JSCE (Journal of System and Computer Engineering)
Vol.6, No.3, July 2025, pp. 240-247
ISSN (online): 2723-1240
DOI : https://doi.org/10.61628/jsce.v6i3.2056

Enhancing Intrusion Detection Using Random Forest and SMOTE on the NSL-KDD Dataset

Febri Hidayat Saputra [1,a,*]; Ilham [2,b]; Muhammad Rizal H [3,c] ; Wisda [4,d]; First Wanita [5,e]; Mursalim [6,f]; Arif Fadillah[7,g]
[1,2,3,6] *Department of Informatics Engineering, Universitas Teknologi Akba Makassar, Indonesia*
[5] *Department of Information Technology Education, University Teknologi Akba Makassar, Makassar, Indonesia*
[4] *Department of Information System, Universitas Teknologi Akba Makassar, Makassar, Indonesia*
[7]*Department of Information Syestem, IkesT Muhammadiyah, Palembang*
[a] *febri@akba.ac.id;* [b] *ilham@akba.ac.id;* [c] *rizal@unitama.ac.id;* [d] *wisda@akba.ac.id;* [e] *firstwanita@akba.ac.id ;* [f] *mursalim@unitama.ac.id;* [g]*afifah170114@gmail.com*
** Corresponding author*

Abstract

Intrusion Detection Systems (IDS) are critical for safeguarding modern networks, yet they often suffer from class-imbalance, leading to poor detection of rare but high-impact attacks. This study develops an IDS that couples Random Forest (RF) with the Synthetic Minority Over-sampling Technique (SMOTE) to mitigate this imbalance when learning from the NSL-KDD benchmark dataset. After standard preprocessing and 5-fold cross-validation on an 80 : 20 train–test split, the proposed RF–SMOTE model attained 99.78 % accuracy, 99.70 % precision, 99.88 % recall, and 99.79 % F1-score. These results indicate markedly improved sensitivity to minority attacks while maintaining a very low false-alarm rate. Our approach contributes an adaptive and readily deployable IDS blueprint for real-world network environments by systematically integrating SMOTE into an RF pipeline.

Keywords— *Intrusion Detection System; Random Forest; SMOTE; Cybersecurity; NSL-KDD Dataset.*

1. Introduction

The increasing complexity and volume of cyberattacks have made network security a top priority in modern information technology infrastructure. Machine Learning-based Intrusion Detection Systems (IDML) have emerged as a key solution to analyze network traffic and automatically identify attack patterns efficiently (Simanjuntak & Sijabat, 2024; Maulani et al., 2023). With the widespread adoption of technologies such as the Internet of Things (IoT), exposure to cyber threats has intensified, necessitating advanced, adaptive, and responsive detection systems to address modern threats.

Previous studies have shown that machine learning algorithms such as Support Vector Machines (SVM) and Neural Networks can outperform traditional approaches in detecting complex and subtle attacks (Tan et al., 2023; Amirah & Sanmorino, 2023). On the other hand, the success of a detection system also greatly depends on the quality of its feature extraction process and classification techniques. Hidayat (2021) emphasized that open-source applications can offer alternative solutions with limited resources, as long as the extracted features are capable of accommodating attack variations. Thus, integrating robust classification methods and data balancing strategies is crucial to strengthening IDML systems.

Although algorithms such as SVM and k-NN have demonstrated solid performance in various studies, one of the major challenges in IDS development remains the class imbalance issue, where minority attack classes are often overlooked due to the dominance of normal traffic

in the dataset (Tasmi et al., 2023). As a result, despite high overall accuracy, systems fail to detect rare but high-risk attacks.

The Synthetic Minority Over-sampling Technique (SMOTE) has been introduced as a data balancing solution by generating synthetic samples from minority classes to improve the model's ability to classify rare events. While this method has proven effective in various classification domains, its application in network intrusion detection systems—especially when combined with Random Forest—has not been extensively explored.

Random Forest is known as a powerful classification algorithm due to its robustness, fast training capability, and ability to handle high-dimensional and noisy data. Several studies have shown that RF can achieve very high accuracy (>99%) in intrusion classification within IoT environments and critical cyber systems (Sulandri et al., 2021). This strength is attributed to its voting mechanism, which minimizes bias from individual decision trees.

To develop more accurate IDML systems, appropriate feature selection and ensemble techniques have been proven to significantly improve performance. The combination of optimization techniques such as ELM and correlation-based feature selection has resulted in high-precision detection systems, as demonstrated by Sulandri et al. (2021). However, such systems often overlook class imbalance issues and have not explicitly integrated SMOTE as a supporting technique.

While numerous studies have examined the use of strong classification algorithms such as SVM, k-NN, or RF, most have focused on overall accuracy without specifically addressing performance on minority classes. In the context of cybersecurity, neglecting minority attacks is a critical weakness due to their potentially severe impact (Tan et al., 2023).

Moreover, there is a lack of comprehensive studies that systematically integrate Random Forest and SMOTE in intrusion detection scenarios. No prior research has thoroughly evaluated the impact of such integration on evaluation metrics such as recall and F1-score for minority classes, particularly with standardized and replicable experimental approaches using benchmark datasets.

This study proposes a prototype Intrusion Detection System (IDS) using Random Forest integrated with the SMOTE technique to address data imbalance. The primary objective is to evaluate how this integration improves sensitivity in detecting minority-class attacks, measured through accuracy, precision, recall, and F1-score. The study fills an existing research gap by systematically assessing the impact of SMOTE integration within a Random Forest pipeline using the NSL-KDD benchmark dataset.

2. Literature Review

Previous research has explored a variety of techniques to address class imbalances in intrusion detection. For example, Shafiq et al. (2022) used the Adaptive Synthetic Sampling (ADASYN) method in combination with the Decision Tree algorithm, resulting in a significant increase in sensitivity to minority classes on the UNSW-NB15 dataset. Similarly, the Random Over-Sampling (ROS) method has been applied by Zhong et al. (2021) in the Support Vector Machine (SVM) model, which showed an increase in rare attack recall of up to 12% compared to no balancing on the CIC-IDS2017 dataset. In contrast, an undersampling approach such as NearMiss was used by Abdulhammed et al. (2020) with the k-NN algorithm, which managed to significantly reduce the rate of false positives, albeit at the risk of losing important information from the majority sample. However, systematic comparative studies between these techniques and the integration of SMOTE in Random Forest, especially in the NSL-KDD dataset, are still very limited, so it is the main basis of this study.

3. Method

This study uses the NSL-KDD dataset. This dataset was chosen because it represents realistic attack scenarios in traffic-congested IoT environments. All experiments were

conducted using the Python programming language, with the support of the Scikit-learn library for the implementation of Random Forest, and Imbalanced-learn for the implementation of the Synthetic Minority Over-sampling Technique (SMOTE). The computation is carried out in a hardware environment with an 8-core processor and 16GB of RAM, which is enough to support the training process of models on medium to large scales. The dataset is converted in numerical format to ensure full compatibility with the machine learning model used. Figure 1 shows the stages of the data analysis process in the research.

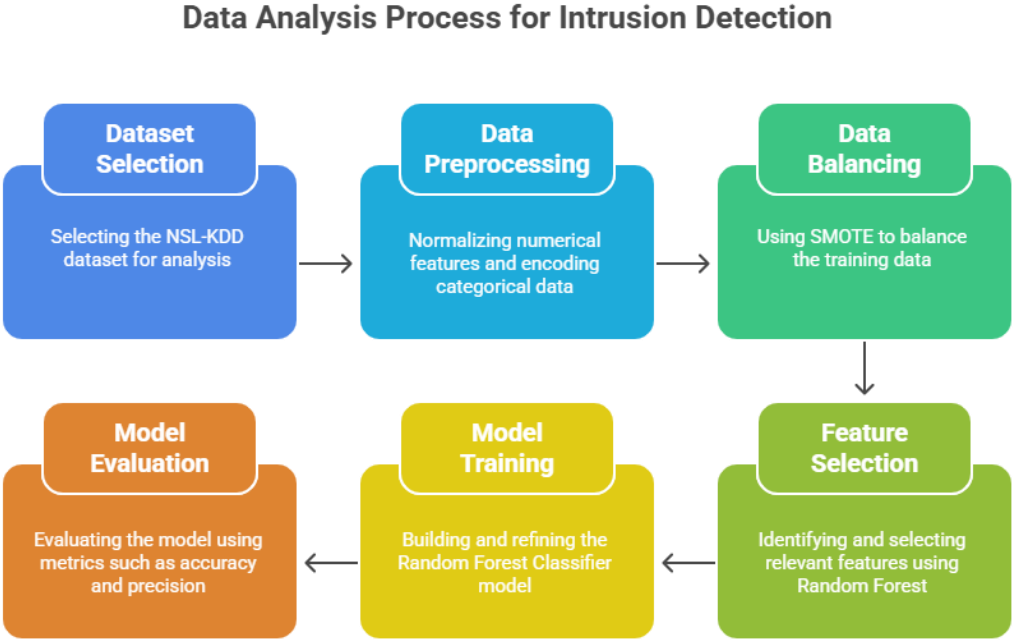

Figure 1. Data Analysis Process for Intrusion Detection

3.1 Dataset

The dataset used in this study is NSL-KDD, which is an improved version of the 1999 KDD Cup dataset. NSL-KDD is designed to address some of the weaknesses in its predecessor dataset, such as duplicate data and extremely unbalanced class distributions. This dataset is widely used in intrusion detection system research because it covers different types of network attacks, including DoS, probing, R2L (Remote to Local), and U2R (User to Root), as well as normal data. The use of NSL-KDD provides a solid foundation for classification algorithm testing as it provides a standardized data structure that is ready for use in machine learning scenarios.

3.2 Data Preprocessing

At this stage, a series of data transformations are carried out to ensure that the input corresponds to the format required by the machine learning algorithm. This process includes normalizing numerical features so that the scales between features are uniform, as well as coding categorical variables using the one-hot encoding or label encoding method. This stage is important to prevent bias in model training as well as accelerate the algorithm convergence process.

3.3 Data Balancing

An unbalanced distribution of classes can cause the model to study dominant patterns only and ignore minority classes. To overcome this problem, the Synthetic Minority Over-sampling Technique (SMOTE) was applied to the training data. SMOTE works by generating synthetic

samples from minority classes based on interpolation between samples, so that the class distribution becomes more balanced and the model can learn more fairly across all data categories.

3.4 Feature Selection

This stage aims to identify the features that have the most influence on the classification process using Random Forest Feature Importance. Feature selection is done to simplify model complexity, reduce the risk of overfitting, and improve computational efficiency. Only features with significant contributions to prediction accuracy are retained for model training. RF feature-importance scores retained the top-10 features.

3.5 Model Training

Once the balanced data and relevant features have been selected, the model training process is carried out using the Random Forest algorithm. The model is built with a number of decision trees that work collectively to produce final predictions through a voting mechanism. Model parameters are set using a finite search grid to obtain the best combination that maximizes classification performance. Table 1 shows the Random Forest configuration.

Table 1. Random Forest configuration

Parameters	**Value**
n_estimators	200
max_depth	None
min_samples_split	2
min_samples_leaf	1
criterion	*gini*
random_state	42

3.6 Model Evaluation

The evaluation stage was carried out to measure the effectiveness and reliability of the model using comprehensive performance metrics, namely accuracy, precision, recall, and F1-score. In addition, a confusion matrix is used to analyze the distribution of true and false classifications in more depth. This evaluation is important to determine the model's ability to detect attacks and minimize misclassifications in intrusion detection systems.

4. Results And Discussion

Figure 2 shows the ten most influential features in the classification process by the Random Forest algorithm on the NSL-KDD dataset. The src_bytes and dst_bytes features topped the list with the largest contribution to model classification decisions, followed by flag, same_srv_rate, and diff_srv_rate. This suggests that the volume of data sent and received, as well as connection attributes such as service types and their differences, are decisive in distinguishing between

normal traffic and attacks. These results confirm that traffic-related numerical features are important indicators in network intrusion detection using Random Forest (SaiRajKumar, 2024).

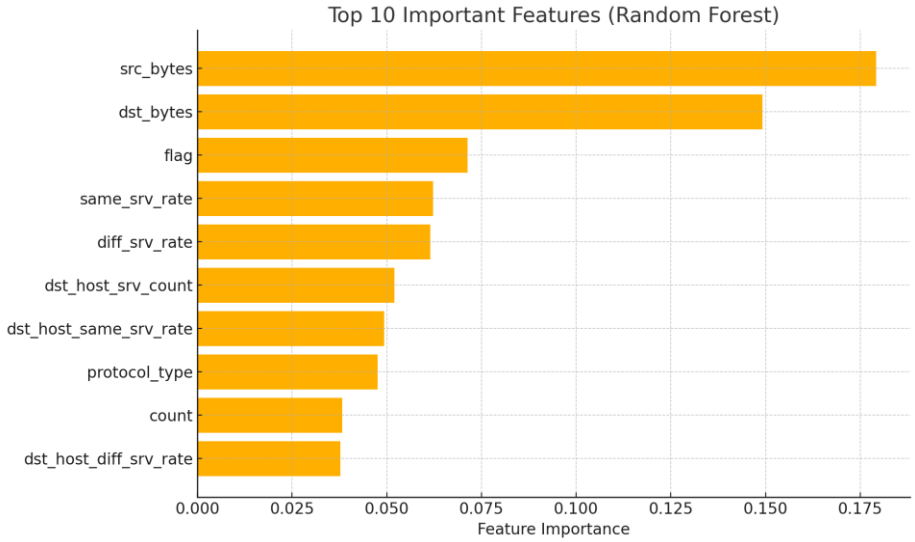

Figure 2. Top Important Features

The results of this feature selection are in line with the findings from Rahim et al. (2021), which emphasize the importance of selecting correlation-based statistical features to improve accuracy and reduce false alarms in intrusion detection systems. They show that the elimination of non-informative features can improve the generalization of the model. Meanwhile, the approach developed by Enache et al. (2015) through the Binary Bat Algorithm also identified traffic features such as src_bytes as the dominant element, showing consistency of results across optimization methods. Thus, the results of this experiment not only confirm the previous findings but also show that Random Forest-based feature selection techniques can simplify the model without sacrificing classification performance.

Figure 3 shows the confusion matrix of the classification results using the Random Forest algorithm on the test data from the NSL-KDD dataset. The model was able to correctly classify 3,504 samples of normal traffic, and only misclassified 12 of them as attacks. Meanwhile, of the total attacks, 4,037 samples were correctly identified as attacks, and only 5 cases were mistakenly classified as normal traffic. Overall, this confusion matrix shows the dominance of the number of correct predictions (True Positive and True Negative) over the number of misclassifications, indicating the excellent performance of the model.

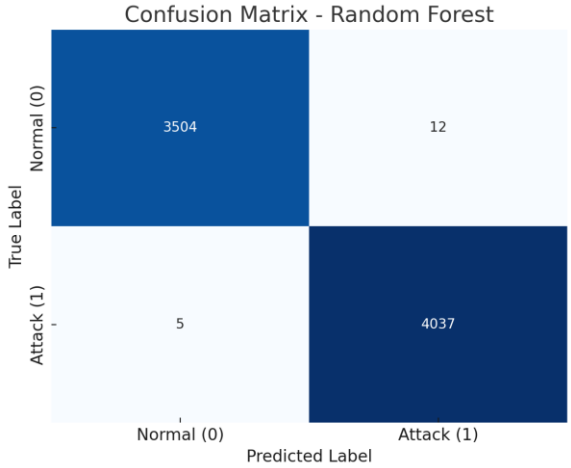

Figure 3. Confusion Matrix

These results support previous literature emphasizing the effectiveness of Random Forest in detecting intrusions with precision. Krstinić et al. (2020) stated that confusion matrix-based evaluations provide a solid basis for calculating performance metrics relevant to intrusion detection systems, such as recall and F1-score, which are particularly important in the context of minority attacks. These findings are also in line with a study by Ramadhani et al. (2024), which emphasized that a high number of True Positives is an indicator of IDS's success in recognizing actual attack patterns. The low False Negative value in these results indicates that the system has a high sensitivity to cyber threats without sacrificing the false positive rate.

Figure 4 shows the performance of the Random Forest model evaluated using four key metrics: Accuracy, Precision, Recall, and F1-score. The results obtained were very high and consistent, with an accuracy value of 99.78%, precision of 99.70%, recall of 99.88%, and F1-score of 99.79%. These numbers indicate that the model is able to accurately detect almost all attacks and normal traffic, with a very low error rate. The high recall value and F1-score also indicate that this model has excellent sensitivity to minority data, i.e. attacks.

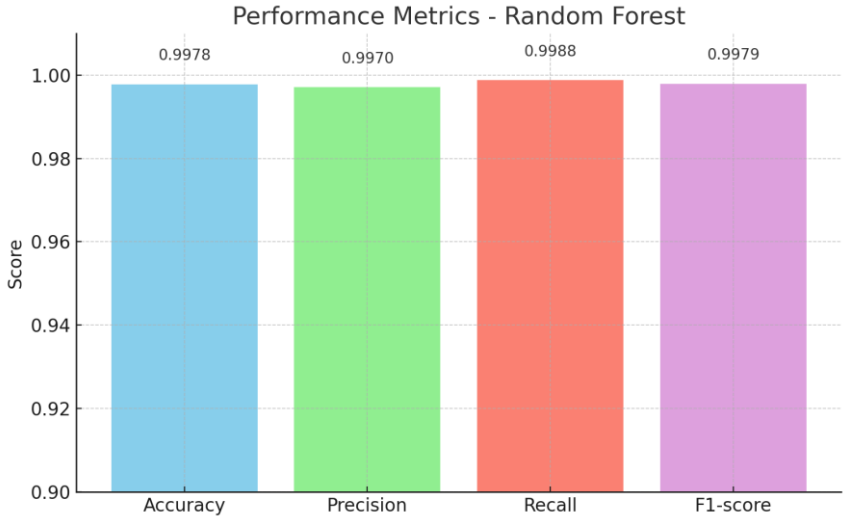

Figure 4. Performance Metrics

Random Forest's very high performance in detecting intrusions in the NSL-KDD dataset has important implications both scientifically and practically. Scientifically, this reinforces the understanding that a combination of ensemble algorithms and balancing strategies such as SMOTE can address the classic challenges of data imbalance in cybersecurity. Practically, organizations can adopt this approach to improve the effectiveness of network monitoring with very low false alarms. The reliability of such models can support the implementation of IDS that is responsive, efficient, and capable of identifying attacks with high accuracy in a real-world production environment (Krstinić et al., 2020; Ramadhani et al., 2024; Zhao et al., 2021).

5. Conclusions

This research has successfully designed and implemented an intrusion detection system based on the Random Forest algorithm combined with the Synthetic Minority Over-sampling Technique (SMOTE) technique to improve the classification performance of unbalanced network data. Based on the results of experiments using the NSL-KDD dataset, the model showed excellent performance with an accuracy of 99.78%, accuracy of 99.70%, recall of 99.88%, and an F1-score of 99.79%. Confusion matrix analysis strengthens the effectiveness of the system in minimizing false positives and false negatives simultaneously.

The use of Random Forest-based feature selection methods has also been shown to be able to identify the most relevant features, which in turn simplifies the complexity of the model without sacrificing accuracy. These results are consistent with the literature showing that feature

selection and class balancing are crucial factors in the development of machine learning-based intrusion detection systems.

A major contribution of this research is the systematic integration between Random Forest and SMOTE as a replicable approach to building IDS that is sensitive to minority attacks and efficient in real-time implementation. For further research, it is recommended to test the model on other, more complex datasets as well as evaluate its performance under real network conditions for further validation of the robustness and scalability of the model.

Acknowledgements

Our research is funded in 2025 by the Ministry of Research, Technology and Higher Education of the Republic of Indonesia through the Beginner Lecturer Research scheme with Grant Number 130/C3/DT.05.00/PL/2025.

References

Amirah, A., & Sanmorino, A. (2023). Deteksi intrusi siber pada sistem pembelajaran elektronik berbasis machine learning. Jurnal Ilmiah Informatika Global, 14(2), 12-16. https://doi.org/10.36982/jiig.v14i2.3227

Abdulhammed, R., Faezipour, M., & Abuzneid, A. (2020). Effective intrusion detection with minority class balancing techniques. Journal of Network and Computer Applications, 157, 102530. https://doi.org/10.1016/j.jnca.2020.102530

Enache, A. C., Sgârciu, V., & Petrescu-Niță, A. (2015). Intelligent feature selection method rooted in binary bat algorithm for intrusion detection. Proceedings of the 2015 IEEE 10th Jubilee International Symposium on Applied Computational Intelligence and Informatics, 517-521. https://doi.org/10.1109/saci.2015.7208259

Hidayat, A. M. N. (2021). Sistem deteksi intrusi dan prevensi berbasis open source. Jurnal Instek (Informatika Sains Dan Teknologi), 6(1), 102. https://doi.org/10.24252/instek.v6i1.18642

Krstinić, D., Braović, M., Šerić, L., & Božić-Štulić, D. (2020). Multi-label classifier performance evaluation with confusion matrix. Computer Science & Information Technology, 100801. https://doi.org/10.5121/csit.2020.100801

Maulani, I. E., Putra, D. R. S., & Komarudin, K. (2023). Sistem deteksi intrusi cerdas: Studi perbandingan algoritma pembelajaran mesin untuk keamanan siber. Jurnal Sosial Teknologi, 3(11), 918-923. https://doi.org/10.59188/jurnalsostech.v3i11.987

Rahim, R., Ahanger, A. S., Khan, S. M., & Masoodi, F. (2021). Analysis of IDS using feature selection approach on NSL-KDD dataset. Proceedings of the International Conference on Computational Intelligence and Data Science, 475-481. https://doi.org/10.52458/978-93-91842-08-6-45

Ramadhani, F., Septiana, D., Amalia, S. N., Fadilah, P. M., & Satria, A. (2024). Klasifikasi risiko gizi buruk pada ibu hamil menggunakan metode random forest. Djtechno Jurnal Teknologi Informasi, 5(2), 370-380. https://doi.org/10.46576/djtechno.v5i2.4815

SaiRajKumar, M. (2024). GuardianAI: Smart intrusion detection for modern threats. Research Square. https://doi.org/10.21203/rs.3.rs-3897226/v1

Simanjuntak, R. P., & Sijabat, R. R. M. (2024). Meningkatkan keamanan siber dalam lingkungan Internet of Things (IoT) dengan menggunakan sistem deteksi intrusi berbasis pembelajaran mesin. Dike, 2(2), 62-68. https://doi.org/10.69688/dike.v2i2.106

Sulandri, S., Basuki, A., & Bachtiar, F. A. (2021). Metode deteksi intrusi menggunakan algoritme extreme learning machine dengan correlation-based feature selection. Jurnal Teknologi Informasi Dan Ilmu Komputer, 8(1), 103. https://doi.org/10.25126/jtiik.0813358

Shafiq, M., Tian, Z., Sun, Y., Du, X., & Guizani, N. (2022). Network intrusion detection using adaptive synthetic sampling and ensemble learning. IEEE Access, 10, 2978–2989. https://doi.org/10.1109/ACCESS.2022.3141617

Tan, T., Sama, H., Wijaya, G., & Aboagye, O. E. (2023). Studi perbandingan deteksi intrusi jaringan menggunakan machine learning: (Metode SVM dan ANN). Jurnal Teknologi Dan Informasi, 13(2), 152-164. https://doi.org/10.34010/jati.v13i2.10484

Tasmi, T., Antony, F., Dhamyanti, D., Setiawan, H., & Oklilas, F. (2023). Pengenalan pola serangan pada Internet of Thing (IoT) menggunakan support vector machine (SVM) dengan tiga kernel. Jurnal Processor, 18(2). https://doi.org/10.33998/processor.2023.18.2.1457

Zhao, Z., Zhou, W., Qiu, Z., Li, A., & Wang, J. (2021). Research on Ctrip customer churn prediction model based on random forest. Lecture Notes in Computer Science, 511-523. https://doi.org/10.1007/978-3-030-92632-8_48

Zhong, Z., Chen, Y., & Gan, C. (2021). Enhancing intrusion detection by random oversampling on imbalanced datasets. Computers & Security, 104, 102159. https://doi.org/10.1016/j.cose.2021.102159