Web Traffic Anomaly Detection using C-LSTM Neural Networks

Sai Anand K
Sidharth Thejas
S R Angelo Antony
Shiva Surendran

Project Guide: Fameela K A

Objectives

1. To address the challenge of detecting anomalies in web traffic data, which can be indicative of network attacks or system failures.
2. To develop a machine learning model that effectively captures both spatial and temporal features in web traffic for accurate anomaly detection.
3. To utilize a Convolutional Long Short-Term Memory (C-LSTM) neural network that combines CNN and LSTM layers for this purpose.
4. To implement the project as a full-stack solution, including a user-friendly dashboard for monitoring and analyzing web traffic data in real-time.

Abstract

The Internet serves as a critical infrastructure in our daily lives, facilitating a vast array of services through web traffic. However, with the growing complexity of the internet, web traffic anomalies, which represent abnormal changes in traffic patterns, have become increasingly prevalent. These anomalies are often indicators of malicious activities, such as Denial of Service (DoS) attacks, which can lead to significant economic and social disruptions. In response to these challenges, this project proposes a novel approach to web traffic anomaly detection using a C-LSTM neural network. The C-LSTM architecture leverages the strengths of Convolutional Neural Networks (CNNs) to extract spatial features from traffic data, while Long Short-Term Memory (LSTM) networks capture the temporal dependencies within these features. The combination of these two models allows for robust detection of anomalies in web traffic, even in the presence of severe data imbalances. This project will be developed as a full-stack solution, featuring a dashboard for monitoring and analysis of web traffic data, providing an interactive and accessible interface for users.

Conclusion

The implementation of a C-LSTM neural network for web traffic anomaly detection represents a significant step forward in safeguarding online services from potential threats. By integrating CNN and LSTM layers, the model is capable of accurately identifying both spatial and temporal anomalies in traffic data. This work not only demonstrates the efficacy of the proposed approach but also highlights the importance of machine learning in enhancing the security and reliability of web services. Additionally, the full-stack approach, complete with a real-time dashboard, ensures that the system is both user-friendly and practical for real-world applications.