AI Based Real Time Network Anomaly Detection

Geethanjali S G[1] Aditya Mohan Jha[2] ,Hemakanth Raju[3], Hitesh V[4],
Department of CSE, Don Bosco Institute of Technology, Bengaluru, Karnataka, India

Abstract Zero-Day Threats (ZDTs) are perhaps the most severe cybersecurity problems, defined by their potential to take advantage vulnerabilities that are unknown to the security community. The exponential growth of virtual holdings and increasing complexity of network infrastructure pose significant challenges to contemporary intrusion detection systems. Traditional signature-based intrusion detection systems fall short in identifying unknown or emerging threats due to their static character. In this research, we propose a robust, AI- based, real-time deploy an anomaly detection system based on deep learning technology to overcome such constraints. The architecture employs a hybrid CNNLSTM framework that utilizes a dual- autoencoder approach, that enhances its ability to detect new and existing threats. Furthermore, graph-based telemetry features provide context-aware information about the network topology, raising detection rates and reducing false alarms. Experimental tests show the system's strong performance on various measures, where its relevance in contemporary largescale, heterogeneous networks.

Keywords: Zero-Day Threats (ZDT), Anomaly Detection, Network Security, Deep Learning, Autoencoders, Cybersecurity, Novelty Detection, Network Flow Telemetry, Graph Features, Real-Time Threat Detection, Adversarial Dataset, Cyber Attack Detection, Intrusion Detection System (IDS)

1. Introduction

Cyber threats have outpaced the advancement of traditional defenses. Network infrastructure is more susceptible and exposed to potential outcomes than ever due to rapid automation, digitization, and advances in IoT and 5G technologies. In this quickly developing and diverse threat landscape, there is a need for more sophisticated detection methods that can operate in constantly changing attack strategies and resource-heavy information flows. Traditional IDS modalities, which may rely on static signatures or rule-based engines, are limited in recognizing unknown threat patterns and adapting to the contextual changes in unknown environments. Given this backdrop, Artificial Intelligence (AI) and Deep Learning (DL) models have emerged as new best practices. These models are able to learn from historical data and draw conclusions about unseen patterns based on baselines constructed from the data. In this research, we describe the development and evaluation of a situationally aware, hybrid deep learning-based intrusion detection system with real-time anomaly detection capabilities. Importantly, the proposed model captures flow-level telemetry and packet data, and graph-based features, helping to capture network behavior from a structural perspective. By leveraging this multidimensional approach the classification model can be generalized to both traditional and Zero-Day attacks.

2. Literature Survey

The limitations of static security tools in mobile circumstances has driven a plethora of research on intelligent threat detection solutions. Multiple studies over the last decade have considered the suitability of machine learning in anomaly detection. Wahed et al. (2024) employed both LSTM and CNN models for real-time intrusion detection in IoT, leveraging deep learning techniques that are empirically proven superior to traditional tools in massively high-velocity environments. Redino et al. (2022) designed a novel dual-autoencoder architecture that took advantage of both flow data and graph features and improved generalizability towards unseen threats. Theres many other notable works such as Bhalerao et al. (2024) who focused on federated learning for developing a risk management framework for 5G networks using deep learning and modeling via an aligned-vocabulary approach with privacy-preserving capabilities, and Ahmad and Petrovski (2024) who utilize a CNN-LSTM hybrid model in the first stage in a two-tier detection mechanism monitoring Cyber-Physical Systems (CPS) then deploying a second stage boosting classifiers in a hybrid framework of any anomaly in the first-phase classification, demonstrating and continuing to explore the high-performance of their approach. Some other worthy papers are (Kukliansky et al. 2024) reviewing quantum neural

networks for anomaly detection in noisy data environments and (Lunardi et al., 2023), who present adversarial regularization for autoencoders to strengthen model robustness against evasion attacks.

3. Compatative Analysis

In our experimental design, we sought to test the proposed system on several datasets: CICIDS2017, NSL-KDD, and custom-simulated adversarial traffic. We made a full comparison against traditional machine learning classifiers, such as Logistic Regression, Decision Trees, Support Vector Machines (SVM), Random Forest, and Gradient Boosting Machines (GBM), as well as standalone CNN and LSTM models. The hybrid CNN-LSTM model performed best across all key metrics. CNN works with spatial features in the payloads of network packets and LSTM works with temporal information between data inputs, which are important characteristics when detecting time-based anomalies, such as DoS, or slow-rate attacks.

.

Model	Accuracy	Precision	Recall	F1-Score	G-Mean
Logistic Regression	84.1%	0.82	0.76	0.79	0.75
Decision Tree	86.7%	0.84	0.80	0.82	0.78
Random Forest	89.2%	0.88	0.84	0.86	0.83
CNN	91.0%	0.89	0.87	0.88	0.86
LSTM	90.3%	0.88	0.86	0.87	0.85
CNN + LSTM (Proposed)	94.3%	0.93	0.90	0.91	0.89

By adding graph characteristics such as betweenness centrality and clustering coefficients enhanced detection of lateral movement and internal threats that would otherwise be difficult to detect through flow alone.

4. Results and Discussion

The findings support the prospects of a hybrid AI approach in fast- moving network environments. The system's detection response was rapid, even with highly imbalanced datasets. This is a common case in cybersecurity applications. Temporal learning also allowed for further investigation of early stage detection of highly sophisticated attacks including APTs (Advanced Persistent Threats) or stealthy malware campaigns. In summary, the evidence reinforces that the integration of CNN, LSTM and graph-based modeling captures a complete picture in identifying behavioral and structural anomalies of networks. However, resource limitations in edge contexts (including environments with fixed bandwidths) and potential performance degradation in scenarios with encrypted traffic cases presented several additional challenges. Future models can also leverage federated training and continual learning paradigms so that model accuracy can be retained across multiple diverse organizations while avoiding the need for centralized access to their training data.

5. Conclusion

This report introduces a fully real-time, AI-based anomaly detection approach to help counteract the increasing complexity of adversarial attacks on networks. It offers spatial, temporal, and structural indications to provide AI the highest level of data comprehension through CNN for spatial, LSTM for temporal, and graph for structural, thus maximizing the potential for improved accuracy and speed based detection. The hybrid deep-learning architecture using dual- autoencoders for anomaly detection provides a detection 'competency' of zero day threats with marginal human intervention. The findings highlighted the promising potential of prediction-oriented AI capabilities to move defenses for cybersecurity and critical infrastructure operations from a traditional state (security and defense) to proactive, active, and scalable. Future work will focus on considering resource-efficiency when deploying to edge networks, creating more resilience against adversarial examples, and providing support for encrypted traffic analysis via federated learning and self-supervised methods.

References

[1] Wahed, M. A., & Balfaqih, M. (2024). Real-Time Intrusion Detection and Traffic Analysis Using AI Techniques in IoT Infrastructure. In Proceedings of IEEE ICETI 2024.

[2] Redino, C., Jung, J., Meunier, P., Neves, F., Zegers, F. (2022). Zero Day Threat Detection Using Graph and Flow Based Security Telemetry. In IEEE ICCCIS 2022.

[3] Bhalerao, S., Prabhu, S., & Ashok, P. (2024). AI Enabled Risk Management Framework in 5G Networks. In IEEE INNOVA 2024.

[4] Ahmad, Z., & Petrovski, A. (2024). Securing Cyber-Physical Systems with Two-level Anomaly Detection. In IEEE ICPS 2024.

[5] Kukliansky, A., Laskin, M., Romashevskiy, A., & Lando, A. (2024). Quantum Neural Networks on Noisy Quantum Computers: Applications for Anomaly Detection. IEEE Transactions on Quantum Engineering.

[6] Lunardi, W., Perera, B., & Di Pietro, R. (2023). Towards AdversariallyRegularized Autoencoders for Network Intrusion Detection. In Proceedings of the 18th ACM Asia Conference on Computer and Communications Security.

[7] Moustafa, N., Creech, G., Slay, J. (2017). Big Data Analytics for Intrusion Detection: A Survey. Journal of Big Data, 4(1), 1–30.

[8] Kim, G., Lee, S., & Kim, S. (2014). A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection with Misuse Detection. Expert Systems with Applications, 41(4), 1690–1700.

[9] Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT Security Techniques Based on Machine Learning: How Do IoT

Devices Use AI to
5
Enhance Security? IEEE Communications Surveys & Tutorials, 22(3), 1646–1685.

[10] Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. IEEE Access, 5, 21954–21961.

[11] Diro, A. A., & Chilamkurti, N. (2018). Distributed Attack Detection Scheme Using Deep Learning Approach for Internet of Things. Future Generation Computer Systems, 82, 761–768.

[12] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A Deep Learning Approach to Network Intrusion Detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41–50.

[13] Doshi, R., Apthorpe, N., & Feamster, N. (2018). Machine Learning DDoS Detection for Consumer Internet of Things Devices. In Proceedings of the IEEE Security and Privacy Workshops (SPW), 29–35.

[14] S. Kastryulin, D. Zakirov, and D. Prokopenko, “PyTorch image qual ity: Metrics and measure for image quality assessment.” 2019. [Online]. Available: https://github.com/photosynthesis-team/piq.

[15] D. P. Kingma and J. Ba, “Adam: A method for stochastic optimization,” 2014, arXiv:1412.6980.

Copyright & License:
© Authors retain the copyright of this article. This work is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.