Available at https://www.iasj.net/iasj
Iraqi Academic Scientific Journals
Journal homepage:
https://journals.uokerbala.edu.iq/index.php/UOKJ

Research Article

A Multi-Class Classification of Intrusion Detection System based on machine learning

Wasan Mueti Hadi
Department of Computer Science, College of Computer Science and Information Technology, University of Kerbala, Iraq.

Article Info

Article history:
Received 1 -12-2025
Received in revised form 29-12-2025
Accepted 29-1-2026
Available online 31 -3 -2026

Keywords:
Intrusion Detection System, Machine Learning, LightGBM, CICIDS2017_SMOTE

Abstract

Intrusion Detection Systems (IDSs) are representing a core of component of organizational network security, as they serve as the first line of defence against a wide range of cyber threats. They are responsible for effectively handling potential intrusions on the network. Internet attacks severely damage a website or server, make them inaccessible to other users. Numerous IDS systems employ flow-based network traffic analysis to identify potential threats. In this paper, we proposed a LightGBM(Light Gradient Boosting Machine) machine learning model that designed to create a flow-based anomaly detection intrusion detection system for multi-class classification. The model is evaluated using the updated CICIDS2017 dataset(CICIDS2017_Cleaned) for multi-attack classification. The model achieved an accuracy of 0.9984,F1-score of 0.9591and precision of 0.9356. The model has excelled in accuracy, detection rate, and low false alarm rate.Because they often use machine learning techniques for rather than intrusion detection systems. The study shows that the results are difficult with multi-class classification on imbalanced data sets, and lacks effective dynamic detection mechanism. In order to remedy this research gap, this article proposes a lightGBM-based dynamic intrusion detection system blending the CICIDS2017 dataset with SMOTE.

Corresponding Author E-mail: wasan.m@uokerbala.edu.iq
Peer review under responsibility of Iraqi Academic Scientific Journal and University of Kerbala.

Introduction

In recent years, the increasing vulnerability of numerous organizations to advanced cyber-attacks has prompted a rapid development of novel Intrusion Detection Systems (IDSs). The advancement of Intrusion Detection Systems (IDSs) is of interest to both the academic and industrial sectors globally, owing to the repercussions of each cyber-attack, including economic costs, reputational harm, and legal issues. Consequently, it is imperative to safeguard networks against unwanted access and to protect user communications and data, as well as to identify emerging security vulnerabilities [1]. Intrusion Detection Systems (IDS) are critical to enhancing corporate security. They provide an additional layer, which is that of defence detecting there and readiness to respond quickly to any threat escaped by preventive measures. Threats identified by this system may include malware and phishing attacks, as well as innumerable types of cyber assaults outside the scope fixed on regular security solutions[2]. The IDS takes PrimeProbe potential failures identified as emerged through a network layer, and identificates them as anomalies.This method is typically static and linked to the rules or algorithms utilized for detecting cyberattacks. However, this static methodology presents difficulties in adapting the recognition of new attack types, since it requires the modification of rules for signature-based IDS or the retraining of the detection model for anomaly-based IDS. Anomaly-based Intrusion Detection Systems (IDS) are closely linked to the application of machine learning (ML) techniques[3]. We deployed an intrusion detection system using the CICIDS2017 dataset, employing the Synthetic Minority Over-sampling Technique (SMOTE).This technique in machine learning is utilized to address class imbalance issues in datasets. SMOTE produces synthetic samples for the minority class by amalgamating existing samples with artificially generated ones, based on the variances within the current data. This is implemented to augment the sample size of the minority class while maintaining balance between the minority and majority classes in the dataset [4]. This balanced data was used to train the Light Gradient Boosting Machine (LightGBM) model, including hyperparameter tuning. Our model reached a classification accuracy of 99% and an F1-score of 95%, which shows just how important it is to model correctly for the best performance [5]. The purpose of this experiment is to evaluate the effectiveness of an intrusion detection system using SMOTE and classification algorithm on recognizing multiple intrusions [6].

Related Work

The feature that the artificial neural network-based intrusion detection systems could identify intrusion patterns more efficiently and therefore to analyze large data collection more easily. Machine learning can best be described as a branch of artificial intelligence where ways are sought for making machines learn by themselves and do things which are not specifically written into their code.Representation and generalization are basic elements involved in machine learning, the two fundamental characteristics that have been selected to support this paper [7]. Zhukabayeva,T. et al. [8] introduced a multi-class classification intrusion detection system for industrial IoT, using XGBoost and Deep Neural Networks (DNN) as machine learning methodologies. How could it be more clear that adaptable strategies against the emergence of cyber threats. When the two datasets are compared, we can see that the XGBoost model scored an accuracy

rate of 79% for dataset D1 increasing to some 99.42% on dataset D2-making them quite efficient in realizing various cyber threats. Alrefaei, A. and Ilyas, M.[9] used a PySpark-based structure, with relevant dataset preprocessing based on SMOTE and feature selection, as well as multiclass classification using the OneVsRest technique, this paper aimed to realize for algorithms such as Extreme Gradient Boosting and Random Forest applied in dataset IoT-23 high-precision real-time IoT attack detection . Singh, T.P. et al.[10] The research introduced two new Intrusion Detection Systems (IDS) based on Deep Learning for multi-class classification: used LuNet alongside Bidirectional LSTMs; and through a combination of TCN,CNN and Bi-LSTM. The models were verified on NSL-KDD as well as UNSW-NB15.the examples displayed enhanced efficiencies compared with typical Machine Learning techniques and current Deep Learning models.The research underscores the effectiveness of ensemble techniques; it boasts classification rates as high as 99%. This affords intrusion detection systems more robustness. Bacevicius, M.and Paulauskaite-Taraseviciene, A.[2] With machine learning methods applied on greatly imbalanced data, this study exploratively examined multi-class classification for intrusion detection, focused on the CIC-IDS2017 and CSE-CIC-IDS2018 datasets. Using many models, including Logistic Regression, Random Forest, Decision Trees, Neural Networks, and so forth to classify network intrusions over different classifications. The study stresses the importance of knowing what kind of particular attack, and uses techniques of explainable AI for explanation accuracy. Among these, decision trees employing CART algorithm attained a highest average macro F1-score of 0.96. Zhang, Y. et al. [11] Its proposed Network Intrusion Detection System (NIDS) makes full use of machine learning techniques such as Random Forest and XGBoost, along with deep learning methods like Deep Neural Networks (DNN) to detect network intrusions and classify attacks. The models achieved high accuracies on binary classification tasks Over 99.25% for the NSL KDD dataset and over 93% for the UNSW NB-15 dataset .The models demonstrated strong performance in multiclass classification tests Exceeding 97.70% for the NSL KDD dataset and over 92.50% for the UNSW NB-15 dataset. Othman, T.S. and Abdullah, S.M. [12] This study brought an IIDS (Intelligent Intrusion Detection System), which takes machine learning approach to the multi-class classification of attack detection in IoT.It examines the IoT23 dataset for training purposes, and considers three types of classifiers: K-Nearest Neighbor, Support Vector Machine and Artificial Neural Network.The IIDS can distinguish in a very successful way between 15 types of attacks and benign activities, which makes up for flaws pointed out in previous research. In addition, the present study takes new attack patterns as its object of examination and makes multi-class classification possible including the identification of zero-day attacks. Tait, K.-A. et al. [13]With 0.9983 as the highest accuracy rate for multiclass classification, the k-Nearest Neighbor algorithm remains best suited for turning away different types of attacks. This focused mode of attack, rather than using all or nothing reaction against an entirely incoming intruding force which while achieving an accuracy rate up to 0.9977 using the Random Forest algorithm. Guo, G. [14] The study is about applyed a multi-classification approach to Intrusion Detection Systems (IDS) using machine learning techniques. TON_IoT network data set was used in this study. In addition, ten different machine learning techniques were evaluated. Finally, the classifier of choice is the XGBoost method. The model also boasts incredible performance

99.17% Matthews Correlation Coefficient (MCC) in multi-category classification reveals its ability to pinpoint numerous different kinds of intrusions within IoT systems. Ahanger, A.S., Khan, S.M. and Masoodi, F. [15]. The paper is on constructing an effective Intrusion Detection System (IDS) by used supervised machine learning techniques with special attention to the multi-class classification problem. The NSL-KDD database is invoked in the project. There were four machine learning algorithms used: Random Forest (RF), Decision Tree (DT), Multilayer Perceptron (MLP)·and Support Vector Machines (SVM) to classify NSL-KDD dataset. The project fully demonstrates the possibility of feature selection helping models achieve a higher level of effectiveness. By reducing the dimensions and complexity in computation, one can achieve an accuracy in classifying many different kinds of intrusions above 99%. Sarraf, J. et al. [16] Compare: In comparison to multi-class classification, this study focuses on binary classification in the detection of network intrusions. Therefore, it employs k-nearest neighbor, artificial neural network, random forest(s) and XGBoost a total of four different machine learning methods for finding when an intrusion occurs and what type it is. Research results show that the classification accuracy rate of intrusion with XGBoost goes upto 83.92%; but the algorithm doesn't handle multi-class situations.

Methodology

This part will explain what methods and materials are used in our study. Figure 1 shows the structure of project.

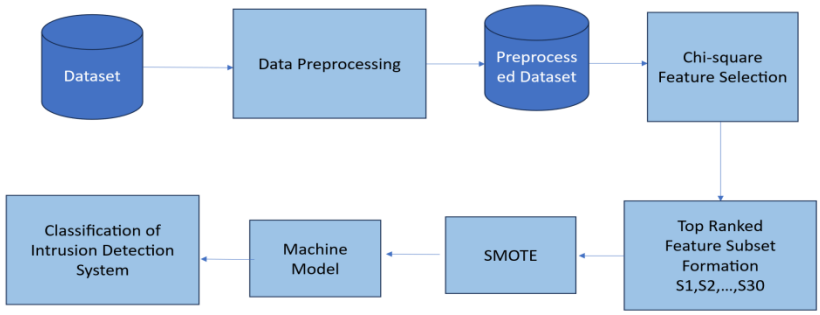


Figure 1 Proposed model architecture

A. CICIDS2017 Dataset Description

It was a matter of fact that the dataset is established by the Canadian Institute for Cybersecurity(CIC) and served as a benchmark for Intrusion Detection Systems (IDS).The dataset, produced in a realistic network environment, simulates typical user behavior and a great variety of current cyber-attacks.At this stage, the data comes with five consecutive days of traffic collection in which over a dozen homes on NWU Campus provided internet access facilities modified terms formatted according to us hearth.The dataset consists of comprehensive flow records in both directions and is obtained with CICFlowMeter.There, people in many fields, such as DoS/DDos; Brute Force Web (XSS and SQL Injection), Botnet

action; Account penetration by brute force; E-mail spoofing through a proxy server, Port Scanning; the HeartBleed vulnerability can get a living wage. Thus, CICIDS2017 is suitable for both task types involving multi-class attack and binary class attacks. This paper makes use of a subset, CICIDS2017_cleaned, cleaned of bad, duplicate and noisy records and standardized features : ensuring standard and high-quality input for machine learning experiments [1].

B. Scaling

C. Chi-square Feature Selection

Feature selection is a critical step in machine learning that one embarks upon to improve model performance, interpretability, and compute efficiency. It seeks to keep useful characteristics while removing redundant ones. Redundant characteristics can lead to problems such as the curse of dimensionality, a mass of information just a shortage knowledge on what to do with it, reduced accuracy but increased time and space complexity. It is necessary to choose a certain ridge in feature space based on the tested characteristics using FS. The objective is to make their number smaller while keeping the precision and reducing Model Build-up Time (MBT). This is done via methods like Chi-square. This strategy facilitates the optimization of the FS process and enhance model performance [18]. The chi-square statistic is calculated by squaring the disparity between observed (O) and expected (E) values, as delineated in Equation (1) [19].

$$X^2 = \sum_{i=1}^{k} (o_i - E_i)^2 / E_i \qquad (1)$$

D. Split Dataset

Moreover, the limited sample size in the datasets renders the classification results highly unstable; hence, We have trained and evaluated our models over 100 iterations. In each cycle, we randomly shuffle and partition the data into training and testing sets, thereafter training them according to the model [20].

When the characteristics of educational data becomes Americanized, and also there are differences in both standard deviations as well as mean value from csv files that accompany it, the result can be that our learning process becomes less effective Analysis was carried out in the method of the paper. Data is placed in file. Abstract the data is standardized using MinMaxScaler standardizing it down until there is a standard deviation between one and zero. The data is normalized using standard scalar from the sklearn library [17].

E. Smote

diminished. This constitutes a fundamental issue in machine learning. The SMOTE technique mitigates the problem of imbalanced data, and given that all characteristics in the CICIDS2017 dataset are numerical traffic-flow attributes derived from CICFlowMeter, the application of SMOTE is suitable. The fundamental concept of SMOTE is to create new synthetic samples by interpolating points randomly among minority-class samples and their nearest neighbors. The K-nearest neighbors of each instance in the minority class are identified first. Assuming an oversampling rate of N, N samples are produced from the K-NN set, where K exceeds N. The interpolation formula utilized in SMOTE is explained in equation (2).

$$Si = X + rand(0,1) \times (yi - X) \qquad (2)$$

where X denotes a data sample from minority-class, $rand$ (0,1) refers to a random number within the interval (0,1), yi represents the i^th nearest neighbors, and Si signifies the interpolated sample [21].

F. Light Gradient Boosting

The LightGBM methodology has undergone optimization. It is a method that relies on a histogram-based decision tree and employs histogram subtraction for accelerating purposes. We used a histogram-based strategy to ease the optimization of sparse characteristics. A leaf growth based on depth restraint is provided in the LIghtGBM format. This is to avoid the occurrence of errors. It can also improve the accuracy. The Leaf-wise method sets a depth limit. With this scheme, it is possible to simultaneously avoid overfitting and improve the accuracy of any model. The cache hit rate has been optimized, and multi-threading optimized. LightGBM has included decision rules in categorical features. It is not designed this way to add any more computational or memory burdens. This procedure involves generating multi-dimensional one-hot encoding for the properties. LightGBM is a Gradient Boosting Decision Tree technique proposed by Ke et al. in 2017, which is applied in many domains of data mining, including classification, regression, and ranking. LightGBM combines two new techniques: a one-sided approach to analyzing gradients, and its exclusive feature bundle [22].

Results and Evaluation

To check the efficacy of the Light Gradient Boosting Machine (LightGBM), the CICIDS2017_cleaned dataset was employed. The results indicate that LightGBM's default parameters same as XGBoost, hence its absolute prediction quality across ordinary evaluation indicators. A correct rate of 0.9984 was recorded, meaning the majority of network traffic cases were accurately classified. For precision-and-recall, there is nowhere thickly shifting that only a bit thin lines criss-cross. It can be read from the data that its level of identification rate (precision) was 0.9356 percent (a fairly high number), that it managed 0.9915 to represent the number identifying items identified correctly and The weighted F1 suggests an overall_corpus summary on both precision and recall: this simple model can handle such vast input volumes as FTP logs while providing superior performance. The weighted F1 of 0.9591 illustrates this harmonious marriage between precision and recall, suggesting that the model itself possesses a strong quality to withstand any attack. In other words, one can rely on this LightGBM to get the job done. This paper demonstrates that LightGBM fits very well low proportion of intrusion detection tasks with imbalanced network traffic datasets like CICIDS2017_cleaned.Data, managing attack and benign traffic POWERFULLY which it also has a strong ability to learn from examples.

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}} \quad (3)$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP+FN}} \quad (4)$$

$$\text{F1} = 2 \times \frac{(\text{Precision}) \times (\text{Recall})}{(\text{Precision}) \times (\text{Recall})} \quad (5)$$

$$\text{Accuracy} = \frac{\text{TP+FP}}{\text{TP+TN+FP+FN}} \quad (6)$$

TP: This is true positive. That is, if the model predicts a positive result, it really is positive. (3)

FP: In this case, FP stands for False Positive; when the actual value is false and the model predicts that it’s positive.

TN stands for True Negative, of course: the model predicts a negative number and indeed there are no positives.

FN stands for False Negative, the event is negative and the model forecasts it can also be determined.

Precision: how many of the model's data points selected as significant actually are. Given in (3).

Recall: Measurement for how well the model accurately detects positive classes in the dataset. Equation: (4)

F1: The accuracy metric for the evaluation as measured in the dataset. Equation: (5)

Accuracy is a measure of the model's effectiveness in spotting real patterns and linkages among features. (Equation: 6).

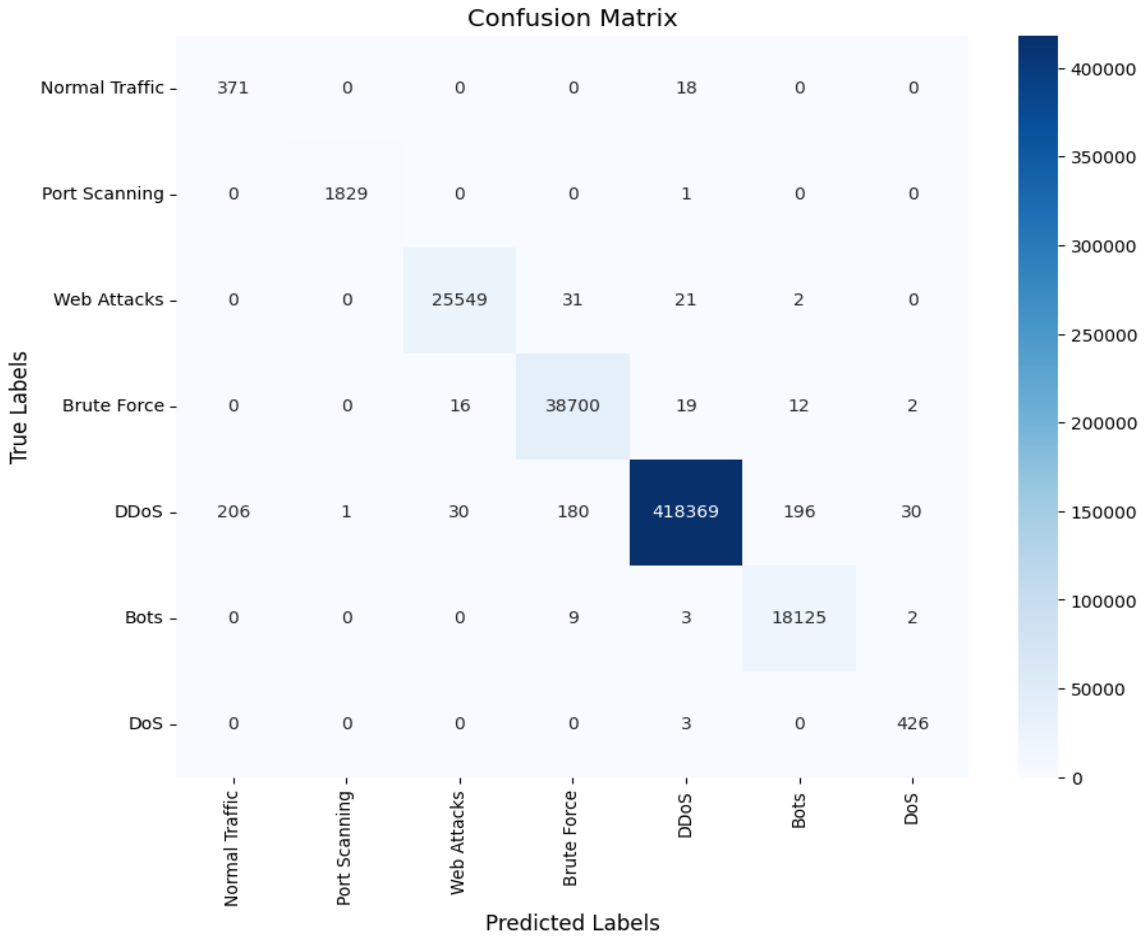


Fig. 2: Confusion Matrix of the LightGBM Classification

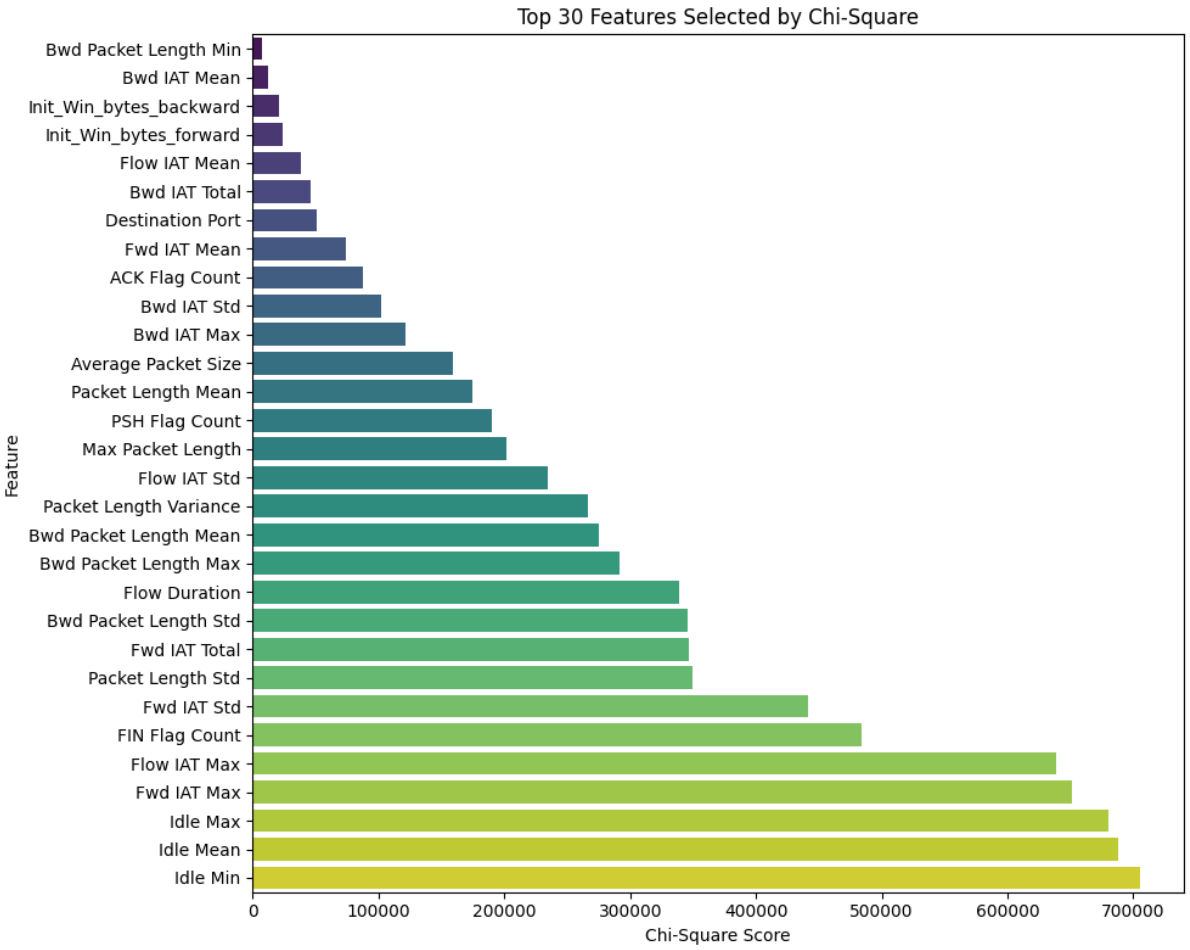


Fig. 3: Feature Selection by Chi-square

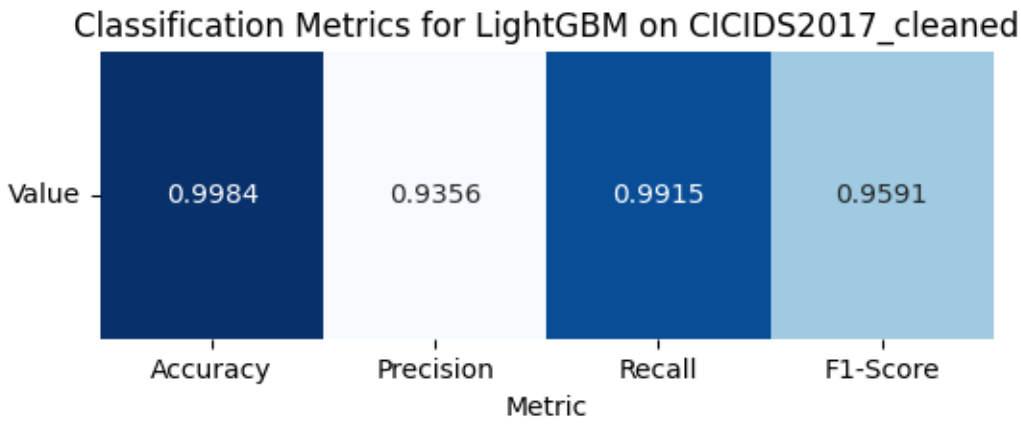


Fig. 4: Classification Metrics for LightGBM

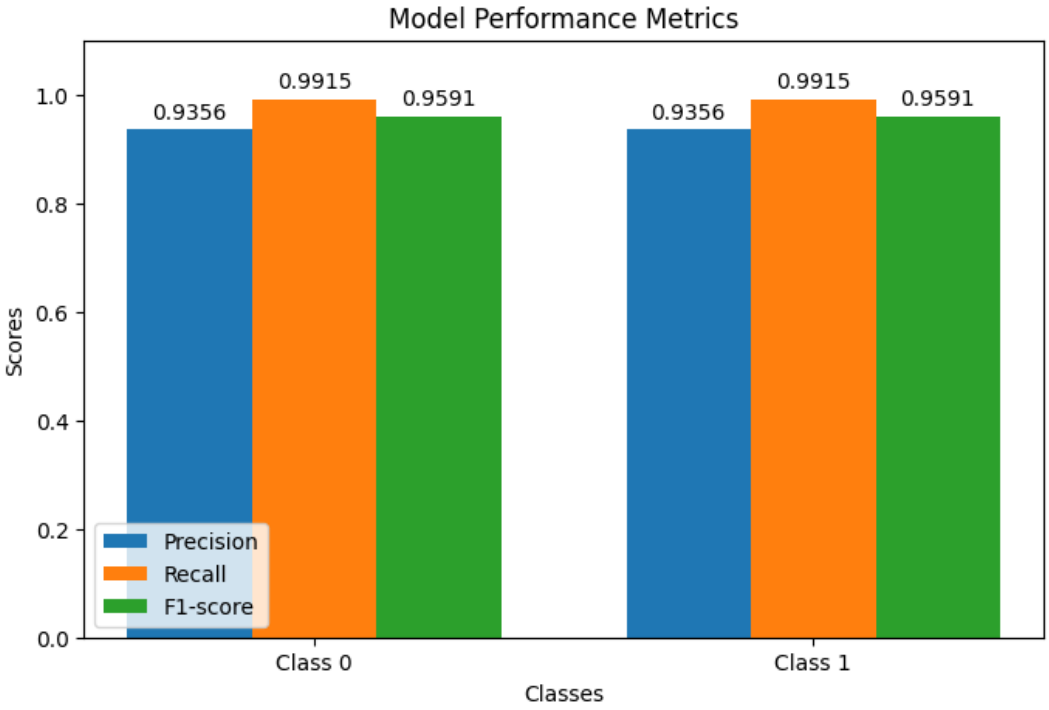
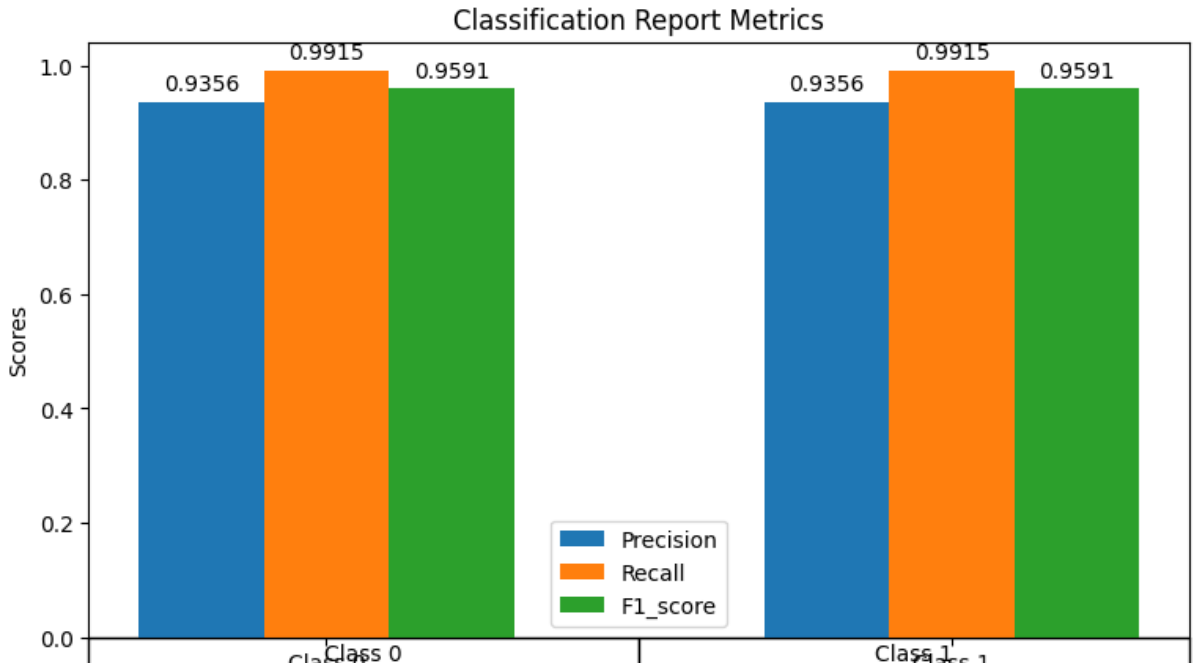


Fig. 5: Model Performance Metrics



	Class 0	Class 1
Precision	0.9356	0.9356
Recall	0.9915	0.9915
F1 Score	0.9591	0.9591
Support	1676045	1676045

Table1: Classification Report for LightGBM

Conclusion

The Light Gradient Boosting Machine (LightGBM) model was used to build a cost-effective intrusion detection solution for network security on the CICIDS2017_cleaned data. The model achieved a chance in performance, with accuracy 0.9984 pointing strongly to its ability accurately specify most of NetFlow cases. At the same time, it had an accuracy 0.9356 and recall 0.9915, showing again that raises True Positives while reducing False Negatives. The F1-score of 0.9591 confirms this model's well-balanced and tenacious performance handling unbalanced data. The results tell us that LightGBM, together with appropriate feature selection and hyperparameter optimization methods, provides a strong, cost-efficient approach to improve intrusion detection systems in complex network environments. It is hoped that future work might study this model's incorporation in deep learning frameworks and ascertain whether or not it can be adapted for more universal use by a wider variety of datasets.

References

1-Toupas, P. et al. (2019) 'An Intrusion Detection System for Multi-class Classification Based on Deep Neural Networks', in 2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA). 2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA), Boca Raton, FL, USA: IEEE, pp. 1253–1258. Available at: https://doi.org/10.1109/ICMLA.2019.00206.

2-Bacevicius, M. and Paulauskaite-Taraseviciene, A. (2023) 'Machine Learning Algorithms for Raw and Unbalanced Intrusion Detection Data in a Multi-Class Classification Problem', Applied Sciences, 13(12), p. 7328. Available at: https://doi.org/10.3390/app13127328.

3-Larriva-Novo, X. et al. (2020) 'An Approach for the Application of a Dynamic Multi-Class Classifier for Network Intrusion Detection Systems', Electronics, 9(11), p. 1759. Available at: https://doi.org/10.3390/electronics9111759.

4-Widodo, A.O., Setiawan, B. and Indraswari, R. (2024) 'Machine Learning-Based Intrusion Detection on Multi-Class Imbalanced Dataset Using SMOTE', Procedia Computer Science, 234, pp. 578–583. Available at: https://doi.org/10.1016/j.procs.2024.03.042.

5-Alharthi, A., Alaryani, M. and Kaddoura, S. (2025) 'A comparative study of machine learning and deep learning models in binary and multiclass classification for intrusion detection systems', Array, p. 100406. Available at: https://www.sciencedirect.com/science/article/pii/S2590005625000335 (Accessed: 24 November 2025).

6-likebupt (no date) SMOTE - Azure Machine Learning. Available at: https://learn.microsoft.com/id-id/azure/machine-learning/component-reference/smote?view=azureml-api-2 (Accessed: 24 November 2025).

7-Dong Lee, J. et al. (2021) 'M-IDM: A Multi-Classification Based Intrusion

Detection Model in Healthcare IoT', Computers, Materials & Continua, 67(2), pp. 1537–1553. Available at: https://doi.org/10.32604/cmc.2021.014774.

8-Zhukabayeva, T. et al. (2025) 'An Intrusion Detection System for Multiclass Classification Across Multiple Datasets in Industrial IoT Using Machine Learning and Neural Networks Integrated with Edge Computing', in A. Nayyar, T.W. Ling, and C. Leung (eds) Advances in Transdisciplinary Engineering. IOS Press. Available at: https://doi.org/10.3233/ATDE250012.

9-Alrefaei, A. and Ilyas, M. (2024) 'Using Machine Learning Multiclass Classification Technique to Detect IoT Attacks in Real Time', Sensors, 24(14), p. 4516. Available at: https://doi.org/10.3390/s24144516.

10-Singh, T.P. et al. (2024) 'YARS-IDS: A Novel IDS for Multi-Class Classification', in 2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI). 2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), pp. 1–6. Available at: https://doi.org/10.1109/ACCAI61061.2024.10601966.

11-Zhang, Y. et al. (2022) 'Improving the Classification Effectiveness of Network Intrusion Detection Using Ensemble Machine Learning Techniques and Deep Neural Networks', in 2022 International Conference on Intelligent Data Science Technologies and Applications (IDSTA). 2022 International Conference on Intelligent Data Science Technologies and Applications (IDSTA), pp. 117–123. Available at: https://doi.org/10.1109/IDSTA55301.2022.9923205.

12-Othman, T.S. and Abdullah, S.M. (2023) 'An Intelligent Intrusion Detection System for Internet of Things Attack Detection and Identification Using Machine Learning', ARO-THE SCIENTIFIC JOURNAL OF KOYA UNIVERSITY, 11(1), pp. 126–137. Available at: https://doi.org/10.14500/aro.11124.

13-Tait, K.-A. et al. (2021) 'Intrusion Detection using Machine Learning Techniques: An Experimental Comparison'. arXiv. Available at: https://doi.org/10.48550/arXiv.2105.13435.

14-Guo, G. (2022) 'An Intrusion Detection System for the Internet of Things Using Machine Learning Models', in 2022 3rd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE). 2022 3rd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE), pp. 332–335. Available at: https://doi.org/10.1109/ICBAIE56435.2022.9985800.

15-Ahanger, A.S., Khan, S.M. and Masoodi, F. (2021) 'An Effective Intrusion Detection System using Supervised Machine Learning Techniques', in 2021 5th International Conference on Computing Methodologies and Communication

(ICCMC). 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), pp. 1639–1644. Available at: https://doi.org/10.1109/ICCMC51019.2021.9418291.

16-Sarraf, J. et al. (2021) 'Detection of Network Intrusion and Classification of Cyberattack Using Machine Learning Algorithms: A Multistage Classifier Approach', in P.K. Pattnaik et al. (eds) Proceedings of International Conference on Smart Computing and Cyber Security. Singapore: Springer, pp. 285–295. Available at: https://doi.org/10.1007/978-981-15-7990-5_28.

17-Sajid, M. et al. (2024) 'Enhancing intrusion detection: a hybrid machine and deep learning approach', Journal of Cloud Computing, 13(1), p. 123. Available at: https://doi.org/10.1186/s13677-024-00685-x.

18-Bilaskar, V.S. et al. (2024) 'An intrusion detection system for industrial IoT using chi-square feature selection', Journal of Statistics and Management Systems, 27(5), pp. 1021–1031. Available at: https://doi.org/10.47974/JSMS-1303.

19-Chhaybi, A. and Lazaar, S. (2026) 'Enhancing malware detection utilizing Chi-Square distribution for optimal feature selection in machine learning black box models', Journal of Dynamics and Games, 14(0), pp. 190–203. Available at: https://doi.org/10.3934/jdg.2025010.

20-Joloudari, J.H. et al. (2023) 'Effective Class-Imbalance Learning Based on SMOTE and Convolutional Neural Networks', Applied Sciences, 13(6), p. 4006. Available at: https://doi.org/10.3390/app13064006.

21-Alex, S.A. et al. (2022) 'Deep LSTM Model for Diabetes Prediction with Class Balancing by SMOTE', Electronics, 11(17), p. 2737. Available at: https://doi.org/10.3390/electronics11172737.

22-Khafajeh, H. (2005) 'AN EFFICIENT INTRUSION DETECTION APPROACH USING LIGHT GRADIENT BOOSTING', . Vol. [Preprint], (05).