aurum

AURUM MÜHENDİSLİK SİSTEMLERİ VE MİMARLIK DERGİSİ
AURUM JOURNAL OF ENGINEERING SYSTEMS AND ARCHITECTURE

Cilt 8, Sayı 2 | Kış 2024
Volume 8, No 2 | Winter 2024

An Efficient Malware Classification Method Using Novel Deep Learning Model

Zinah Khalid Jasim Jasim[1]* and Sefer Kurnaz[2]*

[1]Department of Electrical and Computer Engineering, Altinbas University, Istanbul, 34000, Turkey
203720304@ogr.altinbas.edu.tr;
(https://orcid.org/0000-0002-1176-0043)
[2]Department of Electrical and Computer Engineering, Altinbas University, Istanbul, 34000, Turkey
sefer.kurnaz@altinbas.edu.tr

Received: 31.10.2023
Accepted: 01.11.2023
Published: 31.12.2024
*Corresponding author

Research Article
pp.265-271

DOI: 10.53600/ajesa.1587757

Abstract

Malware attacks getting increased due to the increased complexity in their structures have become a key threat to cybersecurity and require better and more efficient means of detection. Signature and heuristic methods of detecting malware do not perform well due to slow developments in this field and thus current detection uses machine learning and deep learning approaches. However, it is seen that high dimensionality and the complexity of malware data are major problems in terms of existing solutions, such as computational burden and overfitting. The presented work in this thesis aims to design a new malware detection framework using ResNet50 deep neural networks fine-tuned with a new wrapper-based feature selection technique operated by the GOA. The supporting framework also takes advantage of the transfer learning feature in ResNet50, a robust convolutional neural network, for feature extraction from malware data. Every slight hint related to malware is learnt by the model through training using ResNet50 on malware datasets. In addition to this, the GOA-based feature selection approach is used to help define the most important features as input to the neural network as well as to relieve the computational load. To assess the effectiveness of the proposed approach, the benchmark datasets of malware were used, and their results were compared to the traditional and recent methods. The findings affirm that the proposed ResNet50-GOA framework for fine-tuning outperforms the competitors by a significant margin in terms of the detection rate and by improved accuracy, precision, recall, area under the precision-recall curve, and F1-score, which illustrates high robustness and fewer false positive cases and complex computation. In addition, the proposed framework is immune to issues like class imbalance and discovers new patterns of emerging malware. This paper fulfills the following gaps in existing literature: It proposes a new approach for detecting malware that is more efficient and scalable than deep learning and metaheuristic optimization algorithms. The results speak to the promise of a combination of techniques in addressing multi-faceted cybersecurity issues, which opens further possibilities for the improvement of automated threat identification systems in the future.

Keywords: ResNet50, CNN, GOA, Deep Learning.

BAŞLIK

Özet

Yapılarındaki artan karmaşıklık nedeniyle artan kötü amaçlı yazılım saldırıları siber güvenlik için önemli bir tehdit haline gelmiştir ve daha iyi ve daha verimli tespit araçları gerektirmektedir. Kötü amaçlı yazılımları tespit etmek için kullanılan imza ve sezgisel yöntemler, bu alandaki yavaş gelişmeler nedeniyle iyi performans göstermemektedir ve dolayısıyla mevcut tespit, makine öğrenimi ve derin öğrenme yaklaşımlarını kullanmaktadır. Ancak, yüksek boyutluluğun ve kötü amaçlı yazılım verilerinin karmaşıklığının, hesaplama yükü ve aşırı uyum gibi mevcut çözümler açısından büyük sorunlar olduğu görülmektedir. Bu tezde sunulan çalışma, GOA tarafından işletilen yeni bir sarmalayıcı tabanlı özellik seçimi tekniği ile ince ayarlanmış ResNet50 derin sinir ağlarını kullanarak yeni bir kötü amaçlı yazılım tespit çerçevesi tasarlamayı amaçlamaktadır. Destekleyici çerçeve ayrıca, kötü amaçlı yazılım verilerinden özellik çıkarmak için sağlam bir evrişimli sinir ağı olan ResNet50'deki transfer öğrenme özelliğinden yararlanır. Kötü amaçlı yazılımla ilgili her küçük ipucu, kötü amaçlı yazılım veri kümeleri üzerinde ResNet50 kullanılarak eğitim yoluyla model tarafından öğrenilir. Buna ek olarak, GOA tabanlı özellik seçimi yaklaşımı, sinir ağına girdi olarak en önemli özellikleri tanımlamaya ve hesaplama yükünü hafifletmeye yardımcı olmak için kullanılır. Önerilen yaklaşımın etkinliğini değerlendirmek için, kötü amaçlı yazılımların kıyaslama veri kümeleri kullanıldı ve sonuçları geleneksel ve son

yöntemlerle karşılaştırıldı. Bulgular, ince ayar için önerilen ResNet50-GOA çerçevesinin, tespit oranı ve iyileştirilmiş doğruluk, hassasiyet, geri çağırma, hassasiyet-geri çağırma eğrisi altındaki alan ve yüksek sağlamlığı ve daha az yanlış pozitif vakayı ve karmaşık hesaplamayı gösteren F1 puanı açısından rakiplerinden önemli bir farkla daha iyi performans gösterdiğini doğrulamaktadır. Ayrıca, önerilen çerçeve sınıf dengesizliği gibi sorunlara karşı bağışıktır ve ortaya çıkan kötü amaçlı yazılımların yeni modellerini keşfeder. Bu makale, mevcut literatürdeki aşağıdaki boşlukları doldurmaktadır: Derin öğrenme ve metasezgisel optimizasyon algoritmalarından daha verimli ve ölçeklenebilir olan kötü amaçlı yazılımları tespit etmek için yeni bir yaklaşım önermektedir. Sonuçlar, gelecekte otomatik tehdit tanımlama sistemlerinin iyileştirilmesi için daha fazla olasılık açan, çok yönlü siber güvenlik sorunlarının ele alınmasında farklı tekniklerin bir araya getirilmesinin vaadini ortaya koyuyor.
Anahtar Kelimeler: ResNet50, Evrişimli Sinir Ağı (CNN), GOA, Derin Öğrenme.

Introduction

This is potentially due to the nature and speed of technology and the global community's dependency on systems has grown significantly. Malware, whose origin is a shortened form of malicious, can be defined as ILLEGAL software that is usually coded to notify computer systems to do ill will on them, gain unauthorized access, or deliver a false result. Even though current technologies have been developed to enhance detection and prevention methodologies, malware is continually improving its methods thereof traditional methodologies of finding them is almost effective (Shaukat, Luo et al. 2024). Therefore, there is a need for new, effective, and reliable detection strategies for effective protection of digital environments (Ijaz, Khan et al. 2024).

Machine learning in its most advanced form called deep learning has proved impressive results in many fields such as image, voice, and text recognition and anomaly detection. Of these architectures, convolutional neural networks, or CNNs have been most capable of dealing with complicated, large NL research data. ResNet50 refers to a residual network hierarchy at 50 layers; it is considered a deep CNN and is recent, with characteristics that have been proven to learn subtle features while solving vanishing gradient problems (Wasoye, Stevens et al. 2024). The work by researchers using fine-tune ResNet50 proves that the network has prior information that it can apply to the current research topic of malware detection (Singh, Krishnan et al. 2024).

Another remarkable aspect of enhancing the existing system for malware detection is feature selection. Feature selection is the process through which the data analyst seeks to only pick applicable features to improve machine learning model performance while at the same time reducing computational cost (Azeem, Khan et al. 2024). The feature selection techniques that involve using wrappers to assess subsets of features about their ability to predict results have been proven to have an effect in arriving at optimal feature subsets(Njeri, Ivanov et al. 2024). Nevertheless, the applicability of these techniques is highly contingent on the optimization algorithm applied to the selection procedure (Alhammadi, Rahmani et al. 2024).

The Grasshopper Optimization Algorithm (GOA) is one of the new metaheuristic optimization methods based on the real-life observation of grasshopper swarms (Alirezapour, Mansouri et al. 2024). Because of its ability to search and optimize search spaces, it is best applied to feature selection problems (Ingle and Jatoth 2024). There is a potential of adding GOA to models such as the fine-tuned ResNet50, where even more improved feature extraction, with even better optimization, is expected (Harandi, Van Messem et al. 2024).

In this paper, we will develop a new method that has the ability to diagnose different types of Malware. We developed a new algorithm trained on 10 different types of images with a total of 9339 images. The results obtained after training and testing the algorithm were 99.72. This indicates that the developed model has a high ability to detect Malware with high accuracy. Our contribution to this effort will be as follows:

• Employing the CNN approach to identify malware through decreasing the network's learning rate during the training phase.

• Achieving elevated identification precision with a restricted set of malware input images while minimizing recognition errors through the implementation.

• Enhancing the effectiveness of the proposed malware identification designs by increasing accuracy and precision in identifying through the optimal selection of feature subsets via the proposed CNN.

Problem Statement

Anti-malware legacy approaches like signature-based and heuristic ones fail to prevent and/or detect most emerging malware (Liu, Yan et al. 2024). Conventional approaches like signatures and heuristics cannot cope effectively with the ever-changing nature of malware forms. Even the recent approaches that employ machine learning-based methods have presented a feasible solution but the reliance on the quality of features and the way in which the intricacy of data relationships could be modeled(Shaukat, Luo et al. 2023). Popular deep learning models today, despite their capability, tend to be complex and overfitting whenever used on large-dimensional and imbalanced

datasets(Ravi and Alazab 2023). Moreover, the issue of identifying the most suitable inputs out of several thousand remains a critical area of application where significant performance improvements can be made.

1. Methodology

Design

A subset of artificial intelligence called deep learning is capable of processing data incredibly quickly despite sacrificing precision. As a result of deep learning's numerous benefits, it is widely utilized in the healthcare sector to categorize various types of Malware. Convolutional neural networks (CNN), one of the deep learning methods, are made specifically to analyze pictures with two-dimensional measurements (Al-Jumaili, Al-Jumaili et al. 2022). CNN's structure depends on layers, each of which has its own learning process and outputs that are input to subsequent levels. CNN is a hierarchical algorithm for learning that uses a raw input image as its basis (Dabas, Ahlawat et al. 2023). Typically, the conventional structure of CNN is split into a pair of primary components: feature extraction and classification. To obtain characteristics, different kinds of layers are utilized to obtain concealed data from Malware images, which perform an essential role because they have a significant impact on the precision of classification outcomes (Chaganti, Ravi et al. 2023). After that, the classifier will get all the characteristics that were taken from it and divide them into the appropriate classes. Convolution is the most crucial stage in CNN techniques, and it is liable for finding characteristics and applying filters(Kumar 2023). Strides and amount of filters constitute two of the very crucial factors that have a significant impact on the convolutional operation's output, while stride is defined as the space that separates two pixels as well as a number of filters as the number of features in the feature map (Haq, Jianjun et al. 2022) . Two functions, f, and G, are combined mathematically to create H(t), where H reflects the total quantity of overlap of only one function, f(T) as it is moved over the other criteria, G (Yamashita, Nishio et al. 2018). The formal below that are described illustrates this.

$$H(t) = \int_{-\infty}^{\infty} f(T)G(t-T)dT$$

Whenever used, H = f * G

Within Figure 3, the convolution operation's process is depicted. The input matrix is given in (a), and (b) shows the kernel matrix that was used to produce the outcomes in (c). As illustrated in figure 1, the total is applied after what is known as the Hadamard product (element-wise) as the convolution process mechanism.

10	37	1	5	40
4	2	16	55	20
28	17	2	0	47
9	0	19	25	13
8	30	41	6	31

X

0	0	1
0	0	0
1	0	0

=

29	22	42
25	55	39
10	30	88

Figure 1: matrix (a) Input Matrix (b) Kernel Matrix (c) Outcome Matrix

As seen in Figure 2, the six blocks of the convolution layer utilized in our suggested technique for obtaining characteristics from Malware images each have a (convolution Layer, batch Normalization Layer, clipped Relu Layer, and MaxPooling Layer) in them. The approach typically begins from the left upper corner, where the kernel matrix we used was 3x3 fixed for all Convolution layers, giving an outcome similar to that in Figure 1. Next, the kernel matrix 3x3 is utilized again, this time with the kernel matrix 3x3 shifted one column to the right due to the Stride set (1x1), covering the entirety of the image input. In order to expedite training and lessen

network sensitivity, the activation function is crucial in converting linear input data to nonlinear output. Given that ReLU cannot concurrently activate all of the neurons in a cell, it is regarded as one of the most widely employed activation mechanisms. We used a Clipped Rectified Linear Unit (clippedReluLayer), which has a limit technique, to stop the outcome from growing excessively big (Manzil and Manohar Naik 2023). This unit converts all input that is less than zero to zero, and any value that is higher than the ceiling sets it to match the clipping ceiling, which is equal to 10. Additionally, using Max Pooling increased the precision ratio by pooling the convolutional features of the map to obtain the greatest possible average value (Mohammed, Lakhan et al. 2023). Additionally, in the classification section, input characteristics to the three sets of fully connected layers, all of which were preceded via a dropout layer which was (0.5) to prevent over fitting that occurred in the model, following all features retrieved by convolution layers (Gupret, Turner et al. 2024). The final block was composed of the Fully Connected Layer, SoftMax Layer, and Classification Layer.

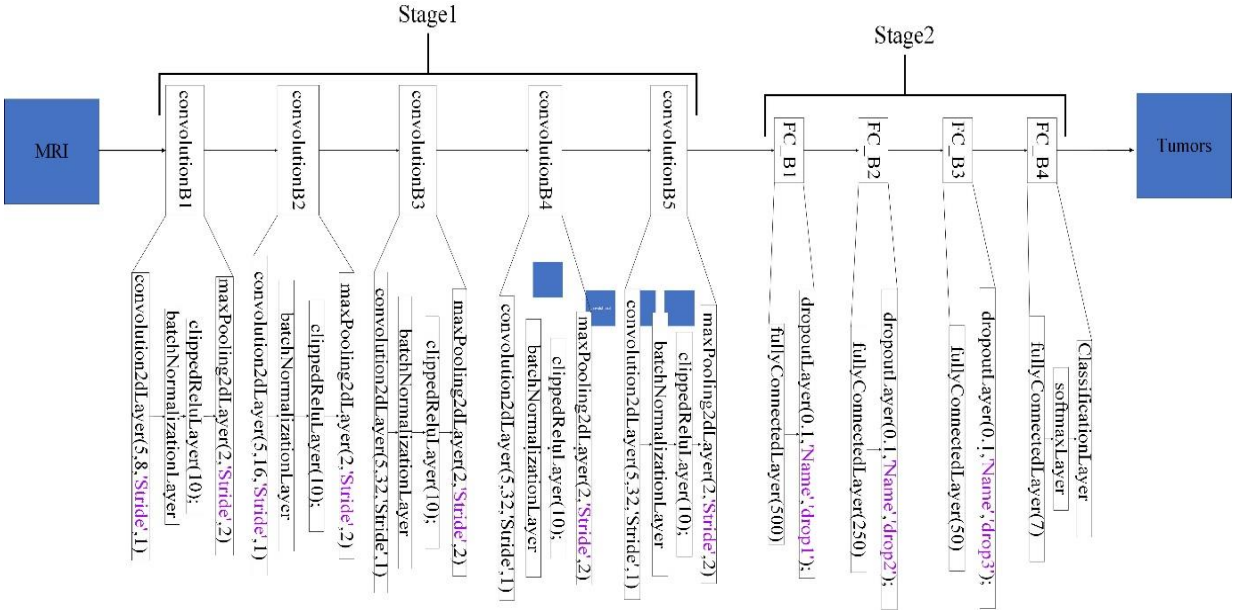

Figure 2: overview of the procedure

Evaluation metrics

In accordance with the confusion matrix results, we employed a variety of assessment measures to assess the efficacy of our suggested model. The means are utilized to evaluate precision, sensitivity, and specificity. According to (Eq. 1), accuracy is determined by the amount of the total dataset's forecasts were accurate. The total amount of accurate positive predictions from every one of the positive predictions is used to determine recall or sensitivity (Eq. 2). Precision, also known as confidence, is the likelihood that a true number will be greater than the whole amount of predicted positives as given in equation (3). While the equilibrium of accuracy and recall is depicted in (Eq. 4) by a harmonic, also known as the F1-Score, the combination of precision and recall signifies. Using F1-Score is a safe way to gain a precise idea of the outcomes we got.

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \quad (1)$$

$$Recall = \text{Sensitivity} = \frac{TP}{TP + FN} \quad (2)$$

$$Precision = Confidence = \frac{TP}{TP + Fp} \quad (3)$$

$$F1 - score = \frac{2 * TP}{2 * TP + FP + FN} \quad (4)$$

Results

The main idea behind this paper is to classify 10 different types of Malware images. The convolutional neural network was the backbone of our proposed model. The structure of the proposed model consists of 6 blocks for extracting discriminatory features from Malware images and 5 blocks for classifying the most relevant features of the four stages as shown in Figure 3. We trained and tested our model to ensure that the results obtained from the proposed method are verified for accuracy, adequacy and efficiency. Based on these results, it was found that the proposed model achieved superior results for the classification of Malware images.

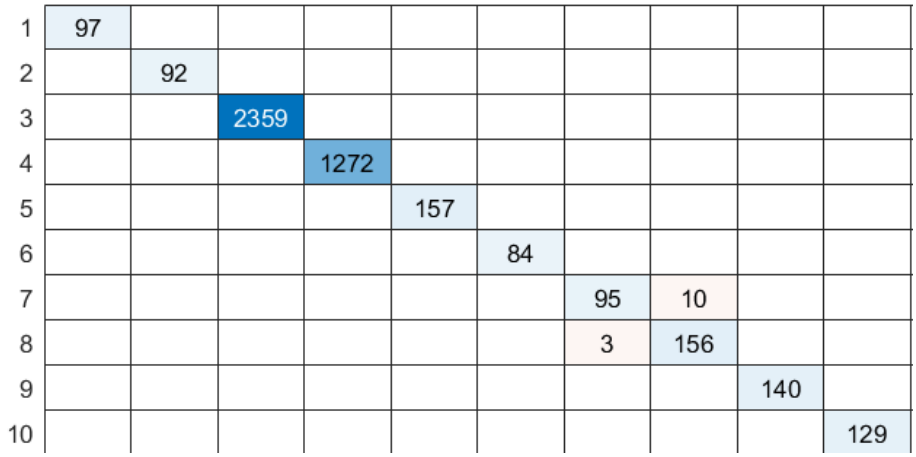

Figure 3: The result for each model and classifier's confusion matrix

We utilized ROC to display the performance of many models in order to make the findings of the models more understandable. The ROC curve generated using the suggested approach is shown in Figure 4

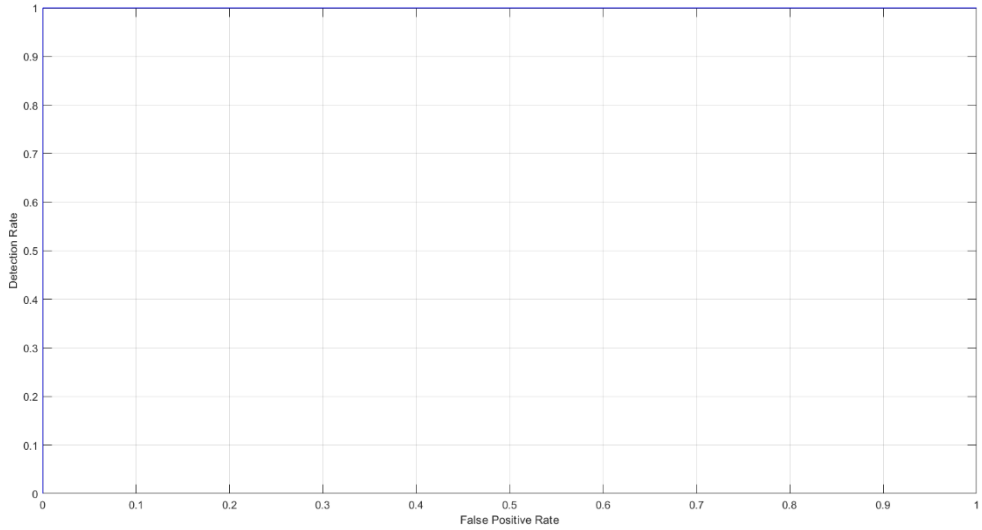

Figure 4The developed CNN ROC Curve

Table 1: Results table for different types of evaluation metrics

	Accuracy	Precision	Recall	F1 Score
Adialer.C	100	100	100	100
Agent.FYI	100	100	100	100

Allaple.A	100	100	100	100
Allaple.L	100	100	100	100
Alueron.gen!J	100	100	100	100
Autorun.K	100	100	100	100
C2LOP.gen!g	100	100	100	100
Dialplatform.B	99.72	90	97	94
Dontovo.A	99.72	98	94	96
Instantaccess	100	100	100	100
Skintrim.N	100	100	100	100

This research methodology developed an algorithm from scratch, one of the deep learning methods, Convolutional neural networks (CNN), with the capability to classify 10 distinct classes of Malware. We utilized this technique for obtaining characteristics from Malware images. We used an open-source dataset of Malware pictures. We attained an accuracy of over 94% by using the CNN classifier in relation to the characteristics that were derived from CNN. Which takes into account the best outcome attained. CNN model can learn directly from raw pixel data. This implies that the most prominent aspects of the pictures, such as edges, forms, colors, textures, and objects, may be automatically discovered and adapted. The magnitude of the training-vector feature set necessitated a lengthy computational training process. Also included in the suggested technique is a new dataset with 10 classes that is used to test its adaptability. Over 99.72% of the classifications were accurate. To the best of the author's knowledge, the published studies of classification Malware by deep learning when compared with our proposed result show less accuracy. In addition, we used a large dataset, that is up-to-date, from the year 2023, the best outcomes as determined by the 10 metrics assessment areas of Accuracy using developed CNN models show an accuracy more than of 99.72 %, and again our proposed method outperformed of them. As a result, the suggested method can be extremely useful in assisting detection of the Malware types that can be a problem for computers, especially for the Windows OS, and can be an early diagnosis to prevent the Malware effect on the system.

Conclusion

Malware is described as "any software that executes something detrimental to the consumer, device, or connection." Malware may appear as written paperwork, a downloadable file, as well as another kind of program. Malware is often categorized into computer worms, viruses, and other types of harmful software. The proliferation of computer traces is going to increase the level of sophistication of such assaults. This article classifies 10 forms of malware. Initially, the Resnet50 process extracts characteristics regarding the dataset, which are subsequently normalized along divided via training and test datasets before being input via the CNN proposed method to identify an ideal subset of features. The most effective selection of characteristics was subsequently provided to the final results which will play an important role in the final results of classification. The suggested method exhibits an accuracy of 99.7%.

References

Al-Jumaili, S., A. Al-Jumaili, S. Alyassri, A. D. Duru and O. N. Uçan (2022). Recent Advances on Convolutional Architectures in Medical Applications: Classical or Quantum? 2022 International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), IEEE.

Alhammadi, A., F. Rahmani, A. Izadi, F. Hajati, S. S. S. Farahani, A. Jabr, W. AL-Salman, S. M. Saneii and R. Barzamini (2024). "Prediction of Environmental Conditions of the Greenhouse Using Neural Networks Optimized with the Grasshopper Optimization Algorithm (GOA)." Journal of Power System Technology **48**(3): 622-635.

Alirezapour, H., N. Mansouri and B. Mohammad Hasani Zade (2024). "A Comprehensive Survey on Feature Selection with Grasshopper Optimization Algorithm." Neural Processing Letters **56**(1): 28.

Azeem, M., D. Khan, S. Iftikhar, S. Bawazeer and M. Alzahrani (2024). "Analyzing and comparing the effectiveness of malware detection: A study of machine learning approaches." Heliyon **10**(1).

Chaganti, R., V. Ravi and T. D. Pham (2023). "A multi-view feature fusion approach for effective malware classification using Deep Learning." Journal of information security and applications **72**: 103402.

Dabas, N., P. Ahlawat and P. Sharma (2023). "An effective malware detection method using hybrid feature selection and machine learning algorithms." Arabian Journal for Science and Engineering **48**(8): 9749-9767.

Gupret, E., A. Turner, C. Evans, R. Morgan and M. Richardson (2024). "Dual-layer ransomware classification using opcode and network traffic similarity."

Haq, E. U., H. Jianjun, X. Huarong, K. Li and L. Weng (2022). "A Hybrid Approach Based on Deep CNN and Machine Learning Classifiers for the Tumor Segmentation and Classification in Brain MRI." Comput Math Methods Med **2022**: 6446680.

Harandi, N., A. Van Messem, W. De Neve and J. Vankerschaver (2024). Grasshopper Optimization Algorithm (GOA): A Novel Algorithm or A Variant of PSO? International Conference on Swarm Intelligence, Springer.
Ijaz, A., A. A. Khan, M. Arslan, A. Tanzil, A. Javed, M. A. U. Khalid and S. Khan (2024). "Innovative Machine Learning Techniques for Malware Detection." Journal of Computing & Biomedical Informatics **7**(01): 403-424.

Ingle, K. K. and R. K. Jatoth (2024). "Non-linear channel equalization using modified grasshopper optimization algorithm." Applied Soft Computing **153**: 110091.

Kumar, M. (2023). "Scalable malware detection system using distributed deep learning." Cybernetics and Systems **54**(5): 619-647.

Liu, W., W. Yan, T. Li, G. Han and T. Ren (2024). "A Multi-strategy Improved Grasshopper Optimization Algorithm for Solving Global Optimization and Engineering Problems." International Journal of Computational Intelligence Systems **17**(1): 182.

Manzil, H. H. R. and S. Manohar Naik (2023). "Android malware category detection using a novel feature vector-based machine learning model." Cybersecurity **6**(1): 6.

Mohammed, M. A., A. Lakhan, D. A. Zebari, K. H. Abdulkareem, J. Nedoma, R. Martinek, U. Tariq, M. Alhaisoni and P. Tiwari (2023). "Adaptive secure malware efficient machine learning algorithm for healthcare data." CAAI Transactions on Intelligence Technology.

Njeri, N., O. Ivanov, S. Rodriguez, A. Richardson and C. Delgado (2024). "Triple-layer bayesian euclidean curve algorithm for automated ransomware classification."

Ravi, V. and M. Alazab (2023). "Attention‐based convolutional neural network deep learning approach for robust malware classification." Computational Intelligence **39**(1): 145-168.

Shaukat, K., S. Luo and V. Varadharajan (2023). "A novel deep learning-based approach for malware detection." Engineering Applications of Artificial Intelligence **122**: 106030.

Shaukat, K., S. Luo and V. Varadharajan (2024). "A novel machine learning approach for detecting first-time-appeared malware." Engineering Applications of Artificial Intelligence **131**: 107801.

Singh, S., D. Krishnan, V. Vazirani, V. Ravi and S. A. Alsuhibany (2024). "Deep hybrid approach with sequential feature extraction and classification for robust malware detection." Egyptian Informatics Journal **27**: 100539.

Wasoye, S., M. Stevens, C. Morgan, D. Hughes and J. Walker (2024). "Ransomware classification using btls algorithm and machine learning approaches."

Yamashita, R., M. Nishio, R. K. G. Do and K. Togashi (2018). "Convolutional neural networks: an overview and application in radiology." Insights into Imaging **9**(4): 611-629.