Ali Abbasov
Kamil Aida-zade (Eds.)

BOOK OF SELECTED PAPERS

6th International Conference on

Problems of Cybernetics and Informatics

PCI 2025

August 25-28, 2025
Baku, Azerbaijan

Ali Abbasov
Kamil Aida-zade
Editors

BOOK OF SELECTED PAPERS

6th International Conference on

Problems of Cybernetics and Informatics

PCI 2025

August 25-28, 2025
Baku, Azerbaijan

Cloud Cyber Attack Images Classification using GAN and ViT+ML Algorithms

Fargana Abdullayeva
Department of Information Security
Institute of Information Technology
Baku, Azerbaijan
a_farqana@mail.ru
https://orcid.org/0000-0003-2288-6255

Gurban Farajov
Department of Information Security
Institute of Information Technology,
Baku, Azerbaijan
farajovqurban@gmail.com

***Abstract*—The emergence of the Industry 4.0 concept and the development of modern technologies have made the detection of cyber attacks in cloud systems an important issue. In the article, a hybrid model based on the combination of machine learning algorithms with Generative Adversarial Networks (GANs) was developed to identify various attack categories targeting cloud systems. In the model, the integration of functions that enhance image quality within the GAN algorithm significantly improved classification performance by increasing the quality of cyber attack images. Here, the damage in the images is repaired, and their appearance is restored and generated to resemble the original as closely as possible. To enhance the model's robustness against various changes in input images, during the data augmentation phase, the process of rotating images and generating them in different variations was also carried out using GAN. The proposed method classified various cyber attacks on cloud systems more effectively than existing methods, achieving a classification accuracy of 0.9451.**

***Keywords*—Deep learning, GANs, CatBoost, Cyber Attacks, vision transformer (ViT)**

Introduction

Cloud systems are one of the main technological pillars enabling the digitalization and automation of industrial enterprises within the framework of Industry 4.0. These systems play a crucial role in the processing of big data, the application of artificial intelligence, and the optimization of production processes [1]. Accessibility from anywhere, scalability, multi-tenancy, and the ability to process complex tasks in parallel are among the advantages of cloud systems [2]. Cloud systems are widely used in the finance, military, healthcare, education, energy, transportation, and e-government sectors [3]. The widespread use of cloud systems across various fields has exposed them to different types of cyber attacks. In cloud systems, the main cyber attacks occur in components such as the network, infrastructure, software, access and account management, and data protection. The realization of these cyber attacks can result in the destruction of target assets and cause significant economic damage. Timely detection of these cyber attacks is considered a critical issue.

There have been real cyber attack incidents targeting cloud systems. On February 21, 2018, hackers gained access to Tesla's Amazon Web Services (AWS) cloud account and used the service (a computer operating on the internet) to mine cryptocurrency [4]. This incident occurred due to configuration errors in the cloud systems, lack of monitoring, and absence of mechanisms for detecting anomalies. In 2014, the account information of the company Code Spaces was compromised on AWS [5]. The attackers who took control were able to delete all customer data belonging to Code Spaces. This incident occurred due to the absence of a multi-factor authentication mechanism. In 2025, the SaaS service hosted on the Microsoft Azure platform by Commvault, a company operating in the field of data protection, was affected by cyber attacks exploiting a zero-day vulnerability [6]. The attackers gained unauthorized access to customers' confidential data and took control of their SaaS services. In 2023, as a result of a cyber attack on Ukraine's huge mobile network Kyivstar, customer access to telephone station and the internet network was disrupted, and the cloud storage and backup systems were destroyed [7].

There are various types of DoS cyber attacks that target the services and resources of cloud systems [8]: DOS Golden, DOS Hulk, DOS Slow, DOS slowloris. These attacks primarily target the availability, service level agreement (SLA), and performance of the cloud. In addition, cyber attacks such as FTP Patator, SSH Patator, and web attack brute force, which are aimed at capturing account login passwords on cloud platforms, are also common [9]. Another type of attack is port scanning. Hackers carry out this attack to identify potential vulnerabilities in the cloud and gather information about open ports. Cyber attacks such as Heartbleed, infiltration, SQL injection, and XSS are also threats that can be executed in cloud systems.

Numerous approaches have been developed for detecting cloud cyber attacks. Compared to traditional methods based on the analysis of conventional features, image-based methods are more effective in detecting cyber attacks [10]. These methods can detect spatial dependencies and contextual relationships with high accuracy, which are often overlooked by traditional feature engineering techniques when identifying cyber attacks. Spatial dependencies refer to how closely pixels are positioned relative to each other. Contextual relationships refer to how different parts of an image are positioned in relation to one another. Existing approaches first segment the images to detect cyber attacks. However, during the segmentation process, useful parts of the image may be cut out and excluded from the analysis. This reduces the confidence in the effectiveness of cyber attack detection systems. In smart systems like the cloud, methods for detecting cyber attacks based on image analysis should include components such as self-attention mechanisms, filtering, and restoration of blurred images.

RELATED WORKS

This section analysis works related to the topic. In [10] a Gaussian mixture model (GMM) based probabilistic model was proposed for detecting malware based on image analysis. In this approach, malware is detected by evaluating the similarity of images. Primarily, changes made in the images are identified. In [11], the DDoSViT approach was proposed for detecting cyber attacks targeting Internet of Things (IoT) devices. The proposed multi-vector DDoS and DoS attack detection approach based on ViT converts attack flows into images and trains ViT on the attack image dataset. The CICIoT2023 and CICIoMT2024 datasets were used for conducting experiments. The effectiveness of the model was evaluated based on accuracy, precision, recall, and F1-score metrics. In [12], gray-scale images were analyzed for malware detection in GCS (Grid Computing Systems). The proposed hybrid model consists of ResNet-50 and Support Vector Machine (SVM). ResNet-50 is used to extract relevant features from the images, while SVM classifies the malware based on the extracted features. In [13], a hybrid method based on multi-objective optimization was proposed, allowing the use of the most efficient features of lightweight deep learning models for cyber attack detection. First, QR code images are generated from large volumes of data with many classes. Then, QR code images are trained on neural networks using CNN models such as MobileNetV2 and ShuffleNet. Features are extracted from the trained images, and the Harris Hawk Optimization (HHO) algorithm is used to select the most effective features for classification purposes. In [14], a supervised machine learning approach was proposed for cyber attack detection. Random Forest, K-Nearest Neighbors (KNN), and Logistic Regression algorithms were used to classify the data into normal and cyber attack categories. In [15], a method for detecting malware based on resource consumption metrics using transformers was proposed. Here, the input data is encoded as a sequence of processes, and each process is described by its resource consumption metrics (CPU, memory, and disk usage). In [16], the application of ViT for detecting cyber threats related to malware and network intrusions was examined. To address this problem, a deep neural network called VINCENT (ViT-based distillation for Cyber-Threat detection) was proposed, which converts cyber threat data into vectors of color images. The ViT block of this model is trained on images to extract visual features from the data for each class. In [17], a ResDNViT approach was proposed by combining ViT and ResNet models for detecting NetFlow-based cyber attacks. In the ResDNViT model, the ViT-based architecture analyzes network traffic by representing NetFlow features as 2D matrices and dividing them into equal-sized submatrices, which serve as input fragments for the encoder component. In [18], a deep learning model was developed for detecting various types of cyber attacks. The algorithm emphasizes the importance of feature selection, and the significance of attention mechanisms for improving feature evaluation within the same model is analyzed. In [19], the application potential of transformers and large language models (LLMs) in cyber threat detection systems was investigated. The fundamentals of transformers, various types of cyber attacks, and the datasets used in this field were discussed. The study explored the use of attention-based models, BERT-type LLMs, GPT, CNN/LSTM-transformer hybrids, and hybrid models such as ViT in intrusion detection systems.

PROPOSED METHOD

The architecture of the proposed approach for detecting cyber attacks in cloud systems is illustrated in Figure 1.

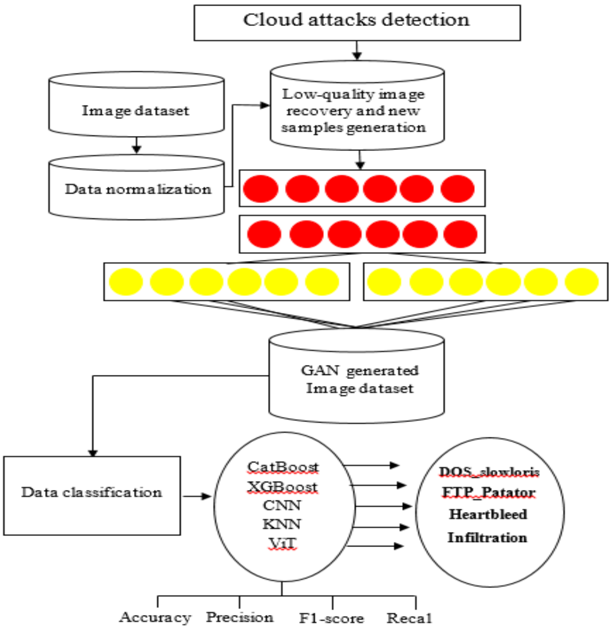


Fig 1. Cloud attacks detection approach

As seen in Fig. 1, the graphical abstract illustrates a hybrid approach that combines GANs with machine learning techniques. The approach consists of the following stages:

In the first stage, GANs are used to restore blurred images and generate new samples based on high-quality images. Subsequently, GANs are also applied to address the class imbalance problem.

In the second stage, feature extraction was performed on the dataset. Each image was first resized to (32, 32, 1), and then converted into a 1024-dimensional vector consisting of pixel intensity values.

In the third stage, the feature vectors composed of pixel values were fed into classifiers to categorize the cyber attack data into different classes.

The operations performed on the data significantly improved the detection accuracy of the proposed approach for cyber attacks. To evaluate its effectiveness, GAN+CatBoost, GAN+XGBoost, and GAN+KNN models were developed for detecting cyber attacks in cloud environments. Compared to traditional methods, the proposed approach demonstrated superior performance.

EXPERIMENTS

For the experiments the Cloud Attack Dataset was used [16]. The Cloud Attack Dataset was created based on the CIC-IDS 2017 dataset from the Canadian Institute for Cyber security. A total of 100,541 traffic samples were extracted from the dataset. These samples belong to 14 traffic classes: one class represents benign traffic, while the other 13 represent attack classes. The network samples were converted into 9x9 sized traffic images. The experiments were carried out on the Linux operating system using the Python 3.9 programming package. Several image samples from the dataset are shown in Figure 2.

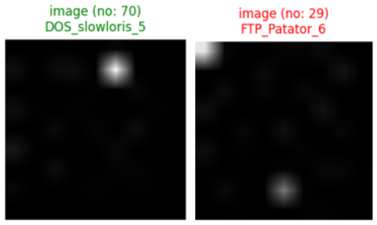


Fig. 2. Cloud Attack Dataset image samples

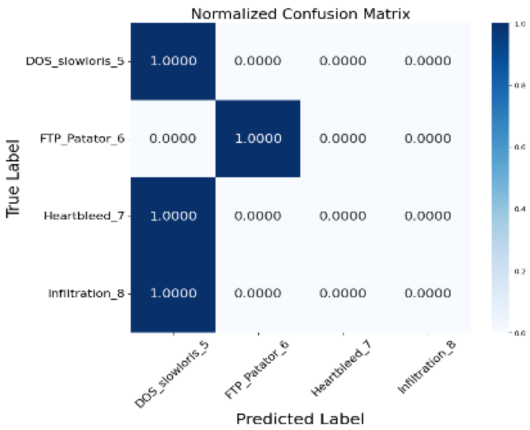
The effectiveness of the methods was evaluated based on accuracy, precision, recall, and F1-score metrics, and the obtained results are presented in Table 1.

Table 1. Comparative analysis of the methods based on the Recall metric

Method Class	CatBoost	GAN+ CatBoost	XGBoost	GAN+ XGBoost	KNN	GAN+ KNN
DOS Slowloris	1.0000	1.0000	0.9815	0.9929	0.9940	0.9965
FTP Patator	1.0000	1.0000	1.0000	1.0000	0.4444	0.9648
Heartbleed	0.0000	0.9852	0.0000	0.9925	0.0000	0.9852
Infiltration	0.0000	0.9754	0.5000	0.9520	0.0000	0.9836

It should be noted that there is a significant class imbalance in the Cloud Attack Dataset. For instance, the DoS Slowloris class contains 635 samples, the FTP Patator class has 59, the Heartbleed class has 11, and the Infiltration class has 24 samples. Due to the small number of samples in some classes, classification using existing machine learning methods resulted in very low performance across all metrics. For example, when applying the CatBoost algorithm to the dataset, classes 1 and 2 were recognized with 100% accuracy according to the Recall metric, whereas samples from the Heartbleed and Infiltration classes were not detected at all by the algorithm, resulting in a recall of 0%. However, the proposed GAN+CatBoost algorithm demonstrated high accuracy in detecting each class. Specifically, this method was able to recognize samples from the DoS Slowloris and FTP Patator classes with 100% accuracy, Heartbleed samples with 0.9852 accuracy, and Infiltration samples with 0.9754 accuracy.

The confusion matrices of the CatBoost and GAN+CatBoost algorithms are illustrated in Figure 3.



CatBoost simple

GAN+CatBoost

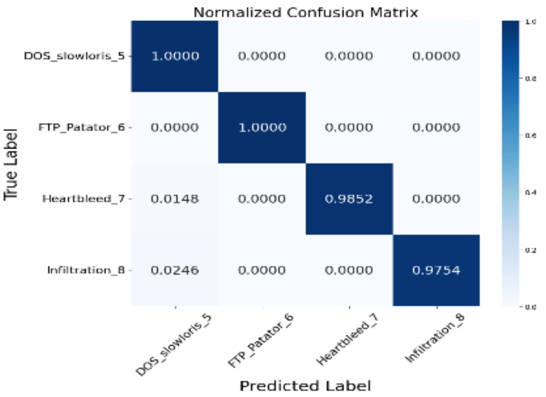
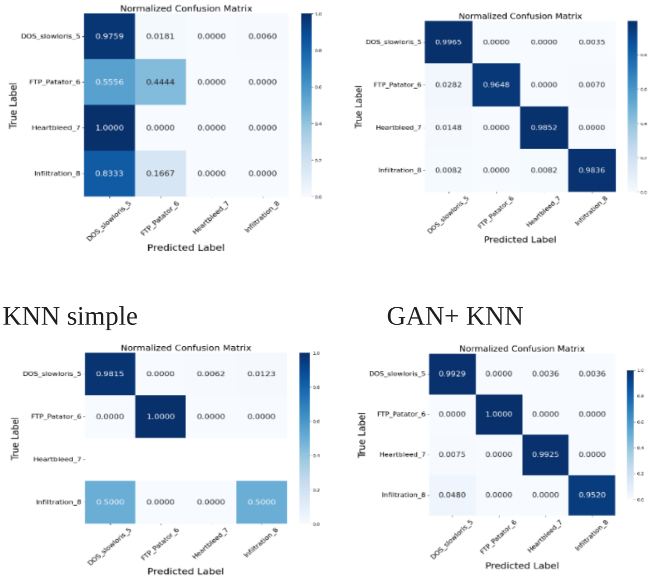


Fig. 3. Confusion matrix of the CatBoost and GAN+CatBoost

As seen in the figure 3, in the first matrix, the samples from the first two classes were recognized with high accuracy by the CatBoost algorithm. However, the algorithm misclassified samples from the other two classes, assigning them to the first class. In this case, the elements of the matrix could not be accurately aligned along the diagonal. In contrast, the second matrix shows the opposite scenario. Here, the proposed GAN+CatBoost algorithm was able to accurately recognize samples from each class, and the matrix elements were precisely aligned along the diagonal.

The confusion matrices of the XGBoost, GAN+XGBoost, KNN, and GAN+KNN algorithms are presented in Figure 4.



KNN simple

GAN+ KNN

XGBoost simple simple

GAN+ XGBoost

Fig. 4. Confusion matrices of the KNN, GAN+KNN, XGBoost, and GAN+XGBoost algorithms

Comparative analysis of the methods based on the Precision metric is presented in Table 2.

Table 2. Comparative analysis of the methods based on the Precision metric

Method / Class	Catboost	GAN+ Catboost	XGBoost	GAN+ XGBoost	KNN	GAN+ KNN
DOS Slowloris	0.9540	0.9827	0.9815	0.9754	0.9429	0.9759
FTP Patator	1.0000	1.0000	1.0000	1.0000	0.6667	1.0000
Heartbleed	0.0000	1.0000	0.0000	0.9925	0.0000	0.9925
Infiltration	0.0000	1.0000	0.6000	0.9917	0.0000	0.9836

Comparative analysis of the methods based on the F1-score metric is presented in Table 3.

Table 3. Comparative analysis of the methods based on the F1-score metric

Method / Class	Catboost	GAN+ Catboost	XGBoost	GAN+ XGBoost	KNN	GAN+ KNN
DOS Slowloris	0.9765	0.9913	0.9815	0.9841	0.9677	0.9965
FTP Patator	1.0000	1.0000	1.0000	1.0000	0.5333	0.9648
Heartbleed	0.0000	0.9925	0.0000	0.9925	0.0000	0.9852
Infiltration	0.0000	0.9876	0.5455	0.9714	0.0000	0.9836

As seen from Table 2 and Table 3, the proposed approach achieved higher Precision and F1-score values across all classes compared to the existing methods.

When image transformations were applied to the dataset and feature reduction techniques were used on the resulting tabular data, better results were achieved across all classes in the dataset. For this purpose, the ViT model was used for feature extraction, and PCA with 45 components was applied for feature reduction. The results obtained on the dataset using the proposed GAN+ViT+PCA+CatBoost model are presented in Table 4.

Table 4. Classification results of the GAN+ViT +PCA+CatBoost model

Method / Class	Precision	Recall	F1-score	Overall accuracy of the model
DOS Slowloris	0.9187	0.9912	0.9536	0.9451
FTP Patator	0.9608	0.8750	0.9159	
Heartbleed	0.9412	0.9412	0.9412	
Infiltration	1.0000	0.9231	0.9600	

As seen from the table 4, the proposed GAN+ ViT+PCA+CatBoost model was able to classify samples from the DoS Slowloris, FTP Patator, Heartbleed, and Infiltration classes with high accuracy. The model achieved an accuracy score of 0.9451.

However, the classification results of the simple ViT+CatBoost model, which was built without applying GAN and PCA techniques, were lower compared to the GAN+ ViT+PCA+CatBoost model. The classification results of the ViT+CatBoost model are presented in Table 5.

Table 5. Classification results of the ViT+CatBoost model

Method / Class	Precision	Recall	F1-score	Overall accuracy of the model
DOS Slowloris	0.9014	1.0000	0.9481	0.9041
FTP Patator	1.0000	0.2857	0.4444	
Heartbleed	0.0000	0.0000	0.0000	
Infiltration	0.0000	0.0000	0.0000	

As seen from the table 5, while the ViT+CatBoost model was able to classify samples from the DoS Slowloris class with high accuracy, it failed to recognize samples from the other three classes.

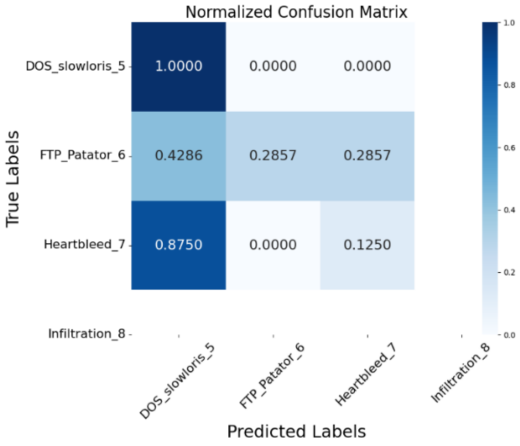
The comparative analysis of the ViT+CatBoost and ViT+GAN+PCA+CatBoost models based on the precision metric is presented in Table 6.

Table 6. Analysis of the precision metrics of the ViT+CatBoost and GAN+ ViT+PCA+CatBoost models

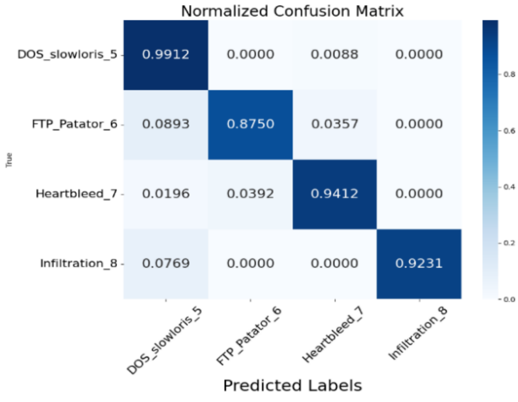
Method / Class	ViT+CatBoost	GAN+ ViT+PCA+CatBoost
DOS Slowloris	0.9014	0.9187
FTP Patator	1.0000	0.9608
Heartbleed	0.0000	0.9412
Infiltration	0.0000	1.0000

It is clearly evident from Table 6 that the GAN+ ViT+PCA+CatBoost model accurately recognized the Cloud Attack Dataset images with high precision.

The confusion matrices of the ViT+CatBoost and GAN+ ViT+PCA+CatBoost algorithms are presented in Figure 5.



ViT+CatBoost



GAN+ViT+PCA+CatBoost

Fig. 5. Confusion matrix of the ViT+CatBoost and GAN+ViT+PCA+CatBoost models

As seen from the confusion matrix, constructing the more complex GAN+ViT+PCA+CatBoost model significantly improved the classification results. This is an expected outcome.

CONCLUSION

In this paper, images from the Cloud Attack Dataset were used to detect cyber attacks on cloud systems. The proposed approach is based on the combination of GAN and machine learning models, which enabled the achievement of high performance in cyber attack detection. The workflow of the approach begins with a preprocessing stage. In this stage, a sharpening operation within the GAN is applied to enhance important image details, filtering is used to remove noise, and rotation is employed to generate image variations.

In the next stage, normalization and data augmentation are performed to improve robustness and eliminate class imbalance in the dataset. During the experiments, 80% of the dataset samples were used for training and 20% for testing. Accuracy, Precision, Recall, and F1-score metrics were used to evaluate the model's effectiveness. The proposed model achieved 0.9451% accuracy in detecting cloud cyber attacks.

However, the extremely small number of samples in some classes of the Cloud Attack Dataset required complex preprocessing operations. In future work, we plan to propose more advanced preprocessing techniques to further improve detection accuracy for cloud-based cyber attacks.

Acknowledgments

This work was supported by the Science Foundation of the State Oil Company of Azerbaijan Republic (SOCAR) (Contract No 01LR-EF/2024)

REFERENCES

[1] M.H. Onik, C.S. Kim, J. Yang, “Personal data privacy challenges of the fourth industrial revolution,” Proc. of the IEEE International conference on advanced communications technology, PyeongChang, Korea (South), pp. 635–638, 17-20 February 2019.

[2] R.M. Alguliev, F.C. Abdullayeva, “An investigation and analysis of security problems of the cloud computing,” Problems of Information Technology, no. 1(7), pp. 3–14, 2013.

[3] “Hökumət buludu”nun (G-cloud) yaradılması və “bulud” xidmətlərinin göstərilməsi sahəsində tədbirlər haqqında Azərbaycan Respublikası Prezidentinin Fərmanı, № 718, 3 iyun 2019-cu il

[4] R. Browne, Hackers hijack Tesla’s cloud system to mine cryptocurrency, Feb 21 2018

[5] J. Goldman, Code Spaces Destroyed by Cyber Attack, June 23, 2014

[6] Commvault Discloses Zero-Day Exploit Breach in Azure Cloud Environment, https://cyberpress.org/commvault-discloses-zero-day-exploit/

[7] Ukraine mobile network Kyivstar hit by 'cyber-attack', 2023, https://www.bbc.com/news/world-europe-67691222

[8] M. Masdari, M. Jalali, “A survey and taxonomy of DoS attacks in cloud computing: DoS attacks in cloud computing,” Security and Communication Networks, vol. 9, no. 16, pp. 28. 2016.

[9] T. Hussain, C. Nugent, J. Liu, A. Beard, L. Chen, A. Moore, “An Attack Impact and Host Importance based Approach to Intrusion Response Action Selection,” Proc. of the 4th International Conference on Information Technology and Computer Communications, Guangzhou, China, pp. 84-91 June 23 - 25, 2022.

[10] F.J. Abdullayeva, “Malware detection in cloud computing using an image visualization technique,” Proc. of the IEEE 13th International Conference on Application of Information and Communication Technologies, Baku, Azerbaijan, pp. 1-5. 23-25 October 2019.

[11] M. Ali, Y. Saleem, S. Hina, G.A. Shah, “DDoSViT: IoT DDoS attack detection for fortifying firmware Over-The-Air (OTA) updates using vision transformer,” Internet of Things, Vol. 30, 101527, 2025.

[12] O. Valikhanli, Detection of malware in ground control stations of unmanned aerial vehicles based on image processing, International Journal of Information and Computer Security, Vol. 26, No. 1-2, pp. 147-158, 2025.

[13] Y. Alaca, Y. Çelik, “Cyber attack detection with QR code images using lightweight deep learning models,” Computers & Security, Vol. 126, 103065, 2023.

[14] Fathima, G.S. Devi, M. Faizaanuddin, “Improving distributed denial of service attack detection using supervised machine learning,” Measurement: Sensors, Vol. 30, 100911, 2023.

[15] Natsos, A.L. Symeonidis, “Transformer-based malware detection using process resource utilization metrics,” Results in Engineering, Vol. 25, pp. 1-19, 2025.

[16] L.D. Rose, G. Andresini, A. Appice, D. Malerba, “VINCENT: Cyber-threat detection through vision transformers and knowledge distillation,” Computers & Security, Vol. 144, pp. 1-13, 2024.

[17] H. Wasswa, H.A. Abbass, T. Lynar, “ResDNViT: A hybrid architecture for Netflow-based attack detection using a residual dense network and Vision Transformer,” Expert Systems with Applications, Vol. 282, pp. 1-14, 2025.

[18] F.J. Rendón, J.A. Álvarez, A.J. Varela, “Paying attention to cyber-attacks: A multi-layer perceptron with self-attention mechanism,” Computers & Security, Vol. 132, 103318, 2023.

[19] H. Kheddar, “Transformers and large language models for efficient intrusion detection systems: A comprehensive survey,” Information Fusion, Vol. 124, pp. 1-32, 2025.

[20] Cloud Attack Dataset, IEEE Dataport, https://ieee-dataport.org/documents/cloud-attack-dataset. (Accessed on 09 June 2025)