Data and Metadata. 2024; 3:577
doi: 10.56294/dm2024577

ORIGINAL

Optimizing Intrusion Detection for DoS, DDoS, and Mirai Attacks Subtypes Using Hierarchical Feature Selection and CatBoost on the CICIoT2023 Dataset

La optimización de la detección de intrusiones para subtipos de ataques DoS, DDoS y Mirai utilizando selección jerárquica de características y CatBoost en el conjunto de datos CICIoT2023

Abdulkader Hajjouz[1], Elena Avksentieva[1]

[1]ITMO University, Faculty of Software Engineering and Computer Technology. Saint Petersburg, Russia.

Cite as: Hajjouz A, Avksentieva E. Optimizing Intrusion Detection for DoS, DDoS, and Mirai Attacks Subtypes Using Hierarchical Feature Selection and CatBoost on the CICIoT2023 Dataset. Data and Metadata. 2024; 3:577. https://doi.org/10.56294/dm2024577

Submitted: 11-05-2024 **Revised:** 01-09-2024 **Accepted:** 21-12-2024 **Published:** 22-12-2024

Editor: Adrián Alejandro Vitón Castillo

Corresponding author: Abdulkader Hajjouz

ABSTRACT

Introduction: modern networks suffer until unheard of vulnerabilities that need for advanced intrusion detection systems (IDS) given the growing danger presented by DoS, DDoS, and Mirai attacks. Research on the identification of certain attack subtypes is still lacking even with the CICIoT2023 dataset, which offers a complete basis for evaluating these cyber hazards. Usually, aggregating attacks into more general categories, existing research neglects the complex characteristics of specific subtypes, therefore reducing the detection effectiveness.
Method: this work presents a novel IDS model aiming at high accuracy detection of DoS, DDoS, and Mirai attack subtypes. Using hierarchical feature selection and the CatBoost algorithm on the CICIoT2023 dataset, our model addresses the problems of high-dimensional data and emphasizes on keeping the most important features by means of advanced preprocessing methods including Spearman correlation and hierarchical clustering. Furthermore, used is stratified sampling to guarantee in the training and testing stages fair representation of attack types, both common and uncommon.
Results: with an amazing Prediction Time per Network Flow of 7,16e-07 seconds, our model shows a breakthrough in intrusion detection performance by means of rigorous stratified cross-valuation, thereby attaining outstanding outcomes in accuracy, recall, and precision.
Conclusions: our method not only closes a significant gap in current knowledge but also establishes a new benchmark in cybersecurity by providing very detailed protection mechanisms against advanced threats. This study marks major progress in network security as it gives companies a more efficient instrument to recognize and minimize certain cyber risks with better precision and effectiveness.

Keywords: Computer Security; Machine Learning; Data Mining; Boosting Machine Learning Algorithms.

RESUMEN

Introducción: las redes modernas sufren vulnerabilidades sin precedentes que requieren sistemas avanzados de detección de intrusiones (IDS), dada la creciente amenaza que presentan los ataques DoS, DDoS y Mirai. La investigación sobre la identificación de subtipos específicos de ataques aún es limitada, incluso con el conjunto de datos CICIoT2023, que ofrece una base completa para evaluar estos peligros cibernéticos. Usualmente, al agrupar los ataques en categorías más generales, las investigaciones existentes pasan por alto las características complejas de los subtipos específicos, lo que reduce la efectividad de la detección.
Método: este trabajo presenta un modelo innovador de IDS dirigido a la detección de alta exactitud de los

subtipos de ataques DoS, DDoS y Mirai. Usando selección jerárquica de características y el algoritmo CatBoost sobre el conjunto de datos CICIoT2023, nuestro modelo aborda los problemas de datos de alta dimensión y pone énfasis en mantener las características más importantes mediante métodos avanzados de preprocesamiento que incluyen correlación de Spearman y agrupamiento jerárquico. Además, se utiliza muestreo estratificado para garantizar una representación justa de los tipos de ataques, tanto comunes como poco comunes, en las etapas de entrenamiento y prueba.
Resultados: con un tiempo de predicción impresionante por flujo de red de 7,16e-07 segundos, nuestro modelo muestra un avance en el rendimiento de la detección de intrusiones mediante una rigurosa evaluación cruzada estratificada, logrando resultados excepcionales en exactitud (accuracy), recuperación (recall) y precisión (precision).
Conclusiones: nuestro método no solo cierra una brecha significativa en el conocimiento actual, sino que también establece un nuevo punto de referencia en ciberseguridad al proporcionar mecanismos de protección muy detallados contra amenazas avanzadas. Este estudio marca un gran progreso en la seguridad de redes, ya que brinda a las empresas una herramienta más eficiente para reconocer y minimizar ciertos riesgos cibernéticos con mayor precisión y efectividad.

Palabras clave: Seguridad Informática; Aprendizaje Automático; Minería de Datos; Algoritmos de Aprendizaje Automático Mejorados.

INTRODUCTION

With the rise of DoS, DDoS, and Mirai attacks in recent years, major challenges can arise if these attacks succeed in disrupting services, resulting in operational delays, financial losses, and unauthorized use of sensitive systems.[1,2,3,4,5,6] Furthermore, as these attacks take advantage of weaknesses in systems, they have grown simpler for malevolent actors to use, therefore raising issues regarding infrastructure protection and system security against such threats. A DoS, DDoS, or Mirai assault overwhelms a network or device with too much data, therefore slowing down or maybe breaking it.[7,8,9] These attacks may make use of system flaws for further damage or control and are meant to cause disruptions to services, therefore depriving consumers of access. Consequently, it is now essential to use solutions able to identify breaches and lower threats to network and computer security.[10] These systems must be real-time, provide interpretable decisions, and find subtypes of attacks to properly handle every one of them.[11,12] The erratic character of breaches causes systems to find it difficult to foresee network traffic, therefore compromising important security criteria like availability, integrity, and confidentiality.[13] As such, the requirement of creating sophisticated intrusion detection systems (IDS) has become increasingly urgent.

The goal of this research is to significantly advance network security by creating a highly accurate and efficient intrusion detection system that is specifically designed to detect and classify various subtypes of DoS, DDoS, and Mirai threats. The dimensionality of the CICIoT2023 dataset was reduced through meticulous data preprocessing and feature selection while retaining all essential information. The carefully tuned CatBoost algorithm was then used to accurately identify both common and rare attack patterns. This work expands the boundaries of existing research by addressing the inherent class imbalance and optimizing for real-time performance, resulting in a model that is not only powerful and interpretable, but also reliable in real-world, high-stakes cybersecurity environments.

This paper's remaining content is as follows: Section 2 discusses the earlier research. The materials and methods are covered in Section 3. The proposed model and the performance assessments are discussed in Section 4. Section 5 discusses the conclusion and the future works.

Related Work

Due to the growing risks of cyberattack threats, intrusion detection systems (IDS) have long been a focus of network security research.[14,15] CICIoT2023 is a current and useful dataset for researching these concerns.[16] Few research has utilized this dataset, and even fewer of those studies have concentrated on identifying the subtypes of attacks within categories such as DoS, DDoS, and Mirai. This makes it abundantly evident that more in-depth research is required to increase the detection accuracy of these crucial assault subtypes. The objective is to create interpretable, real-time-operational, and effectively validated models that go beyond simple superficial tests to guarantee their dependability in practical applications.

Using the CICIoT2023 dataset, a proposed two-stage intrusion detection system (IDS) employs totally connected, convolutional, and LSTM-based deep learning models to improve the detection and mitigating of DDoS assaults in IoT networks.[17] Performance is enhanced by preprocessing methods include random subset selection, feature deletion, duplication removal, and normalizing. The model achieved an accuracy of 91,27 %

using the CNN-based two-stage model, the IDS effectively detects DDoS attacks by using binary and metaclassifier in a two-level approach.

Machine learning (ML) approaches like Logistic Regression (LR), Support Vector Machine (SVM), Random Forest (RF), and K-Nearest Neighbor (KNN) are used with SDN to identify DDoS attacks.[18] This integrated strategy uses SDN controllers to monitor whole networks and ML models to detect abnormalities in network traffic. The research assesses accuracy, recall, precision, and F1-score using the CIC-IoT 2023 dataset. The LR model beats others with 86 % accuracy, compared to 71 % for SVM, 65 % for KNN, and 60 % for RF.

A hybrid feature selection strategy is proposed to enhance the detection of Distributed Denial of Service (DDoS) attacks in Internet of Things (IoT) devices by selecting the most important features for an XGBoost model and focusing only on the CICIoT2023 dataset.[19] To address the rising security challenges in IoT caused by DDoS variations, the research picks 18 critical variables from the dataset, resulting in a 97,64 % recall model.

Federated learning and a deep neural network are used to identify Mirai attacks.[20] This model is developed and validated using the CICIoT2023 dataset to filter Mirai-related network traffic. Federated average improves local and global learning. Researchers compare covariate shift (CS) and concept drift (CD), CD surpasses CS in accuracy and performance. The Mirai botnet detection methodology was over 93 % accurate.

Another study represents the implementation of a unique intrusion detection model that is based on deep learning algorithms.[21] This model is constructed using the CICIoT2023 dataset. Even though the model is 97,46 % accurate when it comes to predicting general attacks, it is ineffective when it comes to discriminating subtypes.

A lightweight IoT intrusion detection model called DL-BiLSTM, integrating bidirectional LSTMs and deep neural networks (DNNs) to improve cyber-attack detection.[22] The model's detection accuracy for general attacks was 93,13 %, however it was not able to distinguish between subtypes. Table 1 is a summary of the information in the studies that were discussed above.

Table 1. Details of related studies

Ref.	Dataset	Year	Technique
17	CIC-IoT-2023	2024	DNN, CNN. LSTM
18	CIC-IoT-2023	2024	LR, SVM, RF, KNN
19	CIC-IoT-2023	2024	XGBoost
20	CIC-IoT-2023	2024	Federated learning approach
21	CIC-IoT-2023	2024	Gaining-Sharing Knowledge (GSK)
22	CIC-IoT-2023	2024	BiLSTM

THEORETICAL FRAMEWORK OF MATERIALS AND METHODS

This section describes the theoretical framework of this study.

Definition of Research Type

This is an applied research, using statistical methods and machine learning to analyze data and get practical results. The study will build an effective model to detect security intrusions by using scientific methods and data analysis on CICIoT2023 dataset.

The CICIoT2023 Dataset and Ethical Compliance

The 2023 Canadian Institute for Cybersecurity CICIoT2023 dataset was used.[16] One of the largest datasets for studying and analyzing IoT device cyberattacks. Many harmful IoT devices target network devices in these attacks. Besides normal traffic, the database contains 45,807,617 DDoS, DDoS, Mirai, and benign network flows. They are spread across 47 features describing connection details like flow duration, header length, and protocol type. TCP, UDP, and ICMP flags and flow statistics like average, minimum, maximum, and variance are also provided.

Since the dataset is public and widely used in research, its use in this study follows the ethical guidelines for open-access datasets. No PII or sensitive data is included.

Data Processing

This section outlines the key data processing steps that were applied to improve the quality and usability of the dataset for building a reliable intrusion detection model.

Data Quality Assurance

Before application of the machine learning model, the first thing that should be done is to ascertain that the data is correct and consistent; this can be achieved using data preprocessing.[23] The aim of these processes

is to enhance efficiency in the use of memory without compromising the specification on the accuracy of the data. Following that, we cleaned the data, removing incorrect values such as infinite and negative values that should not appear in the columns to prevent data distortions. Because the columns represent the dataset's features, any infinite values in a column were replaced with its median value. Similarly, for columns that are not supposed to have negative values, the negative values were replaced by the column's median. Next, we looked for columns with all values identical, indicating zero variance. These columns were removed because they have no analytical value and thus do not provide useful information to machine learning models.[24]

Hierarchical Feature Selection Using Spearman Correlation

Hierarchical Feature Selection with Spearman Correlation provides a useful approach to handle redundant features in any dataset by means of a statistically strong correlation metric. The method clusters statistically similar features while maintaining important feature variability to reduce the amount of features investigated and focus on maintaining the most informative ones. Applying the input data is the first step in the procedure, which also involves calculating the features' Spearman correlation, clustering the features that are statistically comparable, and selecting the most representative feature from each cluster. This method's goal is to decrease the dimensionality of the data without compromising critical information while at the same time maximizing and improving speed and efficacy of machine learning models.[25]

To start, we use Spearman Correlation to measure the relationship between feature pairs; unlike normal correlation, Spearman measures the rankings of two features correlate to each other. After that, we use Hierarchical Clustering to categorize the features that are comparable in terms of their Spearman correlation values, and the Dendrogram technique visually relates features into clusters based on their correlation scores. The aim is to select one feature from each group (cluster) of features which is truly representative of the other features in that group. This reduces the amount of features the model must evaluate, speeding up the model and improving its performance.

The hierarchical feature selection procedure using Spearman correlation is depicted in Figure 1. First, correlation coefficients between features are computed, then similar features are grouped hierarchically, and lastly, the most representative feature is chosen from each cluster.

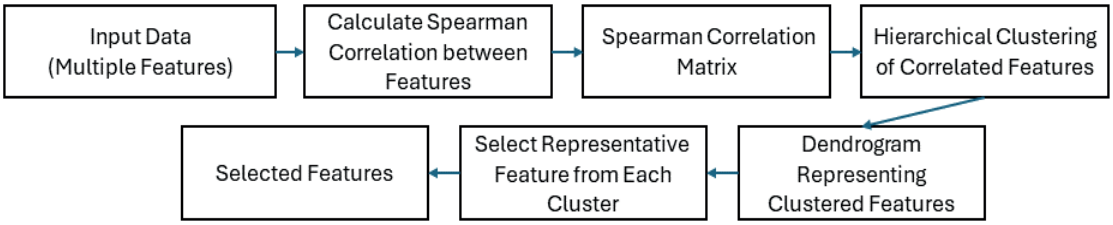

Figure 1. Hierarchical Feature Selection Workflow Using Spearman Correlation

STRATIFIED SAMPLING

Using stratified sampling, we made sure that the training, validation, and test datasets reflected, proportionately, all attack types—including the many subcategories of DoS, DDoS, and Mirai assaults. This approach is especially crucial for spotting not just the broad assault types but also the precise subtypes, therefore enabling the model to learn from both common and uncommon attacks. We enhanced the capacity of the model to identify these important subcategories by preserving the same class distribution across all subsets. Stratified sampling helps to maintain the percentage of each attack subtype, boosting the model's capacity to recognize both generic attack types and their subtle subcomponents.[26,27,28]

Understanding CatBoost and Its Key Parameters for Optimized Performance

CatBoost, an advanced machine learning method, handles complex tabular data and multi-class classification using gradient boosting over decision trees. CatBoost's ability to rectify mistakes at each stage makes it ideal for high-accuracy applications like attack detection and imbalanced data evaluation.[29] CatBoost uses Ordered Boosting to avoid overfitting and bias predictions by training trees on data in an ordered sequence. Ordered Statistics helps CatBoost analyze categorical data properly and natively supports categorical features, avoiding the need for one-hot encoding.

In the case of multi-class classification, the method measures the difference between predictions and actual values using a mathematical loss function known as Cross-Entropy, which is continually reduced as the model trains. We might translate our predictions into probabilities using the Softmax function; but we must make sure that the total of the probability for every sample equals 1. Our last prediction, then, is the one with the greatest probability.

CatBoost's performance relies significantly on the many variables being tuned. Iterations show the number

of incrementally built trees in which each tree corrects the errors of the previous one. The Learning Rate value tells the model how much to change at each step. The depth of a decision tree indicates how many levels it has. L2 Leaf Regularization helps to simplify the model and stop overfitting by punishing big weights in the tree leaves. When we choose Task Type, the model will run on either a GPU or a CPU.[30] Bagging Temperature controls how randomly samples are chosen for each tree. Understanding and optimizing these parameters transforms CatBoost into a powerful and effective tool for dealing with complex tasks in tabular data and multi-class categorization, significantly improving the model's performance.

Figure 2 depicts the CatBoost model workflow and shows how to use Ordered Boosting, adjust weights to correct data imbalance, and handle numerical and categorical data.

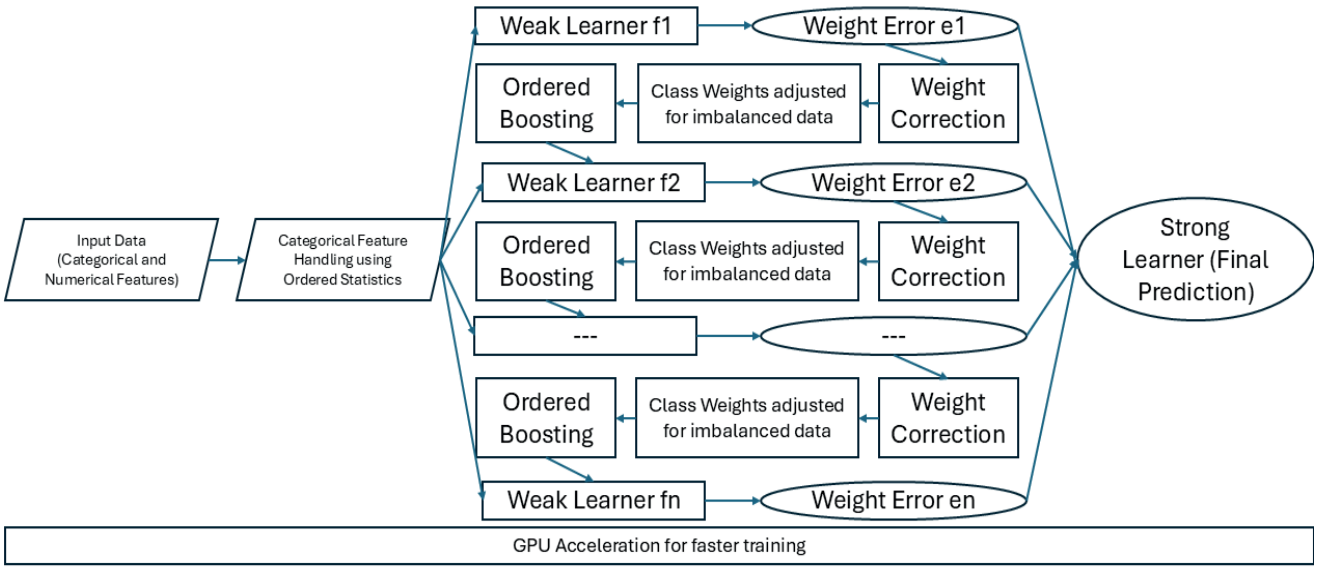

Figure 2. CatBoost Model Workflow: Gradient Boosting with Ordered Statistics and Class Weight Adjustments

Stratified K-Fold Algorithm for Robust Model Evaluation

Cross-Validation is an innovative method in machine learning that fairly assesses performance. One of the most frequently employed methods is Stratified K Fold, where the data is partitioned into diverse groups (or "Folds") in such a way that the class proportions in each fold are similar to the proportions in the overall dataset.[31] This is especially useful when the data is imbalanced (i.e., one class is much more frequent than the other). The primary endeavor of this approach is to overcome bias related to randomization when separating the data. Rather than splitting the data just once to fit and evaluate our model, we will repeat the process multiple times with distinct randomized splits of the data, decreasing the probability of getting bias or error in our performance evaluation. In plain terms, the model will be able to "train on all the data," just in a distributed format, and it will give reliable and more precise professional estimates of the model's ability to "Out-of-Sample" prediction.

INTRUSION DETECTION MODEL ARCHITECTURE AND IMPLEMENTATION

The architecture and specifics of the intrusion detection model are explained in the following sections, following the general structure depicted in figure 3.

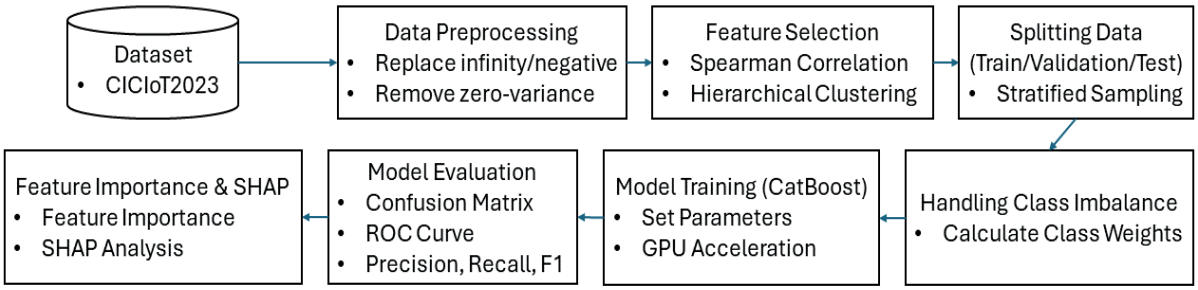

Figure 3. Architecture of the Intrusion Detection Model

https://doi.org/10.56294/dm2024577

Following the selection of network flows, extensive preprocessing was performed to ensure that the dataset was free of any errors. This included looking for and resolving infinite or negative values. We also discovered features with zero variance, which means their values were identical across all samples. These features—"IRC," "SMTP," "SSH," "Telnet," and "cwr_flag_number"—were either useless or meaningless within the context of the chosen attack types. The removal of these protocols and markers allowed the model to focus on more relevant and significant features. As a result, the data set was simplified.

Statistical Analysis

Using all 45,807,617 network flows from the CICIoT2023 dataset linked with the selected attack categories and normal traffic, this study Along with twenty other subtypes of attacks including DoS, DDoS, Mirai, and normal traffic, Care had to be taken to guarantee that both common and rare attack patterns were accurately identified since some attack types in the dataset are far more frequent than others. Table 2 depicts the distribution of flows across attack subtypes and benign conditions.

Table 2. Distribution of Network Flows by Attack Type

Classes	No. Patterns	Per. %	Class
DDoS-ICMP_Flood	7200504	15,72 %	3
DDoS-UDP_Flood	5412287	11,82 %	11
DDoS-TCP_Flood	4497667	9,82 %	10
DDoS-PSHACK_Flood	4094755	8,94 %	5
DDoS-SYN_Flood	4059190	8,86 %	7
DDoS-RSTFINFlood	4045285	8,83 %	6
DDoS-SynonymousIP_Flood	3598138	7,85 %	9
DoS-UDP_Flood	3318595	7,24 %	16
DoS-TCP_Flood	2671445	5,83 %	15
DoS-SYN_Flood	2028834	4,43 %	14
BenignTraffic	1098195	2,40 %	0
Mirai-greeth_flood	991866	2,17 %	17
Mirai-udpplain	890576	1,94 %	19
Mirai-greip_flood	751682	1,64 %	18
DDoS-ICMP_Fragmentation	452489	0,99 %	4
DDoS-UDP_Fragmentation	286925	0,63 %	12
DDoS-ACK_Fragmentation	285104	0,62 %	1
DoS-HTTP_Flood	71864	0,16 %	13
DDoS-HTTP_Flood	28790	0,06 %	2
DDoS-SlowLoris	23426	0,05 %	8

Both Spearman Correlation and Hierarchical Clustering were used in the feature selection process. The first thing we did was figure out the Spearman correlation matrix. This showed how closely the rankings of each pair of traits were linked. This step helped find traits that gave the same kind of information.

Hierarchical clustering was then used to group the features depending on their similarity. The correlation matrix helps one to identify highly linked features (figure 4). Using the Dendrogram (figure 5), we group these features according to their closeness ratings. From every cluster, one element was selected to reduce duplication. While maintaining the integrity of the dataset, the procedure reduced the original feature set to 23 by concentrating on the most critical ones.

Model Training and Optimization

After features selection, we had to divide the data into training, validation, and test sets. So as not to lose the proportions of each of attack subtypes, we used stratified sampling. The data was divided such that 70 % was used for training and 30 % for testing. This technique would ensure that both frequent and rare attacks are consistently distributed across all subsets; hence, the model truly has a balanced representation based on which to learn. In maintaining such a balance, under-represented classes and dominant ones get better generalization with the model, while the model becomes capable of detecting both frequent and rare attack patterns accurately. This will boost the overall capability for generalization and being robust at identifying disparate attack subtypes.

Class weights were computed to help to correct the dataset's class imbalance even more. These weights guarantee that during training the model pays the common and rare attack subtypes the necessary attention. Without this change, the model could favor the more frequent attack forms, so reducing the detection of the

less common ones. We made sure the model treats all attack types fairly by giving uncommon classes—such as DDoS-SlowLoris with a weight of 1908,56—higher weights and lower weights to more common classes—such DDoS-ICMP_Flood with 6,21.

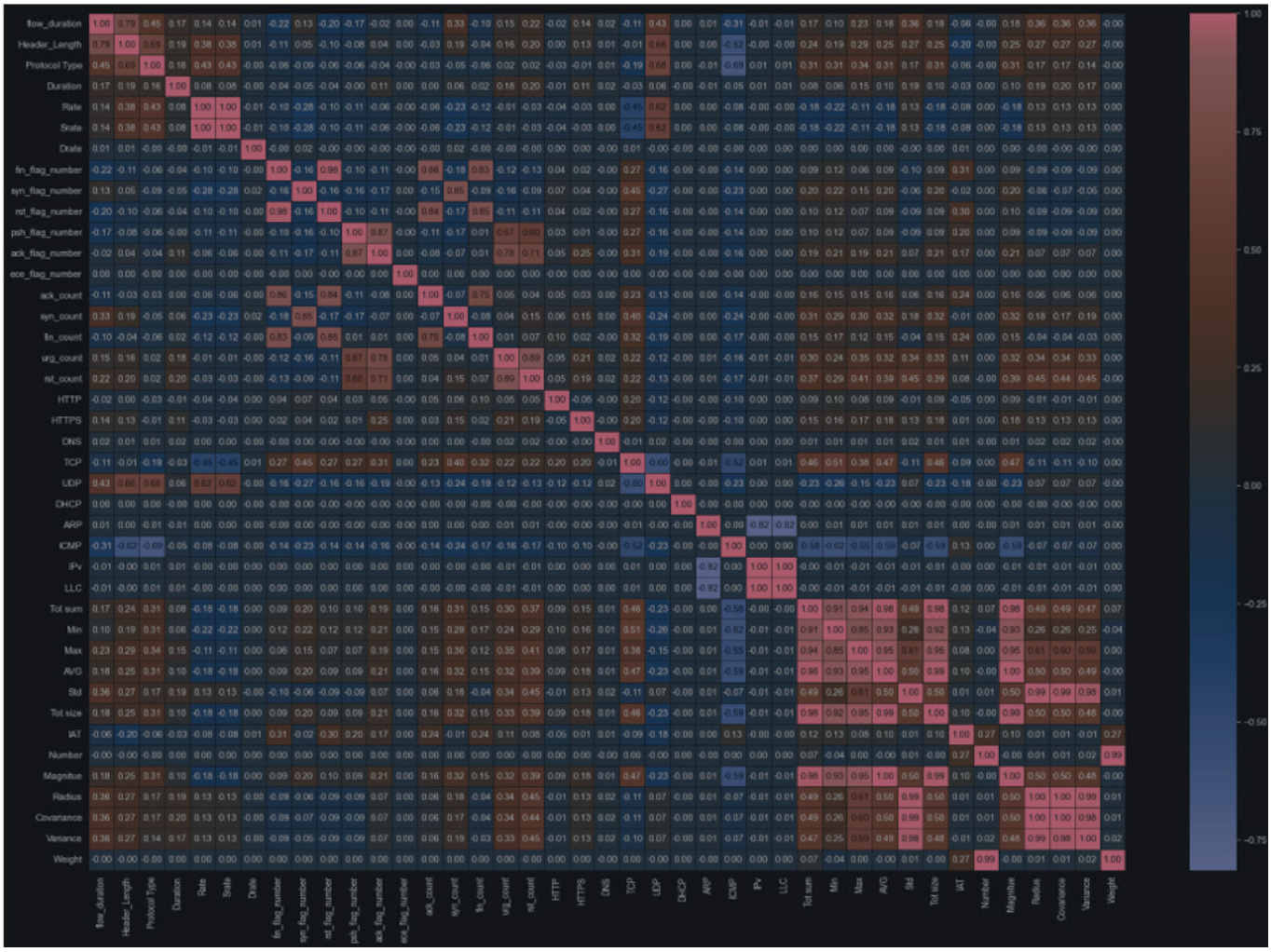

Figure 4. Correlation Matrix for Feature Clustering and Selection

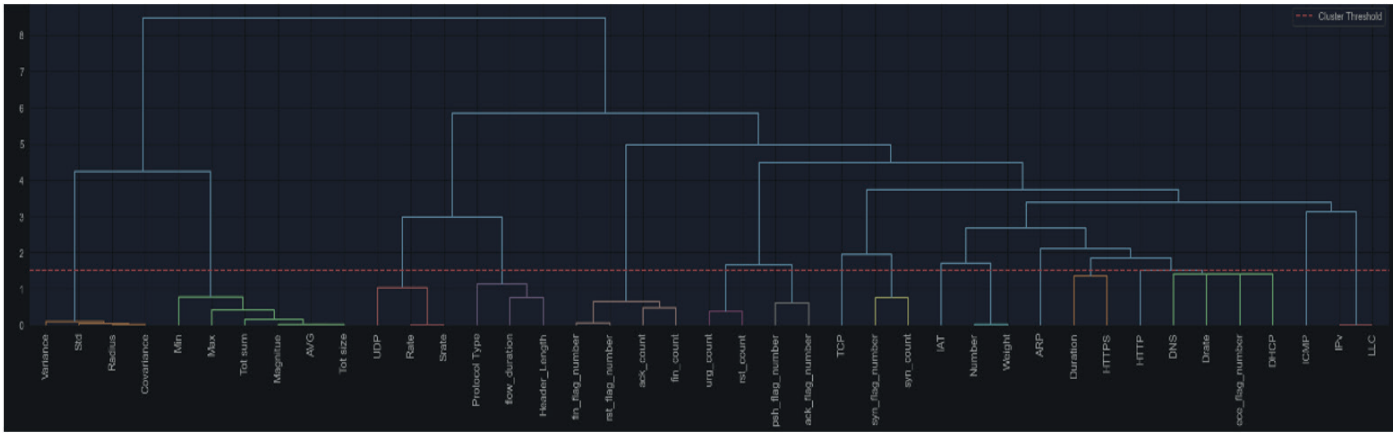

Figure 5. Dendrogram for Feature Clustering

With this class imbalance problem now attained, the next step would then be painstaking tuning of the model with the appropriate parameters. Such settings were chosen in order to ensure that the performance of the model is maximized without leading to overfitting and be computationally efficient at training. Key parameters in training the CatBoost model are summarized in table 3 below.

https://doi.org/10.56294/dm2024577

Table 3. Key Parameters for CatBoost Model Training

Parameter	Value	Description
Iterations	1320	Number of trees to build
Learning Rate	0,03	Controls how quickly the model adapts
Depth	8	Tree depth for capturing complex patterns
Loss Function	MultiClass	Suitable for multi-class classification
Task Type	GPU	Utilizes GPU for faster training
Random Seed	42	Ensures reproducibility of the results
L2 Leaf Regularization	2	Prevents overfitting by regularizing leaf weights
Border Count	256	Controls how many borders for numeric features
Early Stopping Rounds	150	Stops training if no improvement is seen
Leaf Estimation Iterations	10	Ensures accurate leaf value estimation
Bagging Temperature	1,0	Controls randomness in sample selection

We optimized these Parameters to balance training speed and accuracy while using GPU acceleration. The model learned well from the dataset.

RESULTS

After training on the dataset, the CatBoost model was tested on the chosen test set. Accuracy, recall, precision, F1 score, and ROC AUC were used to assess the model's attack detection ability. The model's efficiency, especially for real-time applications, was evaluated by recording testing time for the whole test set and calculating the average prediction time per sample. We used the Stratified K-Fold approach for robust assessment, which validates performance consistently and evenly across data subsets while keeping the class proportions right. Table 4 summarizes the assessment findings and shows how well the model performed across key metrics. The confusion matrix for the multi-class classification of the CatBoost model is shown in figure 6.

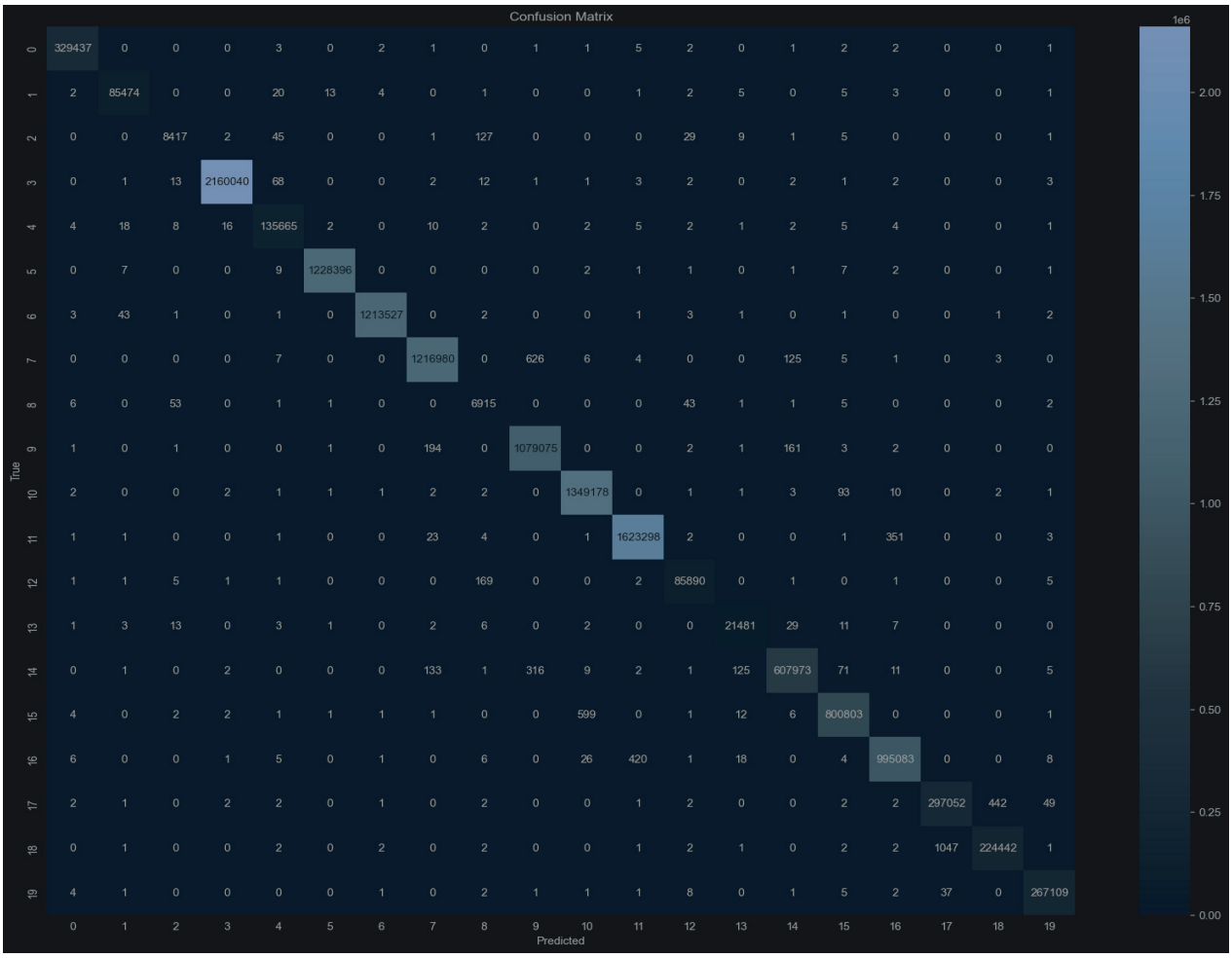

Figure 6. Confusion matrix for CatBoost algorithm

Table 4. Performance Metrics of CatBoost Model Evaluation

Accuracy %	Precision %	Recall %	F-score %	Total Test Time / s	Prediction Time per-Network Flow /s	ROC AUC
99,96	99,96	99,96	99,96	9,84	7,16e-07	1,00

Stratified K-Fold method helped to make validation strong and consistent throughout many data subsets. By maintaining stable class proportions in every fold, the model produced a more balanced evaluation of common and rare attack subtypes, hence enhancing its generalizability. Among the measures demonstrating exceptional performance throughout all six folds used to evaluate the model were accuracy, precision, recall, F1 score, and ROC AUC. Table 5 sums the results of every fold.

Table 5. Catboost Model Stratified K-Fold Validation Results

Fold	Accuracy	Precision	Recall	F1 Score	ROC AUC
1	0,99989	0,99989	0,99989	0,99989	1
2	0,99989	0,99989	0,99989	0,99989	1
3	0,99987	0,99987	0,99987	0,99987	0,999999
4	0,999882	0,999882	0,999882	0,999882	1
5	0,999925	0,999925	0,999925	0,999925	1
6	0,999894	0,999894	0,999894	0,999894	0,999998

After teaching the CatBoost model, we looked at how important each feature was to see which ones helped it make the best guesses. Feature importance tells us which features in the dataset are the most important. This can help us improve the model by focusing on the most important inputs. Figure 7 is a bar chart that shows the relative importance of each feature. The features that have the most effect on finding different types of attacks are highlighted.

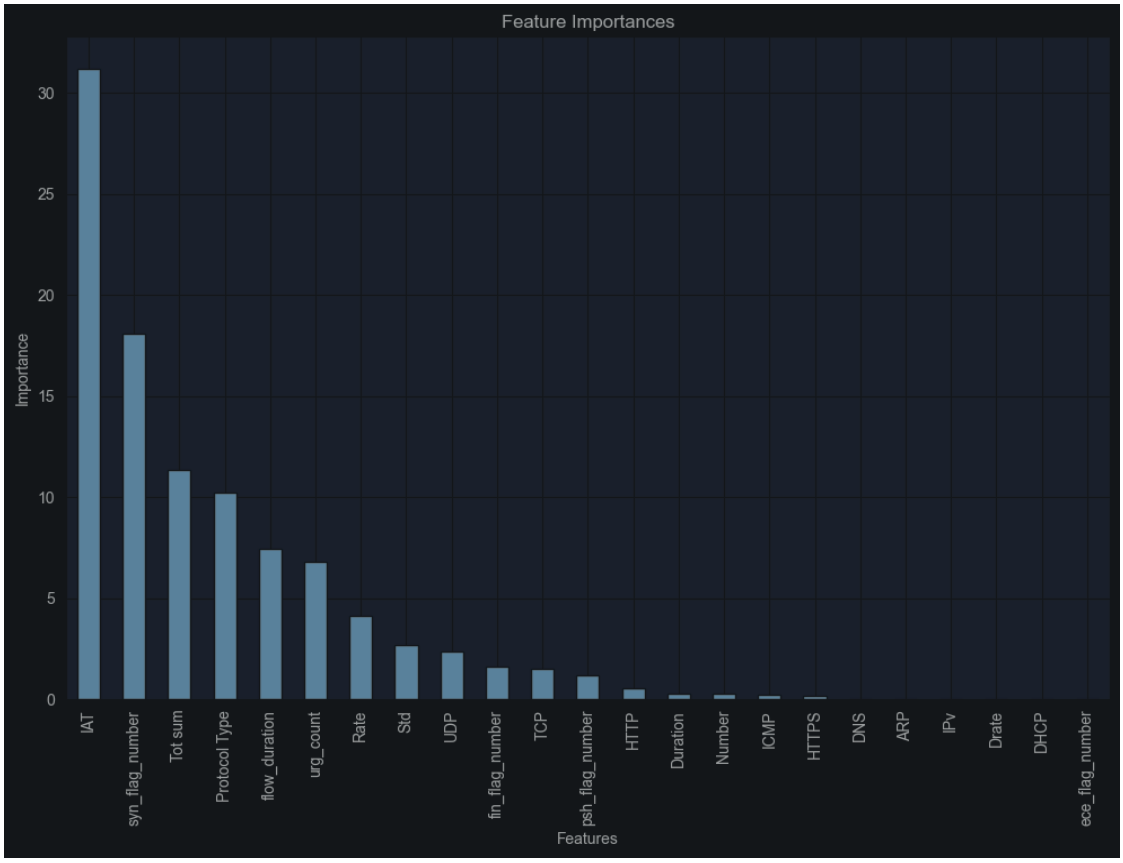

Figure 7. Feature Importance for CatBoost Model Predictions

For even easier understanding of the model, we also used SHAP (SHapley Additive explanations). Because SHAP values give us detailed information about how each trait affects individual prediction, they help us understand how the model makes decisions.[32] Figur 8 shows the SHAP summary plot, which shows how each feature affects the model's predictions for different types of attacks.

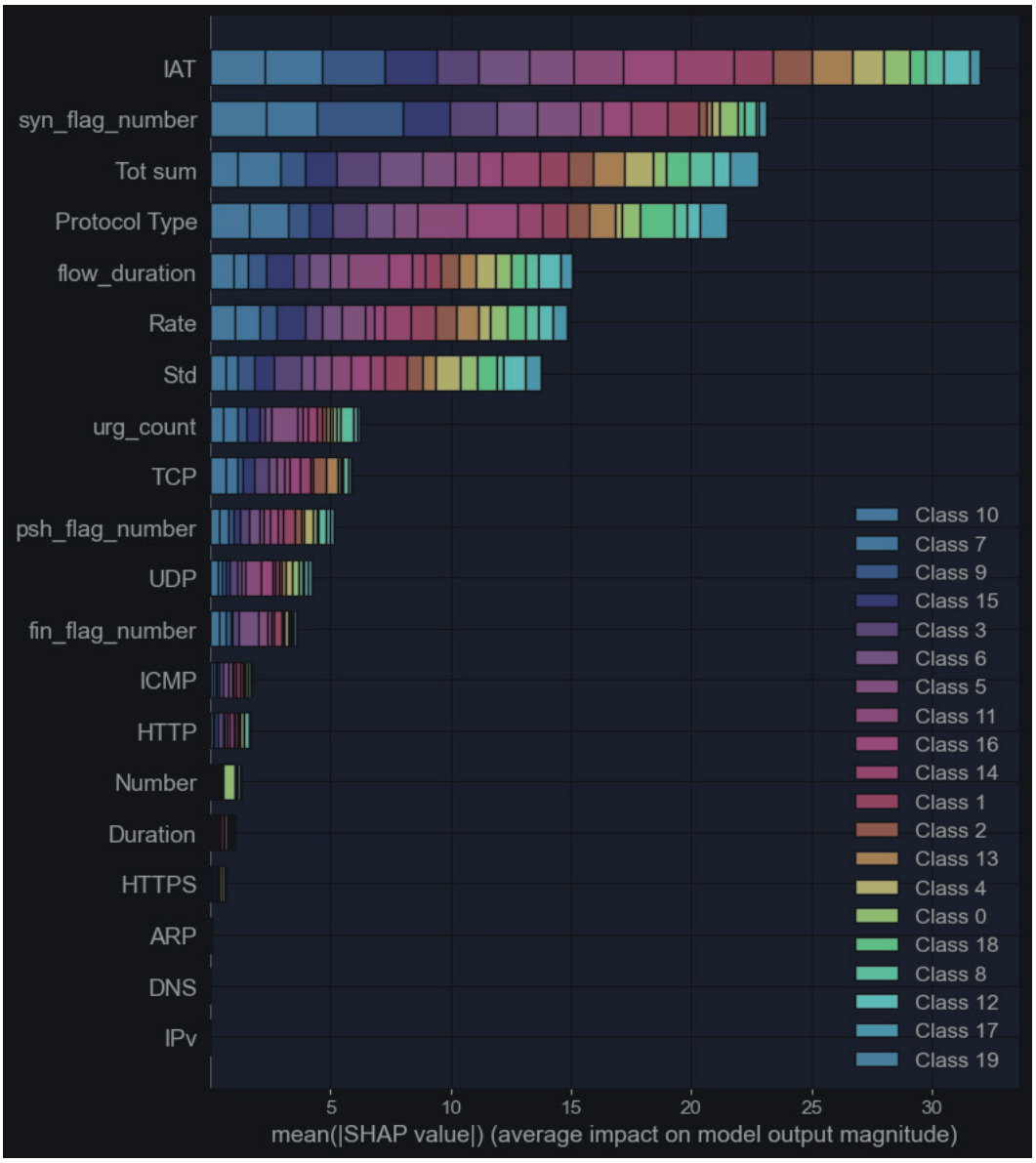

Figure 8. SHAP Analysis for CatBoost Model Predictions

The comparison between the result of the proposed model based on the CICIoT2023 dataset and the previous research is illustrated in table 6.

Table 6. Comparison of Proposed CatBoost Model with Previous Techniques on CICIoT2023 Dataset

Reference No	Technique	Accuracy %	Recall %	Precision %	F-score %
17	DNN	90,053	93,493	91,090	91,752
17	CNN	90,644	93,493	91,090	91,752
17	LSTM	91,273	94,304	91,458	92,329
18	SVM	71	78	82	80
18	LR	86	90	73	81
18	RF	60	47	80	59
18	KNN	65	65	75	69
19	XGBoost	97,642	97,64	95,33	96,47
20	Covariate Shift	92,22	91,16	86,85	N/A
20	Concept Drift	94,05	95,48	77,01	N/A
21	GSK	97,46	97	97	97
22	BiLSTM	93,13	93,13	91,80	91,94
Proposed Model	Catboost	99,96	99,96	99,96	99,96

https://doi.org/10.56294/dm2024577

CONCLUSION

We propose an optimized IDS by hierarchical feature selection and the implementation of a CatBoost algorithm on the CICIoT2023 dataset to identify subtypes of DoS, DDoS, Mirai attacks and benign traffic. Extensive preprocessing was performed on the data: cleaning, handling infinite and negative values, and removal of zero-variance features were applied to maintain dataset integrity. We applied hierarchical feature selection using Spearman correlation and hierarchical clustering, reducing the feature set into the most important 23 features. This boosted the model's efficiency, as a large reduction in the feature set did not come with performance loss. Due to class imbalance, stratified sampling was done along with calculation of class weights, ensuring that both common and rare attack subtypes are well-represented when training the model. Fine-tuning the parameters of CatBoost optimized multiclass classification performance. Also, accuracy, precision, recall, and F1-score for the model were very promising, amounting to 99,96 %, and ROC AUC was close to ideal, revealing outstanding novelty while distinguishing different attack subtypes. Prediction time per network flow came out as 7,16e-07 seconds, which is efficient in real-time applications. Stratified K-fold cross-validation also confirmed robustness and consistency across data splits. The feature importance analysis, together with SHAP values, enriches this interpretability by underpinning the in-depth understanding of the critical features that are contributing to the detection of specific attack subtypes, which is crucial for practical deployment and trust. As described, the proposed IDS is a very accurate and efficient way to spot DoS, DDoS, and Mirai attacks in real time in order to handle such threats, empowering the network to be more secure and resilient against cyber threats. Future research could thus be directed toward deployment in real-world environments for practical applicability and scalability.

REFERENCES

1. Zhang D, Wang QG, Feng G, Shi Y, Vasilakos AV. A survey on attack detection, estimation and control of industrial cyber–physical systems. ISA Transactions. 2021 Oct;116:1–16.

2. Lian Z, Shi P, Lim CC, Yuan X. Fuzzy-Model-Based Lateral Control for Networked Autonomous Vehicle Systems Under Hybrid Cyber-Attacks. IEEE Trans Cybern. 2023 Apr;53(4):2600–9.

3. Zagrouba R, AlHajri R. Machine Learning based Attacks Detection and Countermeasures in IoT. Int j commun netw inf secur [Internet]. 2022 Apr 15 [cited 2024 Dec 7];13(2). Available from: https://www.ijcnis.org/index.php/ijcnis/article/view/4943

4. Zhao K, Lu B, Shi H, Ren G, Zhang Y. A DDoS attack detection and defense mechanism based on the self-organizing mapping in SDN. Internet Technology Letters. 2024 Jan;7(1):e305.

5. Doriguzzi-Corin R, Siracusa D. FLAD: Adaptive Federated Learning for DDoS attack detection. Computers & Security. 2024 Feb;137:103597.

6. Md AQ, Jaiswal D, Daftari J, Haneef S, Iwendi C, Jain SK. Efficient Dynamic Phishing Safeguard System Using Neural Boost Phishing Protection. Electronics. 2022 Sep 29;11(19):3133.

7. Aslan Ö, Aktuğ SS, Ozkan-Okay M, Yilmaz AA, Akin E. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics. 2023 Mar 11;12(6):1333.

8. Agrafiotis I, Nurse JRC, Goldsmith M, Creese S, Upton D. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity [Internet]. 2018 Jan 1 [cited 2024 Dec 7];4(1). Available from: https://academic.oup.com/cybersecurity/article/doi/10.1093/cybsec/tyy006/5133288

9. Kumari P, Jain AK. A comprehensive study of DDoS attacks over IoT network and their countermeasures. Computers & Security. 2023 Apr;127:103096.

10. Kunhare N, Tiwari R, Dhar J. Particle swarm optimization and feature selection for intrusion detection system. Sādhanā. 2020 Dec;45(1):109.

11. Thirimanne SP, Jayawardana L, Yasakethu L, Liyanaarachchi P, Hewage C. Deep Neural Network Based Real-Time Intrusion Detection System. SN COMPUT SCI. 2022 Mar;3(2):145.

12. Patil S, Varadarajan V, Mazhar SM, Sahibzada A, Ahmed N, Sinha O, et al. Explainable Artificial Intelligence for Intrusion Detection System. Electronics. 2022 Sep 27;11(19):3079.

13. Humayun M, Niazi M, Jhanjhi N, Alshayeb M, Mahmood S. Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arab J Sci Eng. 2020 Apr;45(4):3171–89.

14. Khraisat A, Gondal I, Vamplew P, Kamruzzaman J. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecur. 2019 Dec;2(1):20.

15. Khraisat A, Alazab A. A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecur. 2021 Mar 8;4(1):18.

16. Neto ECP, Dadkhah S, Ferreira R, Zohourian A, Lu R, Ghorbani AA. CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment. Sensors. 2023 Jun 26;23(13):5941.

17. Hizal S, Cavusoglu U, Akgun D. A novel deep learning-based intrusion detection system for IoT DDoS security. Internet of Things. 2024 Dec;28:101336.

18. Sharma A, Babbar H. Machine Learning-based Threat Detection for DDoS Prevention in SDN-Controlled IoT Networks. In: 2024 5th International Conference for Emerging Technology (INCET) [Internet]. Belgaum, India: IEEE; 2024 [cited 2024 Dec 7]. p. 1–6. Available from: https://ieeexplore.ieee.org/document/10593167/

19. Modi P. Towards Efficient Machine Learning Method for IoT DDoS Attack Detection [Internet]. arXiv; 2024 [cited 2024 Dec 7]. Available from: https://arxiv.org/abs/2408.10267

20. Dahiya P, Bhattacharya S. MiraiBotGuard: Federated Learning for Intelligent Defense Against Mirai Threats. In: 2024 2nd International Conference on Device Intelligence, Computing and Communication Technologies (DICCT) [Internet]. Dehradun, India: IEEE; 2024 [cited 2024 Dec 7]. p. 1–6. Available from: https://ieeexplore.ieee.org/document/10533028/

21. Gheni HQ, Al-Yaseen WL. Two-step data clustering for improved intrusion detection system using CICIoT2023 dataset. e-Prime - Advances in Electrical Engineering, Electronics and Energy. 2024 Sep;9:100673.

22. Wang Z, Chen H, Yang S, Luo X, Li D, Wang J. A lightweight intrusion detection method for IoT based on deep learning and dynamic quantization. PeerJ Computer Science. 2023 Sep 22;9:e1569.

23. Alpaydin E. Machine learning. Revised and updated edition. Cambridge, Massachusetts: The MIT Press; 2021. 255 p. (The MIT Press essential knowledge series).

24. Theng D, Bhoyar KK. Feature selection techniques for machine learning: a survey of more than two decades of research. Knowl Inf Syst. 2024 Mar;66(3):1575–637.

25. Ali Abd AlHameed K. Spearmans correlation coefficient in statistical analysis. IJNAA [Internet]. 2022 Jan [cited 2024 Dec 7];13(1). Available from: https://doi.org/10.22075/ijnaa.2022.6079

26. Berndt AE. Sampling Methods. J Hum Lact. 2020 May;36(2):224–6.

27. Wei W, Nazura Bt. AM, Bin Abd Rahman MR. Research on the Issues and Paths of Citizen Privacy Protection in China in the Era of Big Data. Salud, Ciencia y Tecnología. 2024;4:.1208.

28. Ananth B. Hybrid Support Vector Machine for Predicting Accuracy of Conflict Flows in Software Defined Networks. Salud, Ciencia y Tecnología. 2024;4:797.

29. Hancock JT, Khoshgoftaar TM. CatBoost for big data: an interdisciplinary review. J Big Data. 2020 Dec;7(1):94.

30. Samat A, Li E, Du P, Liu S, Xia J. GPU-Accelerated CatBoost-Forest for Hyperspectral Image Classification Via Parallelized mRMR Ensemble Subspace Feature Selection. IEEE J Sel Top Appl Earth Observations Remote Sensing. 2021;14:3200–14.

31. Prusty S, Patnaik S, Dash SK. SKCV: Stratified K-fold cross-validation on ML classifiers for predicting cervical cancer. Front Nanotechnol. 2022 Aug 19;4:972421.

32. Lundberg S, Lee SI. A Unified Approach to Interpreting Model Predictions [Internet]. arXiv; 2017 [cited 2024 Dec 7]. Available from: http://arxiv.org/abs/1705.07874

FINANCING

The authors did not receive financing for the development of this research.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Abdulkader Hajjouz, Elena Avksentieva.
Formal analysis: Abdulkader Hajjouz, Elena Avksentieva.
Methodology: Abdulkader Hajjouz, Elena Avksentieva.
Drafting - original draft: Abdulkader Hajjouz, Elena Avksentieva.
Writing - proofreading and editing: Abdulkader Hajjouz, Elena Avksentieva.