ANOMALY NETWORK DETECTION MODEL

Nakabuuka Regina Desire Namutebi Esther

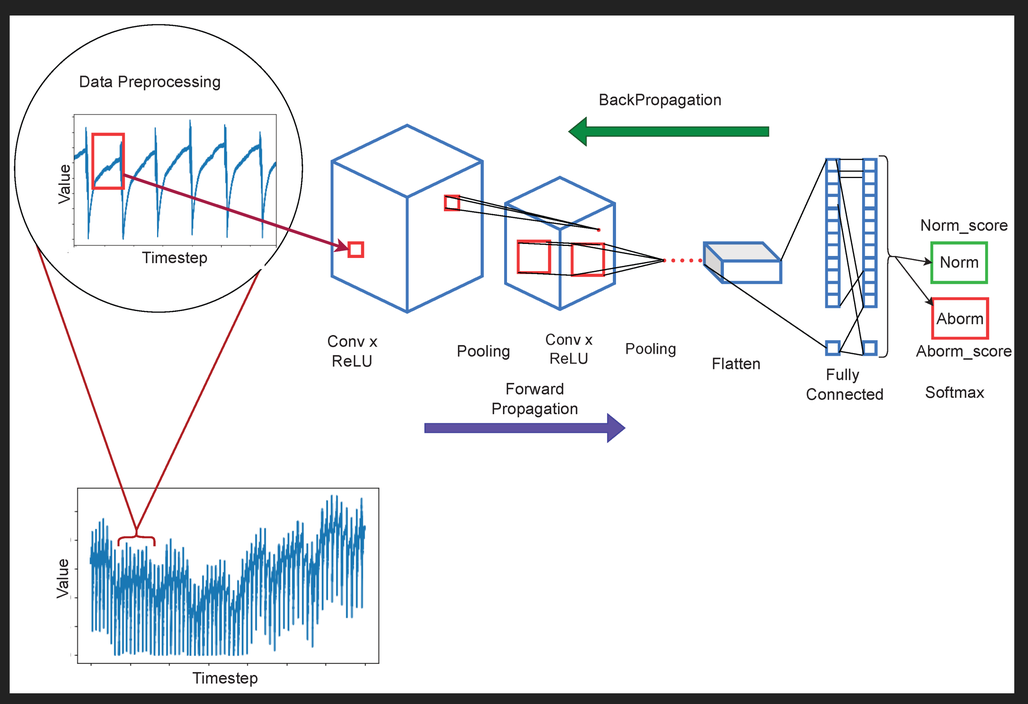
INTRODUCTION

Anomaly network detection is a crucial element in modern cybersecurity, protecting digital ecosystems from emerging threats. Traditional methods often fall short in addressing the dynamic tactics of malicious actors. To meet this challenge, we leverage deep learning techniques to enhance anomaly detection. Our model integrates neural networks and advanced algorithms to uncover subtle patterns indicative of anomalies in network traffic.

OBJECTIVES

- To Enhance Detection Accuracy
- To Capture Complex Patterns
- To Enable Real-time Response
- To Reduce False Positives

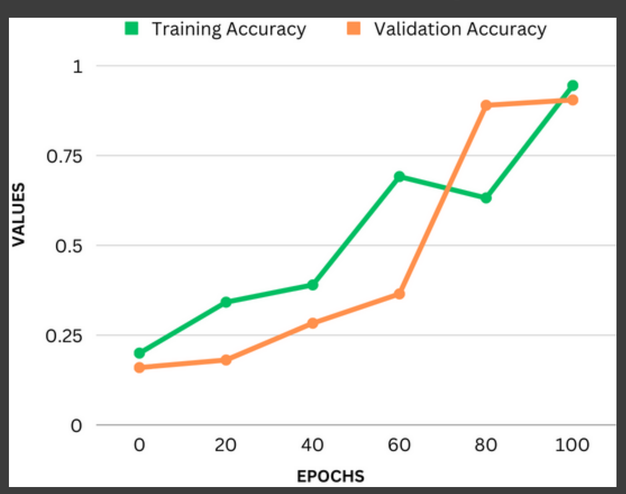
METHODOLOGY



The model utilizes a hybrid architecture combining CNNs for spatial feature extraction and RNNs for capturing temporal dependencies with a final softmax layer to do the classification. It was trained on a diverse dataset, iteratively optimizing its parameters to minimize loss through adaptive learning. Dropout and batch normalization were employed to prevent overfitting.

RESULTS

Model Accuracy

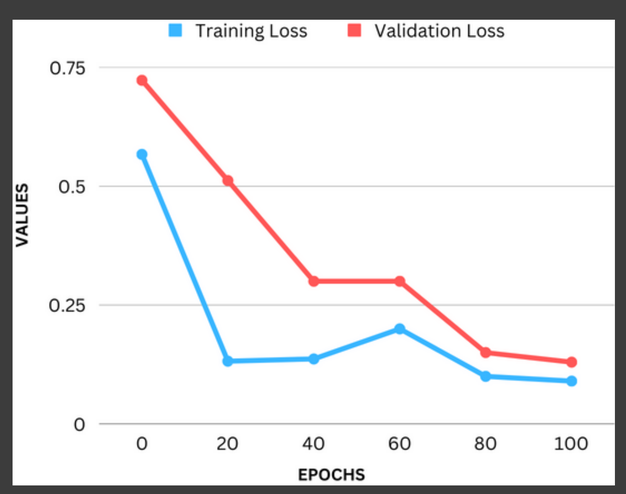


The performance of our anomaly network detection deep learning model was evaluated through rigorous experimentation and validation. The metrics of accuracy and loss provide crucial insights into the model's effectiveness in distinguishing between normal and anomalous network behavior.

Accuracy:
During evaluation, our model achieved an accuracy of 92% showcasing its proficiency in network behavior recognition.

Loss:
Our model consistently minimized its loss function, resulting in 0.13. This reflects the model's successful learning and adaptation to the underlying patterns within the network data.

Model Loss



CONCLUSION

This study has showcased the potential of deep learning in enhancing anomaly network detection. Leveraging convolutional and recurrent neural networks, our model demonstrates effective differentiation between normal and anomalous behavior. By contributing to the advancement of network security, this work underscores the transformative impact of deep learning in addressing evolving cybersecurity challenges.

DATASET

The comprehensive dataset used to train the model encompasses actual network communication data gathered from two distinct sources:

Kabale University's Network: A significant portion of the dataset originates from Kabale University's network. This real-world data offers insights into the network behavior specific to the university's environment.

Internet Data Collection: Supplementary data was obtained from various sources across the internet. This collection process contributes a broader spectrum of network behaviors, enriching the dataset's representative nature.

REFERENCES

[1] Zhang, X., Zhu, Y., & Zhang, L. (2018). Anomaly detection in network traffic based on convolutional neural networks. In 2018 14th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD) (pp. 1357-1361). IEEE.

[2] Akoglu, L., & Tong, H. (2018). Graph based anomaly detection and description: A survey. Data Mining and Knowledge Discovery, 32(3), 601-660.

[3] Xu, Z., Li, W., & Ouyang, Y. (2020). Anomaly intrusion detection method based on deep belief network. In 2020 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA) (pp. 320-324). IEEE.

[4] Mahmood, A. N., Hu, J., & Hu, J. (2019). Deep learning for network intrusion detection: A survey. IEEE Access, 7, 121923-121939.

+256741623148 nakabuukareginadesire@gmail.com