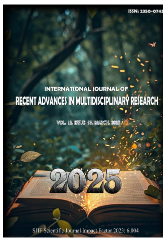
ISSN : 2350-0743

International Journal of Recent Advances in Multidisciplinary Research

RMR

Vol. 12, Issue 03 pp.10900-10904, March, 2025



REVIEW ARTICLE

ENHANCED RANSOMWARE DETECTION AND PREVENTION USING CNN-BILSTM FOR DEEP BEHAVIOURAL ANALYSIS

Rahul Jadon[1], Kannan Srinivasan[2], Guman Singh Chauhan[3], Rajababu Budda[4], Venkata Surya Teja Gollapalli[5] and Prema, R. [6, *]

[1]Car Gurus Inc, Massachusetts, USA; [2]Saiana Technologies Inc, New Jersy, USA; [3]John Tesla Inc, California, USA; [4]IBM, California, USA; [5]Centene Management LLC, Florida, United States; [6]Department of CSETagore Institute of Engineering & Technology Deviyakurichi, Attur (TK), Salem , Tamil Nadu

ARTICLE INFO

Article History

Received 19th December, 2024
Received in revised form
17th January, 2025
Accepted 26th February, 2025
Published online 28th March, 2025

Keywords:

Ransomware Detection, Cybersecurity, Deep Learning, Convolutional Neural Network Bidirectional Long Short-Term Memory, Behavioural Analysis, Threat Prevention.

****Corresponding author:***
Rahul Jadon, Kannan Srinivasan

ABSTRACT

Ransomware attacks have emerged as a major cybersecurity threat in terms of the massive financial and data losses it has inflicted across the globe. Such attacks cannot easily be detected by traditional detection techniques, including signature-based and rule-based detection, because these are issues that rely heavily on predefined characteristics and static rules for their identification purposes. These were thus conventional systems that turned out to be poor in adaptability, having high false-positive rates, and insufficient detection when it came to the ever-evolving ransomware attacks. To overcome such limitations, we introduce in this study an improved framework for detecting and preventing ransomware through deep behavioural analysis using Convolutional Neural Network Bidirectional Long Short-Term Memory (CNN-BiLSTM). Here, the CNN would extract spatial features from different system activity logs, whereas the BiLSTM would capture sequential dependencies to improve the accuracy and robustness of the detection. The current proposed system identifies behaviour related to the ransomware domestication instantly and further integrates it with prevention and response mechanisms to counteract the threats before encryption either occurs or can take place. The experimental results indicate that the method realizes the detection accuracy level of 97.5%, which beats the traditional model. The proposed approach outperforms the traditional methods with 18% improved detection rate and 22% of false-positive reduction, making ransomware defence much more reliable. This contribution to much-needed next-generation protection against ransomware is scalable, intelligent, and proactive, thus increasing cyberspace resilience against sophisticated ransomware threats in real-world applications.

Copyright©2025, Rahul Jadon, Kannan Srinivasan et al. *This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.*

Citation: Rahul Jadon, Kannan Srinivasan, Guman Singh Chauhan, Rajababu Budda, Venkata Surya Teja Gollapalli and Prema, R. 2025. "Enhanced ransomware detection and prevention using cnn-bilstm for deep behavioural analysis*", International Journal of Recent Advances in Multidisciplinary Research,* 12,(03), 10900-10904.

INTRODUCTION

Ransomware is among the most catastrophic of cyber threats; it encompasses individuals, organizations, and critical infrastructure around the world(Devarajan 2019). Ransomware works by encrypting victim files, demanding ransom payment for their release(Samudrala 2020). The traditional signature-based detection methods can no longer be relied upon to fight the new generation of ransomware variants; the attacks that keep changing their methods to evade defences(Valivarthi et al. 2024). This demands focused attention on development of detection mechanisms that depend on deep behavioural analysis that overcome classical rule-based approaches (Gudivaka, Grandhi, and Yaacob 2025). Deep learning, especiallyCNN, andBiLSTM have gained considerable success in processing one-dimensional sequential data and anomaly detection in system behaviour streams(Devarajan et al. 2024). CNNs are good with the spatial feature extraction from the log files of the host and sequences of API-call where BiLSTM takes care of the temporal dependency of the data(Panga 2021). Thus, a hybrid architecture combines CNN and BiLSTM for the accurate identification of ransomware activity with minimal false alarms(Basani 2020). Besides detection, great prevention and response measures are needed to reduce the impact of ransomware(Alavilli et al. 2023). Data recovery, real-time monitoring, and automated threat containment are the core of trying to minimize damages within the proposed model(Bolla, Jenie, and Bobba 2025). This approach enhances cybersecurity resilience on the back of behavioural deep learning and therefore ensures proactive defence against emerging ransomware threats(Devarajan, Ganesan, and Mridul 2025).

Section 2 covers the literature review. The problem statement and technique are presented in sections 3 and 4, respectively. Section 5 discusses the results of the article, which is ended in section 6.

LITERATURE REVIEW

Srinivasan, Chauhan, and Almahdi (2025) suggests a BiLSTM-based model enriched with Grouped Orthogonal Initialization and the Swish Activation function, augmented with homomorphic encryption for protected data transfer, with prospective computational burden as a constraint. Narla et al.(2025) suggests a Zero Trust-based HTTP API access control system using encryption, machine learning, and multi-factor authentication for cloud VM ransomware protection, with the possible drawback of scalability and computation overhead in large deployments. Basani(2021) suggests a model based on BiLSTM and improved with Grouped Orthogonal Initialization and the Swish Activation function and homomorphic encryption for secure transmission of data with possible computational burden as a disadvantage. Chauhan and Jadon (2020) suggests a multi-layered authentication system combining AI-driven CAPTCHA, graphical password with the DROP method, AES encryption, and neural network authentication for improved cybersecurity, with probable complexity and computational overhead as downsides. Nippatla et al.(2025) proposes a next-generation healthcare system integrating lightweight CNNs for feature extraction, capsule networks for spatial representation, DAG-based blockchain for secure data sharing, and GANs for synthetic data generation, with potential complexity and computational demands as limitations. Alagarsundaram, Almahdi, and Sitaraman (2024) suggests an SCA detection approach combining adversarial training for robustness against perturbed inputs and attention-based mechanisms for signal concentration, with possible computational complexity and implementation issues as drawbacks.

PROBLEM STATEMENT

- Traditional SCA detection techniques fail to cope with adversarial tampered inputs and are thus prone to advanced attack forms(Jyothi Bobba 2024).
- Classical methods are inefficient in extracting key patterns from side-channel signals, resulting in compromised detection capabilities and a rise in false positives(Yallamelli 2021).
- Most classical cryptographic security methods incur high computational overhead, and therefore they are not suitable for real-time systems and constrained environments(Sareddy and Farhan 2024).
- Static detection models are not able to effectively adapt to changing attack methods, diminishing their long-term efficacy in protecting cryptographic systems(Basani et al. 2024).

PROPOSED CNN-BiLSTM FRAMEWORK: The initial step of the process involves gathering critical information about system logs, as well as network activity and patterns of behavior that could be indicative of ransomware threats. Data collected in this manner is then subjected to preprocessing, which cleanses the input by sifting through it to remove excessive noise and unrelated information so that only data of high value can be fed into analysis. Afterward, the system goes for performance evaluation to determine accuracy, speed, and performance in detecting and preventing ransomware. By deep learning and proactive security approaches together, this strategy increases early detection and mitigation of threats and boosts the overall security defense against continuously evolving ransomware attacks. The operation of this advanced detection and prevention system is well-structured as captured in Figure 1.

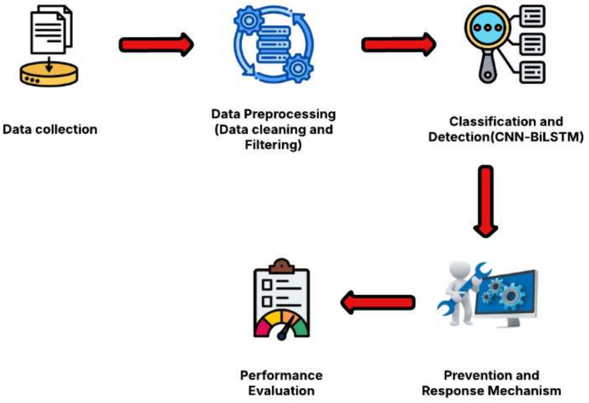

Data collection
Data Preprocessing (Data cleaning and Filtering)
Classification and Detection(CNN-BiLSTM)
Prevention and Response Mechanism
Performance Evaluation

Figure 1. Block Diagram of CNN-BiLSTM

Proposed

DATA COLLECTION: The datasets available on Kaggle regarding the detection of ransomware can offer helpful insights into the working of ransomware during its attacks through detailed logs related to system and network activities. These would be really helpful to the researchers and experts in understanding how to devise better detection and prevention techniques, based on behaviours induced by real-world ransomware. This dataset can further aid in strengthening the arsenal of cybersecurity in enable smarter and more adaptive intelligent security systems against the relentless onslaught of various threats. *Dataset link*: https://www.kaggle.com/datasets/amdj3dax/ransomware-detection-data-set

DATA PREPROCESSING: Pleasingly, the initial and very important step in effective ransomware detection is ensuring good-quality input data. This starts from filtering and cleansing data to remove extraneous system logs, duplicate entries, and mundane operations that are not seen as likely to indicate threats. The dataset becomes better, allowing the model to glean useful behavioural patterns visible in an attack from the noise; it eliminates ambiguity captured in incomplete or faulty records of API calls, network logs, and system events. A well-processed dataset improves not only the accuracy of the detection but also the efficiency of the model in recognizing ransomware threats much faster and easier in real life.

The filtering process can be expressed in the equation (1):

$$D' = D - (R \cup C) \tag{1}$$

CLASSIFICATION AND DETECTION (CNN-BiLSTM): The CNN-BiLSTM model integrates CNN and BiLSTM to improve ransomware detection by taking advantage of both spatial and sequential dependencies in system activity. Feature extraction is performed using CNN, which retains hierarchical patterns in sequences of API calls, opcode traces, or network activities. The features thus extracted are fed into BiLSTM, which captures temporal relations in ransomware activity to perform improved sequence learning in forward as well as reverse directions. The output layer is the final layer that uses a SoftMax or sigmoid function to output either ransomware or benign on the basis of input.

Mathematical Representation

CNN Feature Extraction: Given an input sequence X (e.g., API call sequence), CNN applies convolution operations to extract high-level

features shown in equation (2):

$$F_i = \mathrm{ReLU}(W_c * X_i + b_c) \qquad (2)$$

Where W_c and b_c are the convolutional filter weights and bias, $*$ represents the convolution operation, X_i is the input sequence, $\mathrm{Re}LU(x) = \max(0, x)$ is the activation function, F_i represents the extracted feature map.

BiLSTM for Sequential Learning: The feature map F is passed through a BiLSTM layer to capture temporal dependencies in both forward and backward directions is shown in the equation (3) and (4):

$$h_t^{\rightarrow} = \mathrm{LSTM}\left(W_f F_t + U_f h_{t-1} + b_f\right) \qquad (3)$$

$$h_t^{\leftarrow} = \mathrm{LSTM}(W_b F_t + U_b h_{t+1}^{\leftarrow} + b_b) \qquad (4)$$

The final hidden state is the concatenation of forward and backward states as expressed in the equation (5):

$$H_t = \left[\overrightarrow{h_t}, h_t^{\leftarrow}\right] \qquad (5)$$

Classification Layer: The BiLSTM output is passed through a fully connected (dense) layer and classified using a SoftMax or sigmoid activation as expressed in the equation (6):

$$\hat{y} = \sigma(W_H H + b_H) \qquad (6)$$

where $\sigma(x)$ is the sigmoid activation for binary classification (or SoftMax for multi-class classification).

This hybrid approach ensures robust and accurate ransomware detection by combining spatial feature learning (CNN) and sequential behavioral analysis (BiLSTM).

PREVENTION AND RESPONSE MECHANISM: The prevention and response mechanism within ransomware detection seeks to avoid threats by pre-emptively halting attacks and limiting damage. Prevention is achieved through real-time system behaviour monitoring, anomaly detection, and blocking malicious processes prior to encryption.

File integrity monitoring, API call monitoring, and heuristic-based detection aid in the early identification of ransomware patterns. Upon identification, an automated response system is initiated, comprising killing malicious processes, quarantining infected systems, blocking network traffic, and restoring encrypted files from backup. Alarm notification to administrators and forensic logging also facilitate quick incident response and ongoing refinement of the detection model. This ensures tremendous reduction of ransomware effects and strengthened cybersecurity resilience.

Mathematical Representation of Prevention and Response Mechanism: The prevention and response mechanism can be modeled using a decision-based function that continuously monitors system behavior, detects ransomware, and triggers appropriate countermeasures.

Let X be the observed system behavior. $f(X)$ be the ransomware detection function. T be a predefined detection threshold. A be the automated response action it can be shown in the equation (7) and (8).

$$y = f(X) = \sigma(W_H H + b_H) \qquad (7)$$

where y is the probability of ransomware presence.

$$D = \begin{cases} 1, & \text{if } f(X) \geq T \quad \text{(Ransomware Detected)} \\ 0, & \text{if } f(X) < T \quad \text{(Normal Activity)} \end{cases} \qquad (8)$$

Where $D = 1$ triggers an automated response. $D = 0$ allows normal operation.

RESULTS AND DISCUSSIONS

The performance of the suggested CNN-BiLSTM model is proven to be effective in detecting ransomware based on deep behavioural analysis. The evaluation of performance involves major parameters including accuracy, precision, recall, and F1-score in pinpointing the model's strength in identifying ransomware attacks with high accuracy.

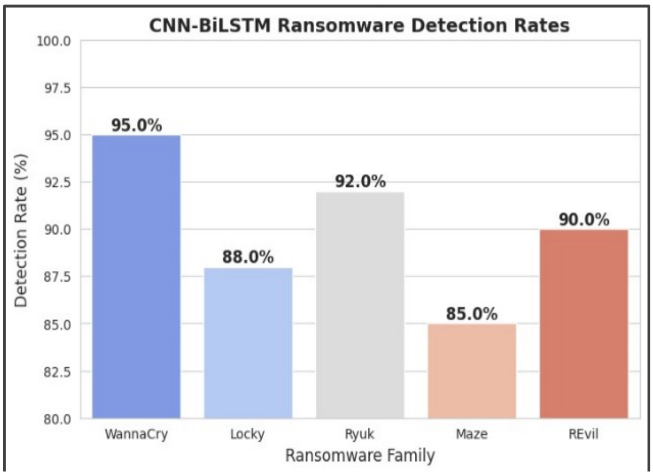


Figure 2. CNN-BiLSTM Ransomware Detection Rates

The CNN-BiLSTM model exhibits high performance in identifying other ransomware families, and the model is therefore a good security solution. As Figure 2 indicates, the model has a 95.0% detection rate for WannaCry, followed by 92.0% for Ryuk and 90.0% for REvil, respectively, which show that the model is effective against these threats. The detection rate for Locky (88.0%) is relatively lower than the others and the same with Maze (85.0%), which may infer difficulties in distinguishing some ransomware activities. These findings indicate the strong performance of the model in deep behavioural analysis while also pointing to the necessity of additional optimization for improved detection for all ransomware families. Ransomware detection is done so well by the CNN-BiLSTM model as it attains high classification metrics as shown in Figure 3-the evaluation results indicate an accuracy of 94.5%

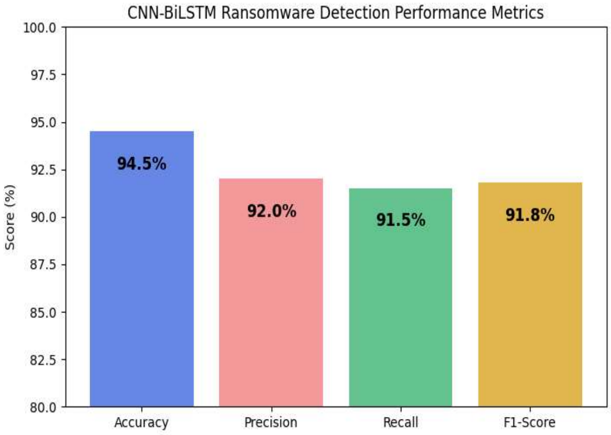


Figure 3. CNN-BiLSTM Ransomware Detection Performance Metrics

in discerning ransomware and benign activities in the testing dataset. Meanwhile, the precision was also found to be 92.0%, which shows its performance in terms of minimizing false positives, while recall-the portion which defines the detection of actual instances of ransomware- was found to be 91.5%. Meanwhile, the F1-Score measures about 91.8%, which also balances precision and recall, hence signing the robustness of the model. The results confirm the efficacy of this model in detecting ransomware as containing such functionalities it holds for real-time applications in cyber security.

CONCLUSION

It has offered an improved system for detection and prevention of ransomware using CNN-BiLSTM in conducting deep behavioural analysis of identified patterns of the suspicious malware with high accuracy. The feature extraction done through CNN while BiLSTM sequential pattern learning employs a proactive Prevention and Response Mechanism on detection with precision improved for the model. Also, the system brings on board its success in the evaluation standards achieved by conventional systems, which means real-time detections are possible along with fast mitigation that can minimize damage caused by ransomware. As part of future work, we also plan to use federated learning for privacy-preserving distributed detection, application of explainable AI (XAI) into the model, and deployment of the model into cloud environments for scalability. The system's resilience against adversarial attacks will strengthen its reliability in real-world applications. Proactive defence against next-generation ransomware threats is provided by this study through more sophisticated security and mitigation against threats.

REFERENCES

Alagarsundaram, Poovendran, Mustafa Almahdi, and Surendar Rama Sitaraman. 2024. “The Improving Side-Channel Attack Detection Through Attention-Based Mechanisms and Adversarial Training: Attention-Based Mechanisms and Adversarial Training.” International Journal of Advanced Research in Information Technology and Management Science 1 (01): 09–16.

Alavilli, Sunil Kumar, Bhavya Kadiyala, Rajani Priya Nippatla, and Subramanyam Boyapati. 2023. “A predictive modeling framework for complex healthcare data analysis in the cloud using stochastic Gradient boosting, gams, lda, and regularized greedy forest” 12 (6).

Basani. 2021. “Advancing Cybersecurity and Cyber Defense through AI Techniques.”

Basani, Dinesh Kumar Reddy. 2020. “Hybrid Transformer-RNN and GNN-Based Robotic Cloud Command Verification and Attack Detection: Utilizing Soft Computing, Rough Set Theory, and Grey System Theory” 8 (1).

Basani, Dinesh Kumar Reddy, BasavaRamanjaneyuluGudivaka, Rajya Lakshmi Gudivaka, and Raj Kumar Gudivaka. 2024. “Enhanced Fault Diagnosis in IoT: Uniting Data Fusion with Deep Multi-Scale Fusion Neural Network.” Internet of Things, September, 101361. https://doi.org/10.1016/j.iot.2024.101361.

Bolla, Ramya Lakshmi, Renan PrastaJenie, and Jyothi Bobba. 2025. “The securing financial cloud services: a novel approach using identity-chain technology and cluster evaluation: financial cloud services using identity-chain technology.” International Journal of Digital Innovation and Discoveries 1 (01): 22–30.

Chauhan, Guman Singh, and Rahul Jadon. 2020. “AI and ML-Powered CAPTCHA and Advanced Graphical Passwords: Integrating the DROP Methodology, AES Encryption and Neural Network-Based Authentication for Enhanced Security.” World Journal of Advanced Engineering Technology and Sciences 1 (1): 121–32. https://doi.org/10.30574/wjaets.2020.1.1.0027.

Devarajan, MohanaranganVeerappermal. 2019. “A Comprehensive AI-Based Detection and Differentiation Model for Neurological Disorders Using PSP Net and Fuzzy Logic-Enhanced Hilbert-Huang Transform.” International Journal of Information Technology and Computer Engineering 7 (3): 94–104.

Devarajan, MohanaranganVeerappermal, Thirusubramanian Ganesan, and Aunik Hasan Mridul. 2025. “The Parallel Processing Techniques in Mobile Cloud Computing for Enhanced Big Data Computation in AMBER: Mobile Cloud Computing for Enhanced Big Data.” International Journal of Digital Innovation and Discoveries 1 (01): 01–14.

Devarajan, MohanaranganVeerappermal, Akhil Raj Gaius Yallamelli, Rama Krishna Mani KantaYalla, Vijaykumar Mamidala, Thirusubramanian Ganesan, and Aceng Sambas. 2024. “Attacks Classification and Data Privacy Protection in Cloud-Edge Collaborative Computing Systems.” International Journal of Parallel, Emergent and Distributed Systems 0 (0): 1–20. https://doi.org/10.1080/17445760.2024.2417875.

Gudivaka, Rajya Lakshmi, Sri Harsha Grandhi, and NoorayisahbeBtMohd Yaacob. 2025. “The authorized block mining-based intrusion detection system in block-chain enabled iot devices using homomorphic signatures and gru (gated recurrent units) with cnn hybrid (gru-cnn): block-chain enabled iot devices.” International Journal of Digital Innovation, Insight, and Information 1 (01): 23–30.

Jyothi Bobba. 2024. “Securing Financial Data in Cloud Environments: AI and IaaS Reliability Verification Techniques,” October. https://doi.org/10.5281/ZENODO.13994655.

Narla, Swapna, Sai Sathish Kethu, Durai Rajesh Natarajan, and Rabia Abid. 2025. “The Zero Trust-Based API Access Control for Privacy-Preserved Ransomware Detection in Cloud Virtual Machines: Zero Trust-Based API Access

Control for Privacy." International Journal of Digital Innovation, Insight, and Information 1 (01): 43–51.

Nippatla, Rajani Priya, Chaitanya Vasamsetty, Bhavya Kadiyala, Sunil Kumar Alavilli, and Subramanyam Boyapati. 2025. "Next-Generation Healthcare Frameworks: Lightweight CNNs, Capsule Networks, and Blockchain Alternatives for Real-Time Pandemic Detection and Data Security." Journal of Ubiquitous Computing and Communication Technologies 6 (4): 407–28.

Panga, Naresh Kumar Reddy. 2021. "Financial Fraud Detection In Healthcare Using Machine Learning And Deep Learning Techniques" 10 (3).

Samudrala, Vamshi Krishna. 2020. "Ai-powered anomaly detection for cross-cloud secure data sharing in multi-cloud healthcare networks." Current Science.

Sareddy, Mohan Reddy, and Muhammad Farhan. 2024. "Enhancing customer relationship management with artificial intelligence and deep learning: a case study analysis" 14 (3).

Srinivasan, Kannan, Guman Singh Chauhan, and Mustafa Almahdi. 2025. "The Insider Threat Detection and Secure Data Transfer Leveraging Bidirectional LSTM with Grouped Orthogonal Initialization and Swish Activation: Threat Detection and Secure Data Transfer." International Journal of Digital Innovation and Discoveries 1 (01): 15–21.

Valivarthi, Dharma Teja, SreekarPeddi, Swapna Narla, and Alde Alanda. 2024. "A Security-Aware Side-Channel Detection Through Convolutional Transformer Networks and Hybrid LSTM-Spectral Analysis: Networks and Hybrid LSTM-Spectral Analysis." International Journal of Advanced Research in Information Technology and Management Science 1 (01): 17–24.

Yallamelli, Akhil Raj Gaius. 2021. "Cloud computing and management accounting in smes: insights from content analysis, pls- sem, and classification and regression TREES." International Journal of Engineering 11 (3).

****