НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
январь–февраль 2025 Том 25 № 1 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
January–February 2025 Vol. 25 No 1 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

doi: 10.17586/2226-1494-2025-25-1-114-127

Enhancing and extending CatBoost for accurate detection and classification of DoS and DDoS attack subtypes in network traffic

Abdulkader Hajjouz[1]✉, Elena Yu. Avksentieva[2]

[1,2] ITMO University, Saint Petersburg, 197101, Russian Federation

[1] hajjouz@itmo.ru✉, https://orcid.org/0000-0002-8256-6790
[2] eavksenteva@itmo.ru, https://orcid.org/0000-0001-5000-4868

Abstract

In the ever changing digital world, the rise of sophisticated cyber threats, especially DoS and DDoS attacks, is a big challenge to Information Security. This paper addresses the problem of classifying malicious from benign network traffic using CatBoost classifier, a machine learning algorithm optimized for categorical data and imbalanced datasets. We used CIC-IDS2017 and CSE-CIC-IDS2018 datasets which simulate various cyberattack scenarios, our research optimized CatBoost to identify specific subtypes of DoS and DDoS attacks including Hulk, SlowHTTPTest, GoldenEye, Slowloris, HOIC, LOIC-UDP-HTTP, LOIT. The methodology involved data preparation, feature selection and model configuration, normalizing outliers, correcting negative values, and refining dataset structures. Stratified sampling ensured a balanced representation of classes in training, validation, and testing sets. The CatBoost model performed well with overall accuracy of 0.999922, high precision, recall, and F1-scores across all categories, and it can process over 3.4 million samples per second. These results show the model is robust and reliable for real-time intrusion detection. By classifying specific attack types, our model improves the precision of the Intrusion Detection Systems (IDS) and allows for targeted response to different threats. The big gain in detection accuracy solves the problem of imbalanced datasets and the need for granular attack types detection. Use CatBoost in advanced Information Security frameworks for critical infrastructure, cloud services, and enterprise networks to defend against digital threats. This paper provides a fast, accurate and scalable solution for network IDS and shows the importance of custom machine learning models in Information Security. Future work should explore CatBoost on more datasets and integrate it with other machine learning techniques to improve robustness and detection.

Keywords

information security, network intrusion detection, DoS attacks, DDoS attacks, machine learning, real-time detection, feature selection, model optimization

For citation: Hajjouz A., Avksentieva E.Yu. Enhancing and extending CatBoost for accurate detection and classification of DoS and DDoS attack subtypes in network traffic. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2025, vol. 25, no. 1, pp. 114–127. doi: 10.17586/2226-1494-2025-25-1-114-127

УДК 004.492.3

Улучшение и расширение CatBoost для точного обнаружения и классификации подтипов DoS и DDoS атак в сетевом трафике

Абдулкадер Хажжуз[1]✉, Елена Юрьевна Авксентьева[2]

[1,2] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация

[1] hajjouz@itmo.ru✉, https://orcid.org/0000-0002-8256-6790
[2] eavksenteva@itmo.ru, https://orcid.org/0000-0001-5000-4868

Аннотация

В постоянно меняющемся цифровом мире рост сложных киберугроз, особенно атак DoS (отказ в обслуживании) и DDoS (распределенный отказ в обслуживании), представляет собой серьезную проблему для информационной безопасности. В работе рассматривается задача классификации вредоносного и безопасного сетевого трафика с

использованием применением классификатора CatBoost — алгоритма машинного обучения, оптимизированного для категориальных данных и несбалансированных наборов данных. Использованы наборы данных CIC-IDS2017 и CSE-CIC-IDS2018, которые имитируют различные сценарии кибератак. оптимизация классификатора CatBoost для распознавания конкретных подтипов атак DoS и DDoS, включая Hulk, SlowHTTPTest, GoldenEye, Slowloris, HOIC, LOIC-UDP-HTTP, LOIT. Разработана методика работы CatBoost для подготовки данных, отбора признаков и настройки модели, нормализации выбросов, корректировки отрицательных значений и улучшения структуры наборов данных. Стратифицированная выборка обеспечила сбалансированное представление классов в обучающих, валидационных и тестовых наборах. Разработанная модель CatBoost продемонстрировала отличные результаты с общей точностью 0,999922, высокой полнотой и значениями F1-меры по всем категориям и способностью обрабатывать более 3,4 млн образцов в секунду. Эти результаты показывают, что модель является надежной и подходит для обнаружения вторжений в реальном времени. Классификация конкретных типов атак улучшает точность системы обнаружения вторжений (Intrusion Detection Systems, IDS) и позволяет целенаправленно реагировать на различные угрозы. Существенное повышение точности обнаружения решает проблему несбалансированных наборов данных и необходимость детектирования различных типов атак. CatBoost рекомендуется к использованию в передовых рамках информационной безопасности для критической инфраструктуры, облачных сервисов и корпоративных сетей для защиты от цифровых угроз. Данная работа предлагает быстрое, точное и масштабируемое решение для сетевой IDS и подчеркивает важность использования кастомизированных моделей машинного обучения в информационной безопасности. В дальнейшем предполагается изучить применение CatBoost на большем количестве наборов данных и его интеграцию с другими методами машинного обучения для повышения устойчивости и точности обнаружения.

Ключевые слова
информационная безопасность, обнаружение сетевых вторжений, атаки DoS, атаки DDoS, машинное обучение, обнаружение в реальном времени, отбор признаков, оптимизация модели

Ссылка для цитирования: Хажжуз А., Авксентьева Е.Ю. Улучшение и расширение CatBoost для точного обнаружения и классификации подтипов DoS и DDoS атак в сетевом трафике // Научно-технический вестник информационных технологий, механики и оптики. 2025. Т. 25, № 1. С. 114–127 (на англ. яз.). doi: 10.17586/2226-1494-2025-25-1-114-127

Introduction

In today's connected world DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks are a big threat to information security [1–5]. The frequency and complexity of these attacks are increasing, and it's hard to differentiate between malicious and normal traffic. This is further complicated by data imbalance where normal traffic is much more than attack instances, making it difficult to detect and requiring robust solutions [1, 6, 7].

Research has proposed approaches using machine learning and deep learning. To summarize the recent approaches, Table 1 below is a comparison of various studies, including the datasets used, the methodologies applied, key findings, and the challenges faced.

The table uses three popular datasets to test network intrusion detection systems. KDD CUP from 1999 is a well known benchmark dataset to develop and compare intrusion detection models. CSE-CIC-IDS from 2018 is more recent and larger dataset of network attacks. CIS-IDS is an additional dataset for research purpose in intrusion detection. These datasets are used to evaluate and validate different intrusion detection methods.

While many significant ones have made a lot of progress in combating DDoS attacks in recent years, existing methods fail because of imbalanced network traffic datasets and the difficulty in processing categorical data [1]. In various research and review papers, there's a lot of focus on a general approach to detect DoS and DDoS attacks rather than classifying specific types of

Table 1. Comparison of approaches in literature review

References	Dataset Used	Approach	Key Findings	Challenges
[8]	KDD CUP 1999, CSE-CIC-IDS2018	CNN with image-based (RGB and grayscale)	CNN outperformed RNN in DoS detection; better performance on simpler datasets like KDD compared to CSE-CIC-IDS2018	Lower performance on complex datasets; requires careful tuning of hyperparameters (image type, kernel size, number of layers)
[9]	CIC-IDS2017	CNN, LSTM	Shows potential in intrusion detection using deep learning	Real-time deployment challenges
[10]	CIC-IDS2017	Agent-based	automatic feature extraction and selection, High accuracy achieved	High computational resource utilization
[11]	CIC-IDS2017	XGBoost	Effective for DoS/DDoS detection	Limited detection range, real-time detectability
[12]	CIC-IDS2017	Deep Belief Network	Deep learning shows promise in cyber threat detection	Imbalanced datasets, categorical data handling

NOTE. CNN — Convolutional Neural Network, LSTM — Long Short-Term Memory

attacks. This general approach misses the nuances and details of DoS and DDoS, hindering the development of countermeasures. According to Cloudflare's Q3 2024 report[1], DDoS attacks were up 49 % from last quarter with almost 6 million attacks, financial services was the most targeted and China was the most affected region. Gcore's H1 2024 report[2] showed 46 % increase in DDoS attacks compared to 2023, with 445,000 attacks in Q2 alone and the largest attack was 1.7 terabits per second. StormWall's analysis showed 102 % year-over-year increase in DDoS incidents, 29 % of which were targeted at government infrastructure — a 116 % increase in this sector — mostly due to election-related motives[3]. So we need more sophisticated detection and mitigation for these threats.

In our previous work [1], we optimized the CatBoost classifier for DoS and DDoS attack detection in network traffic and got significant improvements in detection accuracy and performance. However that work was general attack classification without considering different attack subtypes. Since each subtype of DoS and DDoS attacks exploits different vulnerabilities and requires different mitigation strategies [13–20], we realized the need to extend our work. To address these limitations and improve the effectiveness of intrusion detection systems, this paper builds upon our previous work [1] by introducing an improved methodology that uses the strengths of the CatBoost classifier to detect and classify specific attack subtypes — Hulk, SlowHTTPTest, GoldenEye, Slowloris (DoS) and HOIC, LOIC-UDP-HTTP, LOIT (DDoS). While most of the existing research is focused on general DoS and DDoS attack detection without considering specific subtypes, our approach addresses this gap by using the varied and extensive scenarios in CIC-IDS2017 and CSE-CIC-IDS2018 datasets [21, 22] to enhance the accuracy and performance of intrusion detection systems so they can respond to specific threats better. The code for this work is available on GitHub[4].

Detecting these subtypes is important because different attack subtypes require different mitigation strategies. For example, the Slowloris attack [13, 14], which targets web servers by keeping connections open, requires different defenses than the Hulk attack [15] which floods the network with a high volume of requests. Similarly the SlowHTTPTest attack[5] which sends incomplete HTTP requests to exhaust server resources requires different mitigation than the GoldenEye attack [16] which also floods the server with HTTP requests but in a different pattern. The High Orbit Ion Cannon (HOIC) attack[6] which floods the network with high volume HTTP requests requires rate limiting and IP blocking whereas the Low Orbit Ion Cannon (LOIC) attacks [17] which can use both UDP (User Datagram Protocol) and HTTP floods requires different filtering rules for each protocol. Moreover the LOIT (Low Orbit Ion Torrent) attack [18] which uses different methods to overwhelm network resources requires advanced traffic analysis and dynamic defense mechanisms to counter its multi-faceted attack vectors.

By tuning the CatBoost classifier to detect these specific attack types, our model allows intrusion detection systems to respond to specific threats more effectively. Initial results show a big improvement in detection accuracy setting a new benchmark for real-time intrusion detection. This paper describes our full methodology from data analysis and feature selection to model tuning and evaluation. We have made a big progress in dealing with imbalanced and complex datasets of cyber threats. Our results provide a scalable, accurate, and efficient way to strengthen Information Security against evolving digital threats, the demand for which is critical and growing.

Overview of DoS and DDoS attack subtypes in the dataset

We used the CIC-IDS2017 and CSE-CIC-IDS2018 datasets created by the Canadian Institute for Information Security and the Communications Security Establishment (CSE). These datasets simulate different cyberattack scenarios and have benign and malicious network traffic to develop strong intrusion detection systems [1].

CIC-IDS2017 is a one week simulation of different attacks like DoS and DDoS attacks. CSE-CIC-IDS2018 has more advanced Cyber threats with more kinds of attacks and also has 79 features of different aspects of network traffic[7], so we can classify each kind of network activity more in detail [1, 19, 20].

This will help us to distinguish between malicious and benign traffic. Table 2 shows the instance counts for each class in the datasets.

Table 2. Distribution of Instances by Attack Type in CIC-IDS2017 and CSE-CIC-IDS2018

Class	Number of Instances CIC-IDS2017 + + CSE-CIC-IDS2018
Benign	9,713,988
DoS attacks-Hulk	692,985
DDoS attack-HOIC	686,012
DDoS attack-LOIC-UDP-HTTP	577,921
DoS attacks-SlowHTTPTest	145,389
DDdoS LOIT	128,027
DoS attacks-GoldenEye	51,801
DoS attacks-Slowloris	16,786

[1] Available at: https://radar.cloudflare.com/reports/ddos-2024-q3 (accessed: 10.10.2024).

[2] Available at: https://gcore.com/blog/radar-q1-q2-2024-insights (accessed: 14.10.2024).

[3] Available at: https://stormwall.network/ddos-report-h1-2024 (accessed: 12.10.2024).

[4] Available at: https://github.com/abdulkaderhajjouz/DDoS-DoS-Attack-Detection (accessed: 12.11.2024).

[5] Available at: https://github.com/shekyan/slowhttptest (accessed: 01.03.2024).

[6] Available at: https://sourceforge.net/projects/highorbitioncannon/ (accessed: 05.03.2024).

[7] Canadian Institute for Cybersecurity. A Realistic Cyber Defense Dataset (CSE-CIC-IDS2018). 2018. Retrieved from https://registry.opendata.aws/cse-cic-ids2018/

These datasets and features we use to build a strong and effective intrusion detection model capable of identifying specific network anomalies, thus enhancing cybersecurity.

Data cleaning and processing for selected attack subtypes

To get more accurate results from our intrusion detection, we added a data preparation process to ensure data integrity and addressed three key issues: first, we normalized outliers [21] to prevent extreme values from skewing the analysis and preserve the core data for modeling; second, we corrected negative values [22] and averaged them to keep consistency and differentiate between good and bad network behavior; third, we restructured the dataset to keep everything organized and formatted for proper classification of network activities. These are important for better detection and to make our intrusion detection more reliable and trustworthy [1].

Feature engineering for specific attack subtypes

When it comes to cyber intrusion detection, feature selection is key point [23]. The model can be more accurate, faster, and more interpretable when we identify the right features [24, 25]. There are several steps of careful filtering to narrow down the dataset to the best features. This filtering reduces the computational load and simplifies the model and makes it more robust and interpretable [26, 27]. Following the methodology in [1] we refined the dataset by removing non-contributory attributes, eliminating constant features, examining feature relationships, visualizing and clustering features and finally consolidating clusters to select the most informative ones. The final 32 features selected are shown in Table 3.

After applying these steps, we provide the Spearman Correlation Heatmap for the final set of features illustrating their relationships. However, due to the complexity and detail of the heatmap, it has been made available as a supplementary resource[1].

Diagonal cells are perfect self-correlation with 1, off diagonal cells are correlation between different features. No strong correlation (near 1 or –1) means redundant features have been removed. Most are moderate or weak so each feature gives unique and independent information, makes computation more efficient, and reduces overfitting in the model [28].

Stratified sampling of DoS/DDoS subtypes

In our study involving extensive analysis, we have employed stratified sampling to partition the overall dataset into three subsets, namely, train (80 %), validation (10 %),

[1] Hajjouz Abdulkader, Avksentieva Elena. Spearman Correlation Heatmaps After Feature Selection // Mendeley Data. 2024. V1. https://data.mendeley.com/datasets/hxd7gmrvth/1, doi: 10.17632/hxd7gmrvth.1

Table 3. List of Selected Features

Selected Features	Description	Selected Features	Description
dst_port	Destination port receiving the data	Protocol	Protocol used (e.g., TCP, UDP)
fwd_iat_min	Minimum inter-arrival time for forward packets	bwd_iat_min	Minimum inter-arrival time for backward packets
flow_duration	Total duration of the flow/session	fwd_psh_flags	Number of PUSH flags in forward direction
fin_flag_cnt	Count of FIN flags in the flow	bwd_pkts_s	Backward packets per second
tot_bwd_pkts	Total packets forwarded from destination to source	tot_fwd_pkts	Total packets forwarded from source to destination
totlen_fwd_pkts	Total length of all forward packets	rst_flag_cnt	Count of RST flags in the flow
totlen_bwd_pkts	Total length of all backward packets	active_std	Standard deviation of active state duration
urg_flag_cnt	Count of URG flags in the flow	ack_flag_cnt	Count of ACK flags in the flow
fwd_pkt_len_std	Standard deviation of forward packet length	fwd_pkt_len_mean	Mean packet length in the forward direction
bwd_pkt_len_mean	Mean packet length in the backward direction	down_up_ratio	Ratio of download to upload bytes
bwd_pkt_len_std	Standard deviation of backward packet length	init_fwd_win_byts	Initial TCP window size in the forward direction
flow_byts_s	Bytes per second in the flow	flow_pkts_s	Packets per second in the flow
init_bwd_win_byts	Initial TCP window size in the backward direction	fwd_seg_size_min	Minimum size of segments in the forward direction
flow_iat_std	Standard deviation of inter-arrival times between packets	active_mean	Mean duration of active state of the flow
flow_iat_min	Minimum inter-arrival time between packets	fwd_iat_tot	Total inter-arrival time for forward packets
psh_flag_cnt	Count of PUSH flags in the flow	idle_mean	Mean duration of idle state of the flow

Table 4. Network Traffic Class Distribution Across Training, Validation, and Testing Sets

Class	Set		
	Train	Validation	Test
Benign	777,119	971,399	971,399
DoS attacks-Hulk	554,388	69,299	69,298
DDoS attack-HOIC	548,809	68,602	68,601
DDoS attack-LOIC-UDP-HTTP	462,337	57,792	57,792
DoS attacks-SlowHTTPTest	116,311	14,539	14,539
DDoS LOIT	102,422	12,802	12,803
DoS attacks-GoldenEye	41,441	5,180	5,180
DoS attacks-Slowloris	13,429	1,678	1,679

and test (10 %), which are denoted in Table 4. We selected this sampling approach in order to maintain the same proportional ratios in these data subsets [1], as stratified sampling contains a component of balanced allocation:

$$n_k = (N \times N_k)/N_{tot},$$

where n_k represents the sample size allocated to each class k within a given subset, N is the total number of samples in that subset, N_k indicates the total number of samples for class k across the dataset, and N_{tot} is the total number of samples in the dataset.

Stratified sampling was used to ensure each class is represented proportionally across the training, validation, and test sets. This is important for our study as it allows the model to be trained and tested on data that reflects the overall class distribution [29], including less common attack subtypes like DoS Slowloris and DDoS LOIT. By keeping the class distribution consistent, we avoid bias towards majority classes and don't introduce artificial noise by oversampling or undersampling. This also allows for more accurate metrics like precision, recall, and F1-score for each attack subtype [30].

Understanding CatBoost

CatBoost is a library based on Gradient Boosting specifically designed to work with categorical and complex data [31], so it's perfect for applications that require high accuracy and speed, like cyber threat detection and imbalanced data classification. It uses "Ordered Boosting" which trains trees in a specific order to prevent overfitting and reduce bias [32]. CatBoost also uses "Ordered Statistics" to process categorical data directly without need for traditional complex encoding, so it reduces computational cost and preserves data accuracy [33, 34].

CatBoost training process starts by processing categorical features with ordered statistics, then applies ordered boosting in multiple stages of "weak learners". Class weights are adjusted at each stage to handle imbalanced data. At each step errors from previous stage are corrected and finally the "strong learner" is produced which gives the final prediction. This structure gives high accuracy and speed so CatBoost is perfect for applications that require top performance and speed in data analysis [32–34].

CatBoost outperforms other gradient boosting libraries like XGBoost and LightGBM in terms of prediction quality and speed, and also has native support for both numerical and categorical features [32]. It also has built-in visualization tools to understand model performance and interpret results, fast training with multiple GPUs and distributed training via Apache Spark and Command-Line Interface which makes training fast and reproducible [33, 34]. Although it requires significant resources for large and complex datasets, experiments have shown that CatBoost outperforms others across different data types [33], so it's the best choice for classifying DoS and DDoS attack subtypes in this research.

Model configuration, training, and validation

When we are doing machine learning for cybersecurity, especially for network intrusion detection, the model configuration and training are everything [1]. We chose to use the CatBoostClassifier, a decision tree based ensemble model, because it performs well with categorical data and imbalanced datasets, which is important for detecting specific attack subtypes [33–35].

We assigned specific class weights to each attack type to address the data imbalance in our dataset. The weights for each class were calculated using:

Weight for each class = (Total number of samples) / (Number of samples in the class).

For example, the weights were: {'Benign': 1.2367, 'DDoS LOIT': 93.8307, 'DDoS attack-HOIC': 17.5112, 'DDoS attack-LOIC-UDP-HTTP': 20.7864, 'DoS attacks-GoldenEye': 231.9038, 'DoS attacks-Hulk': 17.3350, 'DoS attacks-SlowHTTPTest': 82.6261, 'DoS attacks-Slowloris': 715.6398}. These were set using the class_weights parameter in the CatBoost algorithm which gives more importance to the less frequent classes, not increasing the overall accuracy of the model but making it more sensitive to the rare and critical attacks. Results showed that using class_weights reduced the number of instances where attacks were misclassified as "Benign" (false negatives) and thus made the model more able to detect rare attack patterns. This is important in cybersecurity where reducing false negatives is key to responding to critical threats [35].

The key parameters for the model were: 1330 iterations to balance learning and computation, 0.1 learning rate to prevent overfitting, 6 depths to capture the complex patterns,

MultiClass loss function for multi-class classification, trained on a GPU with random seed 42 for reproducibility. Other parameters were: L2 leaf regularization of 4 to balance accuracy and speed; border count of 512 to balance speed and accuracy; early stopping rounds of 250 to prevent overfitting by stopping training when no improvement was seen. Total F1-score was used as the evaluation metric suitable for imbalanced data and gives a balanced measure of the model ability to detect each attack subtype.

During training, the model was evaluated on a separate validation set with early stopping based on Total F1-score to prevent overfitting and get the best performance. In this way we could monitor the model ability to detect each subtype across iterations and make sure no subtype is compromised. Our hyperparameter tuning showed that CatBoost can handle complex imbalanced data. The best Total F1-score was 0.99979 at iteration 835, so the model is very good at detecting the subtypes in our dataset.

By using stratified sampling and fine tuning the model we built an intrusion detection model that can detect multiple types of network intrusions. We focused on specific DoS and DDoS attack subtypes, so the model can detect more specific and give tailored response to each type of attack. Our results show that model configuration and training matter in Information Security.

Result analysis and discussion

Confusion matrices are used to measure the performance of machine learning algorithms [36] for network intrusion detection systems. Matrices are important to measure system classification skill for types of network activity, such as Benign traffic, DoS attacks-Hulk, DdoS attacks-HOIC, DdoS attacks-LOIC-UDP-HTTP, DoS attacks-SlowHTTPTest, DdoS LOIT, DoS attacks-GoldenEye, DoS attacks-Slowloris showed as in Fig. 1.

Using the confusion matrix as in Fig. 1 we get important metrics to evaluate each class in our network intrusion detection [1]:

$$\text{Accuracy} = ((TP + TN) / (TP + FP + FN + TN))\times 100\ \%$$
$$\text{Precision} = TP / (FP + TP)$$
$$\text{Recall} = TP / (FN + TP)$$
$$\text{F1-score} = 2 \times (\text{Precision} \times \text{Recall}) / (\text{Precision} + \text{Recall})$$
$$\text{FAR} = FP/(FP + TN)$$

— Accuracy: This is the percentage of true cases (true positives and true negatives) out of total cases. Accuracy doesn't give more info but just tells us how often the model is right.
— Precision: Precision is true positives out of total positive predictions made by the model. Precision tells us how well the model is in distinguishing useful positives from non-informative false positives.
— Recall: Also known as sensitivity, Recall shows how well the model finds all actual positives, i.e., how many true positives out of all actual positives which means how well the model did in finding the presence of a positive.
— F1-score: F1-score is the average of Precision and Recall. F1-score is good for overall model, especially when class distribution is not equal.
— False Alarm Rate (FAR): FAR measures how often the system generates false alerts when there is no threat. Lower FAR means the system is better in avoiding false positives and filtering out false alerts.

The CatBoost classifier performance on the test set is impressive with an overall accuracy of 0.999922. It can clearly differentiate between benign traffic, DDoS and DoS attacks as shown by high precision, recall, and F1-scores across all categories. As we can see from Table 5, the model has near perfect F1-scores 0.999955 for Benign traffic, 0.999688 for DdoS LOIT and 0.999978 for DdoS attack-HOIC and many others. This shows that the model is robust and reliable in classifying different types of network traffic, a great tool to enhance Information Security. This is very important in imbalanced classes where the consequences of false prediction are big. The support column in Table 5 indicates the number of actual instances for each class in the test data, which helps provide context for the precision, recall, and F1-scores calculated for each category. The high scores across all attack types means minimal false positives and false negatives, the model is useful in maintaining strong Information Security defenses.

Fig. 2, *a*, shows the Receiver Operating Characteristic (ROC) Curve and Fig. 2, *b*, shows the Precision-Recall curve for the CatBoost model which is for multi-class classification of benign, DDoS, DoS traffic in a network intrusion detection system. The ROC Curve shows macro-average Area Under the Curve (AUC) of 1.00 which means the model is performing ideally and also means AUC

Table 5. Performance metrics of CatBoost classifier on test data

Class	Precision	Recall	F1-score	Support
Benign	0.999999	0.999911	0.999955	971,399
DDOS LOIT	0.999454	0.999922	0.999688	12,803
DDOS attack-HOIC	0.999956	1.000000	0.999978	68,601
DDOS attack-LOIC-UDP-HTTP	0.999792	1.000000	0.999896	57,792
DoS attacks-GoldenEye	0.997688	0.999807	0.998747	5,180
DoS attacks-Hulk	0.999423	0.999971	0.999697	69,298
DoS attacks-SlowHTTPTest	0.999656	0.999862	0.999759	14,539
DoS attacks-Slowloris	0.991721	0.998809	0.995252	1,679

NOTE: Overall Accuracy — 0.999922, False Alarm Rate — 0.000374.

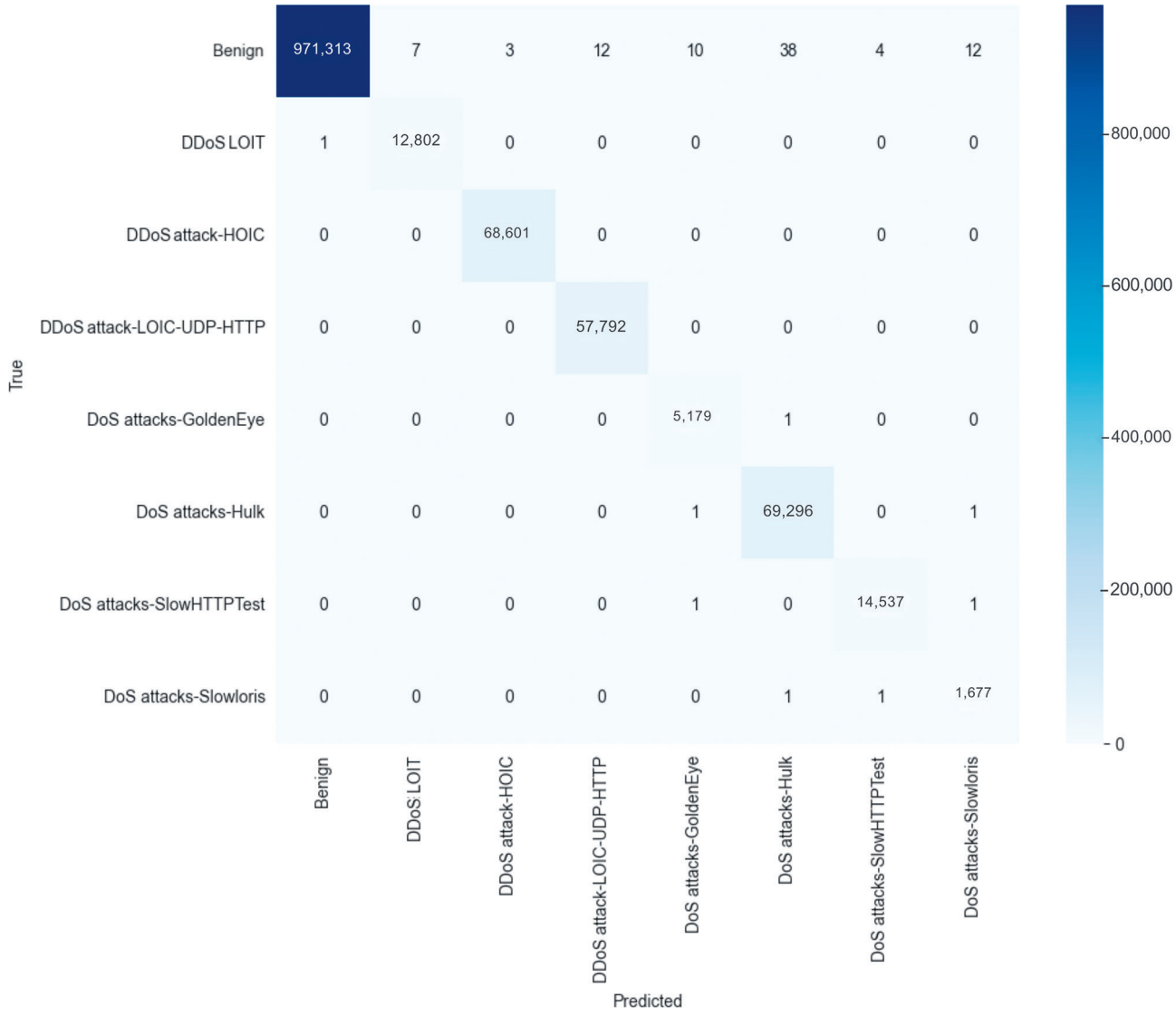

Fig. 1. Confusion Matrix of Predictions by CatBoost classifier on test set

values of the model across all traffic types. The model is balanced as verified by the Precision-Recall curves, shown in Fig. 2, *b*, which demonstrates almost ideal Average Precision (AP), indicating excellent precision and recall scores for class classification. All results show the model capabilities and stability in identifying multiple types of

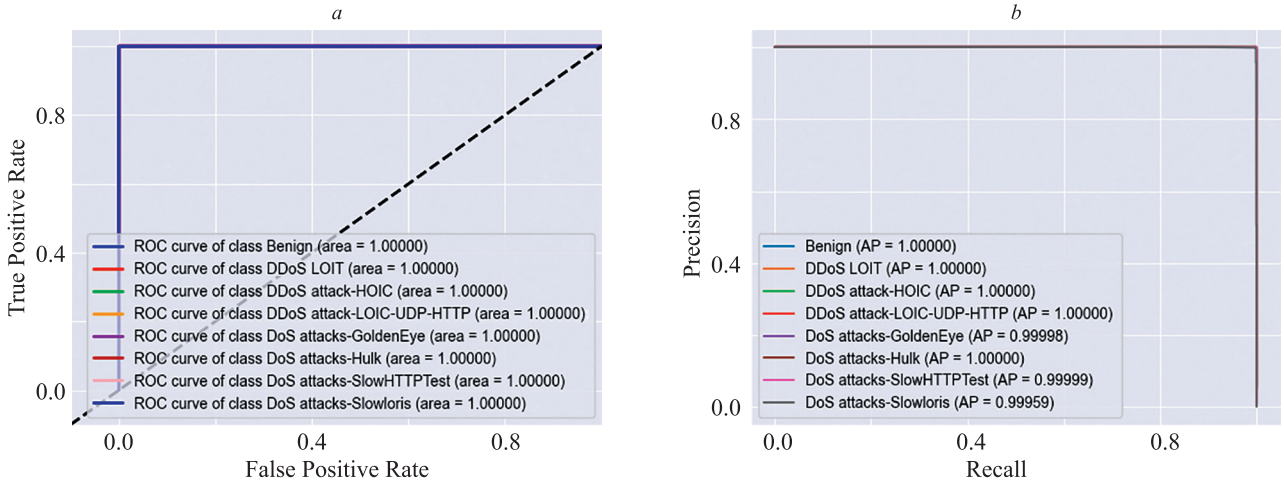

Fig. 2. ROC Curve (*a*) and Precision-Recall Curve (*b*) for CatBoost classifier

Table 6. Matthews correlation coefficient scores for CatBoost classifier

Class	MCC
Benign	0.999766
DoS attacks-Hulk	0.999684
DDoS attack-HOIC	0.999977
DDoS attack-LOIC-UDP-HTTP	0.999891
DoS attacks-SlowHTTPTest	0.998742
DDoS LOIT	0.999679
DoS attacks-GoldenEye	0.999756
DoS attacks-Slowloris	0.995252

network intrusion and it can be used to advance some aspects of Information Security.

The Matthews Correlation Coefficient (MCC) scores in Table 6 show our classifier is doing great in multi-class classification of Benign, DDoS and DoS traffic. MCC is very useful in imbalanced datasets [37] and our model scores are high, which means precision and correlation between predicted and actual labels is good. This defines how reliable and accurate our model is and can be deployed in real world network intrusion detection.

We looked at our results and found the top parameters to the model. The top parameters are flow_iat_min (Minimum Flow Interarrival Time), fwd_seg_size_min (Minimum Forward Segment Size), and fwd_pkt_len_mean (Mean Forward Packet Length) as they contributed the most to network intrusion prediction. Fig. 3 represents feature importance and displays the ranking of features based on their overall impact on the model. The SHAP (SHapley Additive exPlanations) value summary allows us to see the effect of a parameter on the model predictions across all classes. The SHAP values show the importance of parameters on the classes of interest, for example, dst_port, fwd_seg_size_min, and init_fwd_win_byts (Initial Forward Window Bytes) have high SHAP values across multiple classes in Fig. 4.

SHAP value and feature importance show us the important features and how much they contribute to the model, so we can see how the model is making decisions and how reliable it is for network intrusion detection [38–40].

Fig. 5 shows the CatBoost classifier performance on our dataset, classifying network traffic into Benign, DoS (Hulk, SlowHTTPTest, GoldenEye, Slowloris) and DDoS (HOIC, LOIC-UDP-HTTP, LOIT) categories. Using a dataset of 12,012,909 samples, the classifier ran 100 iterations on hardware with an RTX 3080 GPU, Intel Core i7 13700k CPU, and 32 GB of DDR5 RAM [1], with an average of 3,408,673.13 samples per second. The consistent speed across iterations shows the classifier is stable and works well for real-time intrusion detection systems.

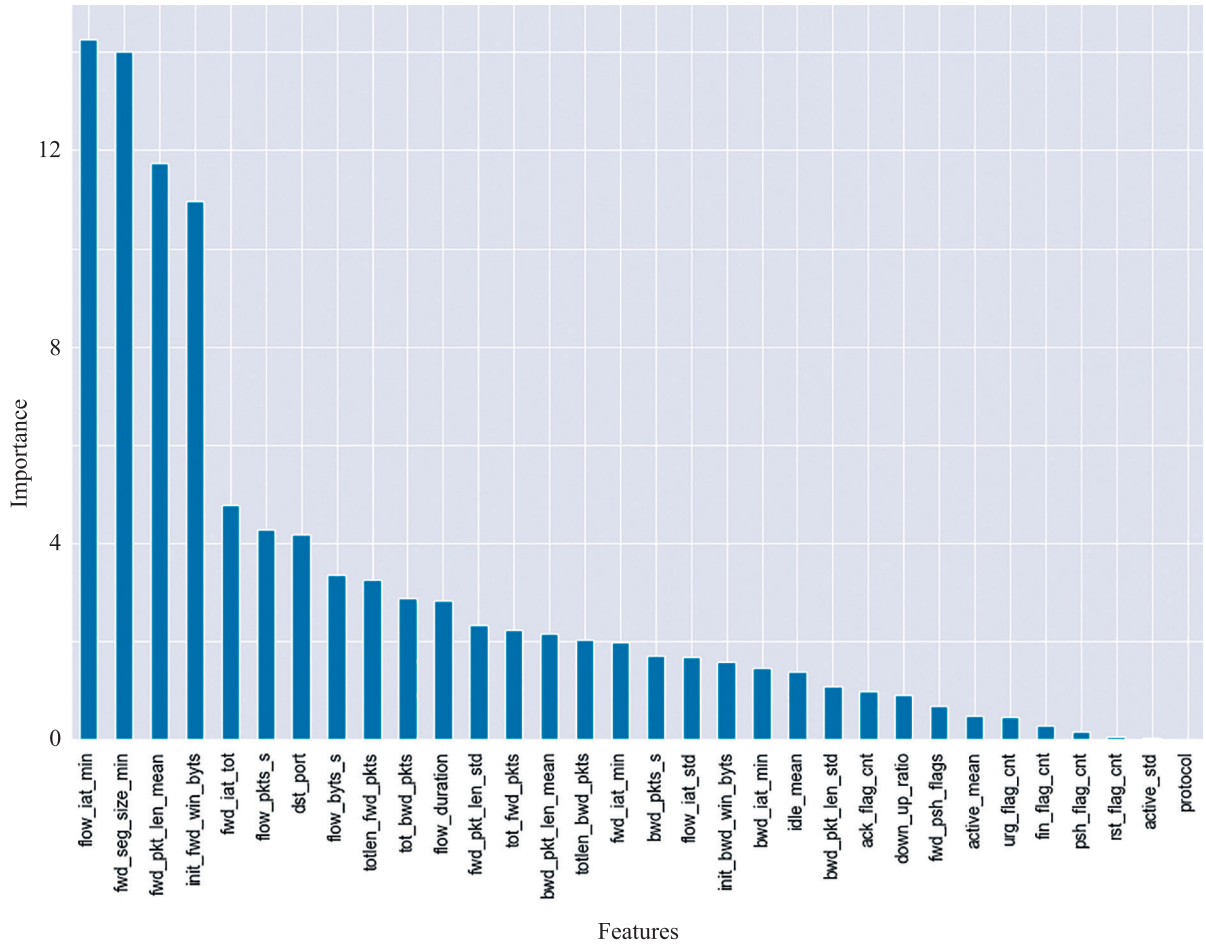

Fig. 3. Feature importance for analyzing feature impact

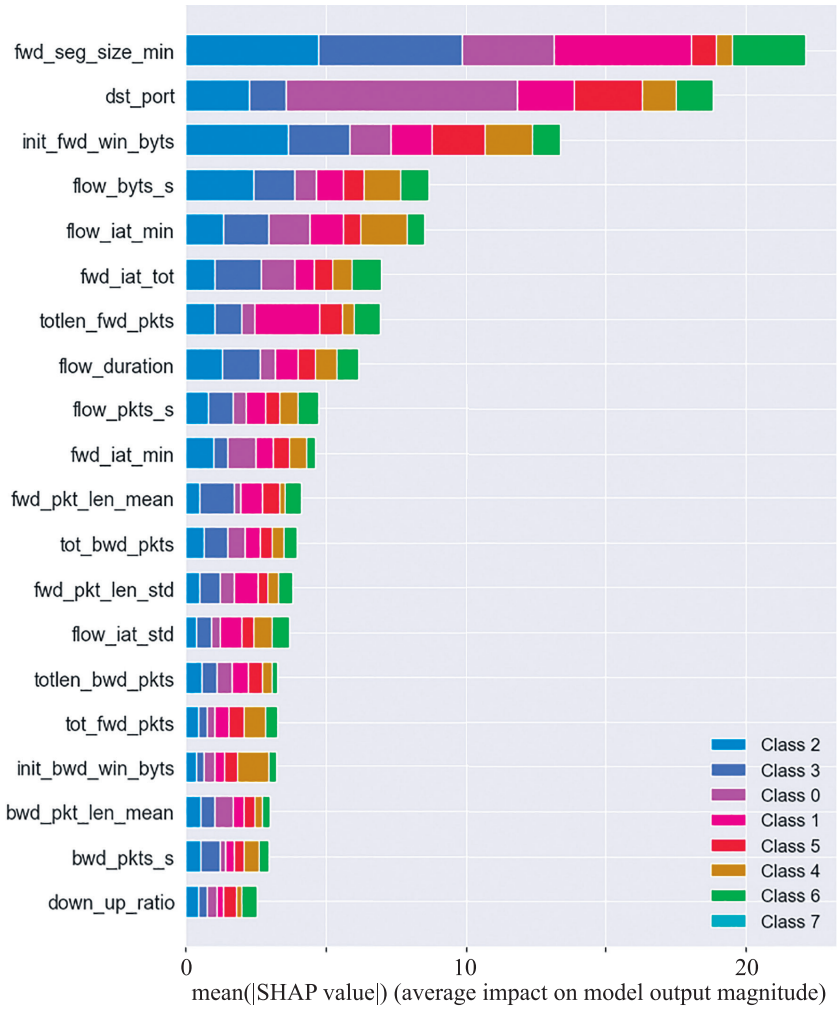

Fig. 4. SHAP value summary for analyzing feature impact where benign situation corresponds class 0, DDoS LOIT corresponds class 1, DDoS attack-HOIC corresponds class 2, DDoS attack-LOIC-UDP-HTTP corresponds class 3, DoS attacks-GoldenEye corresponds class 4, DoS attacks-Hulk corresponds class 5, DoS attacks-SlowHTTPTest corresponds class 6, and DoS attacks-Slowloris corresponds class 7

Fig. 5. Analysis of CatBoost classifier speed and stability over iterative runs

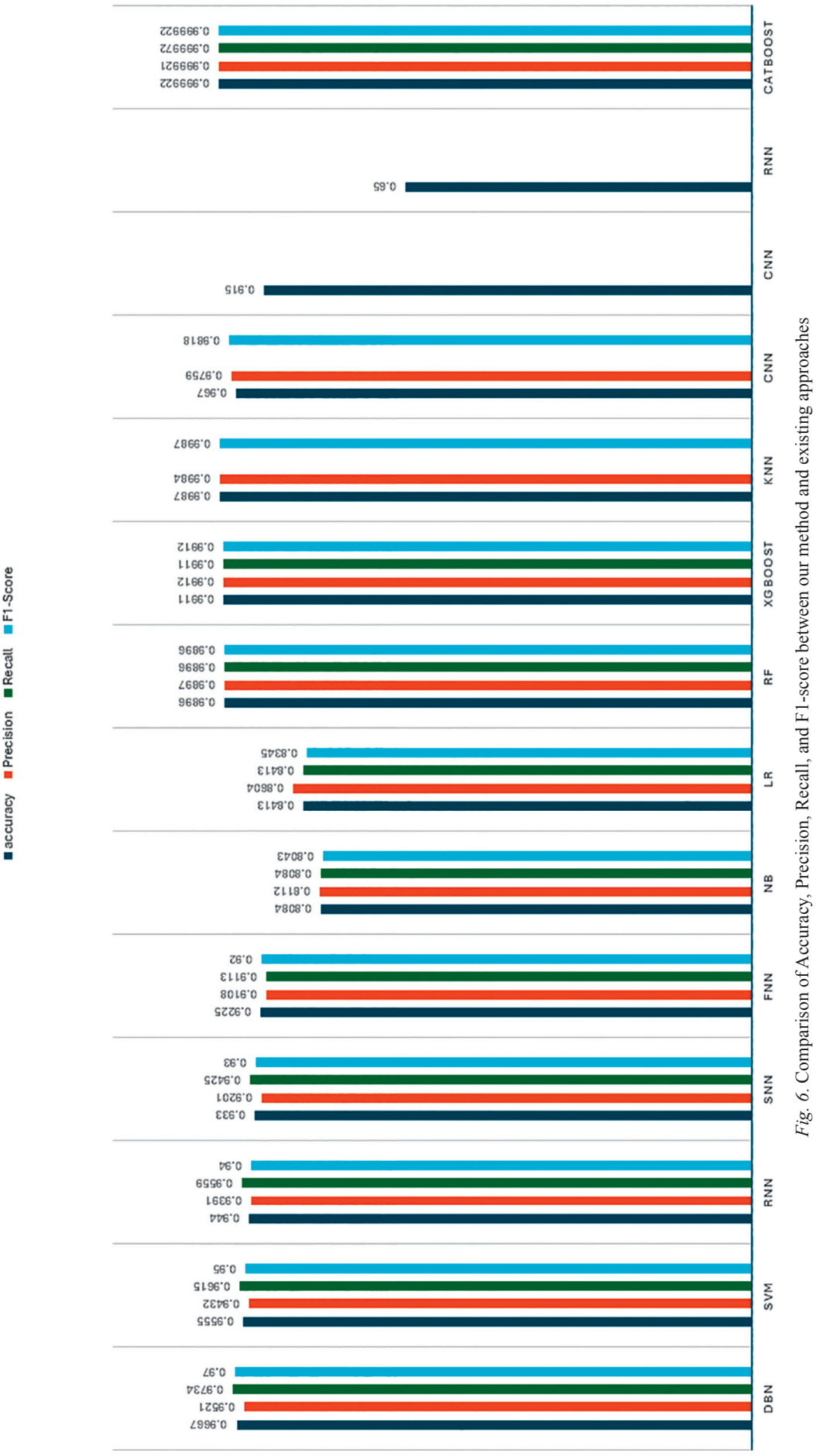

Fig. 6. Comparison of Accuracy, Precision, Recall, and F1-score between our method and existing approaches

Table 7. Accuracy and performance metrics over 10-fold cross-validation

Fold	Accuracy	Precision	Recall	F1-score	ROC AUC
1	0.994072	0.994826	0.994072	0.994283	0.999915
2	0.992342	0.993351	0.992342	0.99262	0.999929
3	0.989641	0.991059	0.989641	0.990012	0.999912
4	0.994425	0.995107	0.994425	0.994621	0.999938
5	0.995427	0.996099	0.995427	0.995633	0.999974
6	0.996599	0.99703	0.996599	0.996726	0.999989
7	0.995264	0.99594	0.995264	0.995468	0.999963
8	0.994993	0.995512	0.994993	0.995139	0.999949
9	0.998675	0.998701	0.998675	0.998681	0.999999
10	0.989773	0.991204	0.989773	0.990149	0.999884

The cross-validation results [41, 42] for the CatBoost model in Table 7 show good performance across 10 folds. The model gets near perfect scores for all metrics, accuracy, precision, recall, and F1-score. However there are some small variations in some folds, especially in accuracy and recall where it dips below 0.99 in folds 3 and 10. This might be due to not applying stratified sampling during cross-validation which can lead to imbalanced distribution of attack and normal instances across the folds. But the ROC AUC scores are consistently close to 1.0, which shows the model is very good at discrimination. These results show the robustness and reliability of the CatBoost classifier for network intrusion detection.

We used CatBoost on combined CIC-IDS2017 and CSE-CIC-IDS2018 datasets and got very good results in network intrusion detection. Unlike previous methods which only identified benign, DoS, and DDoS traffic without identifying subtypes, our model can identify these variations. With a very low False Alarm Rate of 0.000374 it reduced false positives. As shown in Fig. 6, other models like DBN, SVM, RF and XGBoost [8–12] performed good results but none of them performed overall precision and reliability of CatBoost.

We also re-divided the data into 70 % for training, 15 % for validation, and 15 % for testing. The results remained stable and consistent with previous outcomes, even without using class weights, although there was a slight increase in the number of attacks misclassified as “Benign”. This confirms that our model configuration is robust and effective without signs of overfitting.

These results show CatBoost is ready for real-world Information Security use cases. Consistency across all metrics means our model and approach is working. CatBoost is effective in various network intrusion detection tasks including classifying different types of attacks so it’s ready for use.

Conclusion

In summary, our work advances network intrusion detection by using the CatBoost classifier to tackle imbalanced datasets and categorical data. The main results show CatBoost performance in identifying various network traffic types including specific subtypes of DoS and DDoS attacks. The classifier had an overall accuracy of 0.999922 with near perfect precision, recall, and F1-score across all traffic categories. It can distinguish between benign traffic and multiple attack types, so we can have tailored and effective mitigation strategies. A feature selection process refined the dataset to the top 32 features and class weights addressed the imbalance in the dataset. Also the model is very fast, so it’s suitable for real-time intrusion detection. CatBoost performance proves it can be used to enhance network intrusion detection systems and respond to Information Security threats in time. Future work should be done on CatBoost with more diverse and changing datasets and combining it with other Machine Learning techniques like anomaly detection to detect new types of attacks. Expanding the dataset and hybrid approaches will make the model more robust and adaptable to dynamic environments. Practical applications are building advanced Information Security frameworks for critical infrastructure, cloud services, and enterprise networks to defend against emerging digital threats. Our work provides a scalable, accurate, and efficient solution to Information Security, to fill the need for better intrusion detection and to lay the ground for future work on securing digital environments from evolving cyber threats.

References

1. Hajjouz A., Avksentieva E.Y. An approach to configuring CatBoost for advanced detection of DoS and DDoS attacks in network traffic. *Vestnik of Astrakhan State Technical University. Series: Management, computer science and informatics*, 2024, vol. 2024, no. 3, pp. 64–74. https://doi.org/10.24143/2072-9502-2024-3-65-74
2. Zhou L., Zhu Y., Zong T, Xiang Y. A feature selection-based method for DDoS attack flow classification. *Future Generation Computer*

Литература

1. Hajjouz A., Avksentieva E.Y. An approach to configuring CatBoost for advanced detection of DoS and DDoS attacks in network traffic // Vestnik of Astrakhan State Technical University. Series: Management, computer science and informatics. 2024. V. 2024. N 3. P. 64–74. https://doi.org/10.24143/2072-9502-2024-3-65-74
2. Zhou L., Zhu Y., Zong T, Xiang Y. A feature selection-based method for DDoS attack flow classification // Future Generation Computer

Systems, 2022, vol. 132, pp. 67–79. https://doi.org/10.1016/j.future.2022.02.006
3. Eliyan L.F., Di Pietro R. DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. *Future Generation Computer Systems*, 2021, vol. 122, pp. 149–171. https://doi.org/10.1016/j.future.2021.03.011
4. Ignatev N.A., Tursunmurotov D.X. Censoring training samples using regularization of connectivity relations of class objects. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2024, vol. 24, no. 2, pp. 322–329. (in Russian). https://doi.org/10.17586/2226-1494-2024-24-2-322-329
5. Alhijawi B., Almajali S., Elgala H., Salameh H.B., Ayyash M. A survey on DoS/DDoS mitigation techniques in SDNs: Classification, comparison, solutions, testing tools and datasets. *Computers and Electrical Engineering*, 2022, vol. 99, pp. 107706. https://doi.org/10.1016/j.compeleceng.2022.107706
6. Li Y., Liu Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 2021, vol. 7, pp. 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126
7. Karatas G., Demir O., Sahingoz O.K. Increasing the performance of machine learning-based IDSs on an imbalanced and up-to-date dataset. *IEEE Access*, 2020, vol. 8, pp. 32150–32162. https://doi.org/10.1109/ACCESS.2020.2973219
8. Kim J., Kim J., Kim H., Shim M., Choi E. CNN-based network intrusion detection against denial-of-service attacks. Electronics, 2020, vol. 9, no. 6, pp. 916. https://doi.org/10.3390/electronics9060916
9. Dora V.R.S., Lakshmi V.N. Optimal feature selection with CNN-feature learning for DDoS attack detection using meta-heuristic-based LSTM. *International Journal of Intelligent Robotics and Applications*, 2022, vol. 6, no. 2, pp. 323–349. https://doi.org/10.1007/s41315-022-00224-4
10. Abu Bakar R., Huang X., Javed M.S., Hussain S., Majeed M.F. An intelligent agent-based detection system for DDoS attacks using automatic feature extraction and selection. *Sensors*, 2023, vol. 23, no. 6, pp. 3333. https://doi.org/10.3390/s23063333
11. Farhat S., Abdelkader M., Meddeb-Makhlouf A., Zarai F. Evaluation of DoS/DDoS Attack Detection with ML Techniques on CIC-IDS2017 Dataset. *Proc. of the 9th International Conference on Information Systems Security and Privacy ICISSP*, 2023, vol. 1, pp. 287–295. https://doi.org/10.5220/0011605700003405
12. Manimurugan S., Al-Mutairi S., Aborokbah M.M., Chilamkurti N., Ganesan S., Patan R. Effective attack detection in internet of medical things smart environment using a deep belief neural network. *IEEE Access*, 2020, vol. 8, pp. 77396–77404. https://doi.org/10.1109/ACCESS.2020.2986013
13. Rios V.D.M., Inácio P.R., Magoni D., Freire M.M. Detection and mitigation of low-rate denial-of-service attacks: A survey. *IEEE Access*, 2022, vol. 10, pp. 76648–76668. https://doi.org/10.1109/ACCESS.2022.3191430
14. Faria V.D.S., Gonçalves J.A., Silva C.A.M.D., Vieira G.D.B., Mascarenhas D.M. SDToW: a slowloris detecting tool for WMNs. *Information*, 2020, vol. 11, no. 12. pp. 544. https://doi.org/10.3390/info11120544
15. Mahjabin S. Implementation of DoS and DDoS attacks on cloud servers. *Periodicals of Engineering and Natural Sciences*, 2018, vol. 6, no. 2, pp. 148–158. https://doi.org/10.21533/pen.v6i2.170
16. Kshirsagar D., Kumar S. An ontology approach for proactive detection of HTTP flood DoS attack. *International Journal of System Assurance Engineering and Management*, 2023, vol. 14, suppl. 3, pp. 840–847. https://doi.org/10.1007/s13198-021-01170-3
17. Cai Y.X., Chen S.C., Wang C.C. An Implementation of feature selection for detecting LOIC-based DDoS attack. *Proc. of the International Conference on Consumer Electronics — Taiwan (ICCE-Taiwan)*, 2023, pp. 607–608. https://doi.org/10.1109/ICCE-Taiwan58799.2023.10226733
18. Nayyar S., Arora S., Singh M. Recurrent neural network based intrusion detection system. *Proc. of the International Conference on Communication and Signal Processing (ICCSP)*, 2020, pp. 136–140. https://doi.org/10.1109/ICCSP48568.2020.9182099
19. Hajjouz A., Avksentieva E. Evaluating the effectiveness of the CatBoost classifier in distinguishing benign traffic, FTP BruteForce and SSH BruteForce traffic. *Proc. of the 9th International Conference on Signal and Image Processing (ICSIP)*, 2024, pp. 351–358. https://doi.org/10.1109/ICSIP61881.2024.10671552

Systems. 2022. V. 132. P. 67–79. https://doi.org/10.1016/j.future.2022.02.006
3. Eliyan L.F., Di Pietro R. DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges // Future Generation Computer Systems. 2021. V. 122. P. 149–171. https://doi.org/10.1016/j.future.2021.03.011
4. Игнатьев Н.А., Турсунмуротов Д.Х. Цензурирование обучающих выборок с использованием регуляризации отношений связанности объектов классов // Научно-технический вестник информационных технологий, механики и оптики. 2024. Т. 24. № 2. С. 322–329. https://doi.org/10.17586/2226-1494-2024-24-2-322-329
5. Alhijawi B., Almajali S., Elgala H., Salameh H.B., Ayyash M. A survey on DoS/DDoS mitigation techniques in SDNs: Classification, comparison, solutions, testing tools and datasets // Computers and Electrical Engineering. 2022. V. 99. P. 107706. https://doi.org/10.1016/j.compeleceng.2022.107706
6. Li Y., Liu Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments // Energy Reports. 2021. V. 7. P. 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126
7. Karatas G., Demir O., Sahingoz O.K. Increasing the performance of machine learning-based IDSs on an imbalanced and up-to-date dataset // IEEE Access. 2020. V. 8. P. 32150–32162. https://doi.org/10.1109/ACCESS.2020.2973219
8. Kim J., Kim J., Kim H., Shim M., Choi E. CNN-based network intrusion detection against denial-of-service attacks // Electronics. 2020. V. 9. N 6. P. 916. https://doi.org/10.3390/electronics9060916
9. Dora V.R.S., Lakshmi V.N. Optimal feature selection with CNN-feature learning for DDoS attack detection using meta-heuristic-based LSTM // International Journal of Intelligent Robotics and Applications. 2022. V. 6. N 2. P. 323–349. https://doi.org/10.1007/s41315-022-00224-4
10. Abu Bakar R., Huang X., Javed M.S., Hussain S., Majeed M.F. An intelligent agent-based detection system for DDoS attacks using automatic feature extraction and selection // Sensors. 2023. V. 23. N 6. P. 3333. https://doi.org/10.3390/s23063333
11. Farhat S., Abdelkader M., Meddeb-Makhlouf A., Zarai F. Evaluation of DoS/DDoS Attack Detection with ML Techniques on CIC-IDS2017 Dataset // Proc. of the 9th International Conference on Information Systems Security and Privacy ICISSP. 2023. V. 1. P. 287–295. https://doi.org/10.5220/0011605700003405
12. Manimurugan S., Al-Mutairi S., Aborokbah M.M., Chilamkurti N., Ganesan S., Patan R. Effective attack detection in internet of medical things smart environment using a deep belief neural network // IEEE Access. 2020. V. 8. P. 77396–77404. https://doi.org/10.1109/ACCESS.2020.2986013
13. Rios V.D.M., Inácio P.R., Magoni D., Freire M.M. Detection and mitigation of low-rate denial-of-service attacks: A survey // IEEE Access. 2022. V. 10. P. 76648–76668. https://doi.org/10.1109/ACCESS.2022.3191430
14. Faria V.D.S., Gonçalves J.A., Silva C.A.M.D., Vieira G.D.B., Mascarenhas D.M. SDToW: a slowloris detecting tool for WMNs // Information, 2020. V. 11. N 12. P. 544. https://doi.org/10.3390/info11120544
15. Mahjabin S. Implementation of DoS and DDoS attacks on cloud servers // Periodicals of Engineering and Natural Sciences. 2018. V. 6. N 2. P. 148–158. https://doi.org/10.21533/pen.v6i2.170
16. Kshirsagar D., Kumar S. An ontology approach for proactive detection of HTTP flood DoS attack // International Journal of System Assurance Engineering and Management. 2023. V. 14. Suppl. 3. P. 840–847. https://doi.org/10.1007/s13198-021-01170-3
17. Cai Y.X., Chen S.C., Wang C.C. An Implementation of feature selection for detecting LOIC-based DDoS attack // Proc. of the International Conference on Consumer Electronics — Taiwan (ICCE-Taiwan). 2023. P. 607–608. https://doi.org/10.1109/ICCE-Taiwan58799.2023.10226733
18. Nayyar S., Arora S., Singh M. Recurrent neural network based intrusion detection system // Proc. of the International Conference on Communication and Signal Processing (ICCSP). 2020. P. 136–140. https://doi.org/10.1109/ICCSP48568.2020.9182099
19. Hajjouz A., Avksentieva E. Evaluating the effectiveness of the CatBoost classifier in distinguishing benign traffic, FTP BruteForce and SSH BruteForce traffic // Proc. of the 9th International Conference on Signal and Image Processing (ICSIP). 2024. P. 351–358. https://doi.org/10.1109/ICSIP61881.2024.10671552

20. Sharafaldin I., Lashkari A.H., Ghorbani A.A. Toward generating a new intrusion detection dataset and intrusion traffic characterization. *Proc. of the 4th International Conference on Information Systems Security and Privacy (ICISSP)*, 2018, vol. 1, pp. 108–116. https://doi.org/10.5220/0006639801080116
21. Cabello-Solorzano K., Ortigosa de Araujo I., Peña M., Correia, L., Tallón-Ballesteros A.J., The impact of data normalization on the accuracy of machine learning algorithms: a comparative analysis. *Lecture Notes in Networks and Systems*, 2023, vol. 750, pp. 344–353. https://doi.org/10.1007/978-3-031-42536-3_33
22. Oleghe O. A predictive noise correction methodology for manufacturing process datasets. *Journal of Big Data*, 2020, vol. 7, no. 1, pp. 89. https://doi.org/10.1186/s40537-020-00367-w
23. Umar M.A., Chen Z., Shuaib K., Liu Y. Effects of feature selection and normalization on network intrusion detection. *Data Science and Management*, 2025, vol. 8, no. 1, pp. 23–39. https://doi.org/10.1016/j.dsm.2024.08.001
24. Chandrashekar G., Sahin F. A survey on feature selection methods. *Computers & Electrical Engineering*, 2014, vol. 40, no. 1, pp. 16–28. https://doi.org/10.1016/j.compeleceng.2013.11.024
25. Palo H.K., Sahoo S., Subudhi A.K. Dimensionality reduction techniques: Principles, benefits, and limitations. *Data Analytics in Bioinformatics: A Machine Learning Perspective*, 2021, pp. 79–107. https://doi.org/10.1002/9781119785620.ch4
26. Dunn J., Mingardi L., Zhuo Y.D. Comparing interpretability and explainability for feature selection. *arXiv*, 2021, arXiv:2105.05328. https://doi.org/10.48550/arXiv.2105.05328
27. Li J., Cheng K., Wang S., Morstatter F., Trevino R.P., Tang J., Liu H. Feature selection: A data perspective. *ACM computing surveys*, 2017, vol. 50, no. 6, pp. 1–45. https://doi.org/10.1145/3136625
28. Kathiravan P., Shanmugavadivu P., Saranya R. Mitigating imbalanced data in online social networks using Stratified K-Means Sampling. *Proc. of the 8th International Conference on Business and Industrial Research (ICBIR)*, 2023, pp. 883–888. https://doi.org/10.1109/ICBIR57571.2023.10147677
29. Qi J., Ko T.W., Wood B.C., Pham T.A., Ong S.P. Robust training of machine learning interatomic potentials with dimensionality reduction and stratified sampling. *npj Computational Materials*, 2024, vol. 10, no. 1, pp. 43. https://doi.org/10.1038/s41524-024-01227-4
30. Siblini W., Fréry J., He-Guelton L., Oblé F., Wang Y.Q. Master your metrics with calibration. *Lecture Notes in Computer Science*, 2020, vol. 12080, pp. 457–469. https://doi.org/10.1007/978-3-030-44584-3_36
31. Salakhutdinova K.I., Lebedev I.S., Krivtsova I.E. Gradient boosting trees method in the task of software identification. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2018, vol. 18, no. 6, pp. 1016–1022. (in Russian). https://doi.org/10.17586/2226-1494-2018-18-6-1016-1022
32. Prokhorenkova L., Gusev G., Vorobev A., Dorogush A. V., Gulin A. CatBoost: unbiased boosting with categorical features. *Proc. of the Advances in neural information processing systems 31 (NeurIPS 2018)*. 2018.
33. Dorogush A.V., Gulin A., Gusev G., Kazeev N., Prokhorenkova L.O., Vorobev A. 2017. Fighting biases with dynamic boosting. *arXiv*, 2017, arXiv:1706.09516. https://doi.org/10.48550/arXiv.1706.09516
34. Dorogush A.V., Ershov V., Gulin A. CatBoost: gradient boosting with categorical features support. *arXiv*, 2018, arXiv:1810.11363. https://doi.org/10.48550/arXiv.1810.11363
35. Ami A.S., Moran K., Poshyvanyk D., Nadkarni A. «False negative-that one is going to kill you»: Understanding Industry Perspectives of Static Analysis based Security Testing. *Proc. of the IEEE Symposium on Security and Privacy (SP)*, 2024, pp. 3979–3997. https://doi.org/10.1109/SP54263.2024.00019
36. Heydarian M., Doyle T.E., Samavi R., MLCM: Multi-label confusion matrix. *IEEE Access*, 2022, vol. 10, pp. 19083–19095. https://doi.org/10.1109/ACCESS.2022.3151048
37. Chicco D., Jurman G. The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation. *BMC genomics*. 2020, vol. 21, no. 1, pp. 1–13. https://doi.org/10.1186/s12864-019-6413-7
38. Bowen D., Ungar L. Generalized SHAP: Generating multiple types of explanations in machine learning. *arXiv*, 2020, arXiv:2006.07155. https://doi.org/10.48550/arXiv.2006.07155
39. Lee Y.G., Oh J.Y., Kim D., Kim G. SHAP value-based feature importance analysis for short-term load forecasting. *Journal of*

20. Sharafaldin I., Lashkari A.H., Ghorbani A.A. Toward generating a new intrusion detection dataset and intrusion traffic characterization // Proc. of the 4th International Conference on Information Systems Security and Privacy (ICISSP). 2018. V. 1. P. 108–116. https://doi.org/10.5220/0006639801080116
21. Cabello-Solorzano K., Ortigosa de Araujo I., Peña M., Correia, L., Tallón-Ballesteros A.J., The impact of data normalization on the accuracy of machine learning algorithms: a comparative analysis // Lecture Notes in Networks and Systems. 2023. V. 750. P. 344–353. https://doi.org/10.1007/978-3-031-42536-3_33
22. Oleghe O. A predictive noise correction methodology for manufacturing process datasets // Journal of Big Data. 2020. V. 7. N 1. P. 89. https://doi.org/10.1186/s40537-020-00367-w
23. Umar M.A., Chen Z., Shuaib K., Liu Y. Effects of feature selection and normalization on network intrusion detection // Data Science and Management. 2025. V. 8. N 1. P. 23–39. https://doi.org/10.1016/j.dsm.2024.08.001
24. Chandrashekar G., Sahin F. A survey on feature selection methods // Computers & electrical engineering. 2014. V. 40. N 1. P. 16–28. https://doi.org/10.1016/j.compeleceng.2013.11.024
25. Palo H.K., Sahoo S., Subudhi A.K. Dimensionality reduction techniques: Principles, benefits, and limitations // Data Analytics in Bioinformatics: A Machine Learning Perspective. 2021. P. 79–107. https://doi.org/10.1002/9781119785620.ch4
26. Dunn J., Mingardi L., Zhuo Y.D. Comparing interpretability and explainability for feature selection // arXiv. 2021. arXiv:2105.05328. https://doi.org/10.48550/arXiv.2105.05328
27. Li J., Cheng K., Wang S., Morstatter F., Trevino R.P., Tang J., Liu H. Feature selection: A data perspective // ACM computing surveys. 2017. V. 50. N 6. P. 1–45. https://doi.org/10.1145/3136625
28. Kathiravan P., Shanmugavadivu P., Saranya R. Mitigating imbalanced data in online social networks using Stratified K-Means Sampling // Proc. of the 8th International Conference on Business and Industrial Research (ICBIR). 2023. P. 883–888. https://doi.org/10.1109/ICBIR57571.2023.10147677
29. Qi J., Ko T.W., Wood B.C., Pham T.A., Ong S.P. Robust training of machine learning interatomic potentials with dimensionality reduction and stratified sampling // npj Computational Materials. 2024. V. 10. N 1. P. 43. https://doi.org/10.1038/s41524-024-01227-4
30. Siblini W., Fréry J., He-Guelton L., Oblé F., Wang Y.Q. Master your metrics with calibration // Lecture Notes in Computer Science. 2020. V. 12080. P. 457–469. https://doi.org/10.1007/978-3-030-44584-3_36
31. Салахутдинова К.И., Лебедев И.С., Кривцова И.Е. Алгоритм градиентного бустинга деревьев решений в задаче идентификации программного обеспечения // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. № 6. С. 1016–1022. https://doi.org/10.17586/2226-1494-2018-18-6-1016-1022
32. Prokhorenkova L., Gusev G., Vorobev A., Dorogush A. V., Gulin A. CatBoost: unbiased boosting with categorical features // Proc. of the Advances in neural information processing systems 31 (NeurIPS 2018). 2018.
33. Dorogush A.V., Gulin A., Gusev G., Kazeev N., Prokhorenkova L.O., Vorobev A. 2017. Fighting biases with dynamic boosting // arXiv. 2017. arXiv:1706.09516. https://doi.org/10.48550/arXiv.1706.09516
34. Dorogush A.V., Ershov V., Gulin A. CatBoost: gradient boosting with categorical features support // arXiv. 2018. arXiv:1810.11363. https://doi.org/10.48550/arXiv.1810.11363
35. Ami A.S., Moran K., Poshyvanyk D., Nadkarni A. «False negative-that one is going to kill you»: Understanding Industry Perspectives of Static Analysis based Security Testing // Proc. of the IEEE Symposium on Security and Privacy (SP). 2024. P. 3979–3997. https://doi.org/10.1109/SP54263.2024.00019
36. Heydarian M., Doyle T.E., Samavi R., MLCM: Multi-label confusion matrix // IEEE Access. 2022. V. 10. P. 19083–19095. https://doi.org/10.1109/ACCESS.2022.3151048
37. Chicco D., Jurman G. The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation // BMC genomics. 2020. V. 21. N 1. P. 1–13. https://doi.org/10.1186/s12864-019-6413-7
38. Bowen D., Ungar L. Generalized SHAP: Generating multiple types of explanations in machine learning // arXiv. 2020. arXiv:2006.07155. https://doi.org/10.48550/arXiv.2006.07155
39. Lee Y.G., Oh J.Y., Kim D., Kim G. SHAP value-based feature importance analysis for short-term load forecasting // Journal of

Electrical Engineering & Technology, 2023, vol. 18, no. 1, pp. 579–588. https://doi.org/10.1007/s42835-022-01161-9
40. Hamilton R.I., Papadopoulos P.N. Using SHAP values and machine learning to understand trends in the transient stability limit. *IEEE Transactions on Power Systems*, 2023, vol. 39, no. 1, pp. 1384–1397. https://doi.org/10.1109/TPWRS.2023.3248941
41. Berrar D. Cross-validation. *Encyclopedia of Bioinformatics and Computational Biology*, 2019, vol.1, pp. 542–545. https://doi.org/10.1016/B978-0-12-809633-8.20349-X
42. Tougui I., Jilbab A., El Mhamdi J. Impact of the choice of cross-validation techniques on the results of machine learning-based diagnostic applications. *Healthcare informatics research*, 2021, vol. 27, no. 3, pp. 189–199. https://doi.org/10.4258/hir.2021.27.3.189

Electrical Engineering & Technology. 2023. V. 18. N 1. P. 579–588. https://doi.org/10.1007/s42835-022-01161-9
40. Hamilton R.I., Papadopoulos P.N. Using SHAP values and machine learning to understand trends in the transient stability limit // IEEE Transactions on Power Systems. 2023. V. 39. N 1. P. 1384–1397. https://doi.org/10.1109/TPWRS.2023.3248941
41. Berrar D. Cross-validation // Encyclopedia of Bioinformatics and Computational Biology. 2019. V. 1. P. 542–545. https://doi.org/10.1016/B978-0-12-809633-8.20349-X
42. Tougui I., Jilbab A., El Mhamdi J. Impact of the choice of cross-validation techniques on the results of machine learning-based diagnostic applications // Healthcare informatics research. 2021. V. 27. N 3. P. 189–199. https://doi.org/10.4258/hir.2021.27.3.189

Authors

Abdulkader Hajjouz — PhD Student, ITMO University, Saint Petersburg, 197101, Russian Federation, SC 59362756700, https://orcid.org/0000-0002-8256-6790, hajjouz@itmo.ru
Elena Yu. Avksentieva — PhD (Education Science), Associate Professor, Associate Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, SC 57190830859, https://orcid.org/0000-0001-5000-4868, eavksenteva@itmo.ru

Авторы

Хажжуз Абдулкадер — аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 59362756700, https://orcid.org/0000-0002-8256-6790, hajjouz@itmo.ru
Авксентьева Елена Юрьевна — кандидат педагогических наук, доцент, доцент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 57190830859, https://orcid.org/0000-0001-5000-4868, eavksenteva@itmo.ru

Received 28.07.2024
Approved after reviewing 27.12.2024
Accepted 25.01.2025

Статья поступила в редакцию 28.07.2024
Одобрена после рецензирования 27.12.2024
Принята к печати 25.01.2025