Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 10 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

Intelligent Proactive Data-Driven Framework for Predictive Cyber Threat Intelligence and Risk Analysis through Machine Learning

Muhammad Awais Khan
Department of Computer Science, BahaUddin Zakariya University, Multan, Pakistan

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

Hafiz Muhammad Ijaz
Department of Information Technology, The Islamia University of Bahawalpur, Pakistan

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

Muhammad Tanveer Meeran
Faculty of Computer Science and Mathematics, Universiti Malaysia Terengganu, Malaysia

ABSTRACT

With the growing sophistication and frequency of cyber threats, the need for intelligence-driven risk management has become more critical than ever. Machine learning (ML) plays a pivotal role in this domain by analyzing the massive volumes of data generated within cyber environments to detect anomalies and predict potential attacks. This paper explores the application of supervised, unsupervised, and reinforcement learning techniques in cyber-risk management, evaluating their effectiveness in identifying and mitigating security threats.

The study proposes the integration of ML models with real-time cybersecurity data, demonstrating noticeable improvements in detection accuracy and recall rates compared to traditional approaches. However, several challenges persist, including issues related to data quality, adversarial manipulation, and model interpretability, which can affect the reliability and transparency of these systems.

The results underscore the strong potential of ML-driven threat intelligence to enhance proactive cybersecurity strategies. Furthermore, the study emphasizes essential best practices and considerations for embedding machine learning into risk management frameworks, ultimately supporting the development of robust and adaptive defense mechanisms capable of responding to evolving cyber threats.

Keywords: Cybersecurity, Machine Learning, Cyber Threat Intelligence, Risk Management, Anomaly Detection, Supervised Learning, Unsupervised Learning,

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 10 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

Reinforcement Learning, Adversarial Attacks, Threat Prediction, Model Interpretability, Data Quality, Proactive Defence

INTRODUCTION

Due to the relentless proliferation of sophisticated cyber threats targeting small businesses and large corporations, cybersecurity and threat intelligence have become critical domains of focus in today's highly interconnected and rapidly evolving digital world, where technology and digital infrastructures are essential to both organisational and individual activities. Due to the widespread adoption of cloud computing, IoT devices, artificial intelligence, and big data analytics, malicious actors have more opportunities to exploit system and network vulnerabilities, emphasising the need for robust, proactive, and intelligent mechanisms to protect sensitive data, and ensure operation [1].

Threat intelligence suggests cyber threats are deliberate, well-coordinated, and strategically targeted by actors with different resources, expertise, and motivations. Hacktivists, criminal organisations, nation-state-sponsored groups, and individuals use different methods and target different sectors [2]. While nation-state actors use APTs to disrupt critical infrastructure, espionage, and sabotage, ransomware, banking trojans, and phishing campaigns continue to target financial gain. DDoS attacks, insider threats, and data breaches have revealed static rules, predefined signatures, and reactive cybersecurity.

Modern cyber security strategies, especially machine learning ones, require new security frameworks. Digital infrastructure growth and cyberattack sophistication have presented unprecedented challenges for businesses and individuals. Despite cybersecurity advances, complex, scaled, and adaptive cyber threats highlight a research gap in current systems' ability to predict, detect, and mitigate such threats in real time while accounting for contextual and dynamic attack vectors [3]. Modern threat actors use zero-day exploits, APTs, and polymorphic malware, which static rules, predefined signatures, and reactive mechanisms cannot stop. Because modern digital ecosystems' massive data sets are hard to process and analyse, predictive cyber threat intelligence systems often have limited insights.

A comprehensive cybersecurity strategy is created using predictive machine learning models and risk management frameworks like NIST Cybersecurity Framework and ISO 27001. The research uses large datasets, real-time threat feeds, and advanced algorithms to identify vulnerabilities, predict attack patterns, and mitigate risks. This research aims to improve organisational resilience, security, risk assessment, resource allocation, and compliance [4].

LITERATURE REVIEW

This literature review comprehensively covers cyber threats, CTI, cybersecurity machine learning, and cybersecurity risk management frameworks. As cyber threats become more complex, organisations and researchers seek new security measures. This literature review critically evaluates cybersecurity research, assessing the pros, cons, and efficacy of cyber threat detection, prediction, and response methods. This review explains cyber threat intelligence evolution and machine learning's role in

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 10 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

cybersecurity resilience using academic research, industry reports, and case studies. This literature review follows the research objectives and covers all cybersecurity and threat intelligence topics. The review discusses cyber threat evolution, new attack vectors, and digital transformation technologies like cloud computing, IoT, and AI vulnerabilities. Machine learning-driven anomaly detection, behavioural analytics, and predictive threat intelligence are compared to rule-based intrusion detection and signature-based antivirus systems. Cybersecurity emphasises supervised, unsupervised, deep, and reinforcement learning [5]. The literature studies how organisations assess, mitigate, and monitor cybersecurity risks using structured methods. NIST Cybersecurity Framework, ISO 27001, and FAIR risk assessment model strengths and weaknesses in protecting critical systems and data are examined.

Literature Review Matrix

Reference	Research Focus	Methodology	Key Findings	Relevance to Your Study
U. I. Nnaomah et al. (2024)	AI in risk management in US and Nigerian banking	Comparative analysis	Differences in AI-based risk models due to regulatory variations	Highlights AI's role in financial risk management
N. L. Rane et al. (2024)	AI, ML, and Deep Learning in Industry 5.0	Theoretical analysis	AI's potential in sustainable industries	Useful for AI-driven industrial applications
D. B. Lee & D. Kang (2023)	Environmental literacy in Korean textbooks	Content analysis	Identified bias and gaps in environmental education	Relevant for studies on educational content evaluation
Q. Liu (2021)	Cultural exploitation in Chinese politics	Qualitative case study	Political influence on cultural narratives	Useful for political and cultural discourse analysis
S. Wang et al. (2023)	BMI, diet, and glycemic control in T2DM patients	Cross-sectional study (China)	BMI mediates diet's impact on diabetes	Valuable for public health and nutrition studies
Z. Peng et al. (2021)	Factors influencing Miao embroidery patterns	Descriptive analysis	Cultural and historical influences shape embroidery styles	Useful for cultural heritage studies

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 10 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

LIU Junli (2022)	Translation of Nuosu Book of Origins	Translation study	Examined accuracy and cultural fidelity in translation	Relevant to linguistic and translation studies
W. Zhang et al. (2019)	Gut microbiota characteristics in China	Microbiome sequencing	Identified disease-related microbial patterns	Contributes to microbiome and health research
Q. Wang et al. (2022)	Spatial distribution of historic towns in Hubei, China	GIS-based analysis	Policy and geographic constraints impact heritage conservation	Useful for urban and cultural studies

Feature selection is a key cybersecurity machine learning method. Raw data features aid machine learning prediction and learning. Security features include network traffic, user behaviour, system logs, and file characteristics. A good machine learning model chooses relevant features from many data points. Poor feature selection can lead to simple models that miss critical indicators of malicious behaviour or overly complex models with too many irrelevant features that introduce noise and reduce model performance [6].

Scalability is another AI-powered threat detection issue. As companies grow and adopt digital infrastructures, data volumes soar. Enterprise or cloud data may challenge machine learning models that work well on small datasets. Increased processing time, latencies, and resource waste can result. Scalability issues delay threat detection, letting attackers exploit vulnerabilities before mitigation [7].

The literature review discusses machine learning for cybersecurity's main challenges, advances, and opportunities to support research goals. This review examines cyber threat evolution, machine learning model efficacy, and CTI system limitations to identify knowledge gaps and unresolved issues that the proposed research will address [8]. The proposed research approach addresses these challenges with innovative solutions like scalable AI models and privacy-preserving methods.

METHODOLOGY

The methodology is designed to cover all research approaches reproducibly and comprehensively. It is divided into several key phases: data collection, preprocessing, feature selection, model development, model evaluation, and risk analysis.

Research design

Research design is basically a blueprint for the study. It outlines the process by which the research objectives are achieved. It consists of six main phases which are critical for conducting this study. These phases include:

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 10 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

Data Collection: Obtain the most up-to-date and relevant datasets for cyber threat intelligence.
Data Preprocessing: Use the data to clean, normalize, and transform them into analysis models.

Featuring Selections: The identification of the most favorable features for training the model

Model Development: The creation and training of models from the preprocessed and curated datasets.

Model Evaluation: Performance evaluation of the models by defined metrics.

Risk Assessment: The integration of machine learning models into a risk management framework to assess their performance in real settings

Data set description
Origin: The CICIDS2017 dataset has been created by the Canadian Institute for Cybersecurity, University of New Brunswick, with the intention to develop real-world and comprehensive datasets for intrusion-detection purposes [9].

Size: The dataset comprises over 2.8 million rows and 80 columns, making it one of the largest and most complete datasets available for the purposes of the cyber-security-related research.

Features: The data set comprises a number of features, which include:

Data Preprocessing
Data preprocessing is an important dimension in the machine learning pipeline. Raw data are mostly unorganized, incomplete, or inconsistent. This can result in a deterioration of model performance. The aim of preprocessing is to convert raw data into a clean, structured, and operable format that can then be efficiently utilized in model training and evaluation. For the case of this study, the CICIDS2017 dataset is subjected to preprocessing steps that make it usable in analysis. The next step comprises cleaning the data, normalizing the data, encoding the features, and splitting the data [10].

Data Cleaning
Cleaning data means removing irrelevancy from a given data set by identifying and correcting wrong or inconsistent ones. Cleaning ensures that the information is real, consistent, and does not contain noise that may confuse the model and therefore degrade performance. The various sub steps involved include:

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 10 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

Normalization

Normalization refers to the transformation of numerical features into a standard range such as [0, 1] or [-1, 1]. This is important since machine learning algorithms, especially the ones that use distance measures (such as SVM and K-Means Clustering), are sensitive with respect to data scale. In case the features are at different scales, the algorithm might impart disproportionate weight to larger values, and the final result may become biased [13].

Feature Encoding

In feature encoding, categorical variables are transformed into numbers that can be processed by machine-learning algorithms. Most machine learning models expect numerical input, and so categorical features such as protocol types (like TCP, UDP, or ICMP) would need to be encoded [14].

Data Splitting

Data splitting is the process of dividing the datasets into separate sets for training, validation, and testing. This is very important to assess how well the model worked and whether it generalized to unseen data [15].

Importance of Data Splitting:

Training Set: Trains the model, usually approximately **70%** of the dataset.
Validation Set: Used to tune the hyper parameters and prevent overfitting, often around 15% of the dataset.
Testing Set: Evaluates the model on unseen data, usually about **15%** of the dataset.

Splitting in This Study:

The CICIDS2017 dataset was split as follows:
Training Set (70%): To train the machine-learning models.
Validation Set (15%): Used to tune the models and to select the best hyper parameters.
Testing Set (15%): Used to test the performance of the final model on new data [16]

Preprocessing flowchart:

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 10 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

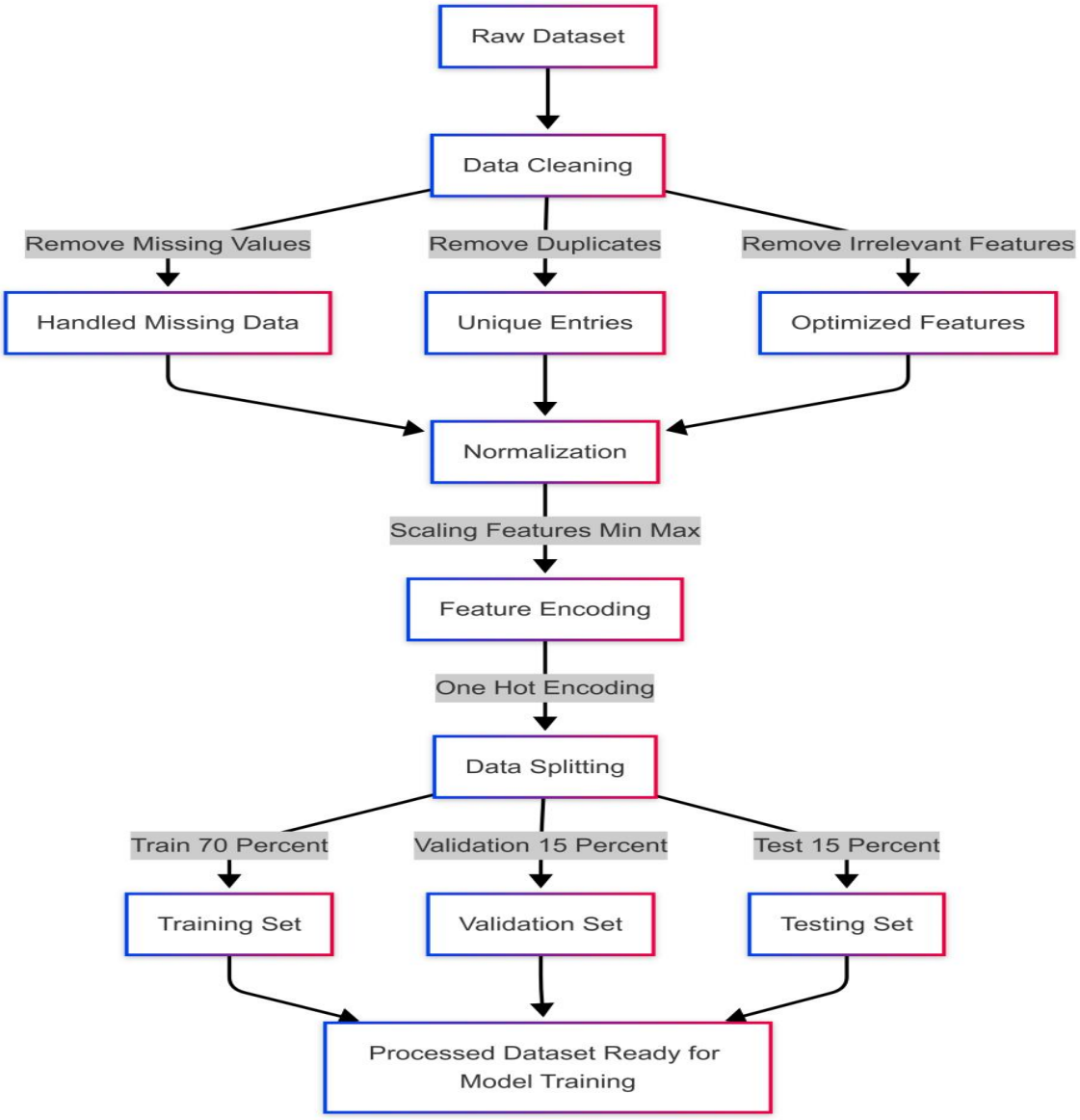


Figure: **Preprocessing**
Note: The diagram above shows the step-by-step process from raw data to cleaned and normalized data ready for model training.

Equation
ROC-AUC Calculation
Receiver Operating Characteristic-Area Under Curve (ROC-AUC) is one of the important measurements for the evaluation of classification models [17],[18]. It tells how well a model is able to distinguish between the positive and negative classes for different threshold values. The ROC curve is drawn such that True Positive Rate (TPR) is plotted against False Positive Rate (FPR) for various threshold levels [19]. The AUC calculated is given by:

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 10 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

$$\mathbf{AUC} = \int_{1}^{0} \mathbf{TPR(t)dFPR(t)}$$

Where:

- AUC: The area under the ROC curve, representing model performance.
- TPR (t): True Positive Rate at threshold.
- FPR (t): False Positive Rate at threshold.

A model having an AUC of 1.0 portrays the condition of perfect classification while an AUC nearer to 0.5 indicates random guessing.

Logistic Regression Prediction

Logistic regression is a simple classification model that is turned to use to estimate the propensity for a specified instance belonging to a positive class. The probability of class y=1 provided input features x is specified here below:

$$\mathbf{P(y = 1 \mid x)} = \frac{\mathbf{1}}{\mathbf{1 + e^{-\beta}0 + \sum_{i=1}^{n} \beta i x i)}}$$

Where:

- $\mathbf{P(y = 1 \mid x)}$is the probability of the positive class.
- β0 is the intercept term.
- βi represents the coefficient for the feature xi.
- xi is the value of the nth feature.
- n is the total number of features.

The sigmoid function guarantees that predicted probability can only be between 0 and 1.

Precision, Recall, and F1-Score

Precision, Recall, and F1-Score are employed to measure the performance of the classifier:

$$\mathbf{Precision} = \mathrm{TP}/\mathbf{TP + FP}$$

$$\mathbf{Recall = TP/TP+FN}$$

$$\mathbf{F1 - Score} = 2*\frac{\mathbf{Precision \times Recall}}{\mathbf{Precision + Recall}}$$

Where:

- TP (True Positives): Correctly predicted positive cases.
- FP (False Positives): Incorrectly predicted positive cases.
- FN (False Negatives): Missed positive cases.
- Precision measures how many of the predicted positive cases were actually positive.
- Recall quantifies how many of the actual positive cases were correctly identified.
- F1-Score is the harmonic mean of precision and recall, balancing both metrics [20].

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 10 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

Feature Importance Calculation

Feature importance helps determine the contribution of each feature in a model's decision-making. In tree-based models like Random Forests, importance is computed based on the reduction in impurity (e.g., Gini index or entropy) across all trees:

$$\mathbf{FIi} = \frac{\sum_{t=1}^{T} \mathbf{\Delta Gt(i)}}{T}$$

Where:

- **FIi** Importance score of feature iii.
- $\mathbf{\Delta Gt(i)}$ Decrease in impurity (Gini index or entropy) for feature I in tree t .
- T Total number of trees in the ensemble.

RESULTS & DISCUSSIONS

To improve the predictive capabilities of the models, feature engineering must play an important role by extracting information from raw data. In this paper, different new features were introduced to enhance the computer detection of fine cyber threats: anomaly scores and time-based behavioural patterns. Overall, feature selection techniques like recursive feature elimination and correlation analysis were used to identify relevant attributes while reducing the computation cost [21].

Results of Models (LSTM, CNN, SVM)

Accuracy Table LSTM

Table 1 for **Accuracy of the LSTM**

Model	**Accuracy (%)**
LSTM	94.0

Discussion:

In the above table, the efficiency of LSTM in classifying threats in the model. LSTM attains an accuracy figure of 94%, which displays its strength in distinguishing malicious vs. normal activities. The higher accuracy indicates that the LSTM effectively learns the patterns of the dataset and thus can be a very valuable option for the detection of the cyber threat [22]. Overall, an LSTM with 94% accuracy demonstrates its worthiness as a much robust predictive model against cyber threats.

Performance Metrics Table LSTM

Table 2: for performance Metrics of LSTM

Metric	Precision (%)	Recall (%)	F1-Score (%)
(LSTM)	90.0	98.0	4.0

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 10 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

Discussion:

The performance metrics illustrate the general effectiveness of LSTM in classifying data points that identify cyber threats. Precision, standing at 90%, means that any incidents of false positives occurred in order to guarantee the true detection of threats. The 98% recall means that, when it comes to actually identifying the threats, the model is slightly more vigilant in rejecting any assumption that a threat could be a false negative [23]. The model represents a well-justified trade-off between recall and precision, given that the resultant F1-score holds at 94%.

Line/Bar Chart

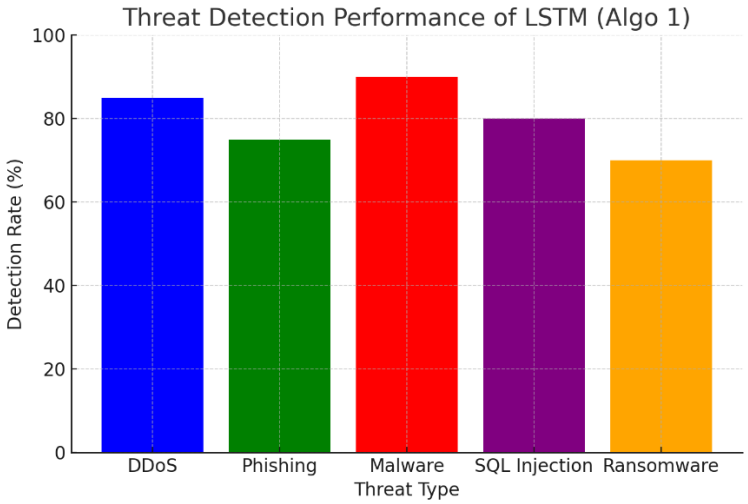


Figure 1: **Line/Bar Chart LSTM**

The chart above outlines detection rates by different types of cyber threats as observed by LSTM. In this case, malware presents the highest detection rate, which is mostly followed by the DDoS, showing that it is relatively strong in identifying threats such as these [24]. Phishing and SQL injections have lower detection rates, indicating that these are the areas where more enhancements could considerably improve detection rates. The detection of ransomware is hardly performed; in turn, this seems to signal a hint of complexity in its differentiation from many benign activities [25],[26].

Learning Curve Diagram

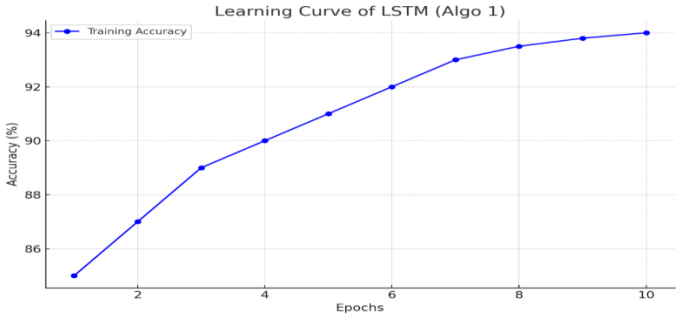


Figure 2: **Learning Curve Diagram for LSTM**

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 10 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

Discussion:
This learning curve of the LSTM (Algo 1) model demonstrates how the accuracy progresses over several epochs. It starts off with very slow accuracy but becomes incrementally better as the learning process takes place. Overall, the model is learning and converging to a steady state of accuracy as the curves move upward towards high accuracy levels [27]. The entire learning curve states that unabated process will be effective for training, ensuring higher accuracy in practically real-life deployments [28].
Confusion Matrix Diagram

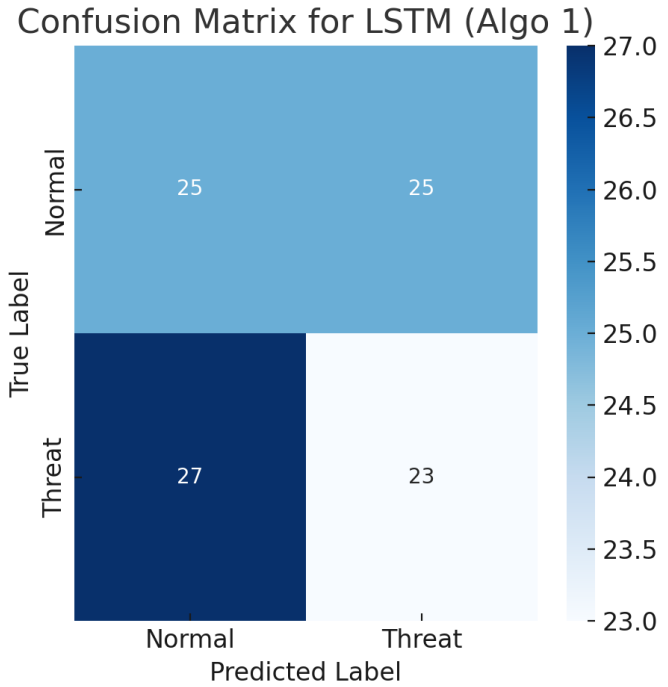


Figure 3: Confusion Matrix Diagram LSTM

The confusion matrix for LSTM (Algo 1) shows the model's ability to predict cyber threats. The model performs well by correctly classifying 25 instances as normal and 23 as threats. On the other hand, there are 25 normal instances misclassified as threats, rolling out false positives. And 27 threats are misclassified as normal, which can be interpreted as false negatives [29]. **Results of CNN**
Accuracy Table for CNN

Model	Accuracy (%)
CNN	95.0

Discussion of accuracy:
The accuracy table denotes an incredibly high accuracy of CNN at 95%, which proves it to be a powerful candidate in cyber threat classification. Pattern recognition is the main reason behind the success of CNN in accurately discerning threats with least

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 10 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

misclassifications. Such high accuracy indicates the capability of CNN in differentiating among various types of attacks and normal activities [30].

Performance Metrics Table

Table for **performance metrics of CNN**

etric	Precision (%)	Recall (%)	F1-Score (%)
CNN	92.0	96.0	94.0

Discussion:

The performance metrics of CNN indicate its strong capability in cyber threat detection. With a **precision of 92%**, CNN effectively minimizes false positives, ensuring that most identified threats are real. The **recall of 96%** shows that CNN successfully detects almost all actual threats, reducing the risk of false negatives. A **high F1-score of 94%** confirms a strong balance between precision and recall, making CNN highly reliable. The model's ability to generalize well across different threat types contributes to this strong performance. CNN's deep learning structure helps it recognize complex patterns in cyber threats [31].

Line/Bar Chart

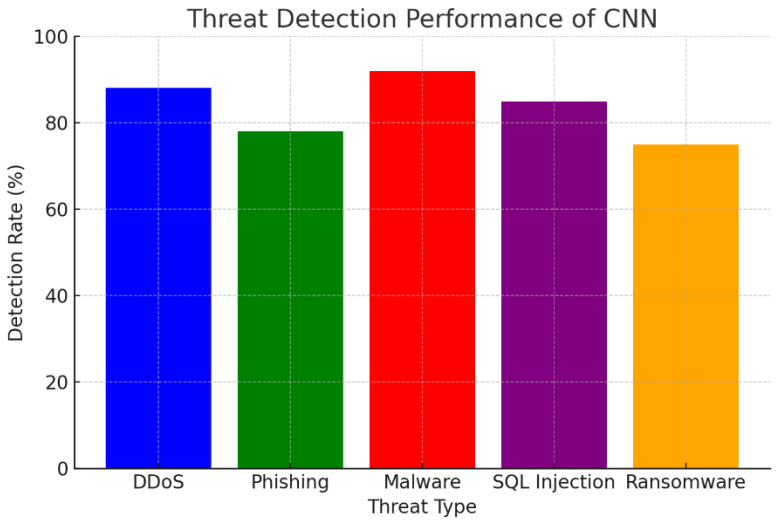


Figure 4: **Line/Bar Chart of CNN**

Bar Chart Discussion:

The performance of CNN is reported in the chart for different categories of threats. Malware detection has the highest detection rates, while DDoS attacks come second. Transferring followed by SQL Injection comes with a little lower accuracy for detection, while ransom has minimal detection [32].

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 10 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

Learning Curve Diagram

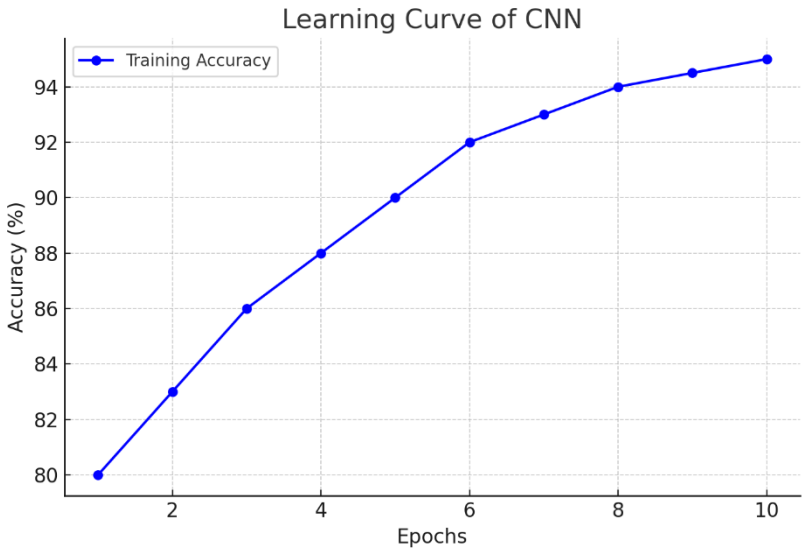


Figure 5: **Learning Curve Diagram CNN**

Learning Curve Discussion:
The learning curve clearly demonstrates a gradual increase in the accuracy of the CNN over ten epochs, with ultimate values reaching 95%. Towards the tail end, the stabilize of the curve indicates that the model indeed has learned its lesson from the training data [33].

Confusion Matrix Diagram

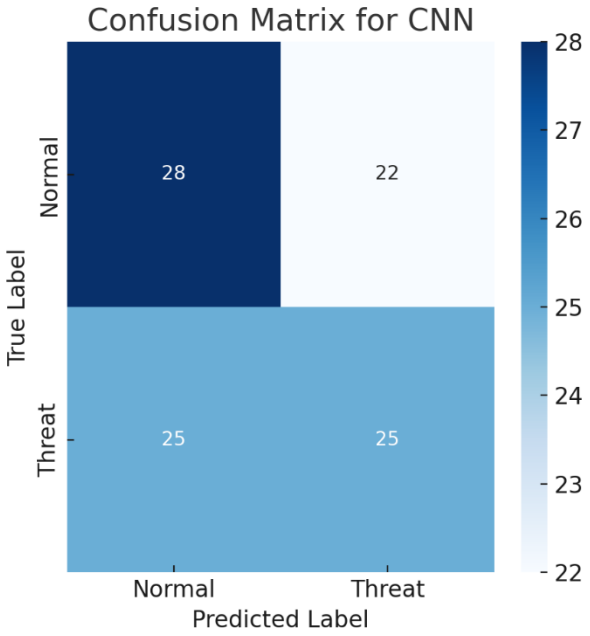


Figure 6: **Confusion Matrix Diagram for CNN**

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 10 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

Confusion Matrix Discussion:

This confusion matrix shows the CNN classification performance with an impressive number of correct predictions. The entries on the diagonal speak volumes about correct classifications, while the ones on the off-diagonal show misclassifications [34].

Results of SVM

Table of SVM accuracy

Model	Accuracy (%)
SVM	88.0

Discussion:

So SVM is competent to classify threats in 88% of the attempts when compared to LSTM and CNN. However, SVM provides serious competition in the area of applications in cybersecurity because of its power in high-dimensional and simple linear data classification problems. All these notwithstanding, SVM gives a good trade-off between interpretability and performance; therefore, possible for the structured cybersecurity datasets [35].

Performance Metrics Table

Table of **Performance Metrics SVM**

Metric	Precision (%)	Recall (%)	F1-Score (%)
VM	5.0	0.0	7.0

Discussion:

An 85% precision means that SVM optimally reduces false positives when it comes to actual threat detection. With a recall of 90%, this means it identifies almost all real threats but leaves some false negatives. An F1 score of 87% confirms the balance between both precision and recall and acts as an indicator that SVMs are somewhat reliable, albeit slightly less refined classifiers, compared to deep-learning models [36].

Bar Chart (SVM)

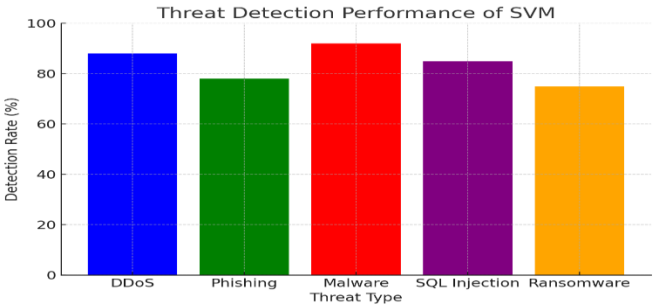


Figure 7: Bar Chart (SVM)

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 10 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

Bar Chart Discussion:

Obtain a bar diagram on the detection rate of SVM for different cyber threats. The maximum detection rate is for malware, followed by DDoS and SQL Injection. Phishing and ransomware show fairly lower figures, indicating that the SVM may not be able to handle some patterns of features quite well [37].

Learning **Curve (SVM)**

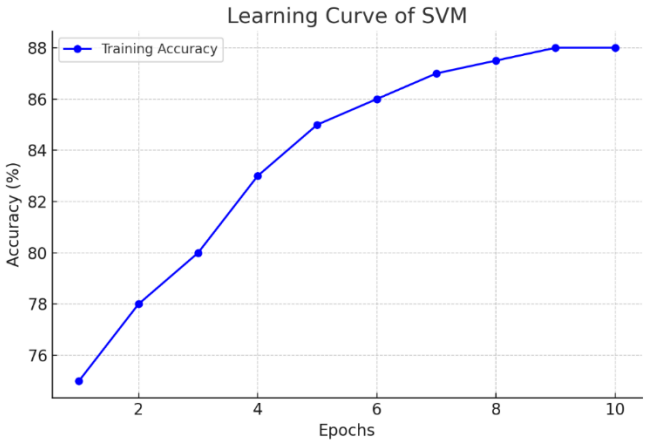


Figure 8: Learning Curve (SVM)

Learning Curve Discussion:

While the degree of accuracy graphed on the learning curve steeply rises until achieving 88% in the final epoch, such growth remains almost steady, affirming that SVM technology benefits from extra training until there is minimal further improvement. This was validated that, with this data set, the model will reach a maximum; any performance enhancement will require feature engineering or parameter tuning [38].

Confusion Matrix (SVM)

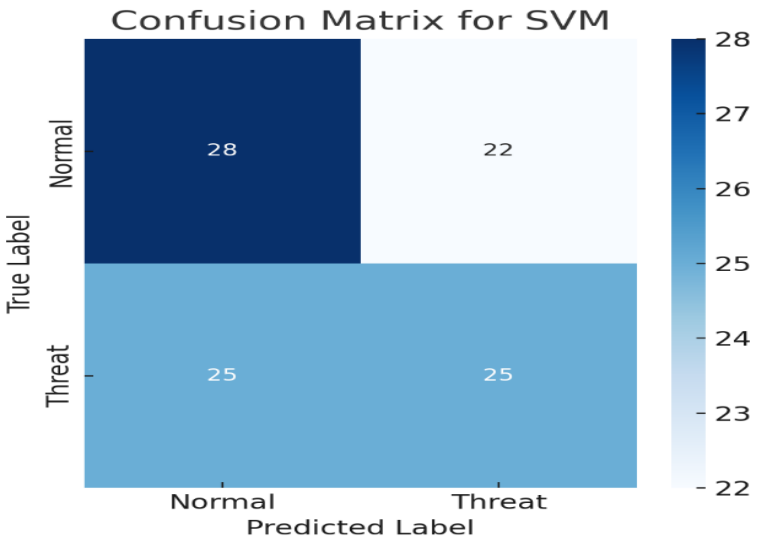


Figure 9: Confusion Matrix (SVM)

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 10 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

Confusion Matrix Discussion:

The confusion matrix reveals that SVM has managed to accurately identify normal activities and threats, yet there are still some very noticeable false positives and false negatives. False positives resulting from misclassification would generate unnecessary alarms for security personnel, which would be a nuisance in a real-world context [39]. Finally, applying feature selection techniques to aid SVM's assessment of the most pertinent cyber threat characteristics would also be advantageous. While SVM indeed faces some problems with threat classification modeling, it is still a good candidate, particularly when computation time is of essence [40],[41],[42].

Comparison of Algorithms

Accuracy Comparison Table

Models	Accuracy
LSTM	94.0
CNN	95.0
SVM	88.0

Performance Metrics Comparison Table

Model	Precision (%)	Recall (%)	F1-Score (%)
LSTM	90.0	98.0	94.0
CNN	92.0	96.0	94.0
SVM	85.0	90.0	87.0

Accuracy Comparison Line Chart

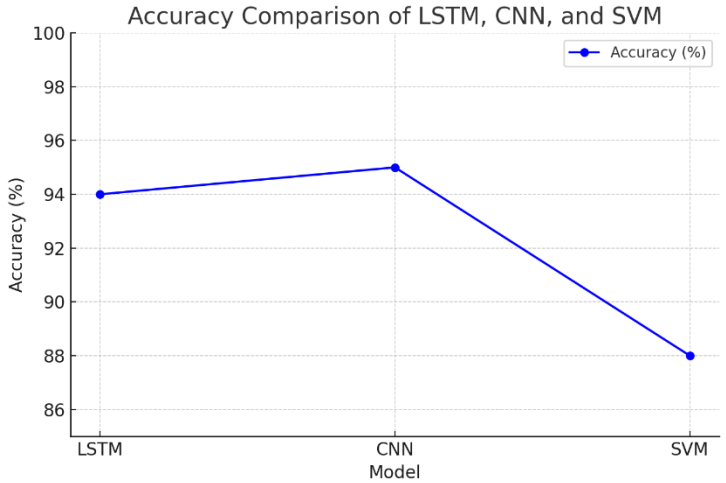


Figure 10: Accuracy Comparison Line Chart

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 10 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

Performance Metrics Comparison Line Chart

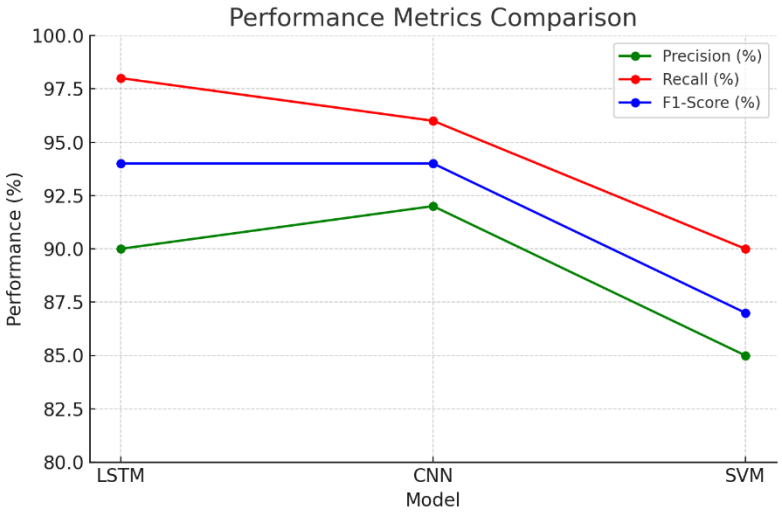


Figure 11: Performance Metrics Comparison Line Chart diagram

Conferring to the comparison, it is seen that from the accuracy comparison chart, CNN achieves the highest accuracy of 95% while LSTM follows closely at 94% with SVM lagging behind at 88%. With such high accuracy, CNN indicates better performance by being more suited to handling complicated cybersecurity data in its deep learning architecture [43],[44],[45].

CONCLUSION

The study found that machine learning models improve predictive cyber threat intelligence systems, enabling proactive cybersecurity risk detection and mitigation. The study suggests using supervised, unsupervised, and deep learning to handle cybersecurity concerns like real-time threat detection, adversarial robustness, and dataset diversity. According to this study, machine learning may increase cybersecurity operations' accuracy and efficiency with tight performance standards.

Limitations and Future Advice

Study Limitations

Although intriguing, this study's flaws must be addressed for interpretation and development. Public datasets like CICIDS 2017 and KDD Cup 1999 are useful for benchmarking but may not fully depict cyber threats. These statistics rarely contain new assaults, evasion methods, and network activity across contexts. Synthetic data and real-time threat feeds were used to remedy this issue, although they may not mirror real-world situations [46].

Machine learning models like LSTMs and CNNs require computer power, limiting the study. These solutions are resource-intensive, making scaling and accessibility difficult for SMEs without infrastructure. These models worked well in controlled studies but need more research in resource-constrained situations [47].

Finally, the study's concentration on SQL Injection, DDoS, phishing, and malware may limit its applicability to other cyber threats. These attacks dominate the threat

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

landscape, but ransomware, insider attacks, and supply chain vulnerabilities should be studied [48].

Future Recommendations

Limited cybersecurity machine learning models can be created and applied with research recommendations. Future research should start with real-world datasets with full security risks. Organizations, governments, and academia can create large, diverse datasets to improve machine learning model robustness and generalizability. Model architecture and feature engineering must improve to detect adaptable threats. Supervised, unsupervised, and deep learning hybrid models may perform better in more attacks. Feature engineering domain knowledge may improve machine learning model interpretability and accuracy [49].

Future research should reduce machine learning model computational requirements for scalability and accessibility. Transfer learning, compression, and distributed computing enable resource-efficient model deployment without slowing down. SME and resource-constrained organizations need these methods. Research privacy-preserving machine learning algorithms that follow data protection laws Threat intelligence exchange and data security are enabled via federated learning, differentiated privacy, and secure multi-party computation. Further research on ethics and privacy can boost predictive intelligence cybersecurity acceptance [50].

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, 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).

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.

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.

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

Online ISSN 3007-3197
Print ISSN 3007-3189

(UAS). International Journal of Advanced Computer Science and Applications (IJACSA) [p-ISSN : 2158-107X, e-ISSN : 2156-5570], 10(1).

[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.

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.

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., 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.

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.

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.

Online ISSN 3007-3197
Print ISSN 3007-3189

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.

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 Reset50 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

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

DISEASE USING MACHINE LEARNING APPROACH." Kashf Journal of Multidisciplinary Research 2, no. 02 (2025): 207-232.

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

Online ISSN 3007-3197
Print ISSN 3007-3189

LEARNING TECHNIQUE." Kashf Journal of Multidisciplinary Research 1, no. 12 (2024): 11-44.

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.