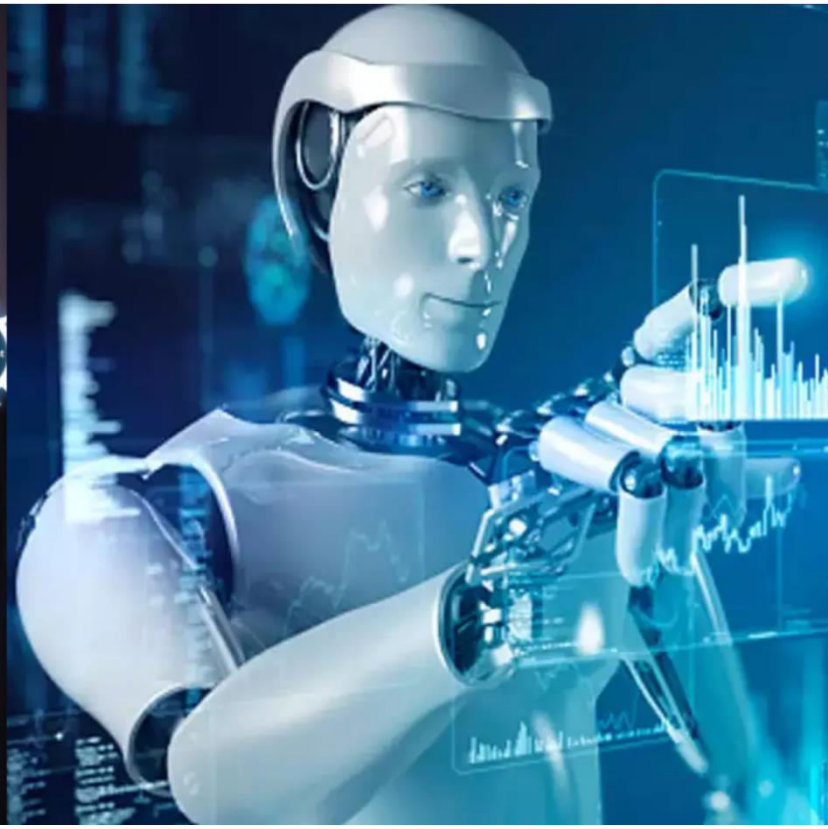
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 6, June 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 6, June 2025

|DOI: 10.15680/IJIRSET.2025.1406150|

Integrating Hybrid Models and Latent Features in Real Time NIDS

J. Akhil[1], P. Harini[2], Y. Bhaskar[3], V. Swetha[4]

U.G. Student, Department of Information Technology, ACE Engineering College, Ankushapur, Telangana, India[1,2,3]

Assistant Professor, Department of Information Technology, ACE Engineering College, Ankushapur, Telangana, India[4]

ABSTRACT: In the era of evolving cyber threats, traditional intrusion detection systems fall short in identifying advanced attacks like DDoS, SQL injections, and phishing. This project presents a real-time Network Intrusion Detection System (NIDS) integrating hybrid deep learning models—CNN and LSTM—and latent feature extraction. The system captures live network traffic, extracts features, and classifies it as normal or malicious using a trained deep learning model. Real-time visualization and alerting are enabled via a Flask dashboard. By leveraging deep learning with PCA and Autoencoders, the model achieves improved accuracy, faster detection, and proactive response, making it suitable for modern cybersecurity environments.

KEYWORDS: Cybersecurity, Deep Learning, Real-Time Threat Detection, CNN-LSTM, Intrusion Detection System, Latent Features, PCA

I. INTRODUCTION

In the modern digital age, cybersecurity threats are increasingly becoming more complex and frequent. Attacks such as Distributed Denial of Service (DDoS), brute force intrusions, SQL injections, and malware are continuously evolving, making traditional defense mechanisms like rule-based firewalls and signature-based Intrusion Detection Systems (IDS) insufficient. These conventional systems struggle to adapt to new threats due to their dependence on static rules and prior knowledge of attack signatures. To address this growing challenge, the integration of Artificial Intelligence (AI), particularly Deep Learning (DL), has emerged as a promising solution.

This project introduces a real-time Network Intrusion Detection System (NIDS) that combines the strengths of Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks. CNNs are employed to identify spatial patterns in network data, while LSTMs detect temporal dependencies between packets. The system is further enhanced with latent feature extraction using Autoencoders and Principal Component Analysis (PCA), enabling it to capture hidden patterns in traffic for better classification accuracy.

Live traffic is captured using PyShark and analyzed through a hybrid model deployed on a Flask-based web interface. The system provides real-time alerts and visual dashboards for network administrators, enabling faster detection and response to cyber threats. This hybrid approach significantly improves detection accuracy and system resilience.

II. LITERATURE SURVEY

A. Sharma et al. (2024) proposed an automated intrusion detection system tailored for IoT environments using a hybrid architecture that combines deep packet inspection with anomaly-based detection. While the model effectively identified both known and unknown threats in resource-constrained IoT networks, scalability remained a challenge under high-traffic conditions. The authors suggested using edge-based optimization and adaptive learning for future improvements.

M. Zhang and Y. Li (2023) introduced a deep learning-based anomaly detection system for NIDS using stacked autoencoders and LSTM. Their model showed high detection accuracy for unknown attack types. However, the system's performance depended heavily on the quality of the training data and lacked robustness against adversarial inputs. The study recommended ensemble methods and adversarial training to enhance generalization.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 6, June 2025

|DOI: 10.15680/IJIRSET.2025.1406150|

K. Patel et al. (2023) developed a hybrid model combining Random Forest and Support Vector Machines (SVM) to balance interpretability and accuracy. While the ensemble model outperformed individual algorithms on the NSL-KDD dataset, high training time and increased model complexity posed challenges for real-time deployment. The authors proposed lightweight fusion techniques to improve inference speed.

III. PROPOSED METHODOLOGY

The proposed system uses a hybrid deep learning model combining Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks for real-time intrusion detection. Network traffic is captured using PyShark, and key features such as IP addresses, ports, and protocols are extracted. Autoencoders and PCA are used to reduce dimensionality and extract latent features. CNN identifies spatial patterns, while LSTM captures temporal dependencies in the traffic. The model classifies data as normal or malicious and triggers real-time alerts. A Flask-based dashboard visualizes live network activity, enabling rapid detection, analysis, and response to cybersecurity threats.

ARCHITECTURE:

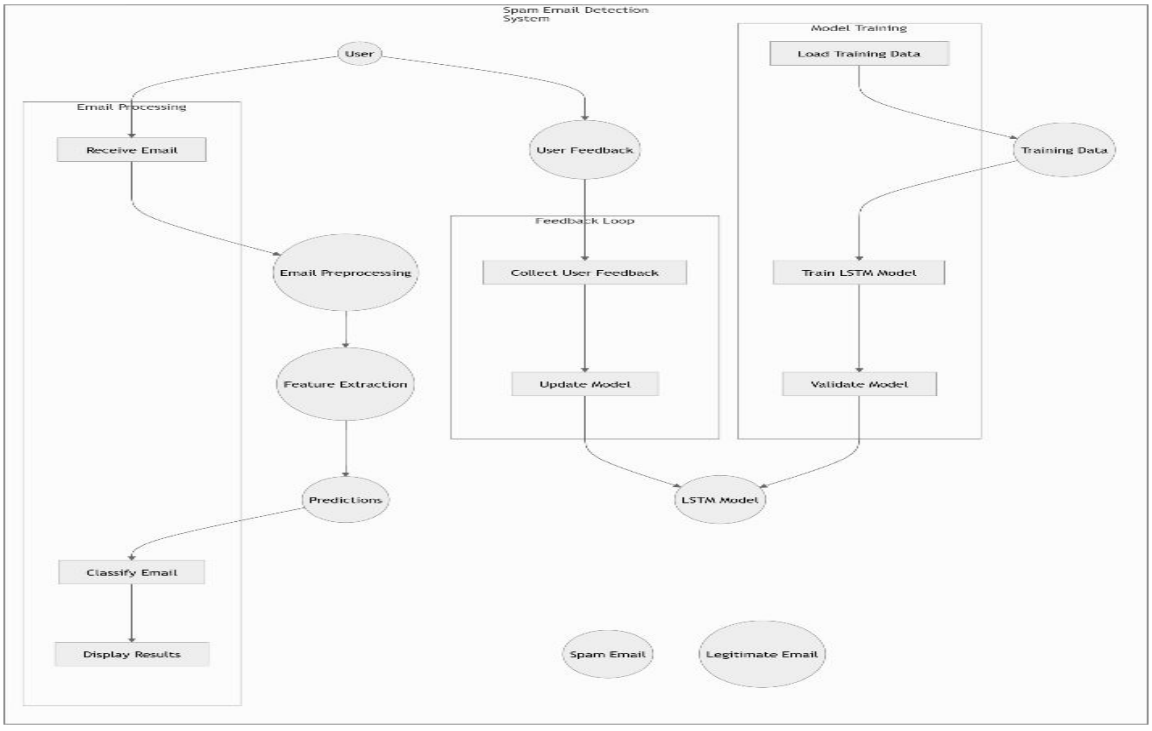


Fig 1: Architecture of the proposed system

Data Preprocessing and Email Validation

The first step involves preprocessing of data, which includes cleansing and standardizing text messages. This involves case folding, removing extraneous characters and stop words, and also tokenizing the messages such that they consist of numerical sequences. Padding is used in order to make all sequences have the same length and therefore making it appropriate for use as input to neural networks. Email addresses within the text of messages are retrieved based on regular expressions.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 6, June 2025

|DOI: 10.15680/IJIRSET.2025.1406150|

IV. EXPERIMENTAL RESULTS

4.1 OUTPUT SCREENS:

Dashboard to view the data: The image displays a real-time Network Intrusion Detection System (NIDS) dashboard powered by a hybrid deep learning model combining Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks. The dashboard presents key system metrics, including system status, threats detected, traffic analyzed, and detection accuracy (90%), indicating that the CNN-LSTM model is actively monitoring network traffic.

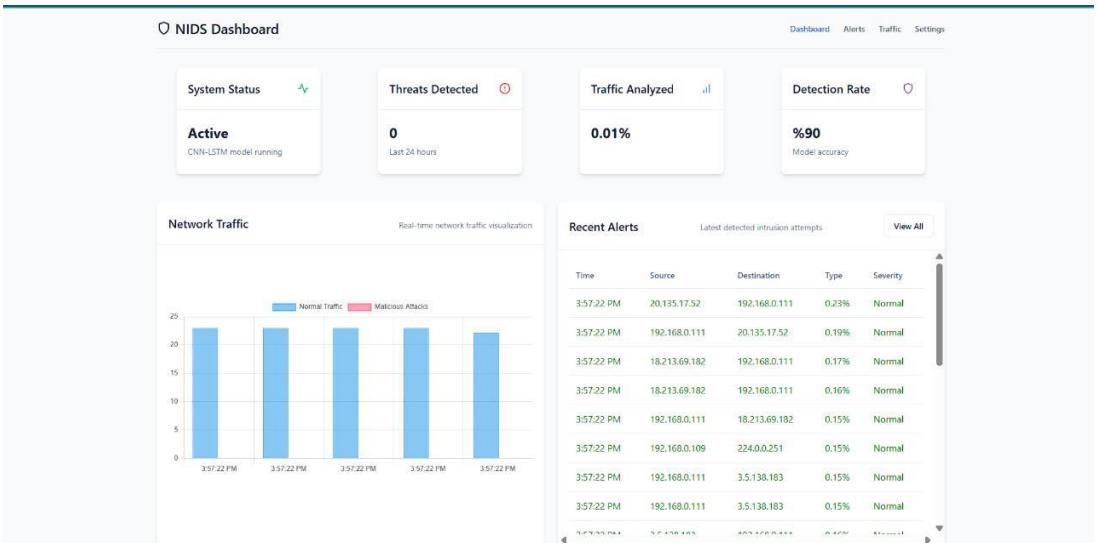


Fig 2: Dashboard to view the data

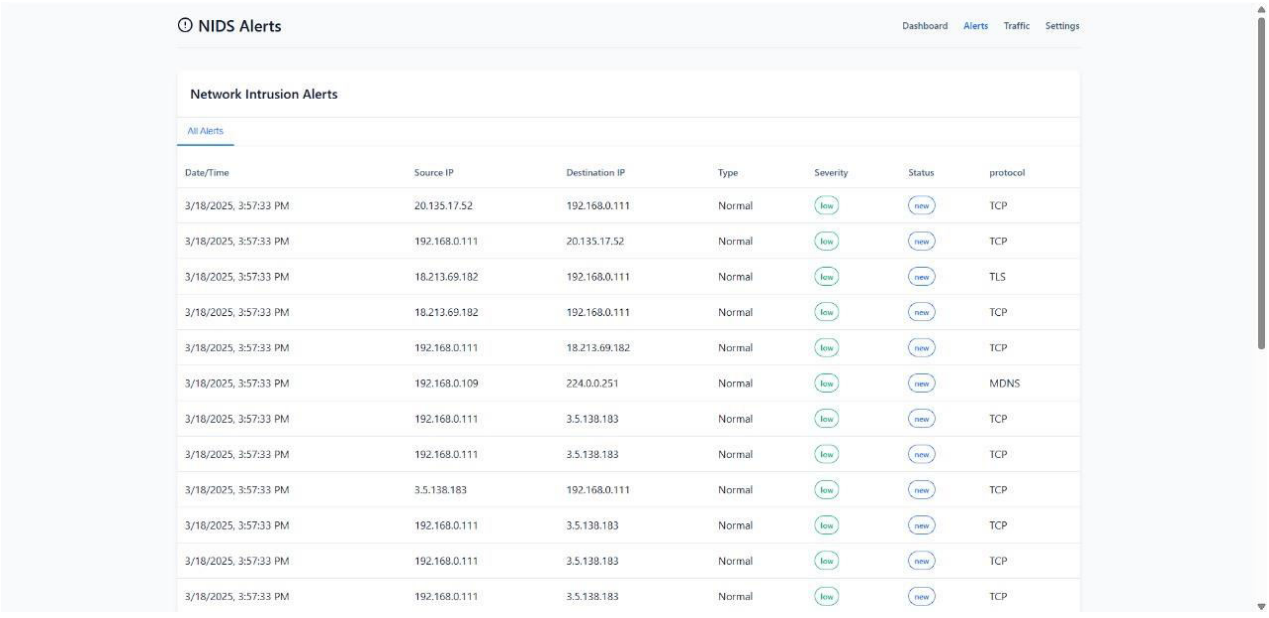


Fig 3: Processed data log files

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 6, June 2025

|DOI: 10.15680/IJIRSET.2025.1406150|

Real-time traffic data analysis:

This screen displays Network Intrusion Detection System (NIDS) Traffic Analysis Dashboard, displaying a real-time overview of both normal and malicious network traffic. The line graph shows traffic flow over time, with blue representing Normal Traffic (MB) and red representing Malicious Traffic (MB). In this instance, the dashboard indicates that 23 MB of normal traffic was detected while no malicious traffic was recorded during the captured timeframe. Supporting metrics such as Total Traffic (1.42%), Packets Analyzed (23), and Average Throughput (0.15 Mbps) offer additional insight into network activity efficiency. This visual representation is integral to the implementation of advanced NIDS technologies, especially when integrating hybrid models combining machine learning (ML) and deep learning (DL) techniques

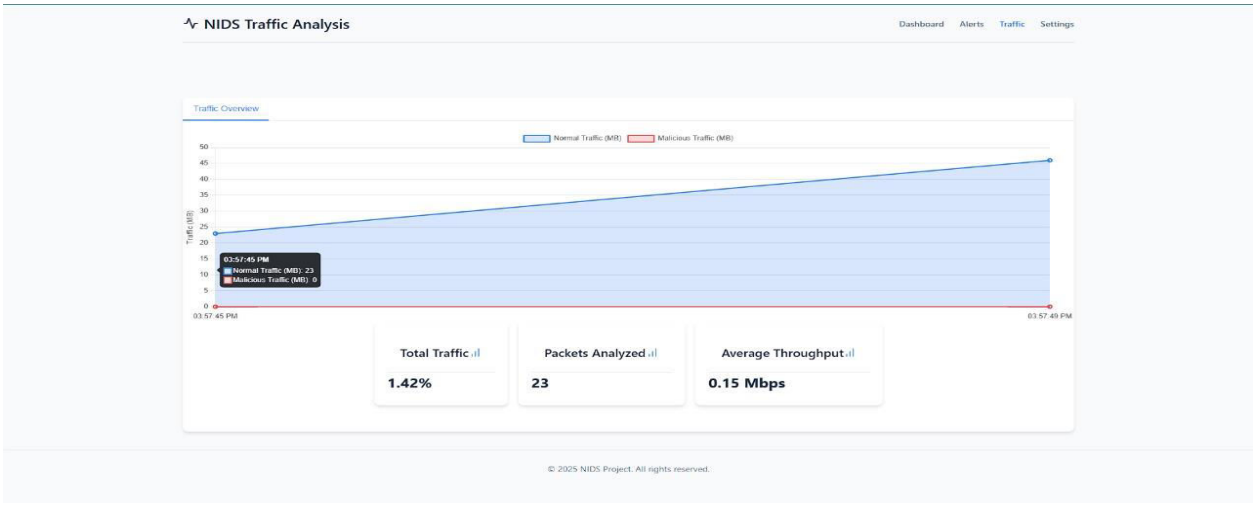


Fig 4: Real-time traffic data analysis

Result Screens:

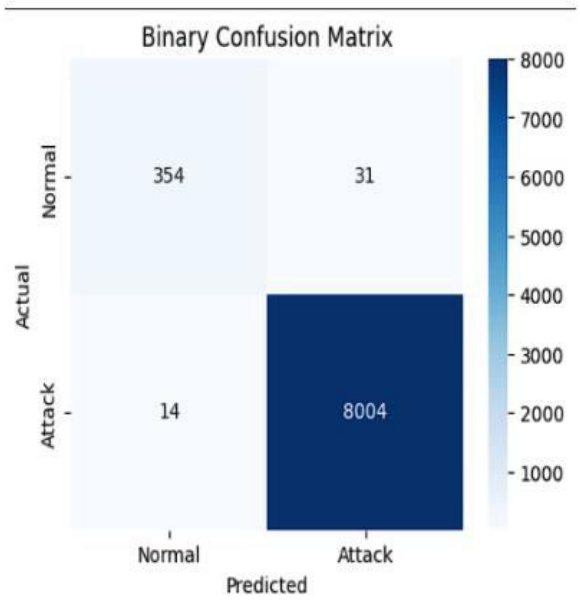


Fig 5: Confusion Matrix of the model.

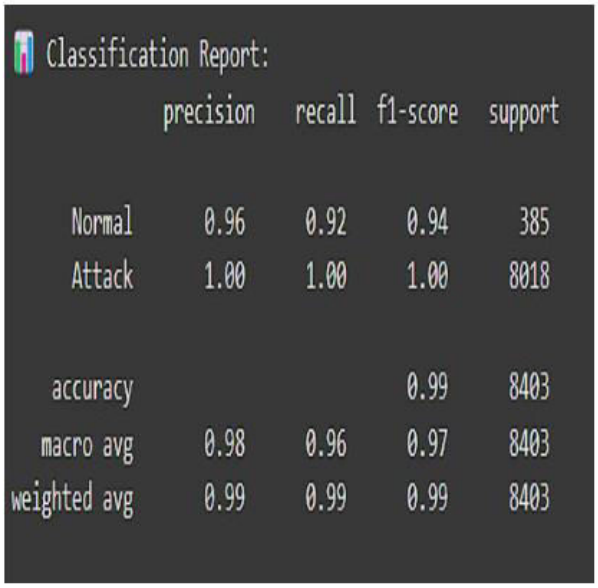


Fig 6: Classification report of the model.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 6, June 2025

|DOI: 10.15680/IJIRSET.2025.1406150|

V. CONCLUSION

The developed spam detection system satisfactorily differentiates spam and ham messages with an overall accuracy rate of success of 99% against the test data set. The combined CNN-LSTM structure spatially and temporally learnt from the text data efficiently as denoting the infrequently appearing near perfect precision and recall for illegitimate spam messages and decent spam detection properly. The use of SMOTE technique to address class imbalance has improved the recall score for spam class and has reduced false negative instances. Enabled with Email validation module, the system also prevented forged and spam email addresses embedded in messages, making it even stronger for Phishing attempt detection. Using interpretability techniques such as LIME, the system enables its users to retrieve insightful information on the hypotheses behind classification decisions made, nurturing trust and accountability over the system. Owing to the features of the system, the project successfully integrates machine learning, NLP, and interpretability in building a spam filter that is effective and easy to use for security communication in practice.

REFERENCES

[1] N. U. Saquib, A. Ahmed & M. Khan, A Hybrid Supervised Learning Approach for Content-Based Spam Filtering. International Journal of Machine Learning Applications, vol. 12, no. 3, pp. 45–52, 2024

[2] S. T. Singh, M. Sharma & A. Gupta, Algorithms for Spam Identification Using Machine Learning and Deep Learning, Journal of Data Science and Artificial Intelligence, vol. 15, no. 4, pp. 78–89, 2023

[3] K. Debnath, R. Singh & P. Roy, Exploring Deep Learning for Spam Filtering: Comparative Study and Limitations, Neural Computation and Applications, vol. 34, pp. 1021–1034, 2022

[4] S. Gadde & A. V. Kumar, Identifying SMS Spam Through Machine and Deep Learning Methods, Proceedings of the International Conference on Intelligent Computing and Communication Systems (ICICCS), pp. 356–363, 2021

[5] S. Kaddoura, R. Abdullah, and N. Mahmoud, Leveraging Deep Learning Techniques for Detecting Spam in English-Language Emails, Expert Systems with Applications

[6] A. A. Abdullahi, M. Adamu & B. A. Salihu, Identifying SMS Spam Using a Combination of Traditional and Deep Learning Approaches, Journal of Information and Communication Technology Advances, vol. 5, no. 2, pp. 144–157, 2018

[7] N. H. Marza, A. Al-Qaysi, & R. T. Rasheed, A Neural Network Method for Spam Detection in Emails, International Journal of Computer Science and Information Security, vol. 19, no. 7, pp. 45–55, 2021

[8] M. Eryilmaz, H. Topal, & S. Aydin, A Spam Filtering Solution Based on LSTM for Turkish Emails Developed with the Keras Library, Turkish Journal of Electrical Engineering and Computer Sciences, vol. 28, no. 4, pp. 2341–2353, 2020

[9] J. Natalie, T. Edwards, and S. Brown, Enhanced Spam Classification Leveraging Recurrent Neural Networks, Proceedings of the International Conference on Applications of Artificial Intelligence (ICAIA), pp. 129–137, 2021

[10] X. Liao, H. Zhang, and Y. Wu, Text-CNN Utilizing Pre-trained Word Embeddings for Spam Email Detection, Journal of Advanced Computational Techniques in Natural Language Processing, vol. 42, no. 6, pp. 213–224, 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details