Uncovering Network Anomalies with Machine Learning

Nagavinay Kongara

Problem statement

Networks generate large amounts of data, and it can be challenging for human operators to manually identify anomalies or unusual patterns in the data.

Solution statement

To develop an unsupervised learning-based model that can learn the normal patterns of network behavior and identify any deviations from these patterns as anomalies. The model should be able to analyze a wide range of network data, including packet headers, flow records, and network logs, and should be scalable to handle large volumes of data in real-time.

Stages of this project

Pre-processing

Statistics

Attack Filtering

Machine Learning Implementation

Python jupyter notebook

Libraries

Pandas	:	Data Analysis Tools
Sklearn	:	Machine Learning Library
Numpy	:	Mathematical Operations
Matplotlib	:	Graphics and Visuality

Conclusion

- In conclusion, Anomaly Detection in Networks Using Machine Learning is a powerful tool for identifying and mitigating security threats in computer networks. Through the use of advanced algorithms and models, machine learning can identify patterns of behavior that deviate from the norm and flag potential anomalies for further investigation.Overall, the integration of machine learning into network security represents an exciting and rapidly evolving field with immense potential for improving the safety and security of our digital systems