| Volume 02 | Issue 06 | November 2026 | ISSN: 3139-1737

International Journal of Advances and Applications in Convergent Studies & Transdisciplinary (IJ-AACST)

Bridging Disciplines, Bridging Knowledge

Aligned with the Vision of NEP 2020 and UGC Guidelines

Website: https://aacstij.org || Email: journaleditor@aacstij.org

Malware Detection Using a Hybrid Cnn–Gru–Bilstm Deep Learning Model

DOI: https://doi.org/10.5281/zenodo.24103078

Ms. Rubina. G. Kureshi[1]*, Dr. R. K. Dhuware[2]

*Corresponding Author: [11]Research Scholar, Department of Electronics and Computer Science, RTMNU, Nagpur, Maharashtra, India

[2]Head, Department of Computer Science Dhote Bandhu Science College, Gondia, Maharashtra, India

ABSTRACT

Cybersecurity is a group of technologies, processes and practices focused to shield systems, software, data and computer networks against malicious exploitation and cyber-attacks. At various levels cybersecurity measures are implemented containing the host, application, data and network levels by using various tools like threat detection systems, firewalls and cyber-attacks prevention systems. Despite the implementation of various cybersecurity measures, the growing number of internet-connected devices has increased the vulnerabilities exposure scope, especially in the context of IoT and enterprises. The latest modern cyber-attacks are becoming more dynamic, complex and challenging to identify as compared to traditional signature-based security solutions that are effective in recognizing well known attacks but inefficient in spotting covert and persistent exploitation activities, newly discovered threat exploits and diverse malwares where the vulnerability is exploited before the patch or signature is available.

Proposed CNN–GRU–BiLSTM model maintained competitive detection performance despite limited labelled data, achieving an accuracy of 96.50% and an F1-score of 0.96. This highlights the effectiveness of the proposed approach in realistic cybersecurity environments where complete labelling of data is often impractical. The results indicate that the model can leverage both labelled and unlabelled data to improve detection capability while reducing dependency on manual annotation.

KEYWORDS: ***Deep Learning, Security Attacks, CNN, Bi-LSTM, GRU***.

1. INTRODUCTION

Cybersecurity is a collection of technologies, processes and practices focused to protect systems, software, data and computer networks against malicious exploitation and cyber-attacks [1], [2]. At various levels cybersecurity measures are implemented containing the host, application, data and network levels by using various tools like threat detection systems, firewalls and cyber-attacks prevention systems [4]. Despite the implementation of various cybersecurity measures, the growing number of internet connected devices has increased the

© 2026 The Author(s). This article is published by the AACST in the IJ-AACST under the Creative Commons Attribution 4.0 International (CC BY 4.0) License. The authors retain copyright and grant AACST a non-exclusive license to publish, distribute, and archive the work.