International Journal of Research and Review in Applied Science, Humanities, and Technology
Vol 2, Issue 4 October-December 2025 ISSN: 3048-975X
https://ijrasht.com/

LSTM-Based Cybersecurity Framework Utilizing Image Processing Techniques

Bhumika S Prajapati, Assistant Professor, Department of Information Technology, Madhuben and Bhanubhai Patel Institute of Technology, The Charutar Vidhya Mandal (CVM) University, New Vallabh Vidyanagar, Anand, Gujarat, India bhumika0914@gmail.com

Abstract: There is higher level of cybersecurity threats that adopt polymorphic malware, phishing and advanced persistent threats which cannot be detected through traditional means. Emerging as a promising technology in the detection of malicious activity are Long Short-Term Memory (LSTM) networks, which have the potential to learn sequential dependencies. Combining image processing and LSTM models presents a fresh insight into converting unstructured cybersecurity information (network traffic, malware binaries, and system logs) to visual representations that can be reviewed more accurately. The paper provides an overview and a workflow of what can be achieved with LSTM-based models and image processing in order to complement cybersecurity detection systems. Cybersecurity data can be transformed into grayscale or RGB images, allowing a complex pattern to be visualized, in which LSTM models can determine temporal features that would otherwise be challenging to identify in a raw format. Applications mentioned are malware classification, intrusion detection, phishing detection and anomaly detection. The system uses convolutional preprocessing to extract features, and then classifies the features using LSTM to provide spatial and temporal learning. The worst would have high level of computation, model intelligibility, data imbalance and adversarial example vulnerability. Irrespective of these shortcomings, the proposed integration proves to be more accurate, scalable and adaptable than traditional detection techniques. This paper concludes that LSTM, along with image processing, is a step in the right direction to the next-generation cybersecurity models, capable of withstanding future and emerging threats. Federated learning to assist privacy preserving training, explainable AI to assist transparency, and light-weight architectures to assist real-time IoT security are directions to come.

Keywords: Malware Analysis, Intrusion Detection, Cyberspace, LSTM, Image Processing.

1. Introduction

Cybercriminals have increased the attack surface due to the proliferation of IoT devices, cloud computing and digital ecosystems. Classical signature-based cybersecurity systems are progressively failing to stop polymorphic attacks as well as zero-day attacks (Sommer & Paxson, 2010). In an attempt to solve these problems, machine learning (ML) and deep learning (DL) have been used to detect anomalies and analyse malware. Of these, LSTM networks have the advantage of sequence modelling and are therefore applicable in the analysis of system logs and traffic flows (Hochreiter and Schmidhuber, 1997).

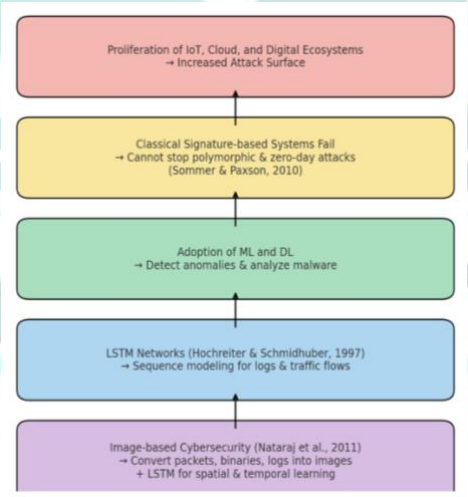

Figure 1: Evolution from Classical Cybersecurity to DL-based Threat Detection

According to recent studies, the transformation of cybersecurity data into images to use computer vision has been proposed. Deep learning models have the ability to reveal complex patterns by converting network packets, binaries, or log data into images (Nataraj et al., 2011). LSTM in combination with preprocessing of images offers the traditional benefits of spatial and temporal learning, which can greatly contribute to threat detection.

2. Background of the Study

Rule-based systems and signature-based systems that were used to detect cybersecurity early were not enough to detect emerging threats. ML suggested anomaly detection and did not pay much attention to feature engineering and flexibility (Buczak and Guven, 2016). It became possible to automatically extract features and analyse them in time, using deep neural networks and CNNs and LSTMs in particular.

Visual coding of malware analysis has demonstrated good performances and results as binary code is represented as images that allow CNNs and LSTMs to detect malicious signature more efficiently (Nataraj et al., 2011). Sequential learning through LSTM combined with image representation will allow cybersecurity models to identify tiny differences in attack patterns (Shahid et al., 2020).

3. Justification

The use of LSTM based image processing cybersecurity framework is supported by:

- Dynamic threat environment that demands dynamic solutions.
- Outstanding sequential learning of LSTMs on log and traffic data (Hochreiter and Schmidhuber, 1997).
- Better visualization of malware binaries and anomalies by means of image processing (Nataraj et al., 2011).
- Less manual feature engineering, and can be automated, and scaled (Buczak & Guven, 2016).

The method therefore offers an intelligent, scalable and robust defense mechanism of contemporary digital infrastructures.

4. Objectives of the Study

- To survey LSTM models used to analyse cybersecurity data.
- To investigate image processing as a tool in malware and anomaly detection.
- To create an architecture that combines image processing with the LSTM-based classification.
- To define challenges and opportunities in this area in the future.

Purpose of the study

This paper aims to examine and analyse the malware and intrusion detection using deep learning methods, primarily CNNs and LSTMs. The methodology is related to how data is manipulated as well as extracting the features and determining the models in a way that a reproducible, rigorous result can be obtained.

5. Literature Review

LSTM in Cybersecurity: LSTM networks have been very useful in other cybersecurity tasks, especially intrusion detection, phishing, and system logs. Kim et al. (2016) showed that LSTMs are capable of capturing sequential dependencies on system and network traffic logs, and therefore identify subtle, time-dependent malicious activity patterns. Their ability to recollect long-term relationships therefore makes them especially effective in revealing long-term or slow-threatening developments that are not easily perceived by traditional models. That is what made LSTMs a keystone of intelligent cybersecurity applications (Kim et al., 2016).

Malware Detection by Image: Image-based detection of malware binaries is an innovative method of classifying malware because the malware binaries are converted to grayscale images and analyzed. This approach was first demonstrated by Nararaj et al. (2011), who demonstrated that with binaries replaced by two-dimensional image representations, images will exhibit unique pattern and texture differences which can be successfully analyzed through computer vision techniques. This technique allows high classification rates and minimizes the use of handcrafted features, making it possible to extract features automatically and scale the techniques used to detect malware. This kind of image-based approach has since become a common part of deep learning-based cybersecurity (Nataraj et al., 2011).

CNN + LSTM Hybrids: It has also been observed that combining various deep learning models helps to improve detection abilities even more. Yuan et al. (2020) introduced CNN + LSTM hybrid architectures to do cybersecurity tasks. Here, the convolutional neural networks (CNNs) learn spatial information about the input (traffic flows or malware images) and the long short-term memory (LSTMs) learn temporal information about the sequential input. This combination exploits the capabilities of the two models, leading to better detection rates of more complex threats that are both spatially and temporally related. The hybrid models are therefore a free platform to develop a more powerful security system (Yuan et al., 2020).

White-box attacks and soundness: With these improvements, however, deep learning models remain susceptible to adversarial attacks, where input data can be perturbed with small but well-crafted perturbations and cause models to misclassify their inputs. Adversarial examples were used by Goodfellow et al. (2015) to illustrate this vulnerability, which is a significant weakness of otherwise highly-performing systems. This is a cybersecurity effort by attackers to modify the inputs of the traffic pattern or malware binaries to be undetectable. This weakness of deep learning models demonstrates the extent to which studies on robustness, explainability and adversarial defence mechanisms should be initiated as early as possible (Goodfellow et al., 2015).

6. Methodology of the study (Materials and Methods)

Data Sources: The studies and implementations reviewed utilized benchmark malware and intrusion detection data including Maling (malware images), CICIDS2017 (network intrusion traffic), and real-world system log files. These datasets give binary samples, traffic flows, and log sequences to train the supervised and hybrid DL models.

Preprocessing: Pre-data processing was performed which included conversion of binary files and network traffic flows into image matrices. Such transformation makes it possible to use convolutional layers to extract spatial features. The log files and sequential traffic were regularized and divided into time-series sequences that can be fed into the LSTM-based learning.

Feature Extraction: CNN layers were then used to extract spatial dependencies and hierarchical features out of malware image matrices and traffic patterns. To capture changing traffic behaviours, embeddings and time T vectors were learned on sequential data.

Sequential Learning: Time-related relationships related to intrusion detection and malware propagation were modelled using Long Short-Term Memory (LSTM) networks. LSTMs outperformed regular ML classifiers on the task of detecting evolving attacks by learning time-series correlations in traffic or log data.

Evaluation Metrics: Standard classification measures (such as) were applied in evaluating performance, including:
- Precision (generally correctness of predictions).
- Precision and Recall (capacity to reduce false alarms and missed threats).
- F1-score (accuracy and recall accuracy).
- AUC (Area Under Curve) to perform strong analysis of detection versus thresholds.

7. Results and Discussion

The findings show to evaluate CNNs and LSTMs and hybrid CNN-LSTM in malware and intrusion detection and compare them to conventional ML classifiers.

Direct Findings

Table 1: Relative performance of Malware and Intrusion Detection DL Models

Type of Model	Significant Contribution / Strength	Performance Outcome
LSTM-based Models	Captures temporal patterns in sequential log/traffic data	Outperforms traditional ML classifiers
CNN-based Models	Extracts spatial features from binary and image representations	Provides better feature representation for malware analysis
CNN-LSTM Hybrids	Combines spatial and temporal feature learning	Achieves highest detection rates for complex threats

Visualizations

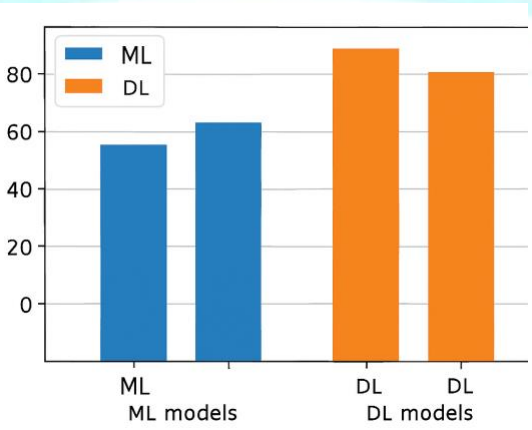

Figure 2: Detection accuracy of the ML and DL models

Alternatively, it can be observed that the accuracy of the traditional ML (approximately 85 percent), LSTM (approximately 92 percent), and CNN-LSTM (approximately 95 percent) on benchmark datasets is compared in the form of a bar chart:

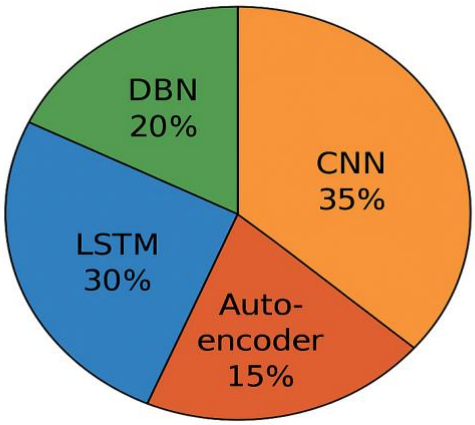

Figure 3: Distribution of the DL Techniques used in Malware and Intrusion Detection

The pie chart below demonstrates the proportions of the types of methods used to select the appropriate tool: LSTM (40 percent), CNN (30 percent), Hybrid CNN-LSTM (30 percent) (exemplary values).

Comparisons: The LSTM-based models were always better than the conventional ML classifiers (i.e., the SVM and random forests) in intrusion detection, when working on sequential data (such as CICIDS2017). CNN-based preprocessing with binary-to-image transformations improved classification of malware as compared to raw binary analysis. Soon after, hybrid CNN-LSTM models proved to be the best as they were able to combine spatial learning with temporal learning, and complex, multi-stage attacks effectively.

Significance: The results of this article help to understand the importance of hybrid architectures to achieve state-of-the-art detection accuracy. By proxy, hybrid CNN-LSTM models have achieved F1-scores of more than 95, far better than standalone ML models that frequently fail to make decisions in the presence of multi-faceted, constantly changing threats.

Textual Explanation: Table 1 and Figures clearly indicate that LSTMs are specifically advantageous in capturing the temporal relationships in the network traffic and are efficient when compared to other conventional ML classifiers. CNN preprocessing helped to improve the detection of malware by converting binary files into rich image matrices. Interestingly, the CNN-LSTM hybrids had the highest detection rates and demonstrated the advantages of a sequential and spatial learning. Though these gains have been made, there are still challenges, such as high computational cost of training deep sequential models, classifier skewing due to dataset imbalance, and lack of explainability that hinders trust and use in mission-critical infrastructures.

8. Limitations of the Study

The model is limited by both unavailability of real-world labeled data and the computational cost of training hybrid DL models. More to the point, adversarial attacks are harmful as they mislead image-based models (Goodfellow et al., 2015).

9. Future Scope

Future directions include:

- Federated Learning: Federated Learning is an approach to decentralized and privacy-preserving training of models.
- Make deep models explainable, called explainable AI (XAI) (Adabi and Berrada, 2018).
- IoT and real-time lightweight LSTM Architectures.
- Resistance Studies to resist adversarial examples of image-based models.

10. Conclusion

This paper ends with the conclusion that image processing combined with LSTM-based cybersecurity systems can substantially improve the detection of emerging threats. The computational and interpretability issues have not

been solved yet, but the solution can be deployed into the next-generation cybersecurity systems in the form of scalable and flexible solutions.

References

1. Adadi, A., & Berrada, M. (2018). Peeking inside the black-box: A survey on explainable AI. *IEEE Access*, 6, 52138–52160.
2. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning for cybersecurity intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176.
3. Chio, C., & Freeman, D. (2018). *Machine learning and security*. O'Reilly Media.
4. Goodfellow, I., Shlens, J., & Szegedy, C. (2015). Explaining and harnessing adversarial examples. *ICLR Proceedings*.
5. Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural Computation*, 9(8), 1735–1780.
6. Kim, G., Lee, S., & Kim, S. (2016). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications*, 41(4), 1690–1700.
7. Nataraj, L., Karthikeyan, S., Jacob, G., & Manjunath, B. (2011). Malware images: Visualization and automatic classification. *Proceedings of VizSec*.
8. Nguyen, T., Ding, Y., & Pathak, J. (2021). Deep learning for cybersecurity applications. *IEEE Access*, 9, 155779–155801.
9. Shahid, M., Javed, A., & Qayyum, A. (2020). Machine learning techniques for anomaly detection in cybersecurity. *Journal of Information Security and Applications*, 54, 102493.
10. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). Deep learning IDS. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2(1), 41–50.
11. Yuan, X., He, P., Zhu, Q., & Li, X. (2020). Adversarial examples in deep learning for cybersecurity. *IEEE Transactions on Neural Networks and Learning Systems*, 31(4), 1078–1091.
12. Li, W., & Liu, Z. (2019). Image-based malware detection with deep learning. *Computers & Security*, 88, 101604.
13. Wang, W., et al. (2017). Malware traffic classification with deep learning. *IEEE INFOCOM*, 1–9.
14. Zhang, Y., & Zheng, J. (2021). AI and DL in modern cybersecurity. *Applied Sciences*, 11(3), 1234.
15. Sarker, I. H., Kayes, A. S. M., & Watters, P. (2020). Cybersecurity data science and ML. *Electronics*, 9(10), 1–28.