**Machine Learning for Anomaly Detection in Encrypted Network Traffic**

**Abstract:**

**Introduction:**

The increasing reliance on network communication and the growing complexity of cyber threats have made anomaly detection a critical aspect of network security which helps to keep the network secure from cyber-attacks. Detecting anomalous patterns in network traffic plays a very crucial role in identifying potential security breaches, preventing cyber-attacks, and ensuring the confidentiality, integrity, and availability of network resources. However, as the need for robust anomaly detection mechanisms grows, so does the concern for preserving the privacy of sensitive network data. This is the case when anomaly detection tasks are outsourced to third-party service providers where protecting the privacy of network traffic becomes even more critical.

Homomorphic Encryption, the holy grail of cybersecurity which had many developments in last decade is a promising solution for preserving the privacy of sensitive data while allowing computations to be performed on encrypted information. By leveraging the power of homomorphic encryption, organizations can outsource anomaly detection tasks to third-party service providers without revealing the underlying network traffic. This approach enables privacy-preserving anomaly detection, allowing organizations to enhance their security and safeguarding sensitive information about their network.

The primary objective of this project is to explore the feasibility and effectiveness of utilizing homomorphic encryption in detecting anomalies based on the statistical measures of network traffic flow. In this progress report, my goal is to provide detailed explanation of the work I have till until now which includes preprocessing the dataset, analysing it, applying machine learning and deep learning algorithms on homomorphically encrypted data for anomaly detection.

**Literature Review:**

**Conclusion:**