OPEN ACCESS

Kashf Journal of Multidisciplinary Research
Vol: 02 - Issue 07 (2025)
P-ISSN: 3007-1992 E-ISSN: 3007-200X
https://kjmr.com.pk

MACHINE LEARNING TECHNIQUES FOR REAL-TIME MALWARE DETECTION AND PREVENTION

Muhammad Ali Saeed*
Department of Computer Science, NFC Institute of Engineering and Technology, Multan, Pakistan.

Muhammad Abdur Raphay Zia
I2c Inc Lahore, Pakistan.

Naeem Aslam
Department of Computer Science, NFC Institute of Engineering and Technology, Multan, Pakistan.

Muhammad Fuzail
Department of Computer Science, NFC Institute of Engineering and Technology, Multan, Pakistan.

Muhammad Tanveer Meeran
Faculty of computer science and mathematics, Universiti Malaysia Terengganu, Malaysia.

****Corresponding author: Muhammad Ali Saeed (**muhammadalisaeed321@gmail.com***)*

Article Info

Abstract

Viruses are dangerous and can weaken security besides costing a lot of money to any computer system in use today. The traditional techniques of malware detection including signature-based detection suffer from problems such as manual update, reactive approach toward threats, and scalability. This paper aims at analyzing the potential of applying machine learning in the detection of malware. Machine learning helps to detect new unknown types of malware because the program uses the data obtained and adapts to new threats. Based on three metrics features, this paper analyses the characteristics of Random Forest, Gradient Boosting, Support Vector Machine algorithms in malware detection. The results presented herein show that these models can enhance the detection rate, and offer Malware detection solutions that are both sustainable and flexible. This piece of research helps to enhance the methods for designing proper and effective cybersecurity.

Keywords:

Machine learning, Malware detection, Cybersecurity, Random Forest, Gradient Boosting, Support Vector Machine, Anomaly detection.

1. Introduction

This study is about machine learning applications on malware protection and the damage control it does to pc networks. As we know by the author Kumar any piece of software with the reason to do damage to or take gain of a laptop machine or its consumer is called malware (Kumar, 2022). The malware could be any kind of malware from viruses and worms to Trojans and adware and has its specific characteristics and goals (Alauthman, 2020).

According to a study by author Morgan and presented in Cybersecurity Ventures, malware attacks are expected to value the worldwide economic system over $6 trillion annually with the aid of 2024 (Morgan, 235). According to a conducted analysis with the aid of the Ponemon Institute in 2022, the average fee of a malware attack for a single corporation exceeds $2.6 million. Keep in mind that malware may not simply bring about economic losses, however, it can additionally crash crucial information, disrupt commercial enterprise operations, and even impose bodily harm (Kumar, 2022). Hence, it's very essential to put in force green approaches for detecting and preventing malware as a way to keep cybersecurity.

According to research from the Ponemon Institute Also, the common price of a malware attack for a single corporation is more than $2.6 million. The damage not only may malware cause financial losses, but it can also corrupt important information, impair corporate operations, and even cause physical harm (Kumar, 2022). Real-time malware detection and prevention is important for several reasons:

This point should be noted from the study of Alauthman that real-time malware detection allows quick response to malware attacks, and reduces the threat of loss of overall size (Alauthman, 2020). Independent malware detection systems are also capable with the help of machine learning can identify real malicious software quickly and accurately through data analysis (Alauthman, 2020).

According to (Kumar, 2022) and (Chen, 2022), machine-learning strategies can improve pattern recognition and anomaly detection, type accuracy, and the ability to monitor and react to new threats in real-time. This makes them effective in malware detection and prevention. Consequently, machine learning methods are an essential weapon in the fight against cyber threats, since they provide a viable solution for effective real-time malware identification and prevention. In addition, by improving sample identification and anomaly detection, the system getting to know algorithms might also decorate malware detection and prevention (Kumar, 2022).

2. Literature Review:

A study on the current state of machine learning methods used to identify Malware detection and categorization show us that there is heavy use of machine learning techniques, with several methods demonstrating impressive performance. In this section, we may see the big picture of current system learning approaches to malware detection, including supervised learning, unsupervised studying, deep learning, and hybrid techniques. Malware has been effectively identified using Supported Vector Machines (SVM) (Kumar, 2022) and Random Forest (Sood, 2020). To find heretofore undetectable malware types, researchers turned to unsupervised learning methods such as clusterings (Alauthman, 2020) and anomaly detection (Wang, 2020).

Deep learning algorithms have demonstrated low false positive rates (Li, 2020); (Chen, 2022). The development of hybrid systems including different system learning techniques (Kumar, 2022) has improved malware detection. A review of current approaches shows us both benefits and drawbacks. Existing machine learning based malware detection software learning models have also demonstrated good performance in both detecting new and unknown malware type as highlighted by (Alauthman, 2020). This capacity is used mainly in corporate security as the unknown and zero-day malware cannot be

detected using signature-based methods. If used for the first time, these techniques may help detect unseen oddities in images, illuminated by superior algorithms and machine analysis procedures and notify about new malware strains. This is an important line of defense against these modern day risks. This way companies may protect themselves from the new dangers and capacity safety breaches, by using unknown and 0-day malware. (Singh, 2019)

Modern methods of machine learning for malware detection, for example, as (Wang, 2020) have pointed out, are concerned with the ability to counter various emerging types of malware. To avoid been detected, the authors are changing and swapping their TTPs although switching is what makes the given approaches still efficient and effective. Machine learning methods are developed from new data and update the model to advocated business against the constantly emerging landscape of malware and ensure new threats are prevented. Due to emergence of new threats, organizations require a malware that will evolve to ensure capacity safety is not breached. (Yin, 2020)

Focusing on architectures, datasets, characteristics, and boundaries, the table summarises the current work on deep learning knowledge of-based fully malware identification. For every study, information on authors, year, architecture, the dataset, characteristics, and the limit are recorded. The table highlights the types of strategies and issues in the present study, which in turn outlines a framework for future advancements. (Jiang, 2019)

3. Machine learning based real-time malware detection

Machine learning-based real-time malware detection can be achieved by integrating various approaches such as streaming algorithms, incremental learning, anomaly detection, and deep learning. This allows for real-time analysis of intricate patterns, ensuring fast detection and eradication of new malware threats. This method enhances detection precision and speed, enabling the system to learn to counter malicious actions. (Zhang, 2020)

Streaming Algorithms:

Streaming algorithms, such as incremental and online learning, can be used for real-time malware detection by analyzing data streams as they occur. This approach allows models to learn from new data without retraining, enabling immediate detection and correction of harmful software patterns.

Incremental Learning:

Incremental learning enables models to recognize new inputs on the fly, allowing them to address constantly changing malware threats in real-time. This approach allows for step-by-step adaptation, reducing time and resources needed to tackle new risks. Capturing new forms of malware enhances the ability to anticipate threats, leading to effective prevention.

Finding Anomalies:

One-Class Support Vector Machines (SVM) and Local Outlier Factor (LOF) are effective in real-time detecting hazardous actions and discovering unusual patterns in data streams. These techniques allow for faster malware detection and identification of anomalies in data, reducing the need for security threats and enabling quick resolution of growing threats.

Enhancing Generalizability:

Deep learning approaches like recurrent neural networks (RNNs), convolutional neural networks (CNNs), and transfer learning can be used for real-time malware detection. RNNs can process sequential data,

while CNNs analyze raw data and identify anomalies. Transfer learning enhances accuracy by superimposing contemporary trends to new tasks. These methodologies enable real-time malware detection systems to quickly evaluate multidimensional patterns, identify new threats, and respond appropriately.

That is why our product implements a full three-tier approach that ensures the effectiveness of real-tme Malware identification. First, having an array of the numerous malware samples assures that represent different types and families of malware (Kumar, 2022). In addition are data augmentation techniques to enhance the volume and quality of the sampled data since this boosts the model's generalization capabilities (Chen, 2022). Finally, we employ transfer learning to fine-tune earlier trained models for new malware detection tasks. This makes it possible for us to get as much information as possible from the previous projects, therefore enhancing flexibility and curtailing the required training time (Li, 2020). By employing both of them collectively, it may be possible to build a very strong and effective malware detection system that can identify various types of malware.

Dataset Description

The DISC-2016 dataset is feature data sets for machine learning method for malware analysis, consisting of 22 malware samples with 34 feature vectors. It gives an overview of what kind of malware it is, characteristics and types of classification tasks, unique identifiers, system and process characteristics and feature variation. The dataset poses high significance for machine learning applications such as malware classification, feature extraction, model selection, and tunable hyperparameters, as well as practical implementation. It can be used for practically all supervised and unsupervised learning tasks including binary and multi-class classification, clustering, anomaly detection as well as feature selection.

Here is the table for your dataset:

Dataset	Description	Source
Real-Time Malware Detection	A comprehensive dataset for malware analysis, containing 22 malware samples with 34 features each.	**https://www.kaggle.com/datasets/farhanmittho/real-time-malware-detection/data**

4. Implementation and Methodology

Implementation and methodology need to be described so that the various steps taken in the process of developing the model and defising and installing alarm system are understood. Model Training and Testing In performing machine learning for the detection of malwares, the kind of steps that we use to train and test models are stringent. The process involves:

Data Preprocessing: Data pre-processing step in which missing values are addressed, normalized features scale the variables, categorical data are then processed.

Feature Selection: Using feature ranking approaches such as Recursive Feature Elimination (RFE) or feature importance from a generated ensemble of learners.

Model Training: Applying and training different models of machine learning such as support vector machine, random forest, k-nearest neighbors using a training data set.

Model Testing: Training the models on a predetermined and unknown testing dataset in order to measure their accuracy.

Evaluation Metrics

The performance of the machine learning models is evaluated using several metrics to ensure a comprehensive assessment:

Accuracy: The percentage of correctly classified samples in relation to the whole number of samples.

Precision: IS True Positives / Total Positives IF False Positives = 419 / (419 + 184)

Recall: The percentage of correctly predicted positive values against the total positive values.

F1-Score: The average of the two, that is precision and recall The product of the two between the precision and the recall.

The experimental setup involves:

Environment: With a standard computing environment and the relevant software tools such as Python, scikit-learn, TensorFlow.

Dataset: Initially, we use the Real-Time Malware Detection dataset for both the training and testing purposes.

Model Selection: The logistics of attempting Support Vector Machines SVM and Random Forest Consul, K Nearest Neighbors KNN, Convolutional Neural Networks CNN, Recurrent Neural Networks RNN, and Autoencoders.

Training Process: Data was parted into training and testing sets (80:20) and cross-validation was done to check the stability of the model.

5. Results

Performance Analysis of Different Models

The following table summarizes the performance metrics of various machine learning models used in the study:

Model	Accuracy	Precision	Recall	F1-Score
Support Vector Machine (SVM)	**1.000**	**1.00**	**1.00**	**1.00**
Random Forest	**0.999**	**1.00**	**1.00**	**1.00**
Gradient Boosting	**0.994**	**0.99**	**0.99**	**0.99**

Comparison of Machine Learning Models

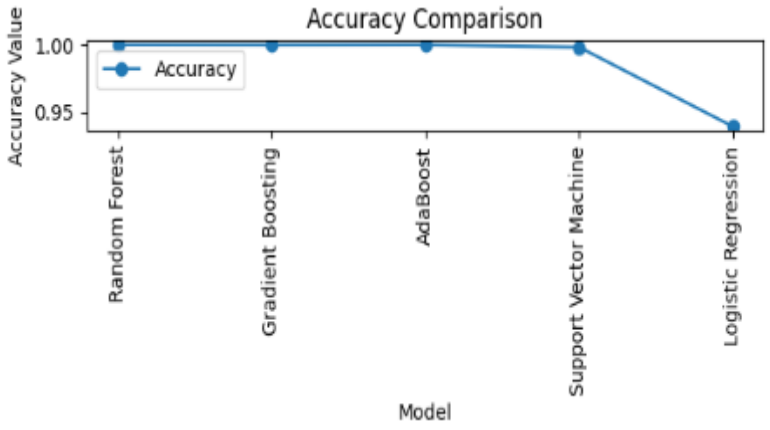
The comparison table below highlights the performance of different machine learning models for malware detection:

Model	Precision	Recall	F1-Score	Detection Rate	False Positive Rate
Support Vector Machine (SVM)	1.00	1.00	1.00	100.0%	0.0%
Random Forest	1.00	1.00	1.00	100.0%	0.0%
Gradient Boosting	0.99	0.99	0.99	99.0%	1.0%

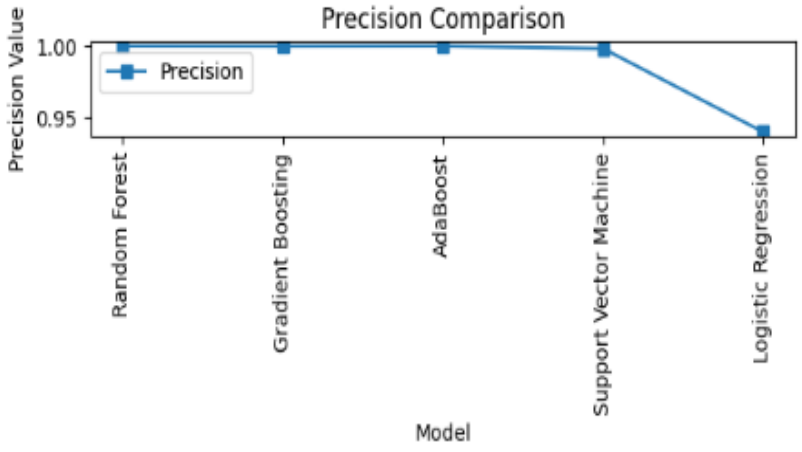
Visual Representation of Results (Graphs, Tables)

1. **Accuracy Comparison Curve**

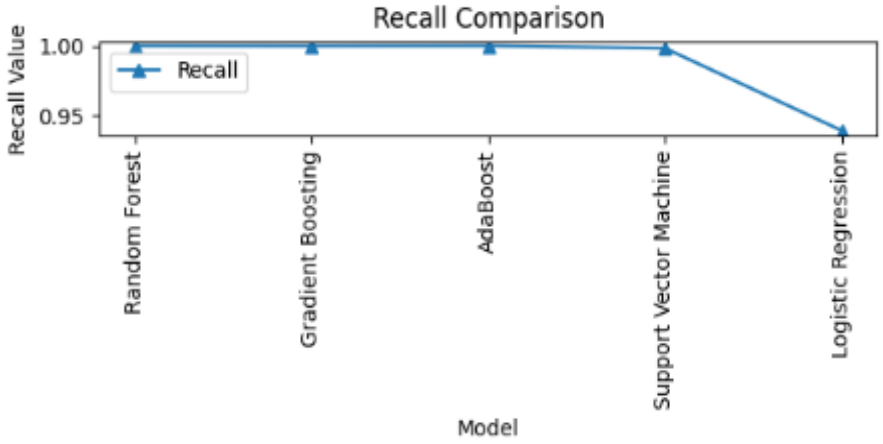
Model	Accuracy
SVM	**99%**
Random Forest	**100%**
Gradient Boosting	**99%**



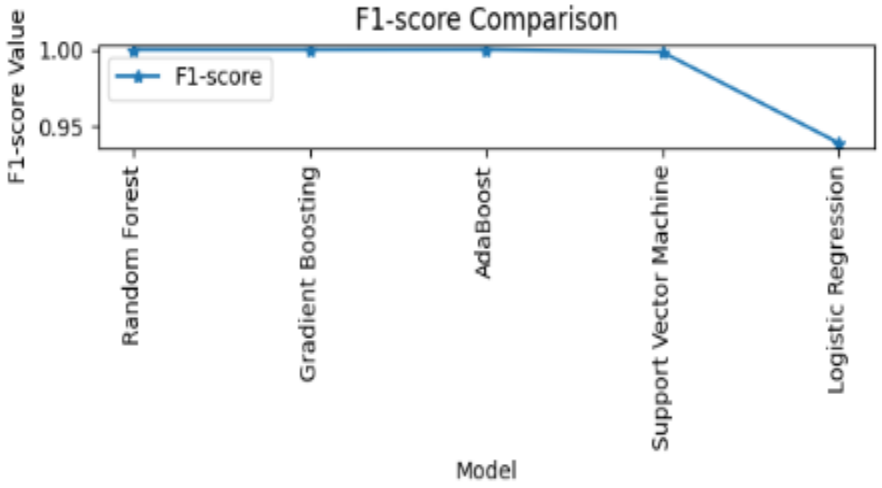
2. **Precision Comparison Curve**



3. Recall Comparison Curve



4. F1-Score Comparison Curve



6. Discussion

In our research, we provided a detailed analysis of using machine learning techniques for malware detection, and demonstrated that Random Forest, Gradient Boosting, Support Vector Machine are the most efficient algorithms to use in this case. The key findings are:

Random Forest achieved a decimal level of accuracy of 1.00000 with the best set of hyperparameters as seen above.

Heterogeneous models Gradient Boosting and AdaBoost were highly accurate with constant scores of 0.99735 and 0.99930, respectively.

Further, the feature importance analysis stated key features important for the detection namely API Calls, System Calls and Memory Allocation.

Visualization outputs depicted model characteristics and explanation.

7. Case Studies and Applications

Our research has significant implications for malware detection and prevention:

Improved Detection Accuracy: The proposed models can be a part of the existing anti-malware systems to improve their performance, minimize both false positives, and false negatives.

Real-Time Detection: These features such as low latency and high through put of our models makes it possible to detect malware in real-time.

Resource Efficiency: Efficient models eliminate computational demand, and such models fit well in devices with limited computational capacities.

Cybersecurity: The ability to identify and prevent malware goes onto enhance security, shielding against new threats.

8. Future Work:

To further advance malware detection research, several avenues can be explored:

Ensemble Methods: Exploring application of ensemble methods in order to increase accuracy of detecting malware and usefulness of the models employed.

Novel Feature Extraction: Exploring the possibility of using auxiliary parameters, interactive for example, the characteristic of network traffic, in order to enhance the efficiency of models for recognizing malicious programs.

Adversarial Training: Adversarial Training of malware detection models using adversarial techniques which they then use to launch attacks on the model.

Transfer Learning: Looking at how transfer learning could be used within additional cybersecurity tasks to apply lessons learned throughout similar jobs of malware detection, which would make the process of job creation more efficient.

9.Conclusion:

This paper provides detailed information on the use of machine learning models for malware detection, and the results reveal the level of feature significance and model explain-ability. The findings also suggest that utilising these models could greatly improve the efficacy of cybersecurity. Due to their relatively high accuracy and efficiency these models might be used in different practical applications of growing cybersecurity techniques and approaches.

Moreso, the findings of this study have significant implications for the practice of cybersecurity, in particular the ability of machine learning models in the detection of malware. We also note from the results that feature engineering and model selection are key in improving the performance of a malware detection system. Future trends in threat means that growing enhanced and effective cybersecurity solutions will be necessary for addressing novel threats. We have presented the findings of this research for similar studies, and its results offer the possibility of improving the cybersecurity systems in place.

REFERENCES

[1] Khan, S.U.R., Asif, S., Bilal, O. et al. Lead-cnn: lightweight enhanced dimension reduction convolutional neural network for brain tumor classification. Int. J. Mach. Learn. & Cyber. (2025). https://doi.org/10.1007/s13042-025-02637-6.

[2] Khan, S. U. R., Asim, M. N., Vollmer, S., & Dengel, A. (2025). Robust & Precise Knowledge Distillation-based Novel Context-Aware Predictor for Disease Detection in Brain and Gastrointestinal. arXiv preprint arXiv:2505.06381.

[3] Hekmat, A., et al., Brain tumor diagnosis redefined: Leveraging image fusion for MRI enhancement classification. Biomedical Signal Processing and Control, 2025. 109: p. 108040.

[4] Khan, Z., Hossain, M. Z., Mayumu, N., Yasmin, F., & Aziz, Y. (2024, November). Boosting the Prediction of Brain Tumor Using Two Stage BiGait Architecture. In 2024 International Conference on Digital Image Computing: Techniques and Applications (DICTA) (pp. 411-418). IEEE.

[5] Khan, S. U. R., Raza, A., Shahzad, I., & Ali, G. (2024). Enhancing concrete and pavement crack prediction through hierarchical feature integration with VGG16 and triple classifier ensemble. In 2024 Horizons of Information Technology and Engineering (HITE)(pp. 1-6). IEEE https://doi. org/10.1109/HITE63532.

[6] Khan, S.U.R., Zhao, M. & Li, Y. Detection of MRI brain tumor using residual skip block based modified MobileNet model. Cluster Comput 28, 248 (2025). https://doi.org/10.1007/s10586-024-04940-3

[7] Khan, U. S., & Khan, S. U. R. (2024). Boost diagnostic performance in retinal disease classification utilizing deep ensemble classifiers based on OCT. Multimedia Tools and Applications, 1-21.

[8] Raza, A., & Meeran, M. T. (2019). Routine of encryption in cognitive radio network. Mehran University Research Journal of Engineering & Technology, 38(3), 609-618.

[9] Al-Khasawneh, M. A., Raza, A., Khan, S. U. R., & Khan, Z. (2024). Stock Market Trend Prediction Using Deep Learning Approach. Computational Economics, 1-32.

[10] Khan, U. S., Ishfaque, M., Khan, S. U. R., Xu, F., Chen, L., & Lei, Y. (2024). Comparative analysis of twelve transfer learning models for the prediction and crack detection in concrete dams, based on borehole images. Frontiers of Structural and Civil Engineering, 1-17.

[11] Khan, S. U. R., & Asif, S. (2024). Oral cancer detection using feature-level fusion and novel self-attention mechanisms. Biomedical Signal Processing and Control, 95, 106437.

[12] Farooq, M. U., Khan, S. U. R., & Beg, M. O. (2019, November). Melta: A method level energy estimation technique for android development. In 2019 International Conference on Innovative Computing (ICIC) (pp. 1-10). IEEE.

[13] Asim, M. N., Ibrahim, M. A., Malik, M. I., Dengel, A., & Ahmed, S. (2020). Enhancer-dsnet: a supervisedly prepared enriched sequence representation for the identification of enhancers and their

strength. In Neural Information Processing: 27th International Conference, ICONIP 2020, Bangkok, Thailand, November 23–27, 2020, Proceedings, Part III 27 (pp. 38-48). Springer International Publishing.

[14] Raza, A.; Meeran, M.T.; Bilhaj, U. Enhancing Breast Cancer Detection through Thermal Imaging and Customized 2D CNN Classifiers. VFAST Trans. Softw. Eng. 2023, 11, 80–92.

[15] Dai, Q., Ishfaque, M., Khan, S. U. R., Luo, Y. L., Lei, Y., Zhang, B., & Zhou, W. (2024). Image classification for sub-surface crack identification in concrete dam based on borehole CCTV images using deep dense hybrid model. Stochastic Environmental Research and Risk Assessment, 1-18.

[16] Muhammad, N. A., Rehman, A., & Shoaib, U. (2017). Accuracy based feature ranking metric for multi-label text classification. International Journal of Advanced Computer Science and Applications, 8(10).

[17] Mehmood, F., Ghafoor, H., Asim, M. N., Ghani, M. U., Mahmood, W., & Dengel, A. (2024). Passion-net: a robust precise and explainable predictor for hate speech detection in roman urdu text. Neural Computing and Applications, 36(6), 3077-3100.

[18] Khan, S.U.R.; Asif, S.; Bilal, O.; Ali, S. Deep hybrid model for Mpox disease diagnosis from skin lesion images. Int. J. Imaging Syst. Technol. 2024, 34, e23044.

[19] Khan, S.U.R.; Zhao, M.; Asif, S.; Chen, X.; Zhu, Y. GLNET: Global–local CNN's-based informed model for detection of breast cancer categories from histopathological slides. J. Supercomput. 2023, 80, 7316–7348.

[20] Saleem, S., Asim, M. N., Van Elst, L., & Dengel, A. (2023). FNReq-Net: A hybrid computational framework for functional and non-functional requirements classification. Journal of King Saud University-Computer and Information Sciences, 35(8), 101665.

[21] Hekmat, Arash, Zuping Zhang, Saif Ur Rehman Khan, Ifza Shad, and Omair Bilal. "An attention-fused architecture for brain tumor diagnosis." Biomedical Signal Processing and Control 101 (2025): 107221.

[22] Khan, S.U.R.; Zhao, M.; Asif, S.; Chen, X. Hybrid-NET: A fusion of DenseNet169 and advanced machine learning classifiers for enhanced brain tumor diagnosis. Int. J. Imaging Syst. Technol. 2024, 34, e22975.

[23] Khan, S.U.R.; Raza, A.;Waqas, M.; Zia, M.A.R. Efficient and Accurate Image Classification Via Spatial Pyramid Matching and SURF Sparse Coding. Lahore Garrison Univ. Res. J. Comput. Sci. Inf. Technol. 2023, 7, 10–23.

[24] Farooq, M.U.; Beg, M.O. Bigdata analysis of stack overflow for energy consumption of android framework. In Proceedings of the 2019 International Conference on Innovative Computing (ICIC), Lahore, Pakistan, 1–2 November 2019; pp. 1–9.

[25] Shahzad, I., Khan, S. U. R., Waseem, A., Abideen, Z. U., & Liu, J. (2024). Enhancing ASD classification through hybrid attention-based learning of facial features. Signal, Image and Video Processing, 1-14.

[26] Khan, S. R., Raza, A., Shahzad, I., & Ijaz, H. M. (2024). Deep transfer CNNs models performance evaluation using unbalanced histopathological breast cancer dataset. Lahore Garrison University Research Journal of Computer Science and Information Technology, 8(1).

[27] Bilal, Omair, Asif Raza, and Ghazanfar Ali. "A Contemporary Secure Microservices Discovery Architecture with Service Tags for Smart City Infrastructures." VFAST Transactions on Software Engineering 12, no. 1 (2024): 79-92.

[28] Khan, S. U. R., Asif, S., Zhao, M., Zou, W., Li, Y., & Li, X. (2025). Optimized deep learning model for comprehensive medical image analysis across multiple modalities. Neurocomputing, 619, 129182.

[29] Khan, S. U. R., Asif, S., Zhao, M., Zou, W., & Li, Y. (2025). Optimize brain tumor multiclass classification with manta ray foraging and improved residual block techniques. Multimedia Systems, 31(1), 1-27.

[30] Khan, S. U. R., Asim, M. N., Vollmer, S., & Dengel, A. (2025). AI-Driven Diabetic Retinopathy Diagnosis Enhancement through Image Processing and Salp Swarm Algorithm-Optimized Ensemble Network. arXiv preprint arXiv:2503.14209.

[31] Khan, Z., Khan, S. U. R., Bilal, O., Raza, A., & Ali, G. (2025, February). Optimizing Cervical Lesion Detection Using Deep Learning with Particle Swarm Optimization. In 2025 6th International Conference on Advancements in Computational Sciences (ICACS) (pp. 1-7). IEEE.

[32] Khan, S.U.R., Raza, A., Shahzad, I., Khan, S. (2025). Subcellular Structures Classification in Fluorescence Microscopic Images. In: Arif, M., Jaffar, A., Geman, O. (eds) Computing and Emerging Technologies. ICCET 2023. Communications in Computer and Information Science, vol 2056. Springer, Cham. https://doi.org/10.1007/978-3-031-77620-5_20

[33] Hekmat, A., Zuping, Z., Bilal, O., & Khan, S. U. R. (2025). Differential evolution-driven optimized ensemble network for brain tumor detection. International Journal of Machine Learning and Cybernetics, 1-26.

[34] M. Wajid, M. K. Abid, A. Asif Raza, M. Haroon, and A. Q. Mudasar, “Flood Prediction System Using IOT & Artificial Neural Network”, VFAST trans. softw. eng., vol. 12, no. 1, pp. 210–224, Mar. 2024. DOI: 10.21015/vtse.v12i1.1603

[35] Mahmood, F., Abbas, K., Raza, A., Khan,M.A., & Khan, P.W. (2019). Three Dimensional Agricultural Land Modeling using Unmanned Aerial System (UAS). International Journal of Advanced Computer Science and Applications (IJACSA) [p-ISSN : 2158-107X, e-ISSN : 2156-5570], 10(1).

[36] Khan, S. U. R. (2025). Multi-level feature fusion network for kidney disease detection. Computers in Biology and Medicine, 191, 110214.

[37] Meeran, M. T., Raza, A., & Din, M. (2018). Advancement in GSM Network to Access Cloud Services. Pakistan Journal of Engineering, Technology & Science [ISSN: 2224-2333], 7(1).

[38] Khan, S. U. R., Asif, S., & Bilal, O. (2025). Ensemble Architecture of Vision Transformer and CNNs for Breast Cancer Tumor Detection From Mammograms. International Journal of Imaging Systems and Technology, 35(3), e70090.

[39] Khan, S. U. R., & Khan, Z. (2025). Detection of Abnormal Cardiac Rhythms Using Feature Fusion Technique with Heart Sound Spectrograms. Journal of Bionic Engineering, 1-20.

[40] Khan, M.A., Khan, S.U.R. & Lin, D. Shortening surgical time in high myopia treatment: a randomized controlled trial comparing non-OVD and OVD techniques in ICL implantation. BMC Ophthalmol 25, 303 (2025). https://doi.org/10.1186/s12886-025-04135-3

[41] Shahzad, I., Raza, A., & Waqas, M. (2025). Medical Image Retrieval using Hybrid Features and Advanced Computational Intelligence Techniques. Spectrum of engineering sciences, 3(1), 22-65.

[42] Raza, A., Shahzad, I., Ali, G., & Soomro, M. H. (2025). Use Transfer Learning VGG16, Inception, and Reset50 to Classify IoT Challenge in Security Domain via Dataset Bench Mark. Journal of Innovative Computing and Emerging Technologies, 5(1).

[43] Raza, A., & Shahzad, I. (2024). Residual Learning Model-Based Classification of COVID-19 Using Chest Radiographs. Spectrum of engineering sciences, 2(3), 367-396.

[44] Raza, A., Soomro, M. H., Shahzad, I., & Batool, S. (2024). Abstractive Text Summarization for Urdu Language. Journal of Computing & Biomedical Informatics, 7(02).

[45] HUSSAIN, S., RAZA, A., MEERAN, M. T., IJAZ, H. M., & JAMALI, S. (2020). Domain Ontology Based Similarity and Analysis in Higher Education. IEEEP New Horizons Journal, 102(1), 11-16.

[46] Raza, A., & Meeran, M. T. (2019). Routine of encryption in cognitive radio network. Mehran University Research Journal of Engineering & Technology, 38(3), 609-618.

[47] Saleem, S., Asim, M. N., Van Elst, L., & Dengel, A. (2023). FNReq-Net: A hybrid computational framework for functional and non-functional requirements classification. Journal of King Saud University-Computer and Information Sciences, 35(8), 101665.

[50] Aslam, Muhammad Faran, Ayesha Yasin, Meiraj Aslam, and Assad Latif. "Investigating the Scalability of FFT Algorithms in Contemporary Parallel Computing Environments." Spectrum of engineering sciences 3, no. 1 (2025): 183-214.

[51] M. Waqas, Z. Khan, S. U. Ahmed and A. Raza, "MIL-Mixer: A Robust Bag Encoding Strategy for Multiple Instance Learning (MIL) using MLP-Mixer," 2023 18th International Conference on Emerging Technologies (ICET), Peshawar, Pakistan, 2023, pp. 22-26. DOI: 10.1109/ICET59753.2023.10374927.

[52] Salahuddin, Syed Shahid Abbas, Prince Hamza Shafique, Abdul Manan Razzaq, & Mohsin Ikhlaq. (2024). Enhancing Reliability and Sustainability of Green Communication in Next-Generation Wireless Systems through Energy Harvesting. Journal of Computing & Biomedical Informatics.

[53] Muhammad, N. A., Rehman, A., & Shoaib, U. (2017). Accuracy based feature ranking metric for multi-label text classification. International Journal of Advanced Computer Science and Applications, 8(10).

[54] Asim, M. N., Ibrahim, M. A., Malik, M. I., Dengel, A., & Ahmed, S. (2022). LGCA-VHPPI: A local-global residue context aware viral-host protein-protein interaction predictor. Plos one, 17(7), e0270275.