Terbit online pada laman web jurnal: **https://ejurnalunsam.id/index.php/jicom/**

Jurnal Informatika dan Teknologi Komputer

Vol. 07 No. 01 (2026) 58 - 63 E-ISSN :2774-7115 P-ISSN: 2775-2089

Imbalance-Aware XGBoost-SHAP untuk Klasifikasi Multikelas Intrusi Jaringan Berbasis Web

Muhammad Rifqi Fadhlan Rahmatullah[1], Hana Kurnia Putri[2], Candhy Fadhila Arsyad[3]

[1]Informatika, Fakultas Teknik, Universitas Doktor Nugroho Magetan

[2]Informatika, Fakultas Teknik, Universitas Doktor Nugroho Magetan

[3]Informatika, Fakultas Teknik, Universitas Doktor Nugroho Magetan

[1]mrifqi.fadhlanr.90@gmail.com*, [2]hanaputri2818@gmail.com, [3]candhy.fadhila.arsyad@gmail.com

Abstract

Network intrusion detection requires models that are accurate for imbalanced traffic and interpretable for administrative use. This study develops a web-based explainable intrusion detection prototype using imbalance-aware multiclass XGBoost and SHAP. The CICIDS2017 flow data were processed into 2,231,759 records with 77 numerical features and seven labels: BENIGN, Bot, Brute Force, DDoS, DoS, PortScan, and Web Attack. Data were split using an 80:20 stratified scheme, while balanced sample weights were applied only to the training set. The trained XGBoost model was evaluated using accuracy, macro precision, macro recall, macro F1-score, Matthews correlation coefficient, and confusion matrix. Model interpretation was presented through global SHAP, class-specific SHAP, local SHAP, and false-positive/false-negative analysis on a Flask dashboard. The model achieved 99.91% accuracy, 92.83% macro precision, 98.97% macro recall, 95.30% macro F1-score, and 0.9967 MCC. Functional local prediction testing on seven scenarios produced four correct classifications and three false negatives due to the prototype mode using 12 top SHAP features while imputing the remaining features with training medians. The results show that the proposed prototype can support explainable network intrusion monitoring while still requiring full-feature batch prediction for operational evaluation.

Keywords: intrusion detection, XGBoost, SHAP, class imbalance, web dashboard

Abstrak

Deteksi intrusi jaringan membutuhkan model yang akurat pada distribusi trafik tidak seimbang sekaligus dapat dijelaskan kepada administrator. Penelitian ini mengembangkan prototipe deteksi intrusi berbasis web menggunakan *imbalance-aware multiclass XGBoost* dan *SHAP*. Data *CICIDS2017* diproses menjadi 2.231.759 *flow* dengan 77 fitur numerik dan tujuh label, yaitu *BENIGN, Bot, Brute Force, DDoS, DoS, PortScan*, dan *Web Attack*. Dataset dibagi menggunakan skema *stratified* 80:20, sedangkan *balanced sample weight* diterapkan hanya pada data latih. Evaluasi dilakukan menggunakan *accuracy*, *macro precision*, *macro recall*, *macro F1-score*, *Matthews correlation coefficient*, dan *confusion matrix*. Interpretasi model disajikan melalui global *SHAP*, *SHAP* per kelas, *local SHAP*, serta analisis *false positive* dan *false negative* pada *dashboard Flask*. Model menghasilkan *accuracy* 99,91%, *macro precision* 92,83%, *macro recall* 98,97%, *macro F1-score* 95,30%, dan *MCC* 0,9967. Pengujian fungsional prediksi lokal terhadap tujuh skenario menghasilkan empat klasifikasi benar dan tiga *false negative* karena mode *prototype* hanya menggunakan 12 fitur *SHAP* teratas, sedangkan fitur lain diisi median data latih. Hasil penelitian menunjukkan bahwa prototipe dapat mendukung monitoring intrusi jaringan yang explainable, tetapi evaluasi operasional tetap perlu menggunakan batch prediction dengan seluruh 77 fitur.

Kata kunci: deteksi intrusi, *XGBoost*, *SHAP*, ketidakseimbangan kelas, *dashboard web*

1. Pendahuluan

Keamanan jaringan komputer menjadi kebutuhan mendasar karena layanan digital sangat bergantung pada ketersediaan dan integritas trafik. Serangan seperti *DDoS, DoS, port scanning, brute force, bot traffic*, dan *web attack* dapat menurunkan ketersediaan layanan, mengganggu proses bisnis, serta meningkatkan beban administrator jaringan. Sistem deteksi intrusi berbasis pembelajaran mesin mulai banyak digunakan karena mampu mempelajari pola trafik dari data historis dan membedakan trafik normal dari pola serangan yang kompleks.

Diterima Redaksi : 16-03-2026 | Selesai Revisi : 21-03-2026 | Diterbitkan Online : 01-04-2026

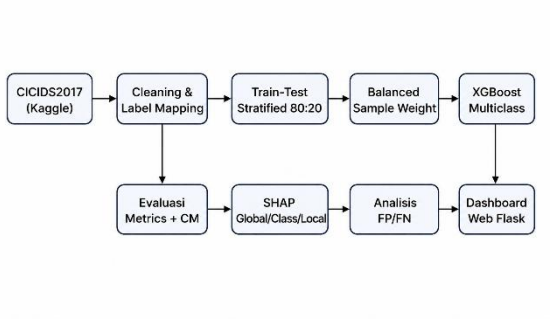
Kajian lima tahun terakhir pada jurnal terakreditasi SINTA 4 memperlihatkan bahwa pendekatan *machine learning* telah digunakan untuk mendeteksi serangan jaringan. Kiswanto dkk. mengembangkan deteksi *DDoS* berbasis *Random Forest*, sedangkan Darip dkk. menerapkan *Support Vector Machine* untuk sistem keamanan jaringan kampus [1], [2]. Lauw dkk. juga menunjukkan bahwa *ensemble learning* dapat digunakan untuk membangun model deteksi serangan jaringan [3]. Meskipun demikian, sebagian penelitian masih menekankan akurasi prediksi dan belum menyajikan interpretasi keputusan model secara rinci untuk mendukung validasi administrator.

XGBoost merupakan algoritma *ensemble* berbasis *gradient boosting* yang banyak dipakai pada data tabular karena mampu menangani pola nonlinier dan interaksi antarfitur. Atsauri dkk. menggunakan *XGBoost* untuk menangani missing data, sedangkan beberapa penelitian lain menggunakan *XGBoost* bersama teknik penyeimbangan data untuk meningkatkan kemampuan model terhadap kelas minoritas [4]–[8]. Pada domain keamanan jaringan, ketidakseimbangan kelas menjadi persoalan penting karena jumlah trafik normal biasanya jauh lebih besar daripada beberapa jenis serangan tertentu.

Aspek interpretabilitas juga menjadi perhatian karena model yang hanya menghasilkan label prediksi sulit dipercaya dalam konteks keamanan. Penelitian terbaru menunjukkan bahwa *SHAP* dapat menjelaskan kontribusi fitur pada model *XGBoost* maupun *Random Forest* di berbagai kasus klasifikasi dan prediksi [9]–[13]. Namun, integrasi antara klasifikasi multikelas intrusi jaringan, penanganan *class imbalance*, interpretasi global-lokal menggunakan *SHAP*, analisis *false positive/false negative*, dan penyajian melalui *dashboard web* masih perlu dikembangkan sebagai *prototype* penelitian yang operasional.

Berdasarkan celah tersebut, penelitian ini mengembangkan *prototype* deteksi intrusi jaringan berbasis web menggunakan *imbalance-aware XGBoost* dan *SHAP*. Kontribusi penelitian meliputi pembentukan dataset tujuh kelas dari *CICIDS2017*, pelatihan *XGBoost* multikelas dengan *balanced sample weight*, evaluasi model menggunakan metrik makro dan *confusion matrix*, interpretasi model melalui *SHAP global*/per kelas/lokal, serta pengujian fungsional prediksi lokal pada *website*. Fokus utama penelitian bukan hanya memperoleh prediksi serangan, tetapi juga menampilkan faktor fitur yang mendorong keputusan model.

2. Metode Penelitian



Gambar 1. Alur penelitian dan implementasi sistem

Penelitian menggunakan pendekatan kuantitatif eksperimental dan pengembangan *prototype*. Alur penelitian dimulai dari pengumpulan data *CICIDS2017*, pembersihan fitur numerik, pemetaan label, pembagian data latih dan data uji, pelatihan *XGBoost*, evaluasi model, interpretasi *SHAP*, analisis kesalahan klasifikasi, dan integrasi ke aplikasi web. Gambar 1 menunjukkan alur penelitian yang digunakan.

2.1. Dataset dan Prapemrosesan

Dataset yang digunakan adalah *CICIDS2017* yang diperoleh melalui repositori *Kaggle*. Dataset ini berisi fitur *flow* jaringan dan label trafik yang mencakup trafik normal serta beberapa jenis serangan. Pada tahap prapemrosesan, kolom identitas nonnumerik seperti *IP, Flow ID,* dan *timestamp* tidak digunakan sebagai fitur model. Fitur numerik dibersihkan dari nilai kosong, nilai tak hingga, dan duplikasi. Label asli kemudian dipetakan ke tujuh kelas penelitian, yaitu *BENIGN, Bot, Brute Force, DDoS, DoS, PortScan,* dan *Web Attack*. Label *Heartbleed* dan *Infiltration* tidak digabungkan ke kelas lain karena jumlahnya sangat kecil, sehingga dikeluarkan untuk menjaga konsistensi eksperimen.

Hasil prapemrosesan menghasilkan 2.231.759 data dengan 77 fitur numerik. Distribusi kelas pada Tabel 1 menunjukkan ketidakseimbangan yang kuat. Kelas *BENIGN* mendominasi 84,92% data, sedangkan kelas *Bot, PortScan,* dan *Web Attack* masing-masing berada di bawah 0,10%. Kondisi ini menjadi alasan penggunaan metrik makro dan strategi penanganan *class imbalance* pada pelatihan model.

Tabel 1. Distribusi kelas dataset hasil prapemrosesan

Kelas	Jumlah	Persentase
BENIGN	1.895.314	84,92%
Bot	1.437	0,06%
Brute Force	9.150	0,41%
DDoS	128.014	5,74%
DoS	193.745	8,68%
PortScan	1.956	0,09%
Web Attack	2.143	0,10%
Total	2.231.759	100%

2.2. Pelatihan *XGBoost* dan Strategi *Imbalance*

Dataset dibagi menggunakan *stratified split* dengan rasio 80% data latih dan 20% data uji. Stratifikasi dilakukan agar proporsi setiap kelas pada data uji tetap merepresentasikan distribusi kelas asli. Penelitian ini tidak melakukan *oversampling* pada data uji. Penanganan ketidakseimbangan kelas dilakukan melalui *balanced sample weight* hanya pada data latih, sehingga model memberi perhatian lebih besar pada kelas minoritas tanpa mengubah distribusi evaluasi.

Model yang digunakan adalah *XGBoost multiclass* dengan *objective multi:softprob*. Konfigurasi utama meliputi 420 estimator, *max depth* 8, *learning rate* 0,075, *subsample* 0,85, *colsample_bytree* 0,85, regularisasi alpha 0,05, lambda 1,0, *eval metric mlogloss*, dan *random state* 42. Output model berupa probabilitas untuk setiap kelas sehingga *prototype* dapat menampilkan kelas prediksi dan *confidence*.

2.3. Interpretasi *SHAP* dan *Prototype Web*

Interpretasi model dilakukan menggunakan *SHAP* untuk menjelaskan kontribusi fitur terhadap keputusan model. *Global SHAP* digunakan untuk mengetahui fitur paling berpengaruh secara keseluruhan, *SHAP* per kelas digunakan untuk melihat karakteristik masing-masing jenis serangan, sedangkan *Local SHAP* digunakan untuk menjelaskan satu prediksi tertentu. Selain itu, sistem menyimpan contoh *false positive* dan *false negative* agar kesalahan model dapat dianalisis secara operasional.

Prototype web dibangun menggunakan *Flask* sebagai *backend* dan *SQLite* untuk penyimpanan riwayat prediksi. *Website* menyediakan menu *Dashboard, Prediksi, SHAP, FP/FN,* dan *Riwayat.* Menu *Dashboard* menampilkan metrik evaluasi dan *confusion matrix*. Menu Prediksi menyediakan input 12 fitur *SHAP* teratas; fitur lain menggunakan median data latih. Mode ini digunakan untuk demonstrasi prediksi lokal, sedangkan evaluasi performa utama tetap memakai data uji *hold-out* dengan 77 fitur lengkap.

2.4. Skenario Pengujian

Pengujian dilakukan dalam dua tingkat. Pengujian pertama adalah evaluasi model pada 446.352 data uji *hold-out* menggunakan *accuracy, macro precision, macro recall, macro F1-score*, *Matthews correlation coefficient (MCC), classification report,* dan *confusion matrix*. Pengujian kedua adalah pengujian fungsional prediksi lokal pada *website* menggunakan tujuh skenario yang mewakili kelas *BENIGN, Bot, Brute Force, DDoS, DoS, PortScan,* dan *Web Attack.*

3. Hasil dan Pembahasan

3.1. Evaluasi Model

Setelah pelatihan pada data latih, model diuji pada 446.352 data *hold-out*. Hasil evaluasi global ditampilkan pada Tabel 2. Model memperoleh *accuracy* 99,91%, *macro precision* 92,83%, *macro recall* 98,97%, *macro F1-score* 95,30%, dan *MCC* 0,9967. Nilai *MCC* yang mendekati 1 menunjukkan korelasi yang sangat kuat antara label aktual dan prediksi pada data uji.

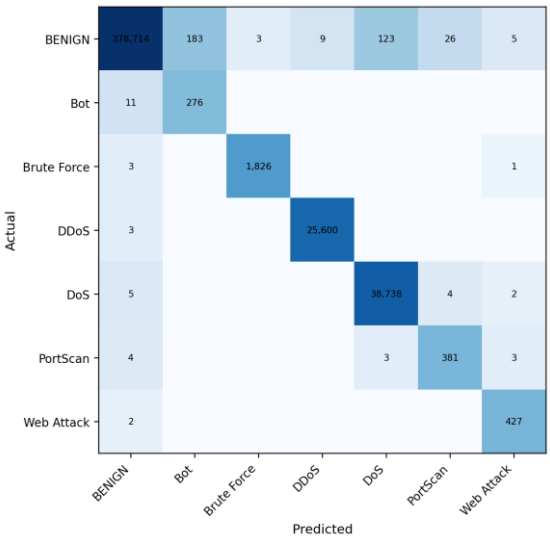
Walaupun *accuracy* sangat tinggi, interpretasi hasil perlu tetap memperhatikan metrik makro karena *dataset* sangat tidak seimbang. *Macro precision* lebih rendah daripada *macro recall*, terutama akibat kelas *Bot* yang memiliki *false positive* cukup tinggi dari trafik *BENIGN*. Hal ini menunjukkan bahwa model sangat sensitif dalam menangkap kelas minoritas, tetapi pada kelas tertentu masih menghasilkan alarm palsu.

Tabel 2. Distribusi kelas dataset hasil prapemrosesan

Metrik	Nilai
Accuracy	99,91%
Macro Precision	92,83%
Macro Recall	98,97%
Macro F1-score	95,30%
MCC	0,9967

Tabel 3. Evaluasi per kelas pada data uji

Kelas	Prec.	Rec.	F1	N
BENIGN	99,99%	99,91%	99,95%	379.063
Bot	60,13%	96,17%	73,99%	287
Brute Force	99,84%	99,78%	99,81%	1.830
DDoS	99,96%	99,99%	99,98%	25.603
DoS	99,68%	99,97%	99,82%	38.749
PortScan	92,70%	97,44%	95,01%	391
Web Attack	97,49%	99,53%	98,50%	429

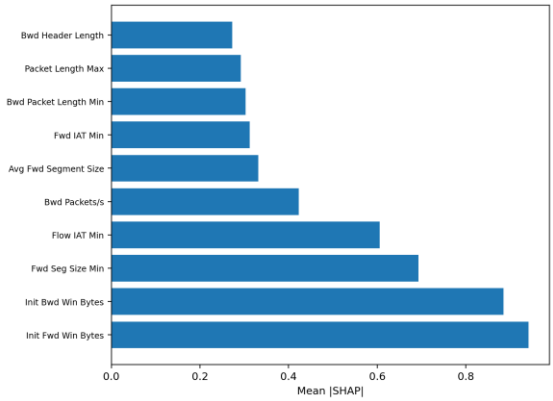


Gambar 2. *Confusion matrix* model *XGBoost* pada data uji

Confusion matrix pada Gambar 2 memperlihatkan bahwa sebagian besar prediksi berada pada diagonal

utama. Kelas *DDoS* memiliki 25.600 prediksi benar dari 25.603 data uji, sedangkan kelas *DoS* memiliki 38.738 prediksi benar dari 38.749 data uji. Pada kelas *BENIGN* terdapat 378.714 prediksi benar dari 379.063 data uji. Kesalahan terbesar terlihat pada *BENIGN* yang diprediksi sebagai *Bot* sebanyak 183 data, sehingga *precision Bot* menjadi 60,13%. Temuan ini penting karena pada sistem keamanan jaringan, *false positive* berpotensi menambah beban verifikasi *administrator*.

3.2. Hasil *SHAP* Global dan Per Kelas



Gambar 3. Sepuluh fitur teratas berdasarkan global *SHAP*

Analisis Global *SHAP* pada Gambar 3 menunjukkan bahwa fitur *Init Fwd Win Bytes, Init Bwd Win Bytes, Fwd Seg Size Min, Flow IAT Min,* dan *Bwd Packets/s* menjadi fitur paling berpengaruh terhadap keputusan model secara keseluruhan. Fitur-fitur tersebut berkaitan dengan karakteristik ukuran *window*, segmentasi paket, interval waktu *flow*, dan laju paket yang secara praktis relevan untuk membedakan pola trafik normal dan serangan.

Analisis *SHAP* per kelas menunjukkan bahwa fitur dominan setiap kelas tidak selalu sama. Pada kelas *BENIGN, Bwd Packet Length Min, Init Bwd Win Bytes,* dan *Flow IAT Min* memiliki kontribusi tinggi. Perbedaan fitur dominan antar kelas mendukung kebutuhan interpretasi *class-specific* karena pola *Bot, DDoS, DoS, PortScan,* dan *Web Attack* tidak dapat dijelaskan hanya dengan satu daftar feature importance global.

3.3. Pengujian Prediksi Lokal Berbasis Web

Pengujian fungsional prediksi lokal dilakukan melalui menu Prediksi pada *website*. Tujuh skenario diambil dari data uji dan dimasukkan ke form yang menampilkan 12 fitur *SHAP* teratas. Hasil pengujian ditampilkan pada Tabel 4. Dari tujuh skenario, empat menghasilkan prediksi benar, yaitu *BENIGN, Brute Force, DoS,* dan *Web Attack*. Tiga skenario lain, yaitu *Bot, DDoS,* dan *PortScan,* diprediksi sebagai *BENIGN*.

Tabel 4. Hasil pengujian fungsional prediksi lokal

No	Aktual	Pred.	Conf.	Status
1	*BENIGN*	BENIGN	100,00%	PASS
2	*Bot*	BENIGN	100,00%	FAIL
3	*Brute Force*	Brute Force	52,12%	PASS
4	*DDoS*	BENIGN	99,99%	FAIL
5	*DoS*	DoS	88,05%	PASS
6	*PortScan*	BENIGN	100,00%	FAIL
7	*Web Attack*	Web Attack	94,96%	PASS

Tabel 5. Fitur Local SHAP dominan pada tujuh skenario

Sken.	Fitur utama	SHAP
BENIGN	BwdPktLenMin; BwdPkts/s; InitBwdWin	+2,729952; +1,361096; +0,633414
Bot	InitFwdWin; AvgBwdSeg; InitBwdWin	+0,882506; +0,859557; +0,550368
Brute Force	InitFwdWin; FwdSegMin; BwdIATMean	+2,629472; +1,869630; -1,029251
DDoS	FlowIATMin; AvgBwdSeg; InitFwdWin	+0,562579; +0,549534; +0,528523
DoS	InitBwdWin; InitFwdWin; BwdPkts/s	+4,394891; +1,236042; -0,362506
PortScan	InitFwdWin; AvgBwdSeg; InitBwdWin	+2,991307; +0,782310; +0,746311
Web Attack	InitBwdWin; PktLenMax; InitFwdWin	+2,539291; +2,360890; +0,858016

Skenario *BENIGN* berhasil diprediksi sebagai *BENIGN* dengan *confidence* 100,00%. *Local SHAP* menunjukkan bahwa *Bwd Packet Length Min* memberikan kontribusi terbesar terhadap keputusan model menuju kelas *BENIGN*, diikuti *Bwd Packets/s* dan *Init Bwd Win Bytes*. Pada skenario *Brute Force*, model menghasilkan prediksi benar dengan *confidence* 52,12%. Probabilitas *BENIGN* mencapai 47,82%, sehingga sampel ini berada dekat dengan batas keputusan antara *Brute Force* dan *BENIGN*. *SHAP* memperlihatkan bahwa *Init Fwd Win Bytes* dan *Fwd Seg Size Min* mendorong keputusan *Brute Force,* sedangkan *Bwd IAT Mean* menahan keputusan tersebut.

Skenario *DoS* dan *Web Attack* juga menghasilkan prediksi benar. Pada skenario *DoS*, *Init Bwd Win Bytes* menjadi faktor pendorong paling besar dengan nilai *SHAP* +4,394891. Pada skenario *Web Attack, Init Bwd Win Bytes, Packet Length Max,* dan *Init Fwd Win Bytes* menjadi tiga kontribusi positif utama. Hasil ini menunjukkan bahwa *prototype* tidak hanya menampilkan label prediksi, tetapi juga memberikan informasi fitur yang menjelaskan arah keputusan model.

Tiga skenario, yaitu *Bot, DDoS,* dan *PortScan*, diprediksi sebagai *BENIGN*. Kesalahan ini perlu ditafsirkan sebagai hasil mode prediksi lokal, bukan performa model penuh. Form manual hanya menggunakan 12 fitur *SHAP* teratas, sedangkan 65 fitur lain diisi menggunakan median data latih. Dengan demikian, karakteristik sampel dapat berubah dari representasi 77 fitur asli. Oleh sebab itu, tujuh skenario

pada Tabel 4 digunakan sebagai uji fungsi prediksi lokal dan *explainability*, sedangkan performa ilmiah model tetap merujuk pada evaluasi *hold-out* 77 fitur pada Tabel 2 dan Tabel 3.

3.4. Pembahasan

Hasil evaluasi menunjukkan bahwa kombinasi *XGBoost* dan *balanced sample weight* mampu menghasilkan performa tinggi pada klasifikasi multikelas intrusi jaringan. *Macro recall* 98,97% menunjukkan bahwa model mampu menangkap sebagian besar kelas serangan, termasuk kelas minoritas. Namun, *macro precision* 92,83% menunjukkan masih adanya *false positive* pada kelas tertentu. Kelas *Bot* menjadi contoh paling penting karena memiliki *recall* tinggi 96,17%, tetapi *precision* lebih rendah 60,13%. Kondisi tersebut memperlihatkan *trade-off* antara sensitivitas deteksi kelas minoritas dan risiko alarm palsu.

Dari perspektif sistem *monitoring, false positive,* dan *false negative* perlu dianalisis secara berbeda. *False positive* dapat meningkatkan beban *administrator* karena trafik normal ditandai sebagai serangan, sedangkan *false negative* lebih kritis karena serangan tidak terdeteksi. Dengan menyediakan menu *FP/FN* dan *Local SHAP*, *prototype* memberi ruang bagi *administrator* untuk melihat kontribusi fitur yang menyebabkan kesalahan prediksi. Hal ini menjadi nilai tambah dibandingkan sistem klasifikasi yang hanya menampilkan label akhir.

Pengujian prediksi lokal memperlihatkan keterbatasan desain antarmuka manual. Input 77 fitur secara manual tidak praktis, sehingga prototype menampilkan 12 fitur *SHAP* teratas. Strategi ini membantu demonstrasi explainability, tetapi tidak cukup untuk menggantikan prediksi batch dengan seluruh fitur. Oleh karena itu, mode manual diposisikan sebagai demonstrasi local *explainability*, sedangkan analisis operasional tetap harus menggunakan *batch prediction* berbasis *CSV* lengkap.

4. Kesimpulan

Penelitian ini berhasil mengembangkan *prototype* deteksi intrusi jaringan berbasis web menggunakan *imbalance-aware multiclass XGBoost* dan *SHAP*. *Dataset CICIDS2017* diproses menjadi 2.231.759 data dengan 77 fitur dan tujuh kelas. Model diuji pada 446.352 data *hold-out* dan menghasilkan *accuracy* 99,91%, *macro precision* 92,83%, *macro recall* 98,97%, *macro F1-score* 95,30%, serta *MCC* 0,9967. Evaluasi per kelas menunjukkan performa sangat tinggi pada *DDoS, DoS, Brute Force, BENIGN, PortScan,* dan *Web Attack*, sedangkan kelas *Bot* masih memiliki *precision* lebih rendah akibat *false positive* dari kelas *BENIGN*. Integrasi *SHAP* memungkinkan sistem menampilkan interpretasi global, interpretasi per kelas, serta interpretasi lokal pada setiap prediksi. Pengujian fungsional prediksi lokal terhadap tujuh skenario menghasilkan empat prediksi benar dan tiga kesalahan yang seluruhnya mengarah ke *BENIGN*. Hasil tersebut menunjukkan bahwa mode prediksi lokal berbasis 12 fitur cocok untuk demonstrasi *explainability*, tetapi tidak boleh digunakan sebagai pengganti evaluasi model penuh berbasis 77 fitur. Pengembangan berikutnya dapat menambahkan fitur *batch prediction* yang lebih eksplisit untuk satu record penuh, kalibrasi probabilitas, dan mekanisme pemilihan sampel uji otomatis dari test set agar validasi berbasis web lebih mudah direproduksi.

Daftar Rujukan

[1] D. Kiswanto, F. Ramadhani, N. M. Surbakti, N. A. Nasution, F. Matematika, and I. P. Alam, "Pengembangan dan Implementasi Sistem Deteksi Serangan DDoS Berbasis Algoritma Random Forest," *Bull. Inf. Technol.*, vol. 6, no. 3, pp. 247–256, 2025, doi: 10.47065/bit.v5i2.2203.

[2] A. Sapaatullah, Rahmat, and M. Darip, "Implementasi One-Class Support Vector Machine untuk Deteksi Serangan Jaringan Kampus," *Bull. Inf. Technol.*, vol. 7, no. 1, pp. 40–49, 2026, doi: 10.47065/bit.v5i2.2602.

[3] C. M. Lauw, A. Anggrawan, and N. Sulistianingsih, "Model Deteksi Serangan Jaringan Menggunakan Machine Learning Dengan Teknik Ensemble Learning," *Jutisi J. Ilm. Tek. Inform. dan Sist. Inf.*, vol. 15, no. 1, p. 24, 2026, doi: 10.35889/jutisi.v15i1.3369.

[4] M. R. Atsauri, A. Rahman Dalimunthe, and N. Syahputra, "Performance Analysis of XGBoost in Handling Missing Data on the Telco Customer Churn Dataset," *Bull. Inf. Technol.*, vol. 7, no. 1, pp. 13–21, 2026, doi: 10.47065/bit.v5i2.2524.

[5] W. Nugraha and M. Syarif, "Teknik Weighting untuk Mengatasi Ketidakseimbangan Kelas Pada Prediksi Churn Menggunakan XGBoost, LightGBM, dan CatBoost," *Techno.Com*, vol. 22, no. 1, pp. 97–108, 2023, doi: 10.33633/tc.v22i1.7191.

[6] M. I. K. Khoirusshofi, F. M. Hana, and T. G. Pratama, "Klasifikasi Gangguan Tidur Menggunakan Algoritma XGBoost dengan SMOTE dan Grid Search," *Sainteks*, vol. 23, no. 1, pp. 1–19, 2026, doi: 10.30595/sainteks.v23i1.30171.

[7] B. Isnanto, L. Indah Sari, and W. Aribowo Probonegoro, "Komparasi Algoritma Klasifikasi Performa Akademik Mahasiswa Bisnis Digital: SVM , Random Forest , XGBoost , dan LightGBM dengan Penanganan Class Imbalance," *JSAI J. Sci. Appl. Informatics*, vol.

09, no. 2, pp. 189–195, 2026.

[8] A. Yusran Siregar and A. Setyo Arifin, "Enhancing XGBoost Classification with SVM-SMOTE & EasyEnsemble for Imbalanced Telemedicine Sentiment Data," *J. Indones. Sos. Teknol.*, vol. 5, no. 10, pp. 3893–3902, 2024, doi: 10.59141/jist.v5i10.1160.

[9] A. S. Iffadah, Trimono, and Dwi Arman Prasetya, "Shapley Additive Explanations Interpretation of the XGBoost Model in Predicting Air Quality in Jakarta," *J. Ris. Inform.*, vol. 7, no. 3, pp. 119–127, 2025, doi: 10.34288/jri.v7i3.366.

[10] M. Sakmar, A. Darmawan, P. A. Shofo, and N. T. Kadir, "An Explainable Spatio-Temporal Decision Support System (DSS) Using XGBoost And SHAP For Urban Complaint Trend Prediction," *J. Sains, Nalar, dan Apl. Teknol. Inf.*, vol. 5, no. 1, pp. 24–31, 2026, doi: 10.20885/snati.v5.i1.44562.

[11] R. Fitriansyah and A. F. Baihaqi, "Perbandingan Kinerja Algoritma Machine Learning Logistic Regression dan XGBoost dalam Memprediksi Gangguan Tidur dengan Analisis SHAP," *J. Inform. dan Multimed.*, vol. 17, no. 2, pp. 66–77, 2025, doi: 10.33795/jtim.v17i2.8661.

[12] S. Muliani, B. Sukma Negara, M. Irsyad, Jasril, and I. Iskandar, "Application of Shapley Additive Explanations (SHAP) in Deep Learning for Lung Disease Detection Using X-ray Images," *J. Artif. Intell. Softw. Eng.*, vol. 5, no. 02, pp. 709–719, 2025, doi: 10.47191/etj/v11i02.20.

[13] J. Ipmawati and K. Kusnawi, "An Explainable Machine Learning Approach Using Random Forest and SHAP for Employee Attrition Prediction," *bit-Tech*, vol. 8, no. 3, pp. 3024–3035, 2026, doi: 10.32877/bt.v8i3.3281.