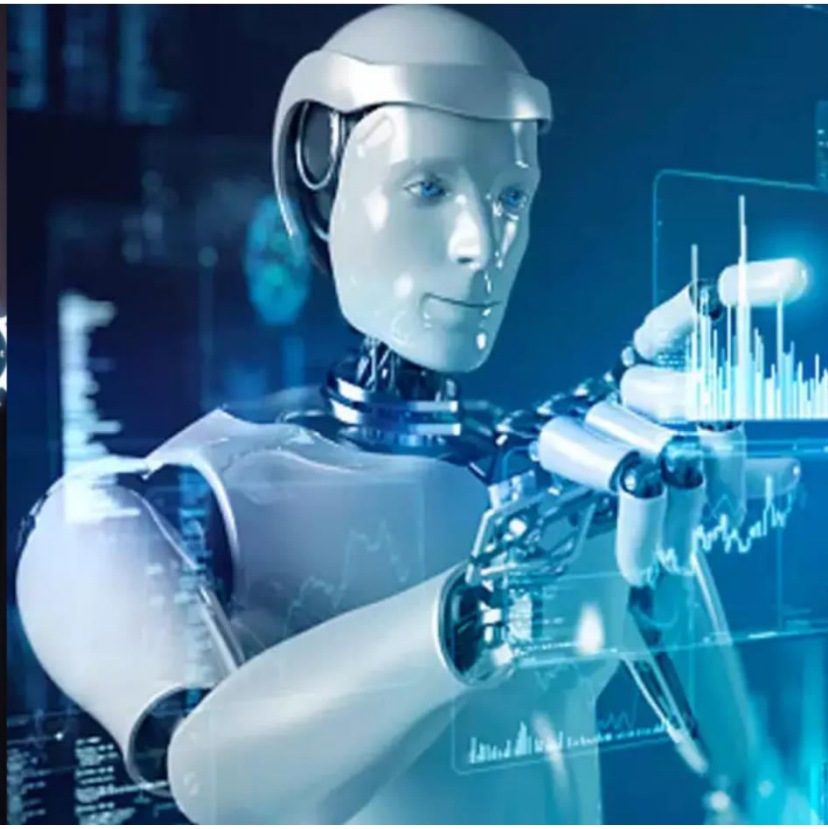
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

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 5, May 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 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405208|

Robust Intelligent Malware Detection using Deep Learning

Ms. Devi S, T. K. Kartheeswari

Department of Computer Applications, M.P.N.M.J Engineering College, Erode, India

ABSTRACT: This paper presents a robust and intelligent malware detection system using deep learning methods. Traditional signature-based malware detection techniques are increasingly ineffective against modern, polymorphic, and metamorphic malware. Our system uses Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks to classify malware by analysing its visual representation as grayscale images. Using the MalImg dataset, the model achieves high accuracy in detecting various malware families. The system includes a user-friendly GUI built with Tkinter, allowing users to upload samples and receive instant predictions. The results demonstrate that deep learning models, especially CNN, are highly effective for identifying both known and unknown malware threats.

KEYWORDS: Malware Detection, Deep Learning, CNN, LSTM, Image Classification, MalImg Dataset, Tkinter GUI, Cybersecurity, Zero-day Threats, Intelligent Systems

I. INTRODUCTION

With the growing sophistication of malware attacks, cybersecurity systems must go beyond traditional signature-based detection. Modern malware uses polymorphic and metamorphic techniques to change their signatures, making them hard to detect using conventional antivirus tools. Machine learning and deep learning approaches have emerged as powerful alternatives, enabling the automatic learning of malware behavior from large datasets. This paper proposes a deep learning-based malware detection system that uses image processing and CNN/LSTM architectures to effectively detect malware families. The proposed system not only increases detection accuracy but also provides a scalable and user-friendly solution.

II. LITERATURE SURVEY

Several studies have explored the application of machine learning in malware detection. Some have focused on static and dynamic analysis techniques, while others have leveraged neural networks for pattern recognition. Researchers have used opcode sequences, API calls, and system behaviour for classification. Recent advancements include the use of image-based malware detection, where binary files are converted to grayscale images and analysed using CNNs. This method has shown improved accuracy and resilience against obfuscation. Our work builds upon these ideas by combining CNN and LSTM with GUI integration.

III. METHODOLOGY

The proposed system consists of several modules: data preprocessing, model training, evaluation, prediction, and GUI interface. Malware binary files are first converted into grayscale images using the MalImg dataset. These images are resized, normalized, and split into training and testing sets. We use multiple classifiers including KNN, SVM, Random Forest, and deep learning models such as CNN and LSTM. The CNN model processes the spatial patterns in the image, while LSTM captures sequential dependencies if needed. The models are trained and evaluated using accuracy, precision, recall, and F1-score. The final system includes a Tkinter-based GUI for real-time malware classification.

IV. EXPERIMENTAL RESULTS

The CNN model outperformed all other classifiers with an accuracy of over 97%. LSTM also achieved strong performance but required more training time. Traditional ML models like Random Forest and SVM showed decent but

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 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405208|

lower accuracy. The GUI successfully integrated the trained models, allowing users to upload images and receive instant predictions. A comparative analysis graph was created to show model performance across different metrics.

V. CONCLUSION

This project successfully demonstrates a deep learning-based approach for robust malware detection using image processing techniques. The CNN model, in particular, showed high effectiveness in identifying various malware families. The system eliminates the need for manual feature selection and is capable of detecting unknown threats. With a user-friendly interface and scalable architecture, this solution can be implemented in real-world cybersecurity environments. Future work can focus on real-time integration with antivirus platforms and expanding the dataset for broader threat coverage.

REFERENCES

1. Nataraj, L., Karthikeyan, S., Jacob, G., & Manjunath, B. S. (2011). Malware images: visualization and automatic classification. Proceedings of the 8th International Symposium on Visualization for Cyber Security, ACM.
2. Raff, E., Barker, J., Sylvester, J., Brandon, R., Catanzaro, B., & Nicholas, C. K. (2018). Malware detection by eating a whole EXE. Workshops at the Thirty-Second AAAI Conference on Artificial Intelligence.
3. Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). ImageNet classification with deep convolutional neural networks. Advances in Neural Information Processing Systems.
4. Simonyan, K., & Zisserman, A. (2014). Very deep convolutional networks for large-scale image recognition. arXiv preprint arXiv:1409.1556.
5. Hochreiter, S., &Schmidhuber, J. (1997). Long short-term memory. Neural Computation.

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