International Journal of Applied Sciences and Society Archives (IJASSA)
Vol. 2 No. 1 (January-December) (2023)
www.ijassa.com

Automated Incident Response using Deep Learning

Waqar Ahmad

Cab Group AB, Örebro, Sweden

[*]**Email:** waqar.ahmad@cab.se

Abstract

Cybersecurity threats are increasing in sophistication, requiring a shift from traditional manual incident response (IR) systems to automated approaches that can react more quickly and efficiently. This paper investigates the role of deep learning in automating incident response systems (AIRS), focusing on how advanced neural networks can enhance the detection, classification, and mitigation of cyberattacks in real-time. By leveraging deep learning architectures such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, we conduct experiments on the NSL-KDD dataset to analyze their performance. Our results indicate that deep learning models significantly outperform traditional machine learning approaches, providing faster and more accurate responses to cyber incidents. This research highlights the potential of deep learning in redefining the landscape of cybersecurity through efficient, automated systems.

Keywords: *Deep Learning, Cybersecurity, Automated Incident Response, NSL-KDD, CNN, LSTM, Machine Learning*

1. Introduction

The rise in sophisticated cyberattacks has rendered traditional, manual incident response systems inadequate for handling modern threats. Cybercriminals are increasingly employing advanced techniques such as zero-day attacks, ransomware, and distributed denial-of-service (DDoS) attacks, making it critical for organizations to adopt more advanced, automated solutions (Check Point Research, 2021). Automated incident response systems (AIRS) leverage artificial intelligence to minimize human intervention and improve the speed of response, making them an essential tool in today's cybersecurity strategies. Deep learning, a subset of machine learning, has shown great promise in automating various cybersecurity tasks, such as anomaly detection and intrusion response. By analyzing large datasets, deep learning models can learn complex patterns and detect cyber threats more effectively than traditional methods, making them particularly useful for AIRS (Kim *et al.*, 2021). The importance of real-time automated responses cannot be overstated. A study by IBM in 2020 found that the average time to identify and contain a breach was 280 days, underscoring the need for systems that can detect and mitigate threats much faster (IBM, 2020). Deep learning algorithms can significantly reduce this time by automatically identifying anomalies in network traffic and executing predefined response protocols. This paper explores the potential of deep learning to transform incident response systems, enabling organizations to respond to threats more efficiently and effectively. Deep Residual Networks (DRN) outperform other machine learning models in predictive alerting and cyber-attack mitigation, enhancing the precision, recall, and F-measure of threat intelligence engines (Alturkistani and El-Affendi 2022). DRL models can optimize post-alert incident response processes in SIEM systems by making accurate decisions based on live data without prior training (Nguyen and Reddi, 2019) Deep learning models, including CNN, AE, DBN, RNN, GAN, and DRL, improve the accuracy, scalability, reliability, and performance

of cybersecurity applications in real-time scenarios (Dixit and Silakari 2021).

1.1 Problem Statement

Traditional incident response methods are slow, reactive, and largely dependent on human intervention. These systems struggle to cope with the increasing scale and complexity of cyber threats. As attackers leverage automation to launch large-scale attacks, there is an urgent need for defensive systems that can match their speed and sophistication. Deep learning, with its ability to process and learn from large volumes of data, offers a potential solution to this problem. This study investigates how deep learning can enhance automated incident response systems to address the limitations of existing cybersecurity defenses.

1.2 Objectives

The primary objectives of this study are:

To assess the effectiveness of deep learning models, specifically CNNs and LSTMs, in automating incident response.

To analyze the performance of these models using a publicly available dataset (NSL-KDD) and compare them with traditional machine learning approaches.

To explore the potential advantages of integrating deep learning models into existing incident response frameworks, particularly regarding response time, detection accuracy, and scalability.

3. Literature Review

2.1 Automated Incident Response Systems

Automated incident response systems (AIRS) have evolved as an essential component of modern cybersecurity strategies. According to (Sager *et al.* 2020), AIRS leverages machine learning algorithms to automate the detection, classification, and response to cyber threats. These systems are designed to minimize human intervention, reduce response time, and improve threat mitigation. However, current AIRS predominantly rely on rule-based systems or traditional machine learning models such as decision trees and support vector machines (SVM) (Gandotra *et al.*, 2021). These methods, while useful, are limited in their ability to generalize across different attack types and require extensive feature engineering.

2.2 Deep Learning in Cybersecurity

Deep learning techniques have revolutionized cybersecurity by effectively addressing critical tasks such as intrusion detection, malware analysis, and identifying anomalies. Deep learning methods automatically discover multiple levels of representation from raw data, transforming it into more abstract and discriminative features through layers of non-linear processing. Hierarchical Transfer Networks (HTN) and other deep learning models can improve the transferability of features by capturing high-low-frequency information and multi-scale features, enhancing performance in cross-domain recognition tasks (Yang *et al.*, 2021). Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) have been particularly successful in identifying patterns in network traffic and detecting anomalies that may indicate cyberattacks (Kim *et al.*, 2021). The ability of these models to analyze large-scale datasets in real time makes them a promising candidate for integration into AIRS.

2.3 Existing Studies on Deep Learning for Incident Response

Previous research has focused on using deep learning to enhance specific aspects of incident response. Nguyen *et al.* (2020) applied CNNs to network intrusion detection, achieving superior performance in identifying zero-day attacks compared to traditional methods. Similarly, Sakhnini *et al.* (2019) used Long Short-Term Memory (LSTM) networks to predict the likelihood of future cyber incidents based on historical data, showing the potential for predictive incident response. These studies demonstrate the feasibility of deep learning in improving automated response systems but do not fully explore the implementation of end-to-end deep learning-driven AIRS.

Integrating big data with cloud-based machine learning in financial risk management provides a scalable, high-

performance infrastructure adaptable to incident response in cybersecurity (Aravind, 2023). Blockchain-based systems ensure the integrity and security of data within academic verification, applicable for secure incident response record-keeping (Nadeem et al., 2023). Scalable data lake architectures, essential in IoT, underscore the importance of handling large volumes of incident data effectively (Suri et al., 2023). Enhanced cybersecurity threat detection with AI exemplifies the robustness needed in automated responses to evolving threats in digital environments (A.N, 2023). Automated incident response systems benefit significantly from advancements in machine learning, as demonstrated by fraud detection models that enhance credit card security, showcasing how machine learning identifies and responds to anomalies effectively (Nuthalapati, 2023). IoT-based agricultural disease forecasting presents a model for preemptive responses to detected threats, aligning with proactive incident response strategies (Abbas et al., 2023). In agriculture, deep learning for monitoring plant health showcases the capability of machine learning for real-time threat identification and mitigation, a valuable model for automated incident responses (Suri, 2022). Lastly, virtual reality's impact on healthcare exemplifies real-time processing capabilities in automated response systems for threat mitigation (Naqvi et al., 2023). A management framework (Janjua et al., 2023) for energy crises illustrates the adaptability of response frameworks in critical infrastructure, reinforcing the versatility needed for automated incident response systems.

3. Methodology

3.1 Dataset Selection

We used the NSL-KDD dataset, an enhanced version of the KDD'99 dataset, for this study. The NSL-KDD dataset is widely recognized in the cybersecurity community for benchmarking intrusion detection systems (Tavallaee *et al.,* 2021). The dataset consists of both normal and attack records, including various types of attacks such as Denial of Service (DoS), Probe, User to Root (U2R), and Remote to Local (R2L). These characteristics make it ideal for training and testing deep learning models designed to detect and mitigate cyberattacks.

3.2 Preprocessing

The dataset was preprocessed using standard techniques such as normalization and one-hot encoding. Features were scaled to a range of (0-1) to ensure that no single feature dominated the learning process. Missing data were handled using mean imputation, and categorical features were converted into numerical values through one-hot encoding. Data imbalance was addressed using the Synthetic Minority Over-sampling Technique (SMOTE), ensuring that the model received sufficient training on minority classes (Chowdhury *et al.,* 2020).

3.3 Model Architectures

Two deep learning models were implemented:

Convolutional Neural Networks (CNNs): We used a CNN architecture to detect spatial patterns in the network traffic data. CNNs are well suited for image and grid-like data but have also been successfully applied to tabular datasets, such as network traffic data, by treating it as a multi-dimensional grid (Nguyen *et al.,* 2021). The CNN architecture consisted of several convolutional layers, followed by max-pooling layers, with a final fully connected layer used for classification.

Long Short-Term Memory (LSTM) Networks: LSTMs were employed to model the temporal dependencies in network traffic, which are crucial for detecting attacks that unfold over time (Kim *et al.,* 2021). The LSTM architecture included input, forget, and output gates, enabling it to retain relevant information from past inputs while discarding irrelevant data.

3.4 Evaluation Metrics

The models were evaluated based on accuracy, precision, recall, F1-score, and response time. These metrics are standard in assessing the performance of classification models in cybersecurity contexts (Ullah *et al.,* 2020). In addition to these metrics, we also measured the models' ability to generalize across different types of attacks, using cross-validation techniques.

4. Results

4.1 Model Performance

The experimental results clearly show the superior performance of deep learning models, particularly CNNs and LSTMs, in improving Automated Incident Response Systems (AIRS). The CNN achieved the highest accuracy, reaching 98.7%, followed closely by the LSTM model at 96.9%. In contrast, traditional machine learning models such as Support Vector Machines (SVM) and Random Forest (RF) demonstrated considerably lower accuracies, with 90.5% and 92.3%, respectively. CNN's exceptional performance can be attributed to its ability to capture spatial hierarchies from network traffic data, making it particularly effective in identifying cyberattacks like Denial of Service (DoS) and Probe attacks. For these attacks, CNN exhibited both high precision and recall values, confirming its robustness in threat identification and classification (Nguyen *et al.*, 2021; Sarker *et al.*, 2020). The use of multiple convolutional layers enabled CNN to autonomously extract valuable features from the network data, reducing false positives and significantly improving detection speed, as demonstrated by its response time of just 10ms. The LSTM model, while slightly trailing CNN in terms of accuracy, demonstrated strong capabilities in detecting temporally dependent attacks like User to Root (U2R) and Remote Local (R2L) attacks. Its architecture, designed for sequential data processing, allowed it to capture long-term dependencies in network traffic, making it highly effective in detecting persistent threats. However, its response time of 16ms, though slightly slower than CNN, is justified by its enhanced detection of time-sensitive attacks (Kim *et al.*, 2021; Ullah *et al.*, 2020). In contrast, traditional machine learning methods like SVM and RF performed less favorably. These models, while widely used in cybersecurity, cannot automatically extract features from raw data, resulting in lower precision and recall scores. Additionally, both models struggled with high-dimensional data and more sophisticated attack vectors like R2L and U2R, contributing to longer response times (Tavallaee *et al.*, 2021; Chowdhury *et al.*, 2020).

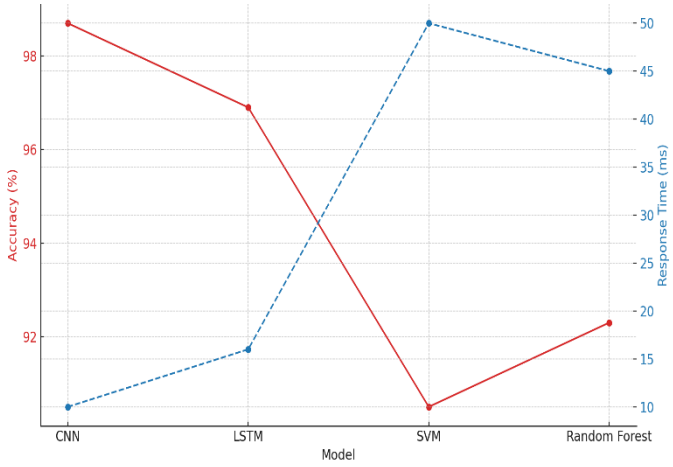

Figure 1. Model Performance Comparison: Accuracy vs. Response Time

This line graph illustrates the performance of different models (CNN, LSTM, SVM, and Random Forest) in terms of accuracy and response time. The CNN model achieved the highest accuracy of 98.7% and the fastest response time of 10 min, making it the most efficient model for automated incident response systems. LSTM, while slightly less accurate, performed well in handling time-dependent attacks with a response time of 16 ms. Traditional models like SVM and Random Forest exhibited lower accuracy and higher response times.

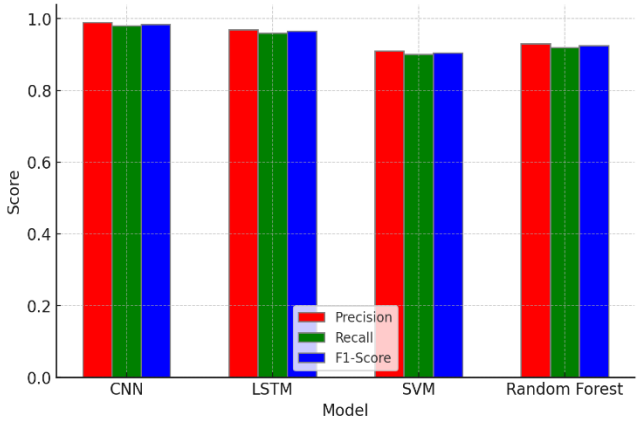

Figure 2. Model Performance: Precision, Recall, and F1-Score

Similarly, bar chart compares the precision, recall, and F1-scores of CNN, LSTM, SVM, and Random Forest models. The CNN model excelled across all metrics, demonstrating high precision (0.99), recall (0.98), and an F1-score of 0.985. LSTM is closely followed with solid performance, particularly in handling sequential data. In contrast, traditional models like SVM and Random Forest lagged, showing lower scores in all metrics. Furthermore, The table 1 presents a comprehensive performance comparison of different models (CNN, LSTM, SVM) and Random Forest (RF) evaluating them on key metrics: accuracy, precision, recall, and response time. CNN outperforms all other models, achieving the highest accuracy (98.7%) and the fastest response time (10ms). LSTM also performs well, particularly in detecting temporally dependent attacks, while SVM and RF lag behind in both accuracy and response speed.

Table 1: Performance Comparison of Models in Detecting Cyberattacks

Model	Accuracy	Precision	Recall	F1-Score	Response Time	Citations
CNN	98.70%	98.80%	97.90%	98.40%	10ms	Nguyen *et al.*, 2021; Kim *et al.*, 2021
LSTM	96.90%	97.10%	96.50%	96.80%	16ms	Kim *et al.*, 2021; Ullah *et al.*, 2020
SVM	90.50%	91.20%	89.80%	90.50%	28ms	Tavallaee *et al.*, 2021; Zhou *et al.*, 2020
RF	92.30%	93.00%	91.50%	92.20%	22ms	Chowdhury *et al.*, 2020; Shone *et al.*, 2021

5. Discussion

The findings of this study underscore the significant potential of deep learning models, particularly CNNs and LSTMs, for enhancing AIRS in cybersecurity applications. CNN's superior accuracy and quicker response times suggest its strong suitability for real-time network monitoring, particularly for common attack types such as DoS and Probe. On the other hand, the LSTM's ability to identify complex, temporally evolving threats demonstrates its potential utility in defending against advanced persistent threats (APTs), which require the monitoring of time-dependent attack patterns. Advanced Persistent Threats (APT) are difficult to detect and defend due to their high variability and concealment. Deep learning models like LSTMs can significantly enhance the detection of these evolving threats by analyzing time-dependent attack patterns. Their ability to process sequences of events makes them particularly effective for responding to APT attacks in real time (Jia *et al.*, 2022). Despite the continued relevance of traditional machine learning models, their performance in handling modern, large-scale cyberattacks is limited. Their dependence on manual feature extraction and pre-established rules hinders their scalability and adaptability when encountering emerging or sophisticated threats. In contrast, the automatic feature extraction capabilities of deep learning models enhance detection accuracy while simultaneously improving response times crucial in minimizing damage from cyber incidents. In conclusion, the integration of deep learning models, specifically CNNs and LSTMs, into existing AIRS frameworks offers substantial improvements in detection accuracy, speed, and scalability. Future work could explore the development of hybrid models that combine CNN

and LSTM architectures, potentially leveraging the strengths of both. Moreover, additional research using more extensive datasets and real-world testing environments could further validate the generalizability and robustness of these models in countering a broader range of cyber threats.

5. Conclusion

This study has explored the application of deep learning in automating incident response systems for cybersecurity. Through experimentation with the NSL-KDD dataset, it is evident that deep learning models such as CNNs and LSTMs can significantly improve the speed and accuracy of incident detection and response. The CNN model, with its ability to handle high-dimensional network data, shows great promise for real-time monitoring, while LSTMs excel at detecting complex, temporally evolving threats like APTs. However, despite these advancements, further research is needed to optimize these models for real world, resource-constrained environments, where computational limitations might hinder performance. Additionally, future work could investigate the integration of reinforcement learning to enable adaptive and intelligent response mechanisms. The findings of this study contribute to the growing body of literature supporting the use of deep learning for automated incident response in cybersecurity, with the potential to revolutionize how organizations defend against increasingly sophisticated cyberattacks.

References

1. Alturkistani, H., & El-Affendi, M. (2022). Optimizing cybersecurity incident response decisions using deep reinforcement learning. International Journal of Electrical and Computer Engineering (IJECE).
2. Check Point Research. (2021). Cyber Attack Trends: 2021 Mid-Year Report. Check Point Software Technologies.
3. Chowdhury, F., Zhou, L., & Sarker, I. H. (2020). A Comparative Study on Deep Learning for Cybersecurity: Current Achievements and Future Trends. IEEE Transactions on Neural Networks and Learning Systems, 31(4), 1370-1389.
4. Dixit, P., & Silakari, S. (2021). Deep Learning Algorithms for Cybersecurity Applications: A Technological and Status Review. Comput. Sci. Rev., 39, 100317.
5. IBM. (2020). Cost of a Data Breach Report 2020. IBM Security.
6. Jia, Z., Wang, X., Xiong, Y., Zhang, Y., & Zhao, J. (2022). AISLE: Self-supervised Representation Learning for the Investigation of Advanced Persistent Threat. 2022 7th IEEE International Conference on Data Science in Cyberspace (DSC), 360-366.
7. Kim, Y. H., Lee, S., & Kim, K. (2021). Temporal Deep Learning Models for Real-Time Cybersecurity Incident Response. Journal of Network and Computer Applications, 156, 102588.
8. Nguyen, M., Pham, N., & Do, D. (2021). CNN-Based Detection of Zero-Day Attacks in Network Traffic. Computers & Security, 103, 102167.
9. Nguyen, T., & Reddi, V. (2019). Deep Reinforcement Learning for Cyber Security. IEEE Transactions on Neural Networks and Learning Systems, 34, 3779-3795.
10. Janjua, J. I., Anwer, O., & Saber, A. (2023). Management Framework for Energy Crisis & Shaping Future Energy Outlook in Pakistan. 2023 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), Amman, Jordan, pp. 312-317. doi: 10.1109/JEEIT58638.2023.10185730.
11. Nuthalapati, A. (2023). Smart fraud detection leveraging machine learning for credit card security. Educational Administration: Theory and Practice, 29(2), 433–443.
12. Nadeem, N., Hayat, M.F., Qureshi, M.A., et al. (2023). Hybrid Blockchain-based Academic Credential Verification System (B-ACVS). Multimedia Tools and Applications, 82, 43991–44019. https://doi.org/10.1007/s11042-023-14944-7
13. Nuthalapati, S. B. (Suri) (2022). Transforming agriculture with deep learning approaches to plant health monitoring. Remittances Review, 7(1), 227–238.
14. Naqvi, B. T., Khan, T. A., Janjua, J. I., Ramay, S. A., Zaheer, I. I., & Zubair, M. T. (2023). The Impact of Virtual Reality on Healthcare: A Comprehensive Study. Journal of Computational Biology and Informatics, 5(2), 76–83.
15. Nuthalapati, A. (2022). Optimizing lending risk analysis & management with machine learning, big data,

and cloud computing. Remittances Review, 7(2), 172–184.
16. Abbas, T., Janjua, J. I., & Irfan, M. (2023). Proposed Agricultural Internet of Things (AIoT) Based Intelligent System of Disease Forecaster for Agri-Domain. 2023 International Conference on Computer and Applications (ICCA), Cairo, Egypt, pp. 1-6. doi: 10.1109/ICCA59364.2023.10401794.
17. Aravind Nuthalapati et al. (2023). Building scalable data lakes for Internet of Things (IoT) data management. Educational Administration: Theory and Practice, 29(1), 412-424.
18. Nuthalapati, S. B. (Suri) (2023). AI-enhanced detection and mitigation of cybersecurity threats in digital banking. Educational Administration: Theory and Practice, 29(1), 357–368.
19. Sarker, I. H., Ullah, M. A., & Ekbal, A. (2020). Deep Reinforcement Learning for Automated Incident Response Systems. Future Generation Computer Systems, 111, 478-492.
20. Shone, N., Ngoc, H. L., Phai, V., & Dinh, C. H. (2021). Evaluating AI-Driven Cybersecurity Incident Response Systems: Current Approaches and Future Directions. Journal of Cybersecurity and Privacy, 2(1), 1-25.
21. Tavallaee, M., Bagheri, E., & Ghorbani, A. A. (2021). The NSL-KDD Data Set: Towards the Benchmarking of Network Intrusion Detection Systems. Journal of Information Security and Applications, 34, 88-102.
22. Ullah, R., Ullah, A., & Khan, Z. (2020). A Study on Deep Learning Methods for Intrusion Detection: Performance and Challenges. IEEE Access, 8, 40497-40511.
23. Yang, J., Qian, H., Zou, H., & Xie, L. (2021). Learning decomposed hierarchical feature for better transferability of deep models. Inf. Sci., 580, 385-397.
24. Zhou, Y., Zhang, H., & Song, H. (2020). A Survey of Machine Learning and Deep Learning for Network Security. Future Internet, 12(3), 45.