JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 14 No. 1, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v14i1.8880

PENERAPAN TEKNIK SMOTE UNTUK MENDETEKSI PERILAKU JARINGAN BERBASIS TRAFIK ENKRIPSI

Ulfi Muzayyanah Fadil[1*], Dea Syahfira Hasibuan[2], Kalfida Eka Wati Siregar[3], Wily Supi Ramadani[4], Hasti Fadillah[5], Ibnu Rusydi[6]

[1,2,3,4,5,6]Program Studi Ilmu Komputer, Fakultas Sains dan Teknologi,Universitas Islam Negeri Sumatera Utara; Jl. Lapangan Golf, Desa Durian Jangak, Kecamatan Pancur Batu, Kabupaten Deli Serdang, Provinsi Sumatera Utara, 20353, Indonesia Telp. (+6261) 4536090, 4579816; Fax. (+6261) 6615683
Email : ulfimuzayyanah826@gmail.com

Keywords:
Deteksi Anomali,
SMOTE,Trafik Enkripsi

Corespondent Email:
ulfimuzayyanah826@gmail.com

Abstrak. Deteksi anomali pada trafik jaringan terenkripsi merupakan tantangan penting dalam keamanan *siber*, terutama karena kesulitan dalam menganalisis *payload* paket. Masalah utama dalam deteksi anomali adalah ketidakseimbangan data antara trafik normal dan anomali, yang dapat mengurangi efektivitas model. Penelitian ini bertujuan untuk meningkatkan deteksi anomali dengan menerapkan teknik *Synthetic Minority Over-sampling Technique* (SMOTE) untuk menyeimbangkan distribusi data. Metode yang digunakan meliputi penerapan SMOTE pada data trafik jaringan terenkripsi dan pelatihan model klasifikasi menggunakan algoritma *Random Forest*. Hasil penelitian menunjukkan bahwa penerapan SMOTE berhasil meningkatkan kinerja model, terutama pada metrik *recall* dan *F1-score*, yang mengindikasikan peningkatan sensitivitas model dalam mendeteksi anomali. Penelitian ini menegaskan pentingnya penggunaan SMOTE untuk mengatasi masalah ketidakseimbangan data dalam deteksi anomali pada jaringan terenkripsi.

Abstract. *Anomaly detection in encrypted network traffic is a significant challenge in cybersecurity, primarily due to the difficulty in analyzing packet payloads. A major problem in anomaly detection is the data imbalance between normal and anomalous traffic, which can reduce the effectiveness of the model. This study aims to improve anomaly detection by applying the Synthetic Minority Over-sampling Technique (SMOTE) to balance the data distribution. The method used includes applying SMOTE to encrypted network traffic data and training a classification model using the Random Forest algorithm. The results show that the application of SMOTE successfully improves model performance, especially in the recall and F1-score metrics, indicating an increase in the model's sensitivity in detecting anomalies. This study emphasizes the importance of using SMOTE to address the problem of data imbalance in anomaly detection in encrypted networks.*

1. PENDAHULUAN

Anomali adalah kejadian atau fenomena yang tidak normal atau tidak biasa terjadi. Dalam bidang data *mining*, anomali dapat diartikan sebagai sebuah kejadian atau observasi yang tidak sesuai dengan pola atau *trend* yang terjadi pada data. Anomali dapat dianggap sebagai data yang tidak "normal" atau outlier dibandingkan dengan data lainnya. Anomali dapat terjadi karena beberapa alasan, seperti kesalahan data, kejadian yang tidak terduga, atau bahkan adanya kecurangan. Anomali dapat merugikan dalam beberapa kasus, seperti dalam sistem keamanan

jaringan yang dapat mengindikasikan adanya aktivitas yang tidak diinginkan seperti serangan *Low RateDDoS*. Namun, anomali juga dapat menjadi informasi yang bermanfaat jika dapat dianalisis dengan baik, misalnya dalam menemukan pola-pola baru atau *trend* yang tidak terduga[7].

Deteksi anomali berfokus pada pemantauan dan analisis aktivitas jaringan kendaraan untuk mengidentifikasi pola yang tidak biasa atau mencurigakan yang mungkin menunjukkan adanya serangan atau pelanggaran keamanan. Tujuan utama dari deteksi anomali ini adalah untuk mendeteksi aktivitas yang menyimpang dari pola komunikasi normal, yang sering kali mengindikasikan adanya ancaman seperti serangan *denial-of-service* (DoS), *fuzzing*, *spoofing*, atau *replay attacks*. Teknik deteksi ini sangat penting dalam konteks kendaraan otonom dan sistem kontrol kendaraan yang sangat bergantung pada jaringan komunikasi internal, seperti *Controller Area Network* (CAN) *bus*, di mana serangan terhadap jaringan ini dapat membahayakan keselamatan kendaraan dan pengendara[3]. Oleh karena itu, deteksi anomali yang akurat dan efisien menjadi kebutuhan yang mendesak dalam pengelolaan jaringan modern. Untuk memastikan bahwa deteksi *anomaly* dapat dilakukan secara langsung, pengembangan sistem inferensi yang efisien menjadi krusial. Sistem tersebut harus mampu mengolah data secara kontinu dan memberikan hasil yang akurat dalam lingkungan jaringan yang dinamis[8].

Salah satu pendekatan untuk meningkatkan keamanan adalah dengan menggunakan deteksi anomali, yang berfungsi untuk mendeteksi aktivitas tidak wajar yang dapat menunjukkan adanya potensi ancaman atau serangan. Seiring dengan perkembangan teknologi, jaringan *neural* (*neural networks*) telah diakui sebagai salah satu metode yang efektif untuk mendeteksi anomali dalam data yang sangat besar dan kompleks, dengan kemampuan untuk mengidentifikasi pola yang tidak terdeteksi oleh sistem tradisional[10]. Anomali sendiri berasal dari bahasa inggris yang berarti penyimpangan. Anomali merupakan sebuah penyimpangan yang terjadi pada model lingkungan. Penyimpangan ini dapat diakibatkan oleh faktor dari dalam sistem itu sendiri maupun dari luar. Pendeteksian *anomaly* yang melibatkan manusia dapat sangat ampuhtetapi memerlukan waktu yang sangat lama dalam penggunaannya. Dalam ilmu *statistic*, *anomaly* atau yang sering disebut *outliner* adalah data atau sekumpulam data yang memiliki bobot sangat berbeda. Pendeteksian anomali sangat penting di industri, seperti keuangan, ritel, dan keamanan *cyber*, tetapi setiap bisnis harus mempertimbangkan solusi deteksi *anomaly*. Salah satu teknik yang dapat digunakan untuk meningkatkan keamanan jaringan komputer adalah dengan menerapkan sistem deteksi anomali. Deteksi anomali merupakan suatu teknik untuk mendeteksi data yang tidak normal atau menyimpang dari pola normalnya. Anomali dalam jaringa n komputer dapat disebabkan oleh berbagai hal, seperti serangan *cyber*, kesalahan konfigurasi, atau kegagalan perangkat keras. Pada masa lalu, deteksi anomali jaringan sering dilakukan secara manual dengan cara memantau data jaringan secara terus-menerus. Namun, metode ini memiliki beberapa kekurangan, seperti membutuhkan tenaga manusia yang banyak dan tidak dapat mendeteksi anomali dengan cepat[14].

Kriptografi merupakan suatu ilmu dan seni yang bertujuan untuk menjaga kerahasiaan informasi dengan cara mengubahnya menjadi format yang sulit dipahami. Penggunaan kriptografi sangat vital untuk melindungi data yang dikirim agar tetap aman dan tidak terungkap. Pesan asli, yang dikenal dengan plaintext, akan diubah menjadi bentuk kode yang tidak dapat dibaca tanpa adanya kunci tertentu. Proses ini disebut sebagai enkripsi, dan hasil yang diperoleh disebut *ciphertext*[5]. kriptografi merupakan teknik penyampaian pesan secara tersembunyi dengan enkripsi, yang berfungsi untuk mengamankan data baik saat disimpan maupun ditransmisikan melalui jaringan komputer, sehingga informasi menjadi terlindungi dari *spamming* atau peretasan ilegal. Penelitian ini menggunakan pendekatan kajian literatur untuk membangun landasan teori kriptografi, termasuk penjelasan fungsi kriptografi dalam menjaga integritas, kerahasiaan, otentikasi, dan *non-repudiation* data[2].

Dalam konteks keamanan jaringan, kriptografi tidak hanya berfungsi untuk menyembunyikan isi data, tetapi juga menjadi garis pertahanan terhadap berbagai jenis serangan seperti spoofing dan sniffing yang

mencoba mengambil atau memodifikasi data dalam transit. Analisis teknik kriptografi dalam skenario serangan jaringan lokal memperlihatkan bagaimana algoritma enkripsi dapat menjaga kerahasiaan dan integritas data sehingga tetap terlindungi dari akses ilegal[6]. Permasalahan utama dalam penelitian ini adalah ketidakseimbangan data (*imbalanced data*), di mana trafik normal jauh lebih banyak dibandingkan trafik anomali (Shiddiq, 2025). Kondisi ini menyebabkan model klasifikasi cenderung bias terhadap kelas mayoritas. Untuk mengatasi hal tersebut, teknik *Synthetic Minority Over-sampling Technique* (SMOTE) diterapkan guna meningkatkan representasi kelas minoritas (anomali) tanpa menambah data nyata[11].

Deteksi anomali pada trafik jaringan, khususnya trafik yang tidak dapat dianalisis *payload*-nya secara langsung, membutuhkan pendekatan berbasis fitur statistik. Pada bagian *Methodology*, penulis menerapkan teknik SMOTE untuk menangani ketidakseimbangan data antara kelas normal dan anomali sebelum proses pelatihan model *deep learning*. Selanjutnya, pada bagian *Results and Discussion*, ditunjukkan bahwa penerapan SMOTE mampu meningkatkan performa model, terutama pada nilai *recall* dan *F1-score*, sehingga model lebih sensitif dalam mendeteksi trafik anomali. Isi ini relevan dengan penelitian deteksi anomali perilaku jaringan berbasis trafik terenkripsi karena menekankan pentingnya *balancing* data sebelum klasifikasi[15].

Trafik jaringan terenkripsi tidak memungkinkan analisis isi data, sehingga deteksi anomali dilakukan melalui analisis perilaku dan pola statistik trafik. Pada bagian *Discussion*, penulis menekankan bahwa ketidakseimbangan jumlah data antara trafik normal dan anomali merupakan salah satu tantangan utama dalam membangun sistem deteksi yang akurat. Walaupun SMOTE tidak diterapkan secara langsung dalam penelitian ini, pembahasan tersebut mendukung penggunaan teknik *oversampling* seperti SMOTE untuk meningkatkan representasi kelas anomali dalam penelitian deteksi anomali trafik terenkripsi[9]. Dengan penggunaan Bi-LSTM pada deteksi anomali trafik jaringan yang mengalami ketidakseimbangan kelas dengan menerapkan teknik *oversampling* termasuk SMOTE untuk menyeimbangkan data minoritas sebelum pelatihan model. Hasil eksperimen menunjukkan bahwa penerapan SMOTE meningkatkan metrik evaluasi seperti *accuracy*, *precision*, *recall*, dan *F1-score* secara signifikan ketika dibandingkan dengan model tanpa oversampling, menghasilkan akurasi deteksi mencapai nilai sangat tinggi. Penelitian ini menegaskan bahwa strategi oversampling seperti SMOTE merupakan bagian penting dalam *pipeline preprocessing* untuk mengatasi *class imbalance* dalam deteksi anomali jaringan, terutama saat dataset trafik memiliki distribusi kelas yang sangat tidak seimbang[1].

Perkembangan teknologi jaringan dan meningkatnya penggunaan enkripsi pada lalu lintas data (seperti HTTPS, VPN, dan TLS) memberikan tantangan baru dalam sistem keamanan jaringan[12]. Di satu sisi, enkripsi melindungi kerahasiaan data, namun di sisi lain menyulitkan proses deteksi serangan karena isi paket tidak dapat dianalisis secara langsung.

Pendekatan tradisional dalam deteksi anomali jaringan umumnya mengandalkan inspeksi payload, sehingga menjadi kurang efektif pada trafik terenkripsi. Oleh karena itu, diperlukan metode deteksi berbasis pola perilaku trafik, seperti ukuran paket, durasi koneksi, frekuensi komunikasi, dan statistik aliran data[4].

2. METODE PENELITIAN

2.1 Pengumpulan Data

Data yang digunakan berupa dataset trafik jaringan terenkripsi, baik dari *dataset* publik maupun hasil capture jaringan. Data ini terdiri dari kelas trafik normal dan trafik anomali (misalnya serangan, penyalahgunaan jaringan, atau aktivitas mencurigakan).

2.2 Ekstraksi Fitur

Karena trafik terenkripsi tidak dapat dianalisis isinya, fitur yang digunakan berbasis statistik trafik, antara lain:

1) Jumlah paket
2) Ukuran paket rata-rata
3) Durasi koneksi
4) Interval waktu antar paket
5) Rasio paket masuk dan keluar

2.3 Penanganan Ketidakseimbangan Data

Teknik SMOTE digunakan untuk menghasilkan data sintetis pada kelas minoritas (anomali). Dengan SMOTE, distribusi data menjadi lebih seimbang sehingga model klasifikasi dapat mempelajari pola anomali dengan lebih baik.

2.4 Klasifikasi dan Deteksi Anomali

Model pembelajaran mesin seperti *Random Forest*, *Support Vector Machine*, atau algoritma lain digunakan untuk mengklasifikasikan trafik menjadi normal atau anomali. Model dilatih menggunakan data sebelum dan sesudah penerapan SMOTE untuk membandingkan hasilnya.

2.5 Evaluasi Model

Kinerja model dievaluasi menggunakan metrik:

a. Akurasi
b. *Precision*
c. *Recall*
d. *F1-Score*

Penekanan utama diberikan pada *Recall* dan *F1-Score* karena penting dalam mendeteksi anomali yang jumlahnya sedikit namun berdampak besar.

4. HASIL DAN PEMBAHASAN

Berdasarkan hasil eksperimen yang dilakukan menggunakan Google Colab, proses pengujian dilakukan dalam dua skenario, yaitu tanpa penerapan SMOTE dan dengan penerapan SMOTE pada *dataset* trafik jaringan terenkripsi. Evaluasi model dilakukan menggunakan metrik akurasi, *precision*, *recall*, dan *F1-score*.

Pada tahap pra-pemrosesan data, penelitian ini menerapkan *Synthetic Minority Over-sampling Technique* (SMOTE) untuk menangani ketidakseimbangan kelas pada data trafik jaringan. SMOTE membangkitkan data sintetis pada kelas minoritas dengan memanfaatkan kedekatan antar data menggunakan pendekatan *k-Nearest Neighbor*.

Secara matematis, data sintetis dibentuk menggunakan persamaan berikut :

$$x_{\text{new}} = x_i + \delta(x_{zi} - x_i)$$

Gambar 1. Persamaan

Dalam penerapannya xi, merepresentasikan satu sampel trafik anomali asli, sedangkan x_{zi} merupakan salah satu tetangga terdekat dari xi yang juga berasal dari kelas anomali. Nilai δ adalah bilangan acak pada rentang 0 hingga 1 yang berfungsi menentukan posisi data sintetis di antara kedua titik tersebut. Proses ini dilakukan secara berulang hingga jumlah data kelas anomali meningkat dan distribusi kelas menjadi lebih seimbang. Penentuan tetangga terdekat pada SMOTE dilakukan menggunakan jarak *Euclidean*, yang dirumuskan sebagai berikut:

$$d(x_i, x_j) = \sqrt{\sum_{n=1}^{N}(x_{in} - x_{jn})^2}$$

Gambar 2. Rumus Jarak *Euclidean*

di mana N merupakan jumlah fitur statistik trafik jaringan. Dalam penelitian ini, fitur-fitur tersebut telah dinormalisasi terlebih dahulu sehingga perhitungan jarak menjadi lebih akurat dan tidak bias terhadap skala fitur tertentu. Setelah data latih diseimbangkan menggunakan SMOTE, tahap selanjutnya adalah pelatihan model klasifikasi menggunakan *Random Forest*. *Random Forest* merupakan metode *ensemble learning* yang membangun sejumlah pohon keputusan secara acak dan menggabungkan hasil prediksinya.

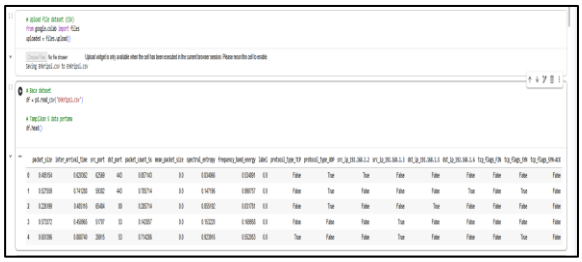
$$\hat{y} = \text{mode}\{h_1(x), h_2(x), \ldots, h_T(x)\}$$

Gambar 3. Fungsi Prediksi

di mana ht(x) adalah hasil prediksi dari pohon keputusan ke-t, dan T menyatakan jumlah total pohon keputusan. Dalam implementasi penelitian ini, nilai T ditetapkan sebanyak 100 pohon untuk memperoleh keseimbangan antara akurasi dan efisiensi komputasi.

Data yang digunakan merupakan data yang berasal dari implementasi sistem yang dilakukan menggunakan Google Colab yakni https://www.kaggle.com/datasets/ziya07/network-traffic-anomaly-detection-dataset, setiap tahapan pemrograman menghasilkan keluaran (*output*) yang saling berkaitan dan berkontribusi terhadap peningkatan kinerja deteksi anomali trafik jaringan terenkripsi. Pada

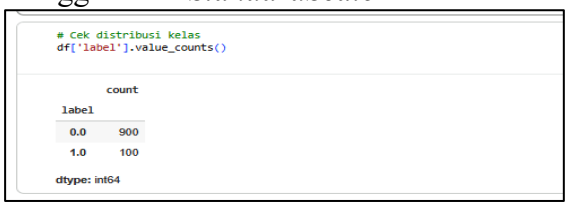
tahap awal, dataset trafik jaringan dibaca dan ditampilkan untuk memastikan struktur data serta keberadaan fitur dan label kelas.



Gambar 4. Tampilan Hasil Struktur Data

Hasil dari tahap ini menunjukkan bahwa dataset telah dimuat dengan benar dan siap untuk diproses lebih lanjut. Analisis distribusi kelas menggunakan fungsi *value_counts*() menghasilkan temuan bahwa jumlah data trafik normal jauh lebih besar dibandingkan trafik anomali. Hasil ini menegaskan bahwa *dataset* bersifat *imbalanced*, sehingga berpotensi menurunkan performa model dalam mendeteksi kelas minoritas apabila tidak dilakukan penanganan khusus.

Tahap berikutnya adalah pemisahan fitur dan label serta normalisasi data menggunakan *StandardScaler*.

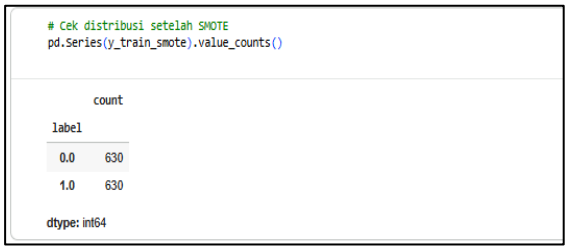


```
# Cek distribusi kelas
df['label'].value_counts()
```

label	count
0.0	900
1.0	100

dtype: int64

Gambar 5. Tampilan Awal Data



```
# Cek distribusi setelah SMOTE
pd.Series(y_train_smote).value_counts()
```

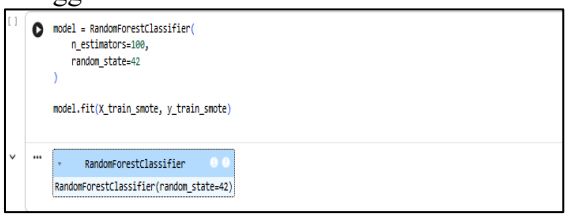
label	count
0.0	630
1.0	630

dtype: int64

Gambar 6. Tampilan Data Setelah SMOTE

Hasil dari proses normalisasi ini adalah data fitur yang berada pada skala yang seragam, sehingga tidak ada fitur tertentu yang mendominasi proses pembelajaran model. Pembagian data menjadi data latih dan data uji secara *stratified* menghasilkan proporsi kelas yang tetap terjaga pada kedua *subset* data. Hasil pembagian ini memastikan bahwa evaluasi model dapat dilakukan secara objektif dan merepresentasikan kondisi data asli.

Selanjutnya, model *Random Forest* dilatih menggunakan data latih hasil SMOTE.



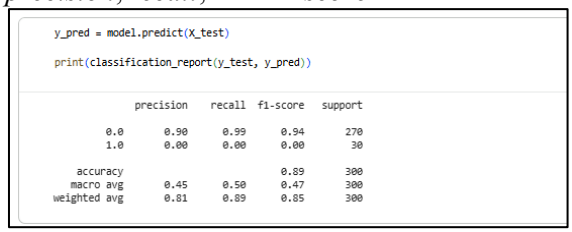
```
model = RandomForestClassifier(
    n_estimators=100,
    random_state=42
)

model.fit(X_train_smote, y_train_smote)
```

RandomForestClassifier(random_state=42)

Gambar 7. Tampilan Latih Data Menggunakan Random Forest

Hasil dari proses pelatihan ini adalah model klasifikasi yang telah mempelajari pola trafik jaringan normal dan anomali secara lebih seimbang. Pengujian model menggunakan data uji menghasilkan nilai evaluasi berupa *precision*, *recall*, dan *F1-score*.



```
y_pred = model.predict(X_test)

print(classification_report(y_test, y_pred))
```

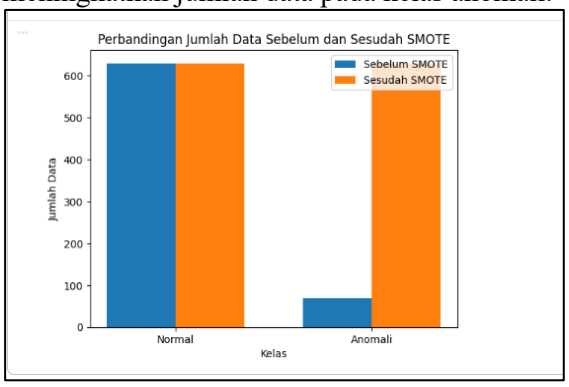
	precision	recall	f1-score	support
0.0	0.90	0.99	0.94	270
1.0	0.00	0.00	0.00	30
accuracy			0.89	300
macro avg	0.45	0.50	0.47	300
weighted avg	0.81	0.89	0.85	300

Gambar 8. Tampilan Hasil Nilai Evaluasi

Hasil evaluasi menunjukkan bahwa nilai *recall* dan *F1-score* pada kelas anomali meningkat secara signifikan dibandingkan dengan skenario tanpa SMOTE. Hal ini menunjukkan bahwa model menjadi lebih sensitif dalam mendeteksi trafik anomali dan mampu mengurangi jumlah anomali yang tidak terdeteksi.

Secara keseluruhan, hasil dari setiap tahapan pemrograman menunjukkan hubungan yang saling mendukung. Mulai dari analisis awal *dataset* yang mengungkap ketidakseimbangan data, penerapan SMOTE yang menghasilkan distribusi kelas lebih seimbang, hingga pelatihan dan evaluasi model yang menunjukkan peningkatan kinerja deteksi anomali. Dengan demikian, dapat disimpulkan bahwa setiap baris kode yang diimplementasikan memiliki kontribusi langsung terhadap hasil akhir penelitian, dan penerapan SMOTE terbukti efektif dalam meningkatkan performa sistem deteksi anomali pada trafik jaringan terenkripsi.

Pada tahap penerapan SMOTE, dilakukan proses oversampling terhadap data latih untuk meningkatkan jumlah data pada kelas anomali.



Gambar 9. Tampilan Penerapan SMOTE Pada Data Latih

Hasil dari proses ini dapat diamati melalui pengecekan ulang distribusi kelas setelah SMOTE, yang menunjukkan bahwa jumlah data kelas anomali meningkat secara signifikan hingga mendekati atau menyamai jumlah data kelas normal. Visualisasi distribusi data dalam bentuk grafik batang memperkuat hasil tersebut, di mana terlihat perbedaan yang jelas antara kondisi sebelum dan sesudah SMOTE. Grafik ini menunjukkan bahwa SMOTE berhasil mengatasi ketidakseimbangan data yang sebelumnya menjadi permasalahan utama.

5. KESIMPULAN

Berdasarkan hasil pengolahan dan pengujian datapelatihan model *Random Forest* tanpa penerapan SMOTE, model cenderung lebih baik dalam mengklasifikasikan kelas mayoritas. Kondisi tersebut menyebabkan kemampuan model dalam mengenali kelas anomali masih terbatas, yang tercermin dari hasil *classification report* pada data uji, khususnya pada metrik evaluasi kelas minoritas. Setelah penerapan SMOTE pada data latih, distribusi kelas menjadi lebih seimbang, sebagaimana ditunjukkan oleh hasil distribusi kelas dan visualisasi grafik perbandingan jumlah data sebelum dan sesudah SMOTE. Data hasil SMOTE kemudian digunakan untuk melatih model *Random Forest*, sehingga model memperoleh representasi data kelas anomali yang lebih baik. Hasil evaluasi menunjukkan adanya peningkatan kemampuan model dalam mendeteksi kelas anomali, terutama pada metrik *recall* dan *F1-score*, tanpa mengorbankan performa klasifikasi kelas normal secara signifikan.

UCAPAN TERIMA KASIH

Terima kasih kepada Fakultas Sains dan Teknologi, Universitas Islam Negeri Sumatera Utara atas dukungan dan fasilitas yang diberikan sehingga penelitian ini dapat terlaksana dengan baik. Penulis juga menyampaikan apresiasi kepada pengelola dataset serta platform Google Colab yang digunakan dalam proses pengolahan dan pengujian data. Selain itu, penulis mengucapkan terima kasih kepada seluruh pihak yang telah memberikan kontribusi, baik secara langsung maupun tidak langsung, dalam penyusunan dan penyelesaian penelitian ini.

DAFTAR PUSTAKA

[1]. Acharya, T. (2023). Optimizing the Performance of Network Anomaly Detection Using Bidirectional Long Short-Term Memory (Bi-LSTM) and Over-sampling for Imbalance Network Traffic Data, *8*(6), 144–154.

[2]. Amalya, N. (2023). Kriptografi dan Penerapannya Dalam Sistem Keamanan Data JURNAL MEDIA INFORMATIKA [JUMIN], *4*, 90–93.

[3]. Ayu. (2025). Tinjauan Literatur: Deteksi Anomali Berbasis Analisis Waktu pada CAN Bus Kendaraan Listrik Literature Review: Timing Analysis Based Anomaly Detection on Electric Vehicle CAN Bus, *6*.

[4]. Chawla, N. (2022). SMOTE : Synthetic Minority Over-sampling Technique, *16*, 321–357.

[5]. Darmansyah, D. (2025). Enkripsi pesan chat menggunakan algoritma chacha20 pada aplikasi komunikasi real-time 1) 1,2), *10*(2), 544–554.

[6]. Dewanto, R. (2022). Analisis Teknik-Teknik Kriptografi Terhadap Serangan Jaringan Local Ragil Aria Dewanto 1 , Aries Suharso 2 1,2 Universitas Singaperbangsa Karawang, *8*(September), 467–476.

[7]. Firdaus. (2023). DALAM LALU LINTAS JARINGAN MENGGUNAKAN NAIVE, *05*(02), 140–148.

[8]. Muhammad. (2025). Implementasi Sistem Deteksi Anomali pada Jaringan Komputer dengan Pendekatan XGBoost dan Data SNMP, *9*(2), 1–7.

[9]. Mukidur, R. (2024). Explainable Anomaly Detection in Encrypted Network Traffic Using

Data Analytics, 272–281. https://doi.org/10.32996/jcsts
[10]. Nursiaga. (2025). MODEL JARINGAN NEURAL UNTUK DETEKSI ANOMALI PADA, *01*(01), 1–9.
[11]. Rahman, R. (2024). IMPLEMENTASI NETWORK TRAFFIC ANALISIS UNTUK MENDETEKSI ANOMALI JARINGAN PADA TWITTER / X DAN INSTAGRAM, *2*(2), 88–96.
[12]. Saputra, F. (2025). Enhancing Intrusion Detection Using Random Forest and SMOTE on the NSL - KDD Dataset, *6*(3), 240–247.
[13]. Shiddiq, W. (2025). Optimizing Machine Learning-Based Network Intrusion Detection System with Oversampling , Feature Selection and Extraction, *11*(2), 225–237. https://doi.org/10.26555/jiteki.v11i2.30675
[14]. Subuhanto, D. (2024). Model Deteksi Anomali Jaringan Komputer Menggunakan Teknik Machine Learning, (1), 239–259.
[15]. Yagual, Q. (2025). A Hybrid Deep Learning-Based Architecture for Network Traffic Anomaly Detection via EFMS-Enhanced KMeans Clustering and CNN-GRU Models, *2*(Ml), 1–29.