

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

A SECURE MACHINE LEARNING MODEL INTEGRATING CRYPTOGRAPHIC TECHNIQUES FOR REAL-TIME MALWARE DETECTION AND DEFENSE FOR SECURE INFORMATION SYSTEMS

Hamza Arif

School of Business and Economics (SBE), University of Management and Technology (UMT), Lahore

Muhammad Usama Javed

Department of Information Technologies, Government College University Faisalabad

Basma

Department of Computer Science, COMSATS University Islamabad, Vehari Campus

Salah Uddin

Department of Computer Science, NFC Institute of Engineering and Technology, Multan, Pakistan Email: msalahuddin8612@gmail.com

ABSTRACT

Malware and computer viruses pose serious threats to information systems, compromising data confidentiality, integrity, and availability, while also resulting in significant financial losses. Conventional malware detection techniques, such as signature-based approaches, face major limitations including manual signature updates, reactive threat response, and poor scalability against evolving attacks. To address these challenges, this research explores the integration of machine learning and cryptographic mechanisms for intelligent malware detection and prevention. Machine learning algorithms possess the ability to identify emerging and previously unseen malware variants by learning from behavioral and encrypted data patterns. Using three core feature metrics, this study evaluates the performance of Random Forest, Gradient Boosting, and Support Vector Machine (SVM) classifiers in identifying malicious activities. The experimental results demonstrate that these models not only improve detection accuracy but also strengthen cryptographic security and data protection frameworks. Overall, this research contributes to the advancement of information security by proposing adaptive, scalable, and secure methodologies for next-generation malware detection systems.

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

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

Introduction

This study focuses on the application of machine learning techniques for malware protection and the mitigation of its damaging effects on computer networks. As defined by Kumar (2022), malware refers to any software intentionally designed to harm a computer system or exploit its user. Malware can exist in several forms, such as viruses, worms, Trojans, and adware—each possessing distinct characteristics and objectives (Alauthman, 2020).

Morgan (2023), in a report presented by *Cybersecurity Ventures*, estimated that by 2024, malware attacks could cost the global economy over \$6 trillion annually. Furthermore, the Ponemon Institute (2022) reported that the average cost of a single malware attack on an organization exceeds \$2.6 million. Beyond financial damage, malware can corrupt critical data, disrupt essential business operations, and, in some cases, even cause physical damage (Kumar, 2022). Therefore, implementing efficient and intelligent detection and prevention mechanisms is vital to maintaining cybersecurity.

Alauthman (2020) emphasized that real-time malware detection is crucial because it enables quick responses to attacks, minimizing the overall impact. Machine learning-powered malware detection systems can efficiently recognize and classify malicious software by analyzing large datasets, thereby improving accuracy and reducing response time.

According to Kumar (2022) and Chen (2022), machine learning algorithms enhance pattern recognition, anomaly detection, classification accuracy, and the capacity to identify and respond to emerging threats in real time. These capabilities make machine learning an invaluable tool in modern malware defense strategies. By strengthening pattern and anomaly detection, these intelligent systems provide a proactive and adaptive approach to identifying and preventing cyber threats effectively.

Literature

Review:

Recent studies on the current landscape of machine learning methods for malware detection and classification reveal extensive use of intelligent algorithms, with many achieving remarkable results. This section provides an overview of the main approaches employed in malware detection, including supervised, unsupervised, deep learning, and hybrid techniques. Supervised learning algorithms such as Support Vector Machines (SVM) (Kumar, 2022) and Random Forest (Sood, 2020) have shown strong performance in identifying various types of malware. Meanwhile, unsupervised learning approaches—such as clustering (Alauthman, 2020) and anomaly detection (Wang, 2020)—have been particularly effective in uncovering previously unknown or undetectable malware variants.

Deep learning models have demonstrated promising results, notably achieving lower false-positive rates compared to traditional approaches (Li, 2020; Chen, 2022). The emergence of hybrid systems, which combine multiple machine learning techniques, has further enhanced detection accuracy and adaptability (Kumar, 2022). A review of

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

existing approaches highlights both their strengths and limitations. Many machine learning-based malware detection systems have proven capable of identifying novel and unknown malware types, a capability especially valuable for corporate cybersecurity where traditional signature-based methods fail to detect zero-day attacks (Alauthman, 2020).

These intelligent techniques, when applied effectively, can recognize anomalies in data and detect new malware strains through advanced algorithms and automated analysis. This proactive ability forms a critical defense layer against evolving cyber threats, enabling organizations to safeguard their systems from emerging vulnerabilities and security breaches (Singh, 2019).

As noted by Wang (2020), modern machine learning-based detection methods are designed to adapt to the rapidly changing behavior of malware. Cybercriminals continuously modify their tactics, techniques, and procedures (TTPs) to evade detection, yet adaptive learning models can update themselves using new data to maintain effectiveness. This dynamic capability allows organizations to stay resilient against evolving threats and protect their security infrastructure (Yin, 2020).

Furthermore, research summarized by Jiang (2019) provides a comprehensive comparison of existing deep learning-based malware detection studies, focusing on architectural design, datasets, features, and limitations. The analysis highlights various methodologies and challenges, offering valuable insights that can guide future developments and improvements in intelligent malware detection systems.

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

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

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-time 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

Implementation and Methodology

Implementation and methodology need to be described so that the various steps taken in the process of developing the model and defining and installing alarm system are understood. Model Training and Testing In performing machine learning for the

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

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: $\text{IS True Positives} / \text{Total Positives IF False Positives} = 419 / (419 + 184)$

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.

Results

Performance Analysis of Different Models

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

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

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:

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

SVM	99%
Random Forest	100%
Gradient Boosting	99%

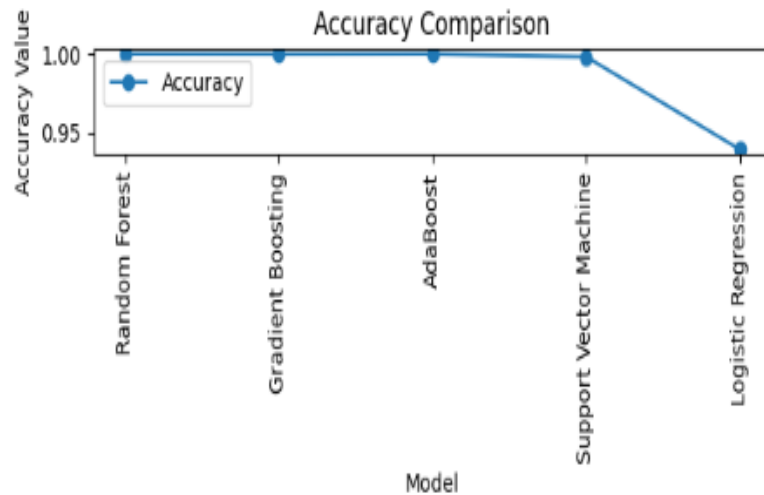
Online ISSN

3007-3197

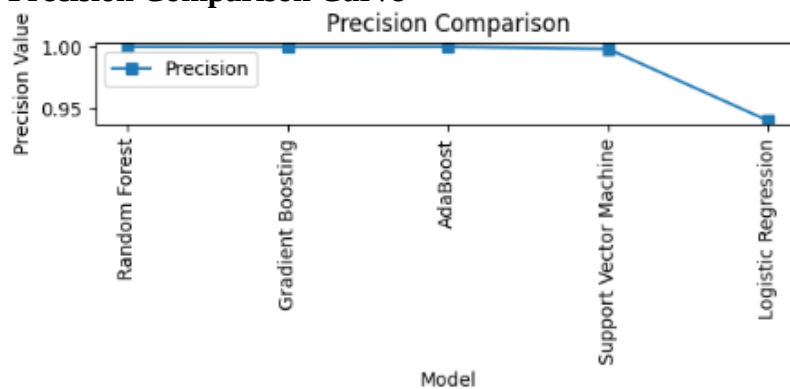
Print ISSN

3007-3189

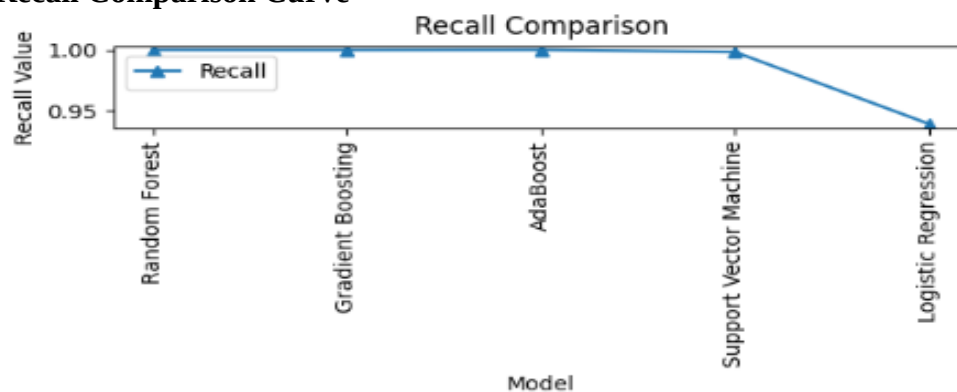
<http://amresearchreview.com/index.php/Journal/about>



Precision Comparison Curve



Recall Comparison Curve



F1-Score Comparison Curve

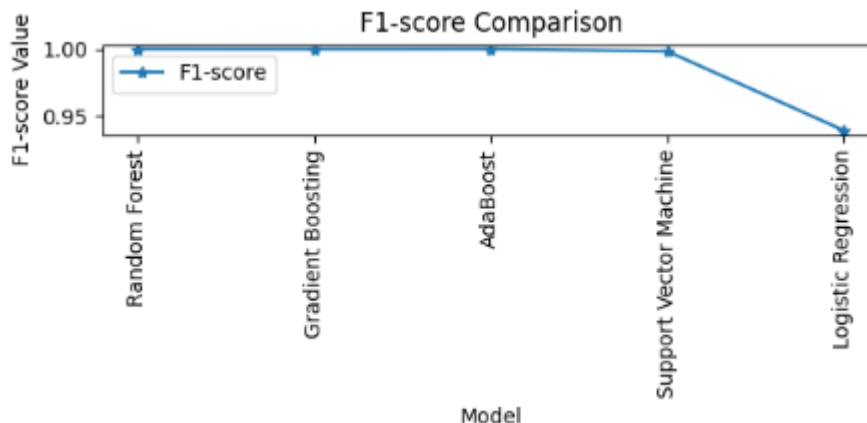
Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>



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.

Case Studies and Applications

Our research carries important implications for advancing malware detection and prevention:

Enhanced Detection Accuracy:

The proposed models can be integrated into existing anti-malware frameworks to improve overall performance by reducing both false positives and false negatives.

Real-Time Detection:

With features such as low latency and high throughput, the models enable rapid identification of malware, supporting real-time threat detection.

Resource Efficiency:

The lightweight and optimized nature of these models reduces computational overhead, making them suitable for devices with limited processing power or memory.

Strengthened Cybersecurity:

By effectively identifying and mitigating malware, the proposed approach enhances overall system security and resilience against emerging cyber threats.

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

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.

Conclusion:

This paper presents an in-depth analysis of the application of machine learning models in malware detection, highlighting the importance of feature significance and model interpretability. The results indicate that incorporating these models can substantially enhance the effectiveness of cybersecurity systems. Given their high levels of accuracy and efficiency, such models have strong potential for integration into various practical cybersecurity applications and defense mechanisms.

Moreover, the findings of this study have notable implications for cybersecurity practices, particularly in leveraging machine learning to detect and mitigate malware. The results emphasize that effective feature engineering and careful model selection play a crucial role in optimizing the performance of malware detection systems. As cyber threats continue to evolve, developing more advanced and adaptive security solutions will be essential to address emerging risks. The insights from this research contribute to ongoing studies in the field and provide valuable direction for improving existing cybersecurity frameworks.

References:

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

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

- [6] 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>.
- 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.
- 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>.
- 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.
- Khan, U. S., Ishfaq, 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.
- 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
- Latif, Sadia, Sami Ullah, Aafia Latif, Ghazanfar Ali, Muhammad Hassnain Azhar, and Salman Ali. "PREDICTIVE MODELING OF CARDIOVASCULAR DISEASE USING MACHINE LEARNING APPROACH." Kashf Journal of Multidisciplinary Research 2, no. 02 (2025): 207-232.
- Irtaza, G., Latif, S., Nadeem, R. M., Hussain, N., & Ijaz, H. M. (2025). Real-time Satellite Image Classification Using Convolutional Neural Networks for Earth Observation and Video Feed Analysis. Kashf Journal of Multidisciplinary Research, 2(03), 204-216.
- 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.
- 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.
- 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>
- 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.
- 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

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

- classification in MRI images. *Biomedical Signal Processing and Control*, 111, 108425.
- 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.
- 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.
- 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.
- Khan, S. U. R., Asim, M. N., Vollmer, S., & Dengel, A. (2025). FloraSyntropy-Net: Scalable Deep Learning with Novel FloraSyntropy Archive for Large-Scale Plant Disease Diagnosis. *arXiv preprint arXiv:2508.17653*.
- 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).
- 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.
- Khan, S. U. R., Asim, M. N., Vollmer, S., & Dengel, A. (2025). FOLC-Net: A Federated-Optimized Lightweight Architecture for Enhanced MRI Disease Diagnosis across Axial, Coronal, and Sagittal Views. *arXiv preprint arXiv:2507.06763*.
- 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>
- Asif Raza, Inzamam Shahzad, Ghazanfar Ali, and Muhammad Hanif Soomro. "Use Transfer Learning VGG16, Inception, and Resnet50 to Classify IoT Challenge in Security Domain via Dataset Bench Mark." *Journal of Innovative Computing and Emerging Technologies* 5, no. 1 (2025).
- 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.
- 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.
- Latif, Sadia, Sami Ullah, Aafia Latif, Ghazanfar Ali, Muhammad Hassnain Azhar, and Salman Ali. "PREDICTIVE MODELING OF CARDIOVASCULAR DISEASE USING MACHINE LEARNING APPROACH." *Kashf Journal of Multidisciplinary Research* 2, no. 02 (2025): 207-232.

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

- 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.
- 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.
- 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
- Latif, Aafia, Sadia Latif, and Furqan Jamil. "UTILIZING BIG DATA ANALYTICS TO OPTIMIZE INFORMATION COMMUNICATION TECHNOLOGY STRATEGIES." *Kashf Journal of Multidisciplinary Research* 1, no. 12 (2024): 122-140.
- 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
- 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*.
- Raza, A., Salahuddin, & Inzamam Shahzad. (2024). Residual Learning Model-Based Classification of COVID-19 Using Chest Radiographs. *Spectrum of Engineering Sciences*, 2(3), 367–396.
- 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.
- Raza, A., Soomro, M. H., Shahzad, I., & Batool, S. (2024). Abstractive Text Summarization for Urdu Language. *Journal of Computing & Biomedical Informatics*, 7(02).
- 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.
- Khan, S. U. R. (2025). Multi-level feature fusion network for kidney disease detection. *Computers in Biology and Medicine*, 191, 110214.
- 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).
- Latif, Sadia, Azhar Mehboob, Muhammad Ramzan, and Muhammad Ans Khalid. "DETECTION OF HCV LIVER FIBROSIS APPLYING MACHINE LEARNING TECHNIQUE." *Kashf Journal of Multidisciplinary Research* 1, no. 12 (2024): 11-44.

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

Aslam, N., Meeran, M. T., Aslam, M., Maqbool, M. S., & Saeed, B. (2025). UNDERSTANDING URBAN EXPANSION THROUGH MULTI-TEMPORAL SATELLITE DATA ANALYSIS. Kashf Journal of Multidisciplinary Research, 2(09), 252-273.

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.