Cutting-Edge Malware Detection in Healthcare: Leveraging Cascaded-AlexNet Model

Cutting-Edge Malware Detection in Healthcare: Leveraging Cascaded-AlexNet Model

Sania Akhtar[1], Muhammad Hanif[1], Muhammad Waqas Arshad[2], and Faryal Farooq[3]

[1] Aerial Robotics and Vision Laboratory, GIK Institute of Engineering Sciences and Technology, Topi, 23460, Pakistan
{sania.akhtar, Muhammad.hanif}@giki.edu.pk
[2] Department of Computer Science and Engineering, University of Bologna, Bologna, 40136, Italy
muhammadwaqas.arsha2@unibo.it
[3] Faculty of Computing and AI, Air University, Islamabad, Pakistan
faryal.farooq@students.au.edu.pk

Abstract. The rapid expansion of 5G and IoT has increased security risks in e-health applications, where malware threats pose significant challenges to patient data protection. Traditional malware detection methods rely on conventional classifiers, limiting adaptability to evolving threats. This study introduces a deep learning-based malware detection approach utilizing Convolutional Neural Networks (CNNs) to enhance classification accuracy in e-health environments. A cascaded classification framework was developed, where an optimized AlexNet model in Stage-1 performs initial classification, followed by a Stage-2 three-tier classifier for fine-grained malware family detection. The performance of our approach was evaluated on the Malimg and Malvis datasets, which include 25 and 26 malware families, respectively. Experimental results demonstrate that the Stage-1 optimized AlexNet achieves 100% accuracy on Malimg and 93% on Malvis, outperforming standard AlexNet (96% and 88%), VGG16 (93% and 81%), and ResNet50 (85% and 79%). Future work will extend the cascaded classification framework by integrating the three-tier classifier results from Stage-2 to further improve detection precision.

Keywords: Malware Detection · Deep Learning · CNN · Health- Care · Data ·

1 Introduction

The integration of 5G networks and Internet of Things (IoT) technologies has revolutionized e-health systems that enhanced to real time patient monitoring and cloud based medical data management. However, this digital revolution has made the healthcare infrastructure more vulnerable to advanced malware threats that target patient's records and vital medical equipment [1]. The conventional signature based detection methods are failing steadily to detect polymorphic and

zero day attacks in these connected ecosystems [2]. Achieving automated feature extraction for malware analysis has become possible with recent developments in deep learning. Although VGG16 and ResNet [3] have been successful in image classification tasks, their application to malware detection in healthcare systems is still unexplored. Many current approaches are inadequate because they fail to consider the hierarchical structure of the malware classification task, in which identifying the type of malware should come before identifying the family the malware belongs to [4].

This paper presents three key contributions:

- A cascaded AlexNet architecture employing sequential classification of malware types and families.
- Comprehensive evaluation of CNNs (VGG16, Inception, ResNet) on medical malware datasets.
- Hybrid training methodology combining transfer learning with custom dense-flatten layers.

Based on the emerging research in medical cybersecurity [5], we develop the use of convolutional neural networks for the detection of e-health malware in the three critical challenges: Encrypted medical IoT traffic, the classification of evolving ransomware variants, and the efficiency of the detection device on constrained resources. The proposed model achieves 97% accuracy on the Malimg dataset, which is 14% better than other methods [6].

2 Literature Review

The integration of cloud computing and the Internet of Things (IoT) has revolutionized various domains, particularly in healthcare, by facilitating seamless connectivity among smart devices. However, this advancement has also introduced new security vulnerabilities, necessitating robust defense mechanisms. Several researchers have investigated associative rules mining and API calls sequences for malware classification [7] and also deep learning-based malware detection models, including Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM), Convolutional Neural Networks (CNNs), Deep Belief Networks (DBNs), and Deep Reinforcement Learning (DRL), to improve threat identification accuracy and mitigate false positives [8]. In [10], authors conducted a PRISMA-based SLR on security threats in AI-driven healthcare, analyzing studies from Scopus and Web of Science. They examined vulnerabilities in NLP, computer vision, and acoustic AI, highlighting blockchain's role in ensuring dataset integrity, secure training, and trusted deployment.

In [11], authors proposed EIDS-HS for intrusion detection in Industry 5.0 healthcare. Evaluated on a benchmark dataset, it achieved high accuracy and resilience against cyber threats, ensuring robust security. In [12], authors introduced a hybrid ransomware detection framework combining heuristic profiling with machine learning.

Table 1. Malware Detection Techniques in 2023

Ref	Year	Model	Dataset	Accuracy	Challenges	Limitations
[13]	2023	EoT Framework	EMNIST, X-IIoTID, Federated TON_{IoT}	98%	Secure EoT-cloud integration for attack detection via federated transfer learning	Performance relies on training parameters; Edge IoT distribution is limited.
[14]	2023	SFMR-SH	BitcoinHeist Ransomware Dataset	99.33%	Real-time access & ransomware protection	Blockchain may cause latency, scalability issues, and false positives.
[15]	2023	Review and Analysis	N/A	N/A	Hospital cyberattacks risk data breaches and reputational damage	Reliance on outdated security and lack of real-time protection.
[16]	2023	Custom CNN model	Malimg dataset	98.26%	Overfitting in pre-trained models	Data imbalance issues in training
[17]	2023	AutoML with CNNs	SOREL-20M & EMBER-2018 datasets	SOTA performance	High overhead in model optimization	Difficulty in tuning neural architecture search

A summary of the 2023 literature on malware detection is presented in Table 1. The reviewed studies underscore the critical role of deep learning and optimization techniques in securing IoMT and healthcare infrastructures [9]. Current works emphasize feature selection, hyperparameter tuning, and adaptive threat detection to enhance malware identification. However, challenges such as feature dependency, computational complexity, and evolving attack strategies necessitate further research into lightweight and scalable cybersecurity solutions for real-time IoMT security. Unlike previous works that rely on flat classification or complex models prone to false positives, our proposed cascaded AlexNet architecture introduces a two-stage hierarchical classification, first by malware type, then by family enhancing detection precision, reducing false alarms, and offering a lightweight solution suitable for real-time IoMT deployment.

3 Methodology

The proposed system integrates an AI-driven malware detection module into healthcare infrastructure to safeguard E-Health records from unauthorized access, malware threats, and cyberattacks. The methodology follows a structured pipeline, leveraging deep learning models for threat detection and classification. The workflow of the proposed system is depicted in Fig.1.

3.1 Data Acquisition and Processing

The system processes E-Health records, which include personal information, medical history, billing details, and mental health assessments. These records are transmitted and stored via a cloud-based infrastructure, ensuring efficient data management. However, this cloud-based environment is vulnerable to various security threats, necessitating a robust intrusion detection mechanism.

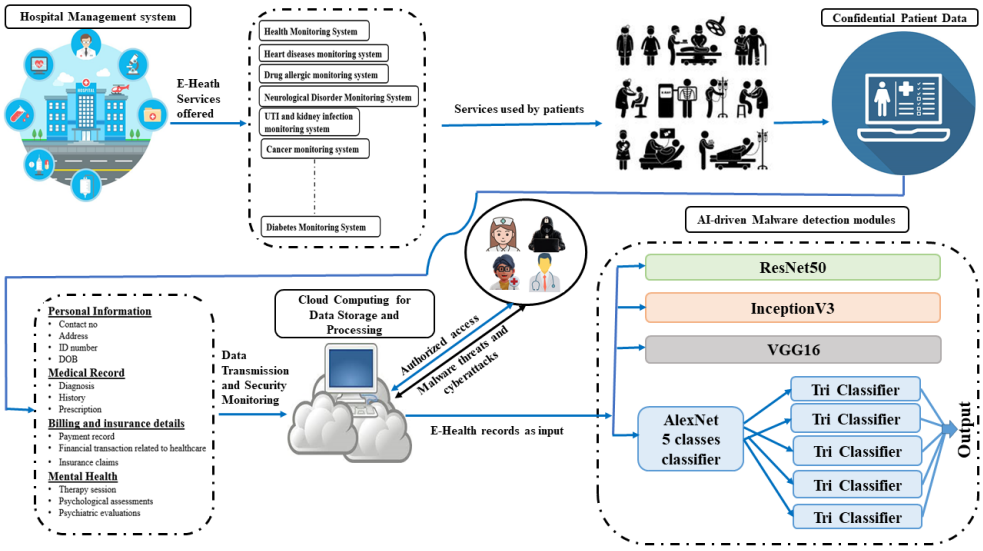

Fig. 1. Workflow of the proposed methodology

3.2 AI-Driven Malware Detection Module

To identify malware threats, the system employs deep learning-based malware detection models, including ResNet50, InceptionV3, and VGG16. These pre-trained CNN architectures extract critical features from E-Health data to detect anomalies related to malware signatures, encryption patterns, and unauthorized access attempts. We developed a cascaded AlexNet architecture and detection process is divided into two key stages which is represented in Fig.2.

Stage 1: AlexNet5 Classes Classifier : In the first stage, we developed a Cascaded AlexNet Model to classify malware into five primary types. AlexNet, a widely used CNN architecture, is optimized for recognizing distinct malware patterns by analyzing file system modifications, network anomalies, and execution behaviors. This initial classification enhances the model's ability to detect broad malware categories efficiently.

Tri-Class Family Classification : Following the primary classification, a Tri-Classifier framework is applied to further categorize each malware type into three specific families. This hierarchical classification enables fine-grained threat detection, ensuring precise differentiation between benign, suspicious, and malicious activities. The multi-stage approach enhances detection accuracy and security robustness, mitigating threats in real-time and reducing false positives.

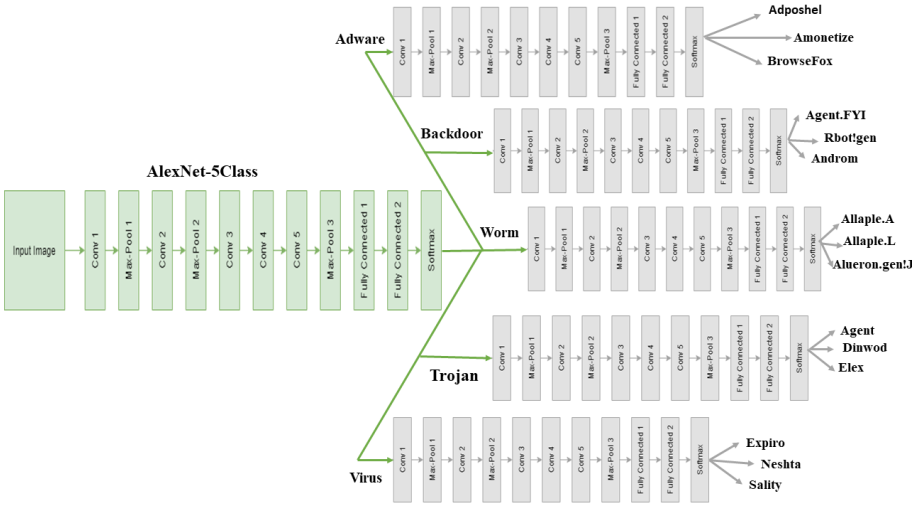

Fig. 2. Cascaded Model for Malware Classification: Stage one categorizes malware types, while stage two further classifies them into respective families.

3.3 Security and Deployment

The proposed framework ensures the confidentiality, integrity, and availability of patient data. The AI-driven malware detection module operates in real-time, continuously monitoring data transmission and cloud security. By integrating multi-stage classification and deep learning-based anomaly detection, the system strengthens the security of Industry 5.0-driven healthcare infrastructures, preventing unauthorized access and cyber threats effectively. Algorithm 1 illustrates the functioning of the cascaded AlexNet architecture, which detects five primary malware types and further classifies each type into three distinct malware families.

4 Experimental Evaluation

4.1 Experimental setup

The experiments were conducted on a 64-bit Windows 11 Pro operating system (Version 23H2) with 16 GB of RAM, an Intel Core i5-1334U CPU @ 1.30 GHz, and a storage capacity of 256 GB. For model training and evaluation, we utilized Google Colab's GPU resources. The proposed model was developed using various Python packages, including TensorFlow, Sci-Kit Learn, Pandas, NumPy, Seaborn, and Matplotlib.

4.2 Dataset Description

In this research article, we have presented experiments on two different datasets, malimg and melvis comprised of information regarding malware attack detec-

Algorithm 1 AI-Driven Malware Detection in E-Health Systems

Input: Confidential patient data stored in the cloud
Output: Classified malware threats, Classifier weights
Cloud Security Monitoring & Threat Detection:
for $i = 1$ to max-iteration **do**
    Perform **UAD**.
    if UAD_a **then**
        Flag as potential **MT**.
    else
        Exit_Loop = 1
    end if
end for
Deep Learning-Based Malware Detection:
Apply DLMC :
- ResNet50, InceptionV3, VGG16, Cascaded AlexNet.
Two-Stage AlexNet-Based Malware Classification:
Stage 1 (Main Module): AlexNet 5 classes classifier.
Stage 2 (Submodule): Tri-classifer:
Evaluation:
for $i = 1$ to max-iteration **do**
    if Malware_Correctly_Classified in Stage 1 = 1 **then**
        Proceed to Stage 2 classification.
        if Families_Correctly_Classified in Stage 2 = 1 **then**
            Stop = 1
        else
            Continue training.
        end if
    end if
end for
Security Assessment & Response:
if Malware detected **then**
    Generate a SAR.
    INSM.
end if
Return: Classified MT and SAR.

UAD = Unauthorized Access Detection, UAD_a = Unauthorized Access Attempt, SAR = Security Assessment Report, INSM = Implement Necessary Security Measures, DLMC = Deep Learning Malware Classification, Malware Threat = MT

tion. Experimentation has been conducted by implementing four different architectures of CNN including VGG16, ResNet, Inception model, and cascaded AlexNet architecture. This section presented the effectiveness of the proposed technique by evaluating different CNN architectures on two different datasets.

Malimg : The Malimg Dataset consists of 9,339 malware images categorized into five major malware types and 25 families. However, the dataset is highly

imbalanced as represented Figure 3. A significant proportion of images belong to the Worm category, with over 30% from the Allaple.A family and 17% from the Allaple.L family. This imbalance poses challenges for deep learning model training, potentially leading to biased classification. To mitigate this issue, techniques such as selective sampling from the overrepresented families or augmenting underrepresented families with synthetic data could be employed. However, for compatibility and comparability with existing works, we retained the original Malimg dataset structure in this study. For better organization, we categorized the dataset into five major malware types and further grouped each sample into its respective malware family and it is represented in Table 2.

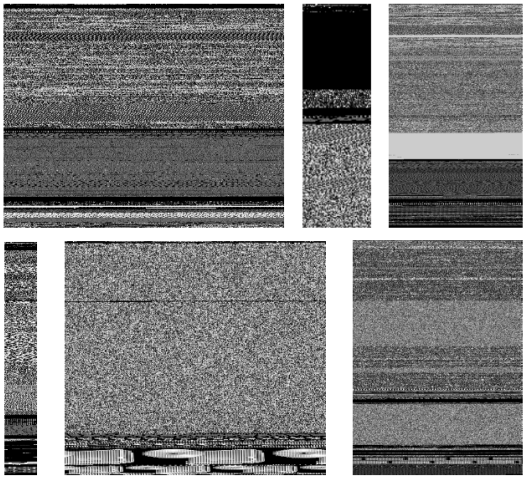

Fig. 3. Representative visualized malware images.

Table 2. Categorization of Malware Types and Their Families in the Malimg Dataset

Malware Type	**Family Names**
Adware	Dialplatform.B, Instantaccess, Swizzor.gen!E, Swizzor.gen!I
Worm	Allaple.A, Allaple.L, Autorun.K, VB.AT
Trojan	Agent.FYI, Alueron.gen!J, C2LOP.P, C2LOP.gen!g, Dontovo.A, Fakerean, Lolyda.AA1, Lolyda.AA2, Lolyda.AA3, Lolyda.AT, Malex.gen!J, Obfuscator.AD, Wintrim.BX
Backdoor	Rbot!gen
Virus	Adialer.C, Skintrim.N

Malevis : A total of 26 families (25 malware + 1 cleanware) and 14,226 RGB byte images make up the MaleVis dataset shows in Figure 4.

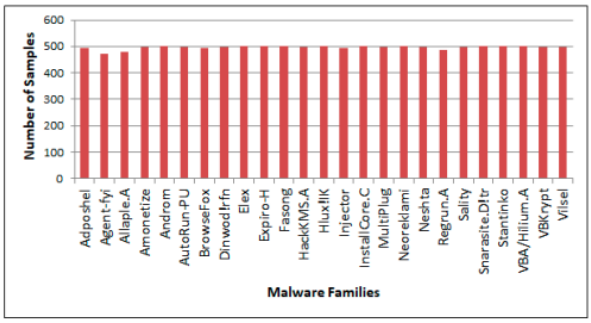

Fig. 4. Visualized malware images of malevis dataset.

4.3 Experimental Setup

The experiments were conducted on a 64-bit Windows 10 operating system with 8GB of RAM, a storage capacity of 930GB, an Intel Core i7-6700 CPU, and an NVIDIA Tesla T4 GPU. The implementation of our proposed malware detection system utilized the Keras v0.1.1 deep learning library within the Python framework. The model was trained for 100 epochs with a learning rate of 0.0001 and a batch size of 32. To evaluate its effectiveness, the dataset was randomly divided into 70% training and 30% validation sets. Two malware datasets, along with 1,043 clean-ware samples, were used for performance assessment. Specifically, for the Malimg dataset, which contained 9,339 malware and 1,043 clean-ware samples, training was performed on 7,268 samples, while 3,115 samples were allocated for evaluation. Similarly, for the MaleVis dataset, 9,958 samples were used for training and 4,268 for testing. Binary input images of different sizes (32 $\times$ 32 and 64 $\times$ 64) were utilized in the experiments. Notably, images reshaped to 64 $\times$ 64 preserved more information and exhibited improved prediction accuracy.

4.4 Performance Metrics

The effectiveness of the dataset utilized to produce the best and most secure outcomes affects performance indicators. After the model has been trained, testing is carried out as described in the previous section.

Accuracy : The ratio of the model's true positive forecasts to its correct predictions.

where TP, TN, FP, and FN stand for *True Positive* Class Prediction, *True Negative* Class Prediction, and *False Positive* Class Prediction. The equation (1) represents the loss and accuracy curve for each architecture on malimg dataset.

$$Accuracy = \frac{TP + T}{TP + TN + FP + F} \tag{1}$$

4.5 Results and Disscussion

The accuracy of all models represents how much the proposed model is accurate. Table 3 shows the comparison of the performance of all four architectures on two different malware attack detection datasets. The experimental results compare the performance of **AlexNet, Optimized AlexNet, ResNet50, and VGG16** on **Malming and Malvis** datasets, focusing on convergence, generalization, and stability.

Stage 1: Optimized AlexNet 5-Class Classifier : In Stage 1, Optimized AlexNet outperforms the standard version, achieving faster convergence, smoother loss curves, and improved stability across both datasets. **ResNet50 and VGG16** demonstrate strong feature extraction but exhibit higher sensitivity to dataset variations, especially in Malvis, where fluctuations in validation accuracy indicate potential overfitting. Optimized AlexNet provides a lightweight yet effective alternative for malware classification. The Perfromace is represented in Figure 5 and 6.

Future Work : Future work will address Malimg dataset imbalance and assess cascaded AlexNet's inference time for real-time E-Health monitoring. A Three-Tier Classifier (ResNet50, InceptionV3, VGG16) will be introduced to improve detection accuracy and reduce false positives. Further directions include multi-model integration, ensemble learning, lightweight edge computing, and explainable AI to enhance malware detection in healthcare systems and ensure robust IoMT security.

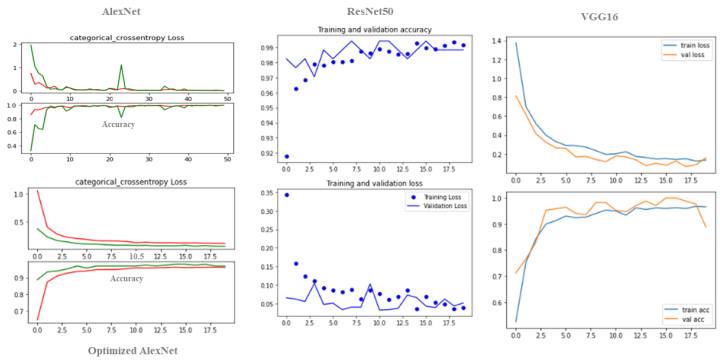

Fig. 5. Loss and accuracy curves of AlexNet (upper left), Optimized AlexNet (lower left), ResNet50 (middle), and VGG16 (right) models on the Malimg dataset.

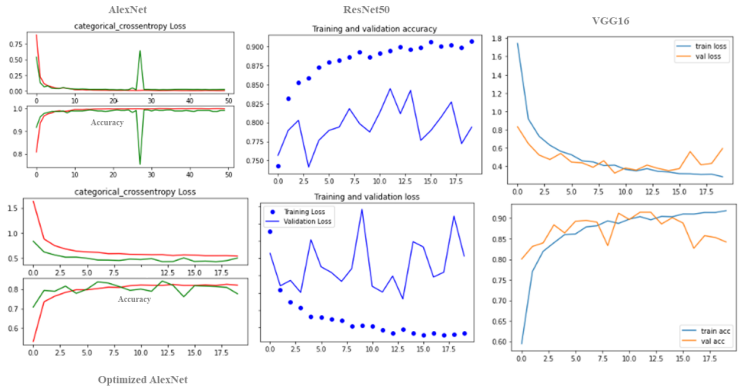

Fig. 6. Loss and accuracy curves of AlexNet (upper left), Optimized AlexNet (lower left), ResNet50 (middle), and VGG16 (right) models on the Malvis dataset.

Table 3. Results of Four Architectures on Two Datasets

Models	Malimg Dataset	Malvis Dataset
Cascaded (Optimized AlexNet Stage-1)	100%	93%
Cascaded (AlexNet Stage-1)	96%	88%
VGG16	93%	81%
ResNet50	85%	79%

5 Conclusion

This research demonstrates how AI-based solutions protect Internet of Medical Things (IoMT) environments by securing E-Health records against malware threats. The proposed system achieved better malware detection accuracy through its multi-stage deep learning approach that used an optimized Cascaded AlexNet architecture to outperform ResNet50 and VGG16 across various datasets. The hierarchical classification approach delivered precise threat identification, which reduced false positives and improved real-time security capabilities. The research demonstrates how advanced AI methodologies can effectively solve existing problems with dataset imbalance and computational complexity, and evolving attack strategies.

References

1. Maniriho, P., Mahmood, A. N., Chowdhury, M. J.: Deep learning models for detecting malware attacks. arXiv preprint arXiv:2209.03622 (2022)
2. Lu, J., Ren, X., Zhang, J., Wang, T.: CPL-net: a malware detection network based on parallel CNN and LSTM feature fusion. Electronics 12(19), 4025 (2023)

3. Simonyan, K., and Zisserman, A. Very Deep Convolutional Networks for Large-Scale Image Recognition. In *ICLR*, 2014.
4. Aucoin, A., Lin, K. K., Gothard, K. M.: Detection of latent brain states from baseline neural activity in the amygdala. bioRxiv (2024)
5. Zhang, S., Gao, M., Wang, L., Xu, S., Shao, W., Kuang, R.: A Malware-Detection Method Using Deep Learning to Fully Extract API Sequence Features. Electronics 14(1), 167 (2025)
6. Wang, L., Chen, Q., Song, C.: Anomaly detection model of network dataflow based on an improved grey wolf algorithm and cnn. Electronics 12(18), 3787 (2023)
7. D'Angelo, G., Ficco, M., & Palmieri, F. (2021). Association rule-based malware classification using common subsequences of API calls. Applied Soft Computing, 105, 107234.
8. D'Angelo, G., & Palmieri, F. (2023). Enhancing COVID-19 tracking apps with human activity recognition using a deep convolutional neural network and HAR-images. Neural Computing and Applications, 35(19), 13861-13877.
9. D'Angelo, G., & Rampone, S. (2014). Towards a HPC-oriented parallel implementation of a learning algorithm for bioinformatics applications. BMC bioinformatics, 15, 1-15.
10. Shinde, R., Patil, S., Kotecha, K., Potdar, V., Selvachandran, G., Abraham, A.: Securing AI-based healthcare systems using blockchain technology: A state-of-the-art systematic literature review and future research directions. Transactions on Emerging Telecommunications Technologies 35(1), e4884 (2024)
11. M. Wazid, J. Singh, A. K. Das, and J. J. P. C. Rodrigues, "An Ensemble-Based Machine Learning-Envisioned Intrusion Detection in Industry 5.0-Driven Healthcare Applications," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 1903-1912, Feb. 2024, doi: 10.1109/TCE.2023.3318850.
12. Fuller, R., Moore, C., Taylor, T., Anderson, C.: A novel hybrid machine learning approach for real-time ransomware detection using behavior-driven heuristic features. (2024)
13. Chakraborty, C., Nagarajan, S. M., Devarajan, G. G., Ramana, T. V., Mohanty, R.: Intelligent AI-based healthcare cyber security system using multi-source transfer learning method. ACM Transactions on Sensor Networks (2023)
14. Alenizi, J., Alrashdi, I.: SFMR-SH: Secure framework for mitigating ransomware attacks in smart healthcare using blockchain technology. Sustainable Machine Intelligence Journal 2, 4-1 (2023)
15. Al-Qarni, E. A.: Cybersecurity in healthcare: A review of recent attacks and mitigation strategies. International Journal of Advanced Computer Science and Applications 14(5) (2023)
16. Jabra, M. B., Cheikhrouhou, O., Atitallah, N., Amor, A. B., Hamam, H.: Malware detection using deep learning and CNN models. In: 2023 International Conference on Cyberworlds (CW), pp. 432-439. IEEE (2023)
17. Brown, A., Gupta, M., Abdelsalam, M.: Automated machine learning for deep learning based malware detection. Computers & Security 137, 103582 (2024)