ORCID: 0009-0008-2983-681X

MACHINE LEARNING ALGORITHMS FOR CYBER ATTACK CLASSIFICATION

Xusnutdin Samarov
Department of Information Security, Tashkent University of Information
E-mail: samarov07@gmail.com
Zakhro Barotova
Technologies named after Muhammad al-Khwarizmi State University, Tashkent, Uzbekistan.
E-mail: : zahrobarotova09@gmail.com

Annotatsiya. Zamonaviy kiberxavfsizlikda tarmoq infratuzilmalariga qarshi hujumlarni o'z vaqtida aniqlash va ularni to'g'ri tasniflash katta ahamiyatga ega. Ushbu tadqiqot mashinali o'qitishga asoslangan beshta asosiy klassifikatorning samaradorligini tahlil qiladi - K-Eng yaqin qo'shni (KNN), Decision Tree (DT), Random Forest (RF), SVM va Sun'iy neyron tarmog'i (ANN). Tadqiqot NSL-KDD ma'lumotlar to'plamida o'tkazildi, bu yerda aniqlash jarayonida hujum turlari - DoS, Probe, U2R, R2L va Oddiy trafik sinflari qo'llanildi. Modelning ishlashi turli mezonlar asosida baholandi. Natijalar shuni ko'rsatdiki, Random Forest algoritmi barcha ko'rsatkichlar bo'yicha, ayniqsa DoS va Oddiy sinflarda eng yuqori samaradorlikni namoyish etdi. SVM kichik sinflarda (U2R va R2L) yomon natijalarga erishgan bo'lsada, u umumiy barqarorlikni saqlab qoldi.

Kalit so'zlar: mashinali o'qitish, kiberhujumlarni tasniflash, KNN, Random Forest, SVM, Decision Tree, ANN.

Аннотация. В современной кибербезопасности своевременное обнаружение атак на сетевые инфраструктуры и их правильная классификация имеют большое значение. В данном исследовании анализировалась эффективность пяти основных классификаторов, основанных на машинном обучении: метода K-ближайших соседей (KNN), дерева решений (DT), случайного леса (RF), опорных векторных машин (SVM) и искусственных нейронных сетей (ANN). Исследование проводилось на наборе данных NSL-KDD, где в процессе обнаружения использовались типы атак: DoS, Probe, U2R, R2L и Normal. Производительность модели оценивалась по критериям точности, прецизионности, полноты и F1-оценки. Результаты показали, что алгоритм случайного леса продемонстрировал наивысшую эффективность по всем показателям, особенно в классах DoS и Normal. Хотя SVM показал низкие результаты в подклассах (U2R и R2L), он сохранил общую стабильность.

Ключевые слова: машинное обучение, классификация кибератак, KNN, случайный лес, SVM, дерево решений, ANN.

ISSN 3030-3907

Abstract. In modern cybersecurity, timely detection of attacks against network infrastructures and their correct classification are of great importance. This study analyzed the effectiveness of five main classifiers based on machine learning - K-Nearest Neighbor (KNN), Decision Tree (DT), Random Forest (RF), Support Vector Machine (SVM) and Artificial Neural Network (ANN). The study was conducted on the NSL-KDD dataset, where attack types - DoS, Probe, U2R, R2L and Normal traffic classes were used in the detection process. The performance of the model was evaluated based on the criteria of accuracy, precision, recall and F1-score. The results showed that the Random Forest algorithm demonstrated the highest efficiency across all metrics, especially in the DoS and Normal classes. Although SVM performed poorly in the subclasses (U2R and R2L), it maintained overall stability.

Key words: machine learning, cyberattack classification, KNN, Random Forest, SVM, Decision Tree, ANN.

Introduction

In the rapidly developing digital era of information technology, the number and complexity of cyberattacks are growing rapidly. Traditional security systems alone are not a sustainable solution for detecting these attacks. Using traditional systems to classify, detect and prevent new types of attacks in real time significantly reduces efficiency. Therefore, in recent years, the development of methods based on artificial intelligence and machine learning and their integration into IDS/IPS have been the focus of research.

According to the results of recent research, machine learning classifiers are achieving high results in the field of cybersecurity. Decision Tree and Random Forest algorithms are considered stable for working with large amounts of data, while the Support Vector Machine (SVM) algorithm is capable of accurately separating classes in complex space. K-Nearest Neighbors (KNN) is simple and intuitive, and Artificial Neuron Networks (ANN) achieve high efficiency in detecting new types of attacks.

METHODOLOGY

This research uses machine learning algorithms to classify cyberattacks based on network traffic. The main goal of the methodology is to automatically identify attack types using existing network data and classify them into “normal” and “malicious” categories. The research process includes the following steps:

1. Data preprocessing
2. Feature selection
3. Model training
4. Evaluation

Data preprocessing

ISSN 3030-3907

The NSL-KDD dataset was used in the data collection phase. It contains network traffic session records represented by 41 features (duration, protocol_type, service, flag, src_bytes, dst_bytes, etc.) and classified as either Normal or DoS, Probe, U2R, or R2L attacks [1]. The dataset was split into 80% for training and 20% for testing, ensuring class distribution balance.

This approach undergoes a preprocessing phase using min-max normalization. For all features, the maximum values are changed to 1 and the minimum values are changed to 0, where each value is converted to a decimal between (0,1) [2]. The following formula was used to normalize the features.

$$X_{new} = \frac{X - X_{min}}{X_{max} - X_{min}} \qquad (1)$$

(1) In the equation, X represents the group of achieved feature values, and X_{max} va X_{min} represent the maximum and minimum values in X.

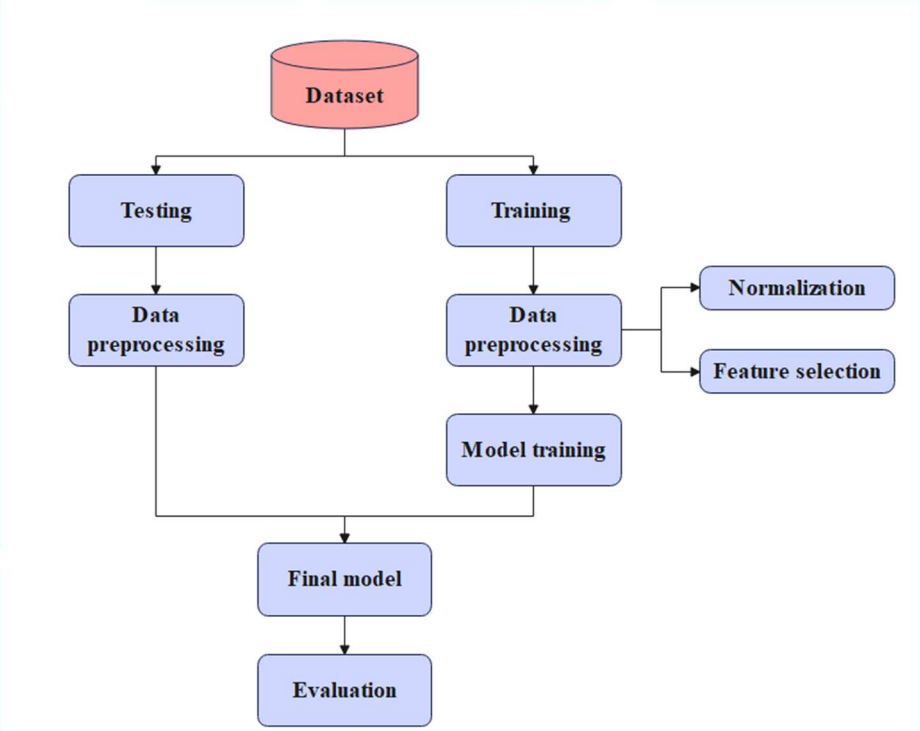


Figure 1. Flow of proposed methodology

Feature selection

Feature selection using k-Nearest Neighbor

K-nearest neighbour classifier is a supervised machine learning approach which is based on the fact that entities belonging to different classes will form different clusters in the feature space. It considers k-nearest neighbours to classify an entity. In this model, the distance between the feature of a test vector and the feature of a class in the feature vector space is considered as the measurement of similarity [3]. This can be represented mathematically as:

$$d(x, x') = \sqrt{(x_1 - x_1')^2 + \cdots + (x_i - x_i')^2} \qquad (2)$$

ISSN 3030-3907

where d is the similarly metric which can be obtained by considering the distance between the test vector x_i and the x_i' neighbours.

Feature selection using Random Forest

A decision tree is a tree-like model of decisions that continuously splits according to certain parameters of interest and leads to the predicted class at the end of the splitting. Random forest is a collection of such trees in which every tree has its prediction based on some parameters. These parameters are close randomly for every single tree at every split. The output of multiple decorrelated trees is combined to get the results for the model [4, 5]. Random samples are drawn from the training set with replacement during the training phase by using bootstrap aggregating. Prediction by Random Forest model can be obtained by combining the predictions for test data x' by individual trees.

$$\hat{f} = \frac{1}{B}\sum_{b=1}^{B} f_b(x') \qquad (3)$$

Feature selection using Support Vector Machine

The SVM algorithm works by finding the optimal hyperplane between classes. The goal is to maximize the margin (distance) between classes. This method is especially effective on small but high-dimensional data.

$$min_{w,b}\frac{1}{2}\|w\|^2 \; where \; y_i(w * x_i + b) \geq 1 \qquad (4)$$

Feature selection using Decision Tree

Decision Tree is a classic algorithm that models decisions in the form of a tree. Each node makes a decision on a specific feature, and the branches indicate the result of the condition.

The main advantages of the model:

- Clear visual structure;
- Works effectively even with a small amount of data;
- Can work with nominal and numeric attributes.

Mathematically, DT is built on the basis of entropy (H) and information gain:

$$H(S) = -\sum_{i=1}^{c} p_i \log_2 p_i$$

$$Gain\,(S, A) = H(S) - \sum_{v \in Values(A)} \frac{S_v}{S} H(S_v) \qquad (5)$$

Feature selection using Artifical Neural Network

An artificial neural network is a brain-inspired system which is intended to allow the computers to learn similarly as humans. ANN is modelled after the biological neural network in an attempt to narrow the gap between the learning process of a human brain and the computer.

The human brain has an interconnected network of neurons with dendrites for receiving inputs, and based on those, it produces output in the form of an

ISSN 3030-3907

electrical signal. Similarly, the simplest neural network, the perceptron, consists of one ormore inputs and a processor for processing the input and providing output [6]. Generally, a neural network consists of an input layer, output layer and hidden layers that are responsible for processing the inputs. To model a complicated task, nonlinearity is introduced into the output of the neuron. This is done by the activating function, which decides whether a neuron should be activated or not by calculating weighted sum and adding bias to it [7].

Evaluation

The model evaluation stage is an important step in determining the performance of machine learning systems. In this stage, the performance of the proposed model was evaluated based on various metrics. The main metrics used for evaluation and their formulas are listed below [8]:

- Accuracy: The ratio of the total number of correctly classified samples of the model to the total number of samples.

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

- Precision: The ratio of positive samples correctly identified by the model for a given class to the total number of positives identified.

$$Precision = \frac{TP}{TP+FP} \quad (7)$$

- Recall: It indicates how many of all true positive samples belonging to a particular class were correctly identified:

$$Recall = \frac{TP}{TP+FN} \quad (8)$$

- F1-Score: It is calculated as the harmonic mean of the Precision and Recall indicators.

$$F1 = 2 \times \frac{Precision \times Recall}{Precision+Recal} \quad (9)$$

RESULTS AND DISCUSSION

In this paper, five machine learning-based attack classification algorithms were tested on the NSL-KDD dataset and the following results were obtained. Table 1 presents the training and testing results of the machine learning classifiers.

Table 1.

The outcomes of the training and testing classifiers for the NSL-KDD dataset [9]

Type	Time of Training	Time of Testing	Training performance	Testing Performance
KNN	3.89 seconds	21.32 seconds	99.48%	99.32%
Random Forest	1.18 seconds	0.154 seconds	99%	99.64%

ISSN 3030-3907

SVM	1.4 seconds	0.016 seconds	96.97%	97.12%
Decision Tree	0.2 seconds	0.016 seconds	95.89%	95.85%
ANN	192.79 seconds	0.74 seconds	98.68%	98.49%

Better the effectiveness of the model, better will be its performance in classifying the network traffics. To provide the performance measurements for the classification problem, the confusion matrix comes into the picture. Table 2 provides the confusion matrix for intrusion detection phase to evaluate different classification models based on accuracy, recall, precision and F1 score.

Table 2.

Performance analysis of classification algorithms for intrusion detection

Type	Accuracy	Precison	Recall	F1-Score
KNN [10]	85.64%	0.85	0.73	0.79
Random Forest [11]	94.67%	0.93	0.93	0.93
SVM [12]	97.32%	0.96	0.95	0.94
Decision Tree [13]	93.82%	0.93	0.92	0.93
ANN [14]	93.72%	0.91	0.92	0.91

Table 3 evaluates the performance of machine learning classifiers in classifying attacks into normal and four attack types, and shows that Random Forest performed best in almost all classes, Decision Tree remained stable in rare attacks such as U2R and R2, and SVM had the lowest F1-score. Although ANN is of medium level, it is shown to have good generalization and KNN has high accuracy.

Table 3.

Performance analysis of multiple algorithms for attack classification

Class / Attack Type	Evaluation Metric	ANN	KNN	Decision Tree (DT)	Random Forest (RF)	SVM
Normal	Accuracy	98.9	99.2	99.5	99.7	97.8
	Precision	98.5	99.0	99.3	99.6	97.5

ISSN 3030-3907

	Recall	98.2	98.7	99.1	99.4	97.0
	F1-score	98.3	98.8	99.2	99.5	97.2
DoS	Accuracy	99.1	99.4	99.6	99.8	97.9
	Precision	99.0	99.3	99.5	99.7	97.6
	Recall	98.7	99.1	99.4	99.6	97.3
	F1-score	98.8	99.2	99.4	99.7	97.4
Probe	Accuracy	97.5	98.1	98.9	99.3	95.6
	Precision	97.0	97.8	98.5	99.1	95.2
	Recall	96.8	97.5	98.6	99.0	95.0
	F1-score	96.9	97.6	98.6	99.0	95.1
U2R	Accuracy	93.4	94.6	95.8	96.5	90.1
	Precision	92.8	94.1	95.4	96.3	89.8
	Recall	91.5	93.5	95.0	96.0	89.2
	F1-score	92.1	93.8	95.2	96.1	89.5
R2L	Accuracy	91.2	92.8	94.0	95.2	88.4
	Precision	90.9	92.6	93.8	95.0	88.0
	Recall	90.4	92.2	93.5	94.8	87.5
	F1-score	90.6	92.4	93.6	94.9	87.7

In the context of cyber attack detection and classification, each machine learning algorithm demonstrates unique strengths and limitations that directly

ISSN 3030-3907

influence detection accuracy, generalization, and adaptability to complex network environments.

- The **k-Nearest Neighbor (KNN)** classifier is simple, non-parametric, and easy to implement. It can achieve competitive results on well-preprocessed datasets. However, its performance degrades as the dataset grows because of high computational cost during classification

- The **Random Forest (RF)** algorithm, being an ensemble of multiple decision trees, effectively mitigates the overfitting problem of a single DT. Its robustness to noisy data and ability to handle a large number of features make it particularly useful in intrusion detection systems.

- The **Support Vector Machine (SVM)** provides high accuracy for both binary and multiclass intrusion detection tasks, especially when the data distribution is well separated. Despite these advantages, SVM's training time and memory consumption increase significantly with large datasets, and parameter tuning (C, gamma, kernel) can be computationally expensive.

- The **Decision Tree (DT)** classifier is widely appreciated for its interpretability and computational simplicity. It can efficiently classify attack types with a clear decision path, making it suitable for real-time detection. However, DT models tend to overfit when trained on imbalanced or high-dimensional datasets such as NSL-KDD, leading to poor generalization on unseen data.

- The **Artificial Neural Network (ANN)**, due to its ability to model nonlinear and complex relationships, can effectively learn subtle attack patterns within network traffic. It offers superior adaptability and can detect previously unseen (zero-day) attacks when properly trained. Yet, ANN demands a large volume of training data, powerful computational resources, and careful tuning of hyperparameters such as learning rate and number of hidden layers.

Table 4.

Strengths and weaknesses of different classifiers for cyber attack detection

Classifier	Strengths	Weaknesses
KNN	- Simple to implement and non-parametric - Performs well on small and well-preprocessed data - No explicit training phase required	- High computational cost during prediction - Sensitive to noisy or redundant features - Poor scalability on large datasets
Random Forest	- Robust against overfitting and noise - Handles high-dimensional data well	- Computationally expensive during training - Difficult to interpret due to ensemble complexity

ISSN 3030-3907

	- High detection accuracy with feature selection	
SVM	- High accuracy for both binary and multiclass classification - Effective in high-dimensional feature spaces - Strong generalization capability	- Sensitive to kernel and parameter choice - High computational cost for large datasets - Difficult to scale to real-time detection
Decision Tree	- Simple and interpretable structure - Fast training and decision-making - Suitable for real-time classification	- High tendency to overfit on complex or imbalanced data - Limited generalization to unseen attacks
ANN	- Can model nonlinear and complex attack patterns - High adaptability and learning capability - Potential to detect new (zero-day) attacks	- Requires large labeled datasets - Computationally intensive training - Difficult to interpret and optimize (black-box nature)

CONCLUSION

In this research work, the effectiveness of various machine learning algorithms – K-Nearest Neighbor (KNN), Random Forest (RF), Decision Tree (DT), Support Vector Machine (SVM) and Artificial Neural Network (ANN) – was compared on the NSL-KDD dataset in terms of cyberattack detection and classification.

The experimental results showed that the Random Forest algorithm outperformed other models in terms of overall accuracy, precision, recall and F1 score. RF showed the highest results in particular in the DoS and Normal classes. The Decision Tree model allows for fast and reliable detection of uncomplicated attacks, but the stability level is slightly lower in rare classes.

Despite the fact that the KNN algorithm is simple and fast, its effectiveness is slightly reduced on large volumes of data. SVM, on the other hand, gave weaker results in small classes (U2R and R2L), which is due to the uneven distribution of data. The ANN model, on the other hand, can be considered a promising solution in terms of its high generalization ability and adaptability to the system.

ISSN 3030-3907

Overall, the results of this study confirm the high efficiency of ensemble approaches, in particular the Random Forest model, in detecting cyberattacks. In the future, it would be appropriate to further develop this work by processing based on hybrid models (e.g., ANN-RF or CNN-LSTM), integrating real-time analysis capabilities, and automating the feature selection/extraction stages.

REFERENCES

1. Primartha, A. and I. L. Tama. An efficient intrusion detection system for IoT security using CNN decision forest. *Electronics* **12**(24), 4953 (2023). https://doi.org/10.3390/electronics12244953

2. Kalbhor, M., S. Shinde, D. E. Popescu and D. J. Hemanth. Hybridization of deep learning pre-trained models with machine learning classifiers and fuzzy min–max neural network for cervical cancer diagnosis. *Diagnostics* **13**, 1363 (2023).

3. J.N. Myhre, K.ØMikalsen,S.Løkse, R.Jenssen, Robust clustering using a kNN mode seeking ensemble. Pattern Recogn. 76, 491–505 (2018)

4. P. Dollár, C.L. Zitnick, Structured forests for fast edge detection, in Proceedings of the IEEE International Conference on Computer Vision, pp. 1841–1848

5. L.F. Nicolas-Alonso, J. Gomez-Gil, Brain computer interfaces, a review. Sensors 12(2), 1211 1279

6. F.M. Bayat, M. Prezioso, B. Chakrabarti, H. Nili, I. Kataeva, D. Strukov, Implementation of multilayer perceptron network with highly uniform passive memristive crossbar circuits. Nat. Commun. 9(1), 1–7 (2018)

7. S. Sharma, Activation functions in neural networks. Towards Data Sci. 6

8. Alsamhi, S. H., N. S. Rajput and M. S. Ansari. Hybrid deep learning model with KNN for intrusion detection system. *Computers, Materials & Continua* **66**(3), 2713–2727 (2020). https://doi.org/10.32604/cmc.2020.012076

9. D. Dasgupta, Z. Akhtar, and S. Sen, "Machine learning in cybersecurity: a comprehensive survey," 10.1177/1548512920951275.

10. P. Odim and R. Shrestha, "Analysis of K-Nearest Neighbor for Network Intrusion Detection," *International Journal of Scientific and Hybrid Research in Engineering (IJSHRE)*, vol. 10, no. 5, pp. 41–47, 2023. Available: https://ijournals.in/wp-content/uploads/2023/06/6.IJSHRE-110508

11. R. A. Faizal, H. F. T. Ahmad, and M. H. Jabar, "Intrusion Detection System Using Random Forest on the NSL-KDD Dataset," *in Proc. Int. Conf. on Electrical Engineering and Informatics (ICEEI)*, IEEE, 2019, pp. 1–6. Available: https://www.researchgate.net/publication/335718695

12. S. H. Shah and S. U. Rehman, "A Comparative Study of Intrusion Detection Systems Applied to NSL-KDD Dataset," *in Proc. Int. Conf. on Emerging Trends in Computer Science and Electronics Engineering (ETCSEE)*, 2022, pp. 45–52. Available: https://www.researchgate.net/publication/357762378

ISSN 3030-3907

13. A. Y. Abdullahi, A. S. Alfa, and M. A. Muhammad, "Performance Evaluation of Intrusion Detection System using Selected Features and Machine Learning Classifiers," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 23, no. 3, pp. 1610–1618, 2021. Available: https://www.researchgate.net/publication/352556899

14. P. S. Vijayarani and S. Sylviaa, "Intrusion Detection System with Customized Machine Learning Techniques for NSL-KDD Dataset," *in Proc. Int. Conf. on Communication and Signal Processing (ICCSP)*, 2023, pp. 1–6. Available: https://www.researchgate.net/publication/376861280

ISSN 3030-3907