponen utama, karena jumlah ini dinilai mampu mempertahankan sebagian besar variansi informasi sekaligus menjaga keseimbangan antara efisiensi komputasi dan kemampuan representasi fitur.

**Hasil Pembagian Data**

*Dataset* dibagi menjadi data pelatihan, validasi, dan pengujian dengan proporsi 70:15:15 untuk menyeimbangkan proses pembelajaran model, pemantauan kinerja selama pelatihan, dan evaluasi akhir. Pembagian data dilakukan secara *stratified* untuk menjaga proporsi kelas *Benign* dan *Mirai* pada setiap subset, sementara pengaturan parameter acak digunakan memastikan konsistensi pembagian data. Ringkasan distribusi *dataset* disajikan pada tabel 3.

**Tabel 3.** Distribusi Pembagian Data

| Subset Data | Jumlah Sampel | Persentase |
|---|---|---|
| Data *Training* | 140.714 | 70% |
| Data *Validation* | 30.153 | 15% |
| Data *Testing* | 30.154 | 15% |
| **Total** | **201.021** | **100%** |

**Evaluasi Hasil**

Perbandingan kinerja antara model RNN *baseline* dan RNN teroptimasi disajikan pada tabel 4 untuk mengevaluasi peningkatan deteksi serangan *Mirai*.

**Tabel 4.** Performa Model RNN *Baseline* dan RNN Teroptimasi

| Parameter Evaluasi | RNN *Baseline* | RNN + *Bayesian* | Peningkatan (+/-) |
|---|---|---|---|
| *Accuracy* | 0,9795 | 0,9969 | + 0,0174 |
| *Precision - Mirai* | 0,9753 | 0,9966 | + 0,0213 |
| *Recall - Mirai* | 0,9715 | 0,9955 | + 0,0240 |
| *F1-Score - Mirai* | 0,9734 | 0,9960 | + 0,0226 |
| *Loss* Validasi Terendah | 0,0729 | 0,0101 | – 0,0628 (lebih baik) |
| AUC *Score* | 0,9957 | 0,9999 | + 0,0042 |
| *False Negative* (FN) | 332 sampel | 53 sampel | – 279 sampel |
| *False Positive* (FP) | 287 sampel | 40 sampel | – 247 sampel |

Penerapan *Bayesian Optimization* pada arsitektur RNN menghasilkan peningkatan performa yang konsisten pada seluruh metrik evaluasi dibandingkan model *baseline*. Model teroptimasi mencapai akurasi 99,69% dengan nilai AUC 0,9999, yang mencerminkan stabilitas konvergensi serta kemampuan diskriminasi yang sangat tinggi terhadap pola serangan *Mirai*. Temuan paling krusial ditunjukkan oleh penurunan *False Negative* sebesar 84% dari 332 menjadi 53 sampel. Penurunan FN ini menunjukkan bahwa optimasi *Bayesian* meningkatkan sensitivitas RNN dalam mengenali pola komunikasi *Mirai* yang berulang. Hal ini secara signifikan mengurangi risiko perangkat IoT terinfeksi lolos dari deteksi dan berkontribusi langsung pada pencegahan pembentukan *botnet* skala besar. Selain itu, penurunan *False Positive* sebesar 86% turut meningkatkan efisiensi operasional dengan menekan alarm palsu yang membebani pengelolaan jaringan. Secara keseluruhan, hasil ini menegaskan bahwa

optimasi *hyperparameter* berbasis *Bayesian* efektif menangani kompleksitas data sekuensial pada *dataset* CIC IoT-DIAD 2024. Pendekatan ini menghasilkan model yang akurat sekaligus mempertahankan beban komputasi yang terkontrol pada lingkungan IoT modern.

## 5. KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa integrasi *Recurrent Neural Network* (RNN) dan *Bayesian Optimization* efektif dalam mendeteksi serangan *Mirai* pada ekosistem *Internet of Things* (IoT). Pemanfaatan *dataset* mutakhir CIC IoT-DIAD 2024 memberikan representasi lalu lintas jaringan yang lebih realistis dibandingkan *dataset* konvensional. Hasil eksperimen mencapai akurasi tertinggi sebesar 99,69% dengan tingkat stabilitas sistem yang sangat baik. Meskipun menunjukkan performa yang tinggi, keterbatasan pada penggunaan satu arsitektur model membuka peluang penelitian lanjutan untuk menguji ketahanan model pada variasi skenario serangan serta *dataset* IoT lainnya guna memperkuat kemampuan generalisasi sistem deteksi intrusi.

## UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada pihak-pihak yang telah memberikan dukungan selama pelaksanaan penelitian ini. Artikel ini merupakan bagian dari penelitian yang telah dikembangkan dan disesuaikan untuk keperluan publikasi ilmiah.

## DAFTAR REFERENSI

Ali, M. N., Imran, M., din, M. S. ud, & Kim, B.-S. (2023). Low Rate DDoS Detection Using Weighted Federated Learning in SDN Control Plane in IoT Network. *Applied Sciences*, *13*(3), 1431. https://doi.org/10.3390/app13031431

Alsadhan, A. A., Al-Atawi, A. A., karamti, H., Jameel, A., Zada, I., & Nguyen, T. N. (2024). Malware Attacks Detection in IoT Using Recurrent Neural Network (RNN). *Intelligent Automation & Soft Computing*, *39*(2), 135–155. https://doi.org/10.32604/iasc.2023.041130

Andika Surya, I. M., Cahyanto, T. A., & Muharom, L. A. (2025). Deep Learning dengan Teknik Early Stopping untuk Mendeteksi Malware pada Perangkat IoT. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *12*(1), 21–30. https://doi.org/10.25126/jtiik.2025128267

Azarudeen, K., Ghulam, D., Rakesh, G., Sathaiah, B., & Vishal, R. (2024). Intrusion Detection System Using Machine Learning by RNN Method. *E3S Web of Conferences*, *491*, 04012. https://doi.org/10.1051/e3sconf/202449104012

Azmi, A. F., & Voutama, A. (2024). Prediksi Churn Nasabah Bank Menggunakan Klasifikasi Random Forest Dan Decision Tree Dengan Evaluasi Confusion Matrix. *Komputa : Jurnal Ilmiah Komputer Dan Informatika*, *13*(1), 111–119. https://doi.org/10.34010/komputa.v13i1.12639

Bikila, D. D., & Čapek, J. (2025). Machine Learning-Based Attack Detection for the Internet of Things. *Future Generation Computer Systems*, *166*, 107630. https://doi.org/https://doi.org/10.1016/j.future.2024.107630

Borisenko, B. B., Erokhin, S. D., Fadeev, A. S., & Martishin, I. D. (2021). Intrusion Detection Using Multilayer Perceptron and Neural Networks with Long Short-Term Memory. *2021 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO*, 1–6. https://doi.org/10.1109/SYNCHROINFO51390.2021.9488416

BSSN. (2025). *Laporan Hasil Monitoring Bulanan: Juli 2025*. https://idsirtii.or.id/halaman/tentang/laporan-hasil-monitoring.html

Dahiya, P., & Bhattacharya, S. (2024). MiraiBotGuard: Federated Learning for Intelligent Defense Against Mirai Threats. *2024 2nd International Conference on Device Intelligence, Computing and Communication Technologies (DICCT)*, 1–6. https://doi.org/10.1109/DICCT61038.2024.10533028

Holubenko, V., Gaspar, D., Leal, R., & Silva, P. (2025). Autonomous intrusion detection for IoT: a decentralized and privacy preserving approach. *International Journal of Information Security*, *24*(1), 7. https://doi.org/10.1007/s10207-024-00926-9

Isa, I. G. T., & Junedi, B. (2022). Hyperparameter Tuning Epoch dalam Meningkatkan Akurasi Data Latih dan Data Validasi pada Citra Pengendara. *Prosiding Sains Nasional Dan Teknologi*, *12*(1), 231–237. https://doi.org/10.36499/psnst.v12i1.6697

Jin, H., Jeon, G., Aneka Choi, H. W., Jeon, S., & Seo, J. T. (2024). A threat modeling framework for IoT-Based botnet attacks. *Heliyon*, *10*(20), e39192. https://doi.org/https://doi.org/10.1016/j.heliyon.2024.e39192

Kasongo, S. M. (2023). A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework. *Computer Communications*, *199*, 113–125. https://doi.org/https://doi.org/10.1016/j.comcom.2022.12.010

Muhammad Dzaki Arkaan Nasir. (2024). Optimasi Model Bilstm Untuk Analisis Sentimen Ulasan Film Menggunakan Hyperparameter Tuning Random Search. *Doctoral Dissertation, Universitas Islam Indonesia*.

Palla, T. G., & Tayeb, S. (2021). Intelligent Mirai Malware Detection in IoT Devices. *2021 IEEE World AI IoT Congress (AIIoT)*, 0420–0426. https://doi.org/10.1109/AIIoT52608.2021.9454215

Rabbani, M., Gui, J., Nejati, F., Zhou, Z., Kaniyamattam, A., Mirani, M., Piya, G., Opushnyev, I., Lu, R., & Ghorbani, A. A. (2024). Device Identification and Anomaly Detection in IoT Environments. *IEEE Internet of Things Journal*, *12*(10), 13625–13643. https://doi.org/10.1109/JIOT.2024.3522863

Rahman, R. A., Risma, P., Oktarina, Y., & Yudha, H. M. (2024). Prediksi Temperatur Lingkungan dengan Recurrent Neural Network Menggunakan Data Historis Iradiasi Matahari. *Journal of Applied Smart Electrical Network and Systems*, *5*(1), 16–21. https://doi.org/10.52158/jasens.v5i1.862

Saravanan, V., Madiajagan, M., Rafee, S. M., Sanju, P., Rehman, T. B., & Pattanaik, B. (2023). IoT-based blockchain intrusion detection using optimized recurrent neural network. *Multimedia Tools and Applications*, *83*(11), 31505–31526. https://doi.org/10.1007/s11042-023-16662-6

Shahira, F., Negara, B. S., Yanto, F., & Sanjaya, S. (2025). Optimasi Hyperparameter Deep Learning untuk Deteksi X-Ray Paru-Paru Menggunakan Bayesian Optimization. *Journal of Information Engineering and Educational Technology*, *9*(1), 53–63. https://doi.org/10.26740/jieet.v9n1.p53-63

Sharma, H., Kumar, P., & Sharma, K. (2024). Recurrent Neural Network based Incremental model for Intrusion Detection System in IoT. *Scalable Computing: Practice and Experience*, *25*(5), 3778–3795. https://doi.org/10.12694/scpe.v25i5.3004

Simamora, F. P., Purba, R., & Pasha, M. F. (2025). Optimisasi Hyperparameter BiLSTM Menggunakan Bayesian Optimization untuk Prediksi Harga Saham. *Jambura Journal of Mathematics*, *7*(1), 8–13. https://doi.org/10.37905/jjom.v7i1.27166

Suwaryo, S. R. N., Nawangsih, I., & Rejeki, S. (2021). Deteksi Serangan Pada Intrusion Detection System (IDS) Untuk Klasifikasi Serangan Dengan Algoritma Naïve Bayes, C.45 Dan K-NN Dalam Meminimalisasi Resiko Terhadap Pengguna. *Jurnal Sistem Informasi Universitas Suryadarma*, *8*(2), 171–180. https://doi.org/10.35968/jsi.v8i2.732

Vajrobol, V., Gupta, B. B., Gaurav, A., & Chuang, H.-M. (2024). Adversarial learning for Mirai botnet detection based on long short-term memory and XGBoost. *International Journal of Cognitive Computing in Engineering*, *5*, 153–160. https://doi.org/https://doi.org/10.1016/j.ijcce.2024.02.004