Enhancing Ransomware Detection with a Hybrid Deep Learning Approach: Integrating Convolutional Neural Networks and Long Short-Term Memory Networks for a Robust Cybersecurity Solution

Priynka Sharma* and Kaylash Chaudhary

School of Information Technology, Engineering, Mathematics and Physics, The University of the South Pacific, Suva, 1168, Fiji

**Email*: priynka.sharma@usp.ac.fj (Priynka Sharma)

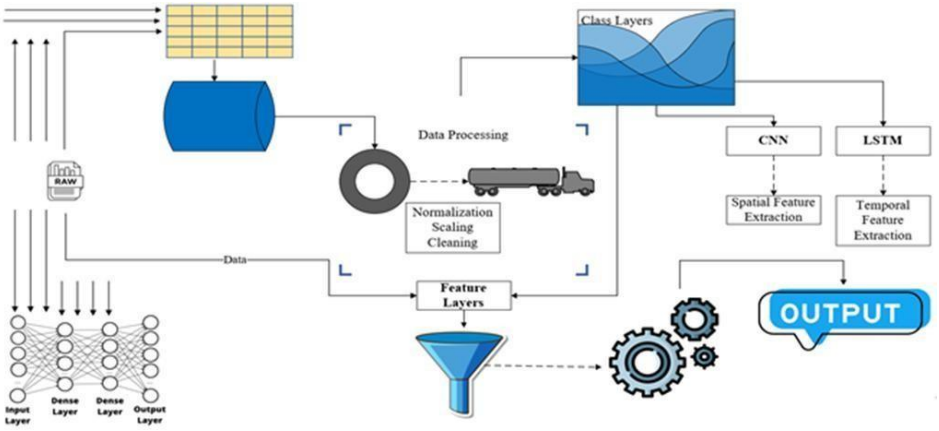
Received: 03 Jan 2025; Revised: 13 April 2025; Accepted: 14 April 2025

Type: Research Paper

Abstract

Ransomware attacks continue to be a significant and evolving cybersecurity threat, with traditional detection techniques often unable to identify new and sophisticated variants. Signature-based and heuristic methods, which rely on pre-existing knowledge of malicious behaviors, frequently fail to detect novel strains, highlighting the need for more dynamic, data-driven detection systems. In this paper, we propose a hybrid deep learning framework that integrates Convolutional Neural Networks (CNNs) and Long Short-Term Memory Networks (LSTMs) to address the limitations of existing detection approaches. The CNN extracts spatial features from raw data, such as file byte sequences, system calls, and network traffic, crucial for identifying ransomware traits. Meanwhile, the LSTM captures temporal dependencies and sequential patterns, essential for detecting dynamic ransomware behaviors over time. The proposed model is evaluated on a comprehensive ransomware dataset comprising 1,000 features, 10,000 samples, and six distinct classes, encompassing both benign and ransomware behaviors. Experimental results demonstrate that the hybrid CNN-LSTM model outperforms traditional methods significantly. By leveraging the strengths of both CNNs for feature extraction and LSTMs for sequence modeling, the proposed hybrid model provides a more accurate, adaptive, and scalable solution for real-time ransomware detection, thereby reducing false positives and enhancing the robustness of cybersecurity systems against emerging threats.

Table of Contents



Innovative Description: The Integration of Convolutional Neural Networks and Long Short-Term Memory Networks for Robust Cybersecurity Solution.