# **Real-time Anomaly Detection using Neural Networks and Big Data in the context of Cybersecurity**

1. Introduction

Data analytics has evolved dramatically in recent years, developing new techniques and technologies for analyzing large amounts of data. One such approach is the use of neural networks, which shows great promise in the ability to learn from and make predictions based on complex data sets. It has been used in a wide range of applications, from image recognition to natural language processing, with impressive results.

In this paper, we will explore the use of neural networks combined with big data storage and processing technologies to develop new real-time anomaly detection techniques. Anomaly detection is a method of identifying unusual or unexpected patterns in data, which may indicate errors, fraud, or other issues By combining the power of neural networks and the amount of data available through big data technology together, we aim for more accurate and efficient methods to detect anomalies in real-time.

Our approach uses big data technology to collect and store large amounts of real-time data, which can then be analyzed by neural networks. These networks are trained to recognize patterns and relationships in the data, enabling them to detect anomalies that might be difficult to detect with traditional methods that. By using this technique in real time we hope to improve our ability to identify abnormalities as they occur, resulting in faster response times and more effective decision-making.

This paper will provide an overview of our approach, including a discussion of relevant literature and a description of our methodology. We will also present the results of our research, including our findings and implications for further analysis of the field. Finally, we will discuss the limitations of our approach and propose future research directions.

1. Literature Review
2. Methodology
3. Results
4. Discussion
5. Conclusion