EAI Endorsed Transactions
on Internet of Things

Research Article

Cyber Attacks Classification on Enriching IoT Datasets

Alend Hasan Jarjis[1], Nassima Yousef Saleem Alzubaidi[2], Meltem Kurt Pehlivanoğlu[3,*]

[1]Department of Computer Engineering, Kocaeli University, Kocaeli, Turkey
[2]Information Systems Engineering, Kocaeli University, Kocaeli, Turkey
[3]Department of Computer Engineering, Kocaeli University, Kocaeli, Turkey

Abstract

In the era of the 5.0 industry, the use of the Internet of Things (IoT) has increased. The data generates from sensors through IoT industrial systems, any fault in those systems affects their performance and leads to real disaster. Protecting them from any possible attacks is an essential task. to secure any system, it needs to predict in the first place possible attacks and faults that could happen in the future. Predicting and initiating the attack type and the accuracy of these predictions can be done with machine learning models nowadays on the datasets produced with IoT networks. This paper classifies several attacks type based on several criteria and techniques to enhance the performance of machine learning (ML) models such as Voting techniques beside six ML models; Random Forest (RF), Decision Tree (DT), K-nearest neighbor (KNN), Support Vector Machine (SVM), Logistic regression (LR), and eXtreme Gradient Boosting (XGBoost) using Enriching IoT dataset [1]. The results showed that 100% accuracy was achieved in estimating process with the XGBoost model.

Received on 12 February 2023; accepted on 27 July 2023; published on 04 August 2023

Keywords: IoT security, machine learning, security attack, Bot-IoT, Ton-IoT

doi:10.4108/eetiot.v9i3.3030

1. Introduction

The increased use of the Internet of Things, as the IoT market expands quickly produces massive volumes of data being transferred between devices. Security concerns appear because there is a huge number of attacks happening. several ML models generated to detect and classify these attacks [2]. Traditional attack detection techniques cannot be employed effectively in the detection process due to network devices' varied environments and architectures. Additionally, the incidents or attacks that could occur might differ from those that are seen on traditional network devices and the IoT has been significantly noted. Additionally, it has been included in other common applications as well, and it evolves into the direction of the Internet's future and offers users various facilities, whether on a personal level or for a variety of manufacturers. Multiple technologies are being developed by researchers to utilize them for all purposes [3]. IoT-based IDS has grown in popularity and importance as a result of the explosive growth of wireless networking, which leads to a significant increase in IoT devices and IoT infrastructure development. According to research, software-defined networking (SDN)-based IDS and ML are effective tools for quick responses to various IoT network attacks [4].

This paper focuses on classifying the combination of both (Bot and Ton) IoT attacks based on the enriched Bot and Ton IOT attacks of the 2022 dataset from [1]. Firstly, we cleaned the data and then balanced it as there is an obvious size difference in the datasets. We use under-sampling and over-sampling as effective techniques for gaining the best results. Then, we apply various ML models to evaluate and compare their accuracy to classify attacks on six different targeted classes where each attack from both Ton and Bot IoT attacks represents a separate class; (class 0: DDoS Bot-IoT, class 1: dos Bot-IoT, class 2: Scanning Bot-IoT, class 3: DDoS Ton-IoT, class 4: dos Ton-IoT, class 5: Scanning Ton-IoT,). Moreover, compared to other work in the same dataset, the results showed better results on all

*Corresponding author. Email: meltem.kurt@kocaeli.edu.tr

used models. Feature importance techniques are used to check the best 10 features, and the results showed enhancement and better performance. Additionally, several model criteria were changed to enhance the accuracy of the multi-classification models which were successfully applied to all models. Finally, Voting techniques (hard voting, and soft voting) are used for the prementioned ML models that led to the models of improved accuracy and better performance.

The rest of this paper is structured as follows: Section 2 provides a list of related work on attack classification and detection using machine learning models. The dataset description and analysis are explained in Section 3. Section 4 explains the model building and the results. Finally, the conclusion is presented in Section 5.

2. Related works

This section mentions several works that are conducted to attack classification and detection using ML models.

This paper [3], classified DDoS attack traffic as normal or attack using 104.000 data cases for each case. It used five methods for classification purposes namely; DT, SVM, Naive Bayes (NB), and KNN and RF. They achieved the highest accuracy score with the SVM model among the other models in terms of accuracy at 97.37%. While another paper [5], applied a binary classification as well as multi-classification with ML methods artificial neural network (ANN), NB, KNN, DT, SVM, RF, and logistic regression (LR) on Bot-IoT dataset. They indicated that RF achieved the highest accuracy score in binary classification as well as, KNN algorithm achieved the highest accuracy score on all types of attacks in multi-class classification. Moreover, another paper [4], used ML method based on the ensemble trees approach, for attack detection enhancement on IoT-based IDS datasets. Indicating that the used method has the best performance with accuracy 100% and F1 score but worst results with AUC in the v2-ToN-NF-IoT dataset. While this paper [6], used collaborative DDoS detection and classification approach to enhance DDoS detection and classification capabilities, performed on the CICD-DoS2019 dataset. Their results reached over 84.2% accuracy. In addition, [1], applies several ML algorithms to their produced data to classify cybersecurity attacks and the results demonstrated that the new simulated datasets improved the performance by 10% in classifying cybersecurity attacks. Another work [2], uses DT, RF, and GB for attack detection and analysis in IoT 2020 dataset as this paper focuses on category classification. The results demonstrated that the DT algorithm performed better in comparison with GB and RF, however, the RF algorithm showed more satisfied results with AUC scores. This paper [7], tested various ML methods that find the problems of binary and multi-class classification while employing them on ToN-IoT datasets that are collected from scaled and, diversified networks, the Chi-square (Chi2) is used to select features and SMOTE technique are used to balance the classes. The paper indicates that the XGBoost performs better than all other used methods. Another paper [8] aimed to use low power, and rate, as well as, the networks with short range to detect attacks by using SVM model and then evaluating using C-SVM and the OC-SVM. The results showed that the C-SVM has the best results with a classification accuracy of 100% and 81% accuracy when operating in an unknown topology. To conclude, most of the mentioned works are using ML techniques to classify or detect network attacks on IoT networks using either Bot-IOT or Ton-IOT datasets despite [1] and [4] that using both sources of the attack data as it is shown in (Table 1).

Table 1. Related work studies comparison.

Study	*Technique*	*Dataset*	*Performance* metrics	*Category*
[3]	RF,KNN DT,SVM	Private	Accuracy F1 score Recall Precision	Classify DDoS Attack
[5]	RF DT,SVM KNN,ANN LR	IoT-Bot	Accuracy F1 score Recall Precision Log Loss CK	Classify Attack based IoT-Bot
[4]	DT, RF	IoT-based IDS	Accuracy F1 score AUC	Detect Attack based IoT-Dataset
[6]	Federated Learning based Methods	CICD-DoS2019 dataset	Performance	Classify DDoS Attack
[1]	RF, DT SVM,KNN ANN LR,GB LDA,ETC	Enriched IoT-dataset	Accuracy F1 score Recall Precision	Classify IoT Attacks
[2]	RF, DT GBM	IoT-2020 dataset	Accuracy AUC	Predict network attacks on IoT
[7]	RF, DT SVM,KNN LR,XGB NB	TON-IoT	Accuracy F1 score Recall Precision FPR	Classify TON-IoT Attacks
[8]	C-SVM OC-SVM	Private	Accuracy MCC Recall Precision	Classify IoT Attacks
This Study	RF, DT SVM,KNN XGB	Enriched IoT-dataset	Accuracy F1 score Recall Precision	Classify IoT-BOT IOT-TON attacks

3. Data description and analysis

3.1. Dataset

The used dataset for this paper is the Enriched IoT dataset from [1]. The dataset consists of Ton IoT attacks and Bot IoT attacks that have been enriched in features and volume of the sources and behavior of the given attack. It consists of the following attacks forms: The Bot-IoT attacks that are in the used dataset are:

- DoS attack: An attack that deliberately targets to overwhelm the traffic of an IoT device internet or the infrastructure around it (sensors). Because of this attack, the IoT device will be unavailable to its intended users [9].
- DDoS attack: A DoS-like attack that floods a targeted IoT device with many attack resources (computers) [9].
- Scanning attack: An infiltration attack style that scans the operating system of the targeted Internet of Things device with the Nmap tool to find network flaws [9].

The Ton-IoT attacks that are in the used dataset are:

- DoS attack: it considers one of the flooding malicious behaviors. A sequence of actions is carried out by the attacker to disrupt services. DoS attacks aim to make services unavailable [7].
- DDoS attack: is typically carried out using networks of bots. Malicious aims to overload the IoT resources that are connected, which depletes the devices [7].
- Scanning attack: the attacker uses scanning to obtain information about the system. The information includes the services that are present on a targeted system and the ports that are opened. Before beginning any kind of attack, the attacker performs scanning [7].

For that, we decided to classify the mentioned attacks, and as a result, our dataset consists of (6) classes as it is shown in (Table 2). The first class is 'class 0' which represents the DDoS attacks on Bot-IoT attacks, while 'class 1' shows DoS of Bot-IoT attacks, 'class 2' is a scanning attack on Bot-IoT, 'class 3' represents DDoS attacks on Ton-IoT attacks, 'class 4' DoS Ton-IoT attacks, and finally, 'class 5' represents scanning attacks on Ton-IoT.

Table 2. Attacks classes.

Class	Attack field	Attack category
0	Bot-IoT	DDos
1	Bot-IoT	Dos
2	Bot-IoT	Scanning
3	Ton-IoT	DDos
4	Ton-IoT	Dos
5	Ton-IoT	Scanning

3.2. Data pre-processing

For any ML project, the core process is data pre-processing and cleaning. For this paper, several pre-processing and cleaning datasets are performed to produce clean raw data so that machine learning algorithms can make accurate predictions. The dataset consists of a bunch of empty unnamed columns, as well as null values cells, columns with most values zero, all are dropped.

3.3. Feature selection

It is important to select suitable features to be used with machine learning algorithms. Features need to be predictable to help give accurate results. According to [1], proposed several features in their produced dataset namely; connectivity features, dynamic features, and layered features, the best features that provided accurate results from machine learning algorithms are the dynamic features. Therefore, for this paper, we select most of our data from dynamic features. we used 8 dynamic features beside 2 connectivity features, and one layered feature (Table 3), to assist algorithms in a better classification process

- Connectivity Features: it consists of features that hold the group of packet characteristics that have a relation amongst them.
- Dynamic features: it holds the group of packets' statistical features.
- Layered features: it studies the network protocol behavior used in several layers of the network.

3.4. Scaling and normalization

The features of the used dataset have various values that vary in length. This variation may lead to incorrect outcomes as the used algorithm may be biased toward features with bigger values. For that, we used scaling and techniques for our selected features. This paper used standard scalar techniques for scaling purposes using the bellow (Equation 1) where x parameter indicates the sample data, u represent the mean of the training samples and s is for the standard deviation of the training samples [10].

$$z = \frac{x-u}{s} \quad (1)$$

Table 3. Classes features.

Dynamic features	
Min	The packet's minimum length
Max	The packet maximum length
Std	Packets standard deviation length
Protocol Name	Integer values of protocols (UDP,TCP and IP)
Tot sum	the overall bytes of Packets
AVG	Packets Average size
Radius	The squared root of two streams variances
Number	The packet-count number
Connectivity features	
ts	The time stamp
Header Length	header transactions total number of bytes
Layered features	
MAC address	A tunnel of access and address techniques

3.5. Data balancing

Unbalanced datasets lead to the lowest probability performance of machine learning results. That makes the algorithm biased to the majority side and trains the model on it which leads to biased and not accurate evaluations. The dataset we use is highly unbalanced where the size of the dataset samples of the DDoS attack was much more than the remaining attacks as it is shown in (Figure 1). We used (sampling and oversampling) techniques together to have a balanced dataset labeling. Undersampling is the action of reducing the number of most of the aimed instances. Tomeks' links, cluster centroids, and other techniques are a few of the frequently used under-sampling techniques and oversampling can be done by increasing the number of minority class instances or samples with the generation of new samples or the repetition of some of the samples [11].

However, in our version, it is not desirable to lose a very large amount of data from a part while containing valuable data for predictions when under-sampling. Similarly, not feeding the minority part with large amounts of not real data. Therefore, we use both techniques and feed them with a fixed proportion to be balanced on both sides. For that, first of all, the class of labels has been created to be able to do balancing techniques on them, Secondly, the datasets that have a high proportion are under-sampled to a specific size. And the datasets with low proportions are balanced to be more with oversampling technique. As a result, the used dataset is balanced with a similar proportion for each label as shown in (Figure 2).

4. Model building and results

After the balancing process, the dataset is divided into two parts (X and Y) where (X) consists of all selected features (Table 3) that will be used for predictions in machine learning models while (Y) handles the labels that represent the actual part to be used for comparing results. Then the data has been divided to train and test sets giving (0.3) of the data to the test set.

For this study, we used four types of machine learning models that are used for multiclass classification purposes namely; random forest, decision tree, KNN, SVM, and XGBoost.

- RF: is the approach that combines several DTs to provide a more accurate model of the data classes [7].
- DT: is a construction technique that represents a tree with its branches and leaves. The inner nodes are the classification constraints; the branch displays the results [7].
- KNN: the method that does not produce any probabilities about how the specified data will be distributed and it is a fundamental strategy that assigns new samples from a test data to the nearest sample of training data based on particular metrics [7].
- SVM: A method that uses hyperplanes to divide training data and makes classification of future predicted results [5].
- XGBoost: its design is primarily based on gradient boost decision trees. XGBoost has been recognized as an accurate performance fast algorithm in comparison to different ML algorithms. It represents a method to lead the boosting in the machine. For tree boosting mechanisms, XGBoost aids in scalable memory and hardware resources [7].

We implement several algorithms, including DT, RF, KNN, SVM, and XGBoost on the enriched Bot and Ton IoT dataset [1]. We compare the accuracy of these models. Then we measure the accuracy and performance using classification reports (precision, recall, and f1 score).

4.1. Dataset Training and Validation

The training process is conducted by applying different classification algorithms to generate a model to be used in calculating predictions from unseen data.

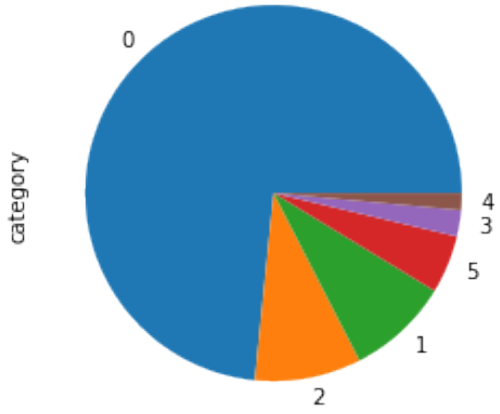

Figure 1. Class portions of the data set before balancing

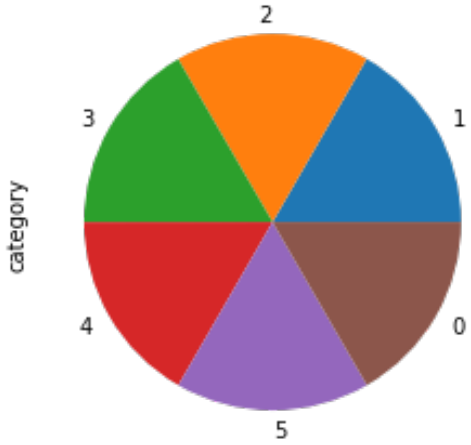

Figure 2. Class portions of the data set after balancing

As we mentioned before, in [1], the authors used the same dataset as us. Firstly, we compared our models to their models by using the same hyper-parameters given in Table 4. Note that, these parameters are taken from [1]. Our results show enhancement in all used ML models compared to their results. Table 5 shows comparable results from both works.

Table 4. Machine learning algorithms hyper-parameters

Algorithm	Hyperparameters
RF	Max depth = 3
KNN	K=3
DT	Criterion = gini, min samples split =2
SVM	C = 1.0
XGB	Learning rate=0.1, min samples split=2

Secondly, to get better results we tried to find the optimal hyper-parameters. Table 6 shows the results in better performance compared to previous results this is after changing several hyper-parameters of each ML algorithm. In RF besides max_depth=3, we added minimum samples split=3, and minimum samples leaf =2. For the DT, we add minimum samples split=2, splitter="random", and minimum samples leaf=2. While SVM has kernel = linear, C = 2.0, and gamma= auto features. In addition, KNN n_neighbors = 3, leaf_size=40, weights="distance", algorithm="brute".

Addressing the essential features that enhance our models, increase credibility in model predictions, and eliminate undesired behavior that can be done by feature importance [12] allows us to achieve one of the main goals of ML algorithms which is to gain accurate prediction and classification after conducting feature importance. Thirdly, in this paper it improves the performance as shown in the results (Table 7), depending on the most 10 important features (AR_P_Proto_P_sport, AR_P_Proto_P_dport, AR_P_Proto_P_SrcIP, average_flow_duration, dst_ip_bytes, Sbytes, UDP, sum_flow_duration, Destination IP and flow_idle_time). As well as conducting a Logistic regression model (LR) which is a statistical model constructed to assess and explain the relationship between dependent variables—whether binary or binomial or having more than two values—and independent variables [13] that provide very satisfying performance.

Researchers are increasingly using ensemble learning models in the field of predictive modelings, such as regression and voting classifiers [14]. Voting ensemble refers to an ensemble machine learning model that combines many multivariate ML models with the goal of enhancing the performance of each model and improving classification performance as a whole [14]. There are two main voting models soft and hard voting.

- Hard voting: based on the vast majority of ML algorithm predictions in the ensemble, generates a whole class prediction [15].
- Soft voting: achieves final class prediction using an ML classifier's confidence based on class prediction probability [15].

Finally, we applied voting models. The parameters and their values of ML Algorithms and ensemble models are shown in (Table 8), as well as the results of hard and soft voting are shown in (Table 9) where we can find that in comparison to the individual models, the hard and soft voting models gives better performance.

Table 5. Results comparison by using the same hyper-parameters given in [1].

This Paper	Metrics	RF	KNN	DT	SVM	XGB
	Precision	0.99018	0.9136	0.99979	0.81857	1.000000
	Recall	0.990257	0.91278	0.99973	0.786030	1.000000
	F1 score	0.990175	0.91233	0.99978	0.783414	1.000000
	Accuracy	0.990214	0.91231	0.99979	0.787336	1.000000
[1]	Precision	0.9814	0.8189	0.9996	0.7780	0.9987
	Recall	0.9766	0.8196	0.9996	0.7713	0.9986
	F1 score	0.9762	0.8141	0.9996	0.7641	0.9986
	Accuracy	0.9766	0.8196	0.9996	0.7713	0.9986

Table 6. Results with the optimal parameters.

Metrics	RF	KNN	DT	SVM	XGB
Precision	0.992424	0.94657	1.000000	0.835593	1.000000
Recall	0.992273	0.94387	1.000000	0.798170	1.000000
F1 score	0.992327	0.94359	1.000000	0.797236	1.000000
Accuracy	0.992389	0.94423	1.000000	0.798465	1.000000

Table 7. Feature importance results.

Metrics	RF	KNN	DT	SVM	XGB	LR
Precision	0.997161	0.99029	0.999808	0.979037	1.000000	0.980475
Recall	0.997148	0.99035	0.999810	0.978836	1.000000	0.980270
F1 score	0.997135	0.99029	0.999809	0.978910	1.000000	0.980330
Accuracy	0.997122	0.99034	0.999808	0.978766	1.000000	0.980301

5. Conclusion

In this paper, we used ML techniques to classify Bot-IOT and Ton-IOT attacks. The label of the actual attack consists of several features that should be classified accordingly by attack field and category. The predictions are conducted and compared to the actual classes. The dataset is balanced using oversampling and under-sampling techniques and scaled and normalized before using it in the ML models. Hard voting and soft voting techniques were conducted on the ML models for the best results.

As a future work and based on the findings of this paper, there are multiple potential directions for the future in the area of attack classification on IoT networks that will enhance the development of effective and adaptable machine learning models. Moreover, Graph Neural Networks (GNN) can be used in detecting and classifying attacks, because in [16–18], the results showed that neural network algorithms, especially GNNs, show a good performance in detecting and classifying attacks. Furthermore, our objectives include gathering a novel dataset comprising diverse attacks, which will be selected based on distinct criteria to accurately depict various network traffic scenarios.

Acknowledgment

Meltem Kurt Pehlivanoğlu is partially supported by the Scientific Research Project Department of Kocaeli University under Project No: FBA-2019-1618.

References

[1] Erfani, M., Shoeleh, F., Dadkhah, S., Kaur, B., Xiong, P., Iqbal, S., Ray, S. *et al.* (2021) A feature exploration approach for iot attack type classification. In *2021 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)* (IEEE): 582–588.

[2] Su, J., He, S. and Wu, Y. (2022) Features selection and prediction for iot attacks. *High-Confidence Computing* **2**(2): 100047.

[3] Elsherif, A.A. (2020) Ddos botnets attacks detection in anomaly traffic: A comparative study. *Journal of Information Security and Cybercrimes Research* **3**(1): 64–74.

[4] Le, T.T.H., Kim, H., Kang, H. and Kim, H. (2022) Classification and explanation for intrusion detection system based on ensemble trees and shap method. *Sensors* **22**(3): 1154.

[5] Churcher, A., Ullah, R., Ahmad, J., Ur Rehman, S., Masood, F., Gogate, M., Alqahtani, F. *et al.* (2021) An experimental analysis of attack classification using machine learning in iot networks. *Sensors* **21**(2): 446.

[6] Neto, E., Dadkhah, S. and Ghorbani, A. (2022) Collaborative ddos detection in distributed multi-tenant iot using federated learning: 1–10. doi:10.1109/PST55820.2022.9851984.

[7] Gad, A.R., Nashat, A.A. and Barkat, T.M. (2021) Intrusion detection system using machine learning for vehicular ad hoc networks based on ton-iot dataset. *IEEE Access* **9**: 142206–142217.

Table 8. ML Algorithms and ensemble models' parameters.

ML Algorithms	Classifier	Parameters
	RF	n_estimators=100, random_state=42
	DT	max_depth=8,criterion="gini", min_samples_split=2 splitter="random", min_samples_leaf=2
	SVM	gamma="scale", random_state=42
	XGB	learning_rate=0.1,min_samples_split=2
	LR	solver="lbfgs", random_state=42
Ensemble models	Hard voting	voting:"hard", weights: "None", n_jobs:"None" flatten_transform:"True"
	Soft voting	voting:"soft", weights: "None", n_jobs:"None" flatten_transform:"True"

Table 9. Hard and soft voting results.

Hard Voting	Metrics	RF	DT	SVM	XGB	LR	Voting Classifier
	Precision	1.000000	0.999810	0.979037	1.000000	0.981863	0.999362
	Recall	1.000000	0.999808	0.978836	1.000000	0.981753	0.999367
	F1 score	1.000000	0.999809	0.978910	1.000000	0.981740	0.999363
	Accuracy	1.000000	0.999808	0.978766	1.000000	0.981644	0.999360
Soft Voting	Precision	1.00000	0.99987	0.98077	1.00000	0.98047	0.99905
	Recall	1.00000	0.99987	0.98043	1.00000	0.98027	0.99903
	F1 score	1.00000	0.99987	0.98056	1.00000	0.98033	0.99904
	Accuracy	1.00000	0.99987	0.98049	1.00000	0.98030	0.99904

[8] Ioannou, C. and Vassiliou, V. (2021) Network attack classification in iot using support vector machines. *Journal of Sensor and Actuator Networks* **10**(3): 58.

[9] Shahin, M., Chen, F., Bouzary, H., Hosseinzadeh, A. and Rashidifar, R., A novel fully convolutional neural network approach for detection and classification of attacks on industrial iot devices in smart manufacturing systems. doi:10.21203/rs.3.rs-1739779/v1.

[10] Singh, D. and Singh, B. (2020) Investigating the impact of data normalization on classification performance. *Applied Soft Computing* **97**: 105524.

[11] Mohammed, R., Rawashdeh, J. and Abdullah, M. (2020) Machine learning with oversampling and undersampling techniques: overview study and experimental results. In *2020 11th international conference on information and communication systems (ICICS)* (IEEE): 243–248.

[12] Hooker, S., Erhan, D., Kindermans, P.J. and Kim, B. (2019) A benchmark for interpretability methods in deep neural networks. *Advances in neural information processing systems* **32**.

[13] Domínguez-Almendros, S., Benítez-Parejo, N. and Gonzalez-Ramirez, A. (2011) Logistic regression models. *Allergologia et Immunopathologia* **39**(5): 295–305. doi:https://doi.org/10.1016/j.aller.2011.05.002, URL https://www.sciencedirect.com/science/article/pii/S0301054611002011.

[14] Peppes, N., Daskalakis, E., Alexakis, T., Adamopoulou, E. and Demestichas, K. (2021) Performance of machine learning-based multi-model voting ensemble methods for network threat detection in agriculture 4.0. *Sensors* **21**(22). URL https://www.mdpi.com/1424-8220/21/22/7475.

[15] Özçift, A. (2020) Medical sentiment analysis based on soft voting ensemble algorithm. *Yönetim Bilişim Sistemleri Dergisi* **6**(1): 42–50.

[16] Jiang, W. (2022) Graph-based deep learning for communication networks: A survey. *Computer Communications* **185**: 40–54.

[17] Huoh, T.L., Luo, Y. and Zhang, T. (2021) Encrypted network traffic classification using a geometric learning model. In *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)* (IEEE): 376–383.

[18] Busch, J., Kocheturov, A., Tresp, V. and Seidl, T. (2021) Nf-gnn: Network flow graph neural networks for malware detection and classification. In *33rd International Conference on Scientific and Statistical Database Management*: 121–132.