Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 4, 2026

INTELLIGENT ADAPTIVE MACHINE LEARNING SCALABLE FRAMEWORK FOR DYNAMIC MALWARE IDENTIFICATION AND PROACTIVE THREAT PREVENTION

[1]Saleh Rehman, [2]Sonia Jamil, [*3]Nasir Hussain, [4]Assad Latif, [5]Sohail Ahmad

[1]Department of Business Administration, University of Education Lahore, Multan Campus.
[2]Department of Computer Science and Information Technology ,University of Southern Punjab,Multan,Pakistan.
[3]Department of Computer Science and Information Technology ,University of Southern Punjab,Multan,Pakistan.
[4]School of Management and Economics North china university of Water Resources and Electric Power, Zhengzhou Henan China
[5]Department of Computer Science & IT, Islamia University Bahawalpur, Pakistan.
*[*3]nasirhussain1192@gmail.com*

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

Article History
Received on 27 March, 2026
Accepted on 15April, 2026
Published on 16 April, 2026

Corresponding Author:
Nasir Hussain

Abstract

Malware and computer viruses continue to pose serious threats to modern digital systems, often compromising security and leading to significant financial losses. As technology evolves, traditional malware detection methods–particularly signature-based approaches–are becoming less effective. These methods rely heavily on manual updates, respond only after threats are identified, and struggle to keep up with the growing volume and complexity of cyberattacks. In this study, we explore the potential of machine learning as a more advanced and proactive solution for malware detection. Unlike conventional techniques, machine learning models can learn from historical data and identify patterns that indicate malicious behavior. This capability allows them to detect previously unknown or emerging malware variants without requiring explicit signatures. The research focuses on evaluating the performance of three widely used machine learning algorithms: Random Forest, Gradient Boosting, and Support Vector Machine. These models are analyzed based on key feature sets and performance metrics to determine their effectiveness in identifying malicious software. Experimental findings demonstrate that these algorithms significantly improve detection accuracy while reducing false positives.Furthermore, the adaptability of machine learning models enables continuous improvement as new data becomes available, making them highly suitable for dynamic threat environments. The proposed approach also supports real-time detection, which is critical for minimizing damage caused by fast-spreading malware. In addition, the scalability of these techniques allows them to be implemented across large and complex networks without major performance degradation. This study also highlights the importance of feature selection and data preprocessing in improving model efficiency and accuracy. By integrating intelligent detection mechanisms, organizations can strengthen their cybersecurity infrastructure and respond more effectively to evolving threats. Overall, this research contributes to the development of robust, flexible, and sustainable malware detection systems, offering a promising direction for future advancements in cybersecurity.

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:

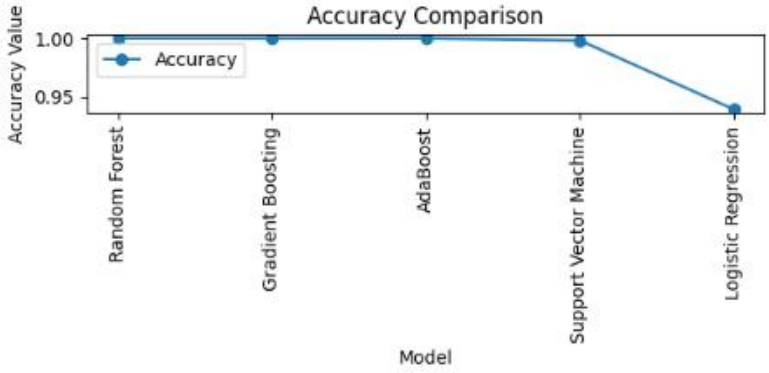
Model	Precision	Recall	F1-Score	Detection Rate	False Positive Rate
Support Vector Machine (SVM)	1.00	1.00	1.00	100.0%	0.0%
Random Forest	1.00	1.00	1.00	100.0%	0.0%
Gradient Boosting	0.99	0.99	0.99	99.0%	1.0%

Visual Representation of Results (Graphs, Tables)

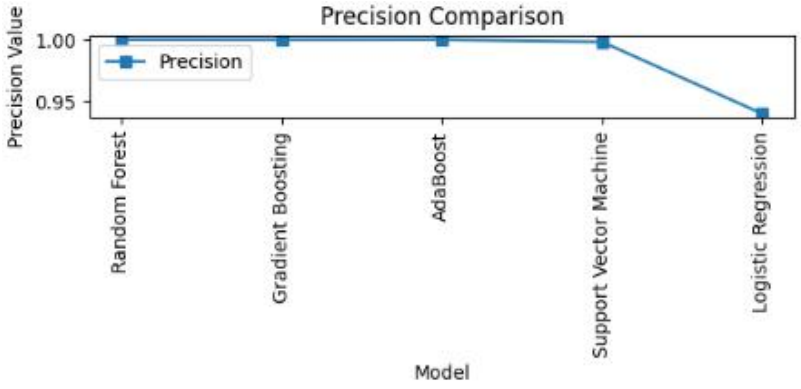
Accuracy Comparison Curve

Model	Accuracy
SVM	99%
Random Forest	100%

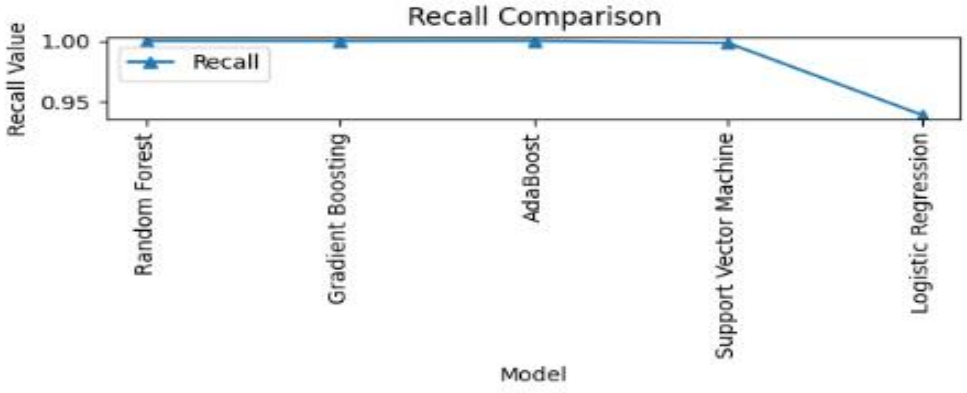
Gradient Boosting	99%



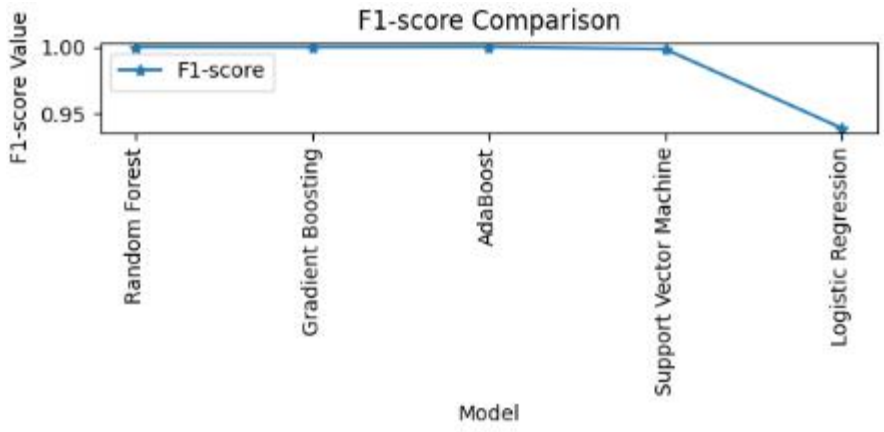
1. **Precision Comparison Curve**



2. **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.Waqas, Muhammd, Muhammad Atif Tahir, and Rizwan Qureshi. "Ensemble-based instance relevance estimation in multiple-instance learning." In 2021 9th European workshop on visual information processing (EUVIP), pp. 1-6. IEEE, 2021.

2.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

3.Shahzad, Inzamam, Jianquan Ouyang, and Saif Ur Rehman Khan. "FedVC-ADDiM: a federated learning framework for diagnosis of alzheimer disease using deep learning." Multimedia Systems 32, no. 3 (2026): 161. https://doi.org/10.1007/s00530-026-02229-6

4.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.

5.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

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

7.Ishfaque, Muhammad, Saif Ur Rehman Khan, and Yulong Lou. "Digitizing Health Monitoring in Engineering Structures Using Deep Learning: A Novel Block Architecture for Concrete Crack Prediction in Surface and Sub-surface Dataset." Journal of Bionic Engineering (2026): 1-23.

8.Khan, Saif Ur Rehman, Asif Raza, Inzamam Shahzad, and Ghazanfar Ali. "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, 2024.

9.Waqas, Muhammad, Zeshan Khan, Shaheer Anjum, and Muhammad Atif Tahir. "Lung-Wise Tuberculosis Analysis and Automatic CT Report Generation with Hybrid Feature and Ensemble Learning." In CLEF (Working notes), pp. 1-10. 2020.

10.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.

11.Waqas, Muhammad, Syed Umaid Ahmed, Muhammad Atif Tahir, Jia Wu, and Rizwan Qureshi. "Exploring multiple instance learning (MIL): A brief survey." Expert Systems with Applications 250 (2024): 123893.

12.Al-Khasawneh, Mahmoud Ahmad, Asif Raza, Saif Ur Rehman Khan, and Zia Khan. "Stock Market Trend Prediction Using Deep Learning Approach." Computational Economics (2024): 1-32

13.Khan, Muhammad Ahmed, Manqiang Peng, Ding Lin, and Saif Ur Rehman Khan. "Deep Learning Based Estimation of Blood Glucose Levels from Multidirectional Scleral Blood Vessel Imaging." arXiv preprint arXiv:2603.12715 (2026).

14.Khan, Saif Ur Rehman, Muhammad Nabeel Asim, Sebastian Vollmer, and Andreas Dengel. "FloraSyntropy-net: scalable deep learning with novel FloraSyntropy archive for large-scale plant disease diagnosis." Plant Methods (2026).

15.Ur Rehman Khan, Saif, Omair Bilal, Arash Hekmat, Inzamam Shahzad, and Asif Raza. "Advancing food safety: deep learning for accurate detection of bacterial contaminants." Memetic Computing 18, no. 1 (2026): 11.

16.Waqas, Muhammad, Muhammad Atif Tahir, Sumaya Al-Maadeed, Ahmed Bouridane, and Jia Wu. "Simultaneous instance pooling and bag representation selection approach for multiple-instance learning (MIL) using vision transformer." Neural Computing and Applications 36, no. 12 (2024): 6659-6680.

17.Hekmat, Arash, Omair Bilal, Zuping Zhang, Saif Ur Rehman Khan, and Sohaib Asif. "FRE-Net: A Fuzzy Richards Functions-Based Ensemble Network for Brain Tumor Detection." Journal of Bionic Engineering (2026): 1-23.

18.Mayumu, Nicanor, Xiaoheng Deng, Antoine Bagula, and Patrick Mukala. "V2X-JEPA: Self-Supervised Multi-Agent Joint Embedding Predictive Architecture for Robust Vehicle-to-Everything Perception." IEEE Internet of Things Journal (2026).

19.Waqas, Muhammad, Muhammad Atif Tahir, and Salman A. Khan. "Robust bag classification approach for multi-instance learning via subspace fuzzy clustering." Expert Systems with Applications 214 (2023): 119113.

20.Bilal, Omair, Arash Hekmat, Inzamam Shahzad, Asif Raza, and Saif Ur Rehman Khan. "Boosting Machine Learning Accuracy for Cardiac Disease Prediction: The Role of Advanced Feature Engineering and Model Optimization." The Review of Socionetwork Strategies (2025): 1-30.

21.Khan, Saif Ur Rehman, Muhammad Nabeel Asim, Sebastian Vollmer, and Andreas Dengel. "Temperature-driven robust disease detection in brain and gastrointestinal disorders via context-aware adaptive knowledge distillation." Biomedical Signal Processing and Control 112 (2026): 108671.

22.Khan, S. U. R., Asif, S., Zhao, M., Zou, W., Li,

Y., & Xiao, C. (2026). ShallowMRI: A novel lightweight CNN with novel attention mechanism for Multi brain tumor classification in MRI images. Biomedical Signal Processing and Control, 111, 108425.

23.Khan, M. A., Khan, S. U. R., Rehman, H. U., Aladhadh, S., & Lin, D. (2025). Robust InceptionV3 with Novel EYENET Weights for Di-EYENET Ocular Surface Imaging Dataset: Integrating Chain Foraging and Cyclone Aging Techniques. International Journal of Computational Intelligence Systems, 18(1), 1-26.

24.Arif, Hamza, Muhammad Tanveer Meeran, Sabiha Anum, and Assad Latif. "SIMULATING NEXT-GENERATION DATA STORAGE ARCHITECTURES USING DNA, GRAPHENE, AND NEURAL ENCODING." Spectrum of Engineering Sciences 4, no. 1 (2026): 240-255.

25.Khan, U. S., & Khan, S. U. R. (2025). Ethics by Design: A Lifecycle Framework for Trustworthy AI in Medical Imaging From Transparent Data Governance to Clinically Validated Deployment. arXiv preprint arXiv:2507.04249.

26.Waqas, Muhammad, Muhammad Atif Tahir, and Rizwan Qureshi. "Deep Gaussian mixture model based instance relevance estimation for multiple instance learning applications." Applied intelligence 53, no. 9 (2023): 10310-10325.

27.Khan, S. U. R., Rehman, H. U., & Bilal, O. (2025). AI-powered cancer diagnosis: classifying viable (live) vs non-viable (dead) cells using transfer learning. Signal, Image and Video Processing, 19(15), 1326.

28. Khan, S. U. R., Asif, S., Zhao, M., Zou, W., Li, Y., & Xiao, C. (2026). ShallowMRI: A novel lightweight CNN with novel attention mechanism for Multi brain tumor classification in MRI images. Biomedical Signal Processing and Control, 111, 108425.

29.Waqas M, Bandyopadhyay R, Showkatian E, Muneer A, Zafar A, Alvarez FR, Marin MC, Li W, Jaffray D, Haymaker C, Heymach J. The Next Layer: Augmenting Foundation Models with Structure-Preserving and Attention-Guided Learning for Local Patches to Global Context Awareness in Computational Pathology. arXiv preprint arXiv:2508.19914. 2025 Aug 27.

30.Shahzad, Inzamam, Asif Raza, and Muhammad Waqas. "Medical Image Retrieval using Hybrid Features and Advanced Computational Intelligence Techniques." Spectrum of engineering sciences 3, no. 1 (2025): 22-65.

31.Bilal, O., Hekmat, A., Shahzad, I. et al. Boosting Machine Learning Accuracy for Cardiac Disease Prediction: The Role of Advanced Feature Engineering and Model Optimization. Rev Socionetwork Strat (2025). https://doi.org/10.1007/s12626-025-00190-w

32.Asif Raza, Inzamam Shahzad, Ghazanfar Ali, and Muhammad Hanif Soomro. "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, no. 1 (2025).

33.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.

34.Waqas, Muhammad, Zeshan Khan, Shaheer Anjum, and Muhammad Atif Tahir. "Lung-Wise Tuberculosis Analysis and Automatic CT Report Generation with Hybrid Feature and Ensemble Learning." In CLEF (Working notes), pp. 1-10. 2020.

35.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.

36.Asif Raza, Salahuddin, Ghazanfar Ali, Muhammad Hanif Soomro, Saima Batool, "Analyzing the Impact of Artificial Intelligence on Shaping Consumer Demand in E-Commerce: A Critical Review", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.17, No.5, pp. 42-61, 2025. DOI:10.5815/ijieeb.2025.05.04

37. Khan, M. A., Khan, S. U. R., Rehman, H. U., Aladhadh, S., & Lin, D. (2025). Robust InceptionV3 with Novel EYENET Weights for Di-EYENET Ocular Surface Imaging Dataset: Integrating Chain Foraging and Cyclone Aging Techniques. International Journal of Computational Intelligence Systems, 18(1), 204.

38.Raza, Asif, Inzamam Shahzad, Muhammad Salahuddin, and Sadia Latif. "Satellite Imagery Employed to Analyze the Extent of Urban Land Transformation in The Punjab District of Pakistan." Journal of Palestine Ahliya University for Research and Studies 4, no. 2 (2025): 17-36.

39.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.

40.Khan, Saif Ur Rehman, Asif Raza, Inzamam Shahzad, and Shehzad Khan. "Subcellular Structures Classification in Fluorescence Microscopic Images." In International Conference on Computing & Emerging Technologies, pp. 271-286. Cham: Springer Nature Switzerland, 2023.

41.Maqsood, H., & Khan, S. U. R. (2025). MeD-3D: A Multimodal Deep Learning Framework for Precise Recurrence Prediction in Clear Cell Renal Cell Carcinoma (ccRCC). arXiv preprint arXiv:2507.07839.

42.Raza, Asif, Salahuddin, & Inzamam Shahzad. (2024). Residual Learning Model-Based Classification of COVID-19 Using Chest Radiographs. Spectrum of Engineering Sciences, 2(3), 367–396.

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

44.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.

45.S. U. R. Khan, A. Raza, I. Shahzad and G. Ali, "Enhancing Concrete and Pavement Crack Prediction through Hierarchical Feature Integration with VGG16 and Triple Classifier Ensemble," 2024 Horizons of Information Technology and Engineering (HITE), Lahore, Pakistan, 2024, pp. 1-6.

46.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).

47.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.

48.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.

49.Raza, A., & Meeran, M. T. (2019). Routine of Encryption in Cognitive Radio Network. Mehran University Research Journal of Engineering and Technology [p-ISSN: 0254-7821, e-ISSN: 2413-7219], 38(3), 609-618.

50.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).

51.Bilal, O., Hekmat, A., & Khan, S. U. R. (2025). Automated cervical cancer cell diagnosis via grid search-optimized multi-CNN ensemble networks. Network Modeling Analysis in Health Informatics and Bioinformatics, 14(1), 67.

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

53.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.

54.N. Mayumu, D. Xiaoheng, P. Mukala, S. U. R. Khan and M. U. Saeed, "Omni-V2X: A Vision-Language Model for Actionable Insights in Vehicle-to-Everything Systems," 2025 International Joint Conference on Neural Networks (IJCNN), Rome, Italy, 2025, pp. 1-8, doi: 10.1109/IJCNN64981.2025.11228491.

55.Khan, S. R., Asif Raza, Inzamam Shahzad, & Hafiz Muhammad Ijaz. (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).

56.M. Waqas, Z. Khan, S. U. Ahmed and Asif. 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.

57.S. ur R. Khan, Asif. Raza, Muhammad Tanveer Meeran, and U. Bilhaj, “Enhancing Breast Cancer Detection through Thermal Imaging and Customized 2D CNN Classifiers”, VFAST trans. softw. eng., vol. 11, no. 4, pp. 80–92, Dec. 2023.

58.Yang, H., Khan, S. U. R., Bilal, O., Chen, C., & Zhao, M. (2025). CEOE-Net: Chaotic Evolution Algorithm-Based Optimized Ensemble Framework Enhanced with Dual-Attention for Alzheimer’s Diagnosis. Computer Modeling in Engineering & Sciences, 145(2), 2401.

59.Chomba, B., Mukala, P., Mayumu, N., & Khan, S. U. R. (2025). DynaKG: Dynamic Knowledge Graph Attention With Learnable Temporal Decay for Recommendation. IEEE Access, 13, 216956-216970.

60.O. Bilal, Asif Raza, S. ur R. Khan, and Ghazanfar Ali, “A Contemporary Secure Microservices Discovery Architecture with Service Tags for Smart City Infrastructures ”, VFAST trans. softw. eng., vol. 12, no. 1, pp. 79–92, Mar. 2024

61.S. U. R. Khan, A. Raza, I. Shahzad and G. Ali, "Enhancing Concrete and Pavement Crack Prediction through Hierarchical Feature Integration with VGG16 and Triple Classifier Ensemble," 2024 Horizons of Information Technology and Engineering (HITE), Lahore, Pakistan, 2024, pp. 1-6, doi: 10.1109/HITE63532.2024.10777242.

62.Ishfaque, M., Khan, S. U. R., & Lou, Y. L. (2026). Towards efficient dam inspection: crack detection via chirplet transform feature and a pruned VGG16 architecture. Memetic Computing, 18(1), 9.

63.S. Ur Rehman Khan, O. Bilal, S. Mistry, N. Deb, M. Mahmud and M. Bhuyan, "KDLight: A Lightweight Knowledge Distillation Framework for Medical Image Classification," 2025 International Joint Conference on Neural Networks (IJCNN), Rome, Italy, 2025, pp. 1-8, doi: 10.1109/IJCNN64981.2025.11228615.

64.O. Bilal, S. Ur Rehman Khan, S. Mistry, N. Deb, M. Mahmud and M. Bhuyan, "Towards Efficient Pruning and Multi-Scale Feature Transformations to Uncover Medical Diseases," 2025 International Joint Conference on Neural Networks (IJCNN), Rome, Italy, 2025, pp. 1-8, doi: 10.1109/IJCNN64981.2025.11229047.

65.Khan, S. R., Raza, A., Waqas, M., & Raphay Zia, M. A. (2024). Efficient and Accurate Image Classification via Spatial Pyramid Matching and SURF Sparse Coding. Lahore Garrison University Research Journal of Computer Science and Information Technology, 7(4).

66.Shahzad, Inzamam, Asif Raza, Hasaan Maqsood, Saif Ur Rehman Khan, and Ghazanfar Ali. "Towards Robust Breast Cancer Diagnosis: A Hybrid Deep Learning Ensemble Framework." In 2025 Horizons of Information Technology and Engineering (HITE), pp. 1-6. IEEE, 2025.

67.Bilal, O., Hekmat, A., Khan, S. U. R., Raza, A., & Ali, G. (2025, December). MS-STO-Net: A Multi-Scale State Transition Optimization-Based Ensemble Network for Accurate White Blood Cell Classification. In 2025 27th International Multitopic Conference (INMIC) (pp. 1-6). IEEE.

68.N. Mayumu, X. Deng, A. Bagula, S. u. R. Khan and P. Mukala, "V2X-JEPA: Self-Supervised Multi-Agent Joint Embedding Predictive Architecture for Robust Vehicle-to-Everything Perception," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2026.3660030.